



Proteger bancos de dados SAP HANA

SnapCenter Software 4.8

NetApp

September 26, 2025

This PDF was generated from https://docs.netapp.com/pt-br/snapcenter-48/protect-hana/concept_snapcenter_plug_in_for_sap_hana_database_overview.html on September 26, 2025. Always check docs.netapp.com for the latest.

Índice

Proteger bancos de dados SAP HANA	1
Plug-in do SnapCenter para bancos de dados SAP HANA	1
Visão geral do plug-in do SnapCenter para banco de dados SAP HANA	1
O que você pode fazer usando o plug-in do SnapCenter para banco de dados SAP HANA	1
Plug-in do SnapCenter para recursos de banco de dados SAP HANA	1
Tipos de storage compatíveis com o plug-in SnapCenter para banco de dados SAP HANA	2
Mínimo de ONTAP Privileges necessário para plug-in SAP HANA	3
Preparar sistemas de storage para replicação do SnapMirror e do SnapVault para bancos de dados SAP HANA	7
Estratégia de backup para bancos de dados SAP HANA	8
Estratégia de restauração e recuperação para bancos de dados SAP HANA	11
Prepare-se para instalar o plug-in do SnapCenter para o banco de dados SAP HANA	14
Fluxo de trabalho de instalação do plug-in SnapCenter para banco de dados SAP HANA	14
Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para banco de dados SAP HANA	14
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows	15
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux	16
Configurar credenciais para o plug-in SnapCenter para banco de dados SAP HANA	17
Configure o gMSA no Windows Server 2012 ou posterior	20
Instalar o plug-in do SnapCenter para bancos de dados SAP HANA	21
Configurar certificado CA	27
Instale o plug-in do SnapCenter para VMware vSphere	35
Implantar certificado CA	35
Configure o arquivo CRL	35
Preparar-se para a proteção de dados	35
Pré-requisitos para usar o plug-in do SnapCenter para banco de dados SAP HANA	35
Como os recursos, grupos de recursos e políticas são usados para proteger bancos de dados do SAP HANA	36
Fazer backup dos recursos do SAP HANA	37
Fazer backup dos recursos do SAP HANA	37
Configure a chave do armazenamento de usuários HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA	38
Descubra recursos e prepare contentores de banco de dados multitenant para proteção de dados	38
Adicione recursos manualmente ao host do plug-in	41
Criar políticas de backup para bancos de dados SAP HANA	43
Crie grupos de recursos e anexe políticas	48
Fazer backup de bancos de dados do SAP HANA	51
Fazer backup de grupos de recursos	55
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para banco de dados SAP HANA	56
Faça backup de bancos de dados usando cmdlets do PowerShell	57
Monitorar operações de backup	61
Cancelar operações de backup para SAP HANA	63

Veja os backups e clones do banco de dados SAP HANA na página topologia	63
Restaure os bancos de dados do SAP HANA	65
Restaure o fluxo de trabalho	65
Restaure e recupere um backup de recursos adicionado manualmente.	65
Restaure e recupere um backup de banco de dados descoberto automaticamente	67
Restaure o banco de dados SAP HANA usando cmdlets do PowerShell	71
Restaure recursos usando cmdlets do PowerShell	73
Monitore as operações de restauração de bancos de dados SAP HANA.	76
Clonar backups de recursos do SAP HANA	77
Fluxo de trabalho clone	77
Clone um backup de banco de dados SAP HANA	78
Clonar backups de bancos de dados do SAP HANA usando cmdlets do PowerShell	80
Monitorar operações de clone de banco de dados SAP HANA.	82
Divida um clone	83
Exclua ou divida clones do banco de dados do SAP HANA após a atualização do SnapCenter	84

Proteger bancos de dados SAP HANA

Plug-in do SnapCenter para bancos de dados SAP HANA

Visão geral do plug-in do SnapCenter para banco de dados SAP HANA

O plug-in do SnapCenter para banco de dados SAP HANA é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento da proteção de dados com reconhecimento de aplicações de bancos de dados SAP HANA. O plug-in para banco de dados SAP HANA automatiza o backup, a restauração e a clonagem de bancos de dados SAP HANA em seu ambiente SnapCenter.

O SnapCenter é compatível com contêineres únicos e contêineres de banco de dados multitenant (MDC). Você pode usar o plug-in para banco de dados SAP HANA em ambientes Windows e Linux. O plug-in que não está instalado no host do banco de dados HANA é conhecido como plug-in de host centralizado. O plug-in de host centralizado pode gerenciar vários bancos de DADOS HANA em diferentes hosts.

Quando o plug-in para banco de dados SAP HANA é instalado, você pode usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume. Você também pode usar o plug-in com a tecnologia NetApp SnapVault para executar a replicação de backup disco a disco para conformidade com os padrões.

O que você pode fazer usando o plug-in do SnapCenter para banco de dados SAP HANA

Ao instalar o plug-in para banco de dados SAP HANA em seu ambiente, você pode usar o SnapCenter para fazer backup, restaurar e clonar bancos de dados SAP HANA e seus recursos. Você também pode executar tarefas de suporte a essas operações.

- Adicionar bancos de dados.
- Criar backups.
- Restauração a partir de backups.
- Backups de clones.
- Agendar operações de backup.
- Monitore operações de backup, restauração e clone.
- Exibir relatórios para operações de backup, restauração e clone.

Plug-in do SnapCenter para recursos de banco de dados SAP HANA

O SnapCenter se integra à aplicação plug-in e às tecnologias NetApp no sistema de storage. Para trabalhar com o plug-in para banco de dados SAP HANA, você usa a interface gráfica do usuário do SnapCenter.

- * Interface gráfica unificada do usuário*

A interface do SnapCenter fornece padronização e consistência em plug-ins e ambientes. A interface do SnapCenter permite concluir operações consistentes de backup, restauração e clone em plug-ins, usar

relatórios centralizados, usar visualizações de painel rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins.

- * Administração central automatizada*

Você pode agendar operações de backup, configurar a retenção de backup baseada em política e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

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

A SnapCenter usa a tecnologia de cópia Snapshot do NetApp com o plug-in para banco de dados SAP HANA para fazer backup de recursos.

O uso do plug-in para banco de dados SAP HANA também oferece os seguintes benefícios:

- Suporte a fluxos de trabalho de backup, restauração e clone
- Delegação de funções centralizada e segurança compatível com RBAC

Você também pode definir as credenciais para que os usuários autorizados do SnapCenter tenham permissões no nível do aplicativo.

- Criação de cópias de recursos com uso eficiente de espaço e pontuais para teste ou extração de dados usando a tecnologia NetApp FlexClone

É necessária uma licença FlexClone no sistema de storage onde você deseja criar o clone.

- Suporte ao recurso de cópia Snapshot do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Funcionalidade de executar vários backups simultaneamente em vários hosts de recursos

Em uma única operação, as cópias Snapshot são consolidadas quando os recursos em um único host compartilham o mesmo volume.

- Funcionalidade de criar cópias Snapshot usando comandos externos.
- Suporte para backup baseado em arquivos.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de storage compatíveis com o plug-in SnapCenter para banco de dados SAP HANA

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e máquinas virtuais (VMs). Você deve verificar o suporte para seu tipo de storage antes de instalar o plug-in SnapCenter para banco de dados SAP HANA.

Máquina	Tipo de armazenamento
Servidores físicos e virtuais	LUNs conectados a FC
Servidor físico	LUNs ligados ao iSCSI

Máquina	Tipo de armazenamento
Servidores físicos e virtuais	Volumes conectados a NFS

Mínimo de ONTAP Privileges necessário para plug-in SAP HANA

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

limpeza da reserva persistente de lun

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

Comandos somente leitura: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior

interface de rede

mostra da interface de rede

svm

Preparar sistemas de storage para replicação do SnapMirror e do SnapVault para bancos de dados SAP HANA

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 bancos de dados SAP HANA

Definir uma estratégia de backup para bancos de dados SAP HANA

Definir uma estratégia de backup antes de criar seus trabalhos de backup ajuda a ter os backups necessários para restaurar ou clonar seus recursos 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.

Sobre esta tarefa

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

Passos

1. Determine quando você deve fazer backup de seus recursos.
2. Decida quantos trabalhos de cópia de segurança necessita.
3. Decida como nomear seus backups.
4. Decida se você deseja criar uma política baseada em cópia Snapshot para fazer backup de cópias Snapshot consistentes com aplicações do banco de dados.
5. Decida se deseja verificar a integridade do banco de dados.
6. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção a longo prazo.
7. Determine o período de retenção das cópias Snapshot no sistema de storage de origem e no destino do SnapMirror.
8. Determine se deseja executar quaisquer comandos antes ou depois da operação de backup e forneça um prescritor ou postscript.

Descoberta automática de recursos no host Linux

Os recursos são bancos de dados SAP HANA e volume não-dados no host Linux gerenciado pelo SnapCenter. Depois de instalar o plug-in do SnapCenter para o banco de dados SAP HANA, os bancos de dados SAP HANA nesse host Linux são automaticamente descobertos e exibidos na página recursos.

A detecção automática é compatível com os seguintes recursos do SAP HANA:

- Contêineres únicos

Depois de instalar ou atualizar o plug-in, os recursos de contentor único localizados em um plug-in de host centralizado continuarão como recursos adicionados manualmente.

Depois de instalar ou atualizar o plug-in, os bancos de dados SAP HANA são automaticamente descobertos apenas nos hosts do SAP HANA Linux, que são registrados diretamente no SnapCenter.

- Contêiner de banco de dados multitenant (MDC)

Depois de instalar ou atualizar o plug-in, os recursos do MDC localizados em um plug-in de host centralizado continuarão como recurso adicionado manualmente.

Você deve continuar a adicionar manualmente os recursos do MDC no plug-in de host centralizado após a atualização para o SnapCenter 4,3.

Para hosts SAP HANA Linux diretamente registrados no SnapCenter, a instalação ou atualização do plug-in acionará uma descoberta automática de recursos no host. Depois de atualizar o plug-in, para cada recurso MDC que estava localizado no host do plug-in, outro recurso MDC será automaticamente descoberto com um formato GUID diferente e registrado no SnapCenter. O novo recurso estará no estado bloqueado.

Por exemplo, no SnapCenter 4,2, se o recurso E90 MDC estava localizado no host do plug-in e registrado manualmente, após a atualização para o SnapCenter 4,3, outro recurso E90 MDC com um GUID diferente será descoberto e registrado no SnapCenter.

A detecção automática não é suportada para as seguintes configurações:

- Layouts RDM e VMDK



Caso os recursos acima sejam descobertos, as operações de proteção de dados não são suportadas por esses recursos.

- Configuração de vários host HANA
- Várias instâncias no mesmo host
- Replicação do SISTEMA HANA com escalabilidade horizontal de várias camadas
- Ambiente de replicação em cascata no modo de replicação do sistema

Tipos de backups suportados

Tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter é compatível com os tipos de backup baseado em cópia de Snapshot e backup baseado

em arquivos para bancos de dados SAP HANA.

Backup baseado em arquivo

Os backups baseados em arquivos verificam a integridade do banco de dados. Você pode agendar a operação de backup baseada em arquivo para ocorrer em intervalos específicos. Somente os locatários ativos são copiados. Não é possível restaurar e clonar backups baseados em arquivos do SnapCenter.

Backup baseado em cópia snapshot

Os backups baseados em cópias snapshot utilizam a tecnologia de cópia Snapshot do NetApp para criar cópias on-line e somente leitura dos volumes nos quais os bancos de dados SAP HANA estão localizados.

Como o plug-in do SnapCenter para banco de dados SAP HANA usa cópias Snapshot de grupo de consistência

Você pode usar o plug-in para criar cópias Snapshot de grupo de consistência para grupos de recursos. Um grupo de consistência é um contentor que pode abrigar vários volumes para que você possa gerenciá-los como uma entidade. Um grupo de consistência é cópias Snapshot simultâneas de vários volumes, fornecendo cópias consistentes de um grupo de volumes.

Você também pode especificar o tempo de espera para que o controlador de storage agrupe cópias Snapshot com consistência. As opções de tempo de espera disponíveis são **urgente**, **Médio** e **descontraído**. Você também pode ativar ou desativar a sincronização WAFL (Write Anywhere File Layout) durante a operação consistente de cópia Snapshot do grupo. O WAFL Sync melhora o desempenho de uma cópia Snapshot de grupo de consistência.

Como o SnapCenter gerencia o gerenciamento de backups de log e dados

O SnapCenter gerencia o serviço de limpeza dos backups de log e dados nos níveis do sistema de storage e do sistema de arquivos e no catálogo de backup do SAP HANA.

As cópias Snapshot no storage primário ou secundário e suas entradas correspondentes no catálogo do SAP HANA são excluídas com base nas configurações de retenção. As entradas do catálogo do SAP HANA também são excluídas durante a exclusão do grupo de recursos e backup.

Considerações para determinar programações de backup para banco de dados SAP HANA

O fator mais crítico na determinação de um agendamento de backup é a taxa de alteração do recurso. 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 do ponto de restauração (RPO).

Os programas de backup têm duas partes, como segue:

- Frequência de backup (com que frequência os backups devem ser executados)

A frequência de backup, também chamada de tipo de programação para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como hora, dia, semanal ou mensal.

- Programações de backup (exatamente quando os backups devem ser executados)

As agendas de backup fazem parte de uma configuração de recurso ou 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

Número de tarefas de backup necessárias para bancos de dados SAP HANA

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

Convenções de nomenclatura de backup para plug-in para bancos de dados SAP HANA

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.

Estratégia de restauração e recuperação para bancos de dados SAP HANA

Definir uma estratégia de restauração e recuperação para recursos do SAP HANA

Você deve definir uma estratégia antes de restaurar e recuperar seu banco de dados para que você possa executar operações de restauração e recuperação com sucesso.

Passos

1. Determine as estratégias de restauração com suporte para recursos do SAP HANA adicionados manualmente

2. Determinar as estratégias de restauração com suporte para bancos de dados SAP HANA descobertos automaticamente
3. Decida o tipo de operações de recuperação que você deseja executar.

Tipos de estratégias de restauração compatíveis com recursos do SAP HANA adicionados manualmente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter. Existem dois tipos de estratégias de restauração para recursos do SAP HANA adicionados manualmente. Não é possível recuperar recursos do SAP HANA adicionados manualmente.



Não é possível recuperar recursos do SAP HANA adicionados manualmente.

Restauração completa de recursos

- Restaura todos os volumes, qtrees e LUNs de um recurso



Se o recurso contiver volumes ou qtrees, as cópias Snapshot obtidas após a cópia Snapshot selecionada para restauração nesses volumes ou qtrees serão excluídas e não poderão ser recuperadas. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

Restauração no nível do arquivo

- Restaura arquivos de volumes, qtrees ou diretórios
- Restaura apenas os LUNs selecionados

Tipos de estratégias de restauração compatíveis com bancos de dados SAP HANA descobertos automaticamente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter. Existem dois tipos de estratégias de restauração para bancos de dados SAP HANA descobertos automaticamente.

Restauração completa de recursos

- Restaura todos os volumes, qtrees e LUNs de um recurso
 - A opção **Reverter volume** deve ser selecionada para restaurar todo o volume.



Se o recurso contiver volumes ou qtrees, as cópias Snapshot obtidas após a cópia Snapshot selecionada para restauração nesses volumes ou qtrees serão excluídas e não poderão ser recuperadas. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

Banco de dados de inquilinos

- Restaura o banco de dados do locatário

Se a opção **Banco de dados do locatário** estiver selecionada, os scripts de recuperação HANA ou HANA

externos ao SnapCenter devem ser usados para executar a operação de recuperação.

Tipos de operações de restauração para bancos de dados SAP HANA descobertos automaticamente

O SnapCenter é compatível com SnapRestore baseado em volume (VBSR), SnapRestore de arquivo único e tipos de restauração de conexão e cópia para bancos de dados SAP HANA descobertos automaticamente.

O SnapRestore baseado em volume (VBSR) é executado em ambientes NFS para os seguintes cenários:

- Quando o backup selecionado para restauração é feito em versões anteriores ao SnapCenter 4,3, e somente se a opção ****recurso completo** estiver selecionada
- Quando o backup selecionado para restauração é feito no SnapCenter 4,3 e se a opção **Reverter volume** estiver selecionada

O SnapRestore de arquivo único é executado em ambientes NFS para os seguintes cenários:

- Quando o backup selecionado para restauração é feito no SnapCenter 4,3, e se apenas a opção **recurso completo** estiver selecionada
- Para contentores de banco de dados multitenant (MDC), quando o backup selecionado para restauração é feito no SnapCenter 4,3 e a opção **Banco de dados do locatário** está selecionada
- Quando o backup selecionado é de um local secundário SnapMirror ou SnapVault e a opção **recurso completo** está selecionada

O SnapRestore de Arquivo único é executado em ambientes SAN para os seguintes cenários:

- Quando os backups são feitos em versões anteriores ao SnapCenter 4,3 e somente se a opção **recurso completo** estiver selecionada
- Quando os backups são feitos no SnapCenter 4,3 e somente se a opção **recurso completo** estiver selecionada
- Quando o backup é selecionado em um local secundário do SnapMirror ou do SnapVault e a opção **recurso completo** está selecionada

A restauração baseada em conexão e cópia é realizada em ambientes SAN para o seguinte cenário:

- Para o MDC, quando o backup selecionado para restauração é feito no SnapCenter 4,3 e a opção **Banco de dados do locatário** é selecionada



As opções **recurso completo**, **Reverter volume** e **Banco de dados do locatário** estão disponíveis na página Restaurar escopo.

Tipos de operações de recuperação compatíveis com bancos de dados SAP HANA

O SnapCenter permite que você execute diferentes tipos de operações de recuperação para bancos de dados SAP HANA.

- Recupere o banco de dados até o estado mais recente
- Recupere o banco de dados até um ponto específico no tempo

Você deve especificar a data e a hora para a recuperação.

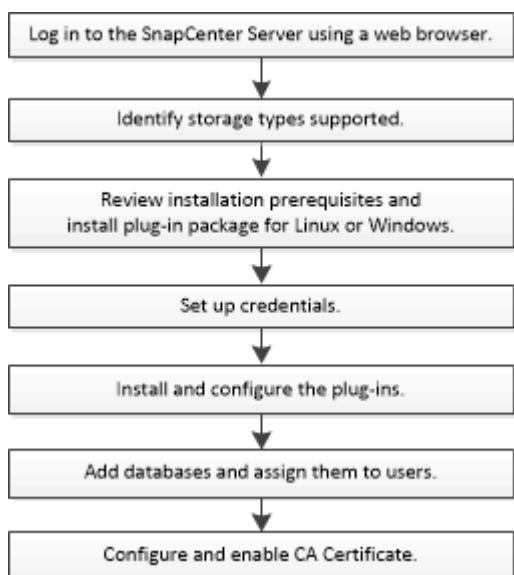
- Recupere o banco de dados até um backup de dados específico

O SnapCenter também fornece a opção sem recuperação para bancos de dados SAP HANA.

Prepare-se para instalar o plug-in do SnapCenter para o banco de dados SAP HANA

Fluxo de trabalho de instalação do plug-in SnapCenter para banco de dados SAP HANA

Você deve instalar e configurar o plug-in do SnapCenter para o banco de dados SAP HANA se quiser proteger os bancos de dados SAP HANA.



Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para banco de dados SAP HANA

Antes de adicionar um host e instalar os pacotes de plug-in, você deve completar todos os requisitos. O plug-in do SnapCenter para banco de dados SAP HANA está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 1,8 64-bit em seu host.



O IBM Java não é suportado.

- Você deve ter instalado o terminal interativo do banco de dados SAP HANA (cliente HDBSQL) no host.
- Para o Windows, o Plug-in Creator Service deve ser executado usando o usuário Windows "LocalSystem", que é o comportamento padrão quando o Plug-in para SAP HANA Database é instalado como administrador de domínio.
- Para o Windows, as chaves de armazenamento de usuários devem ser criadas como usuário DO SISTEMA.
- 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. O plug-in do SnapCenter para Microsoft Windows será implantado por padrão com o plug-in SAP HANA em hosts do Windows.

- Para o host Linux, as chaves HDB Secure User Store são acessadas como usuário HDBSQL os.
- O servidor SnapCenter deve ter acesso ao 8145 ou à porta personalizada do plug-in para o host de banco de dados SAP HANA.

Hosts do Windows

- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Ao instalar o plug-in para banco de dados SAP HANA em um host Windows, o plug-in do SnapCenter para Microsoft Windows é instalado automaticamente.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 1,8 64-bit em seu host Windows.

["Downloads Java para todos os sistemas operacionais"](#)

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

Hosts Linux

- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 1,8 64-bit em seu host Linux.

["Downloads Java para todos os sistemas operacionais"](#)

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

- Para bancos de dados SAP HANA que estão sendo executados em um host Linux, ao instalar o plug-in para banco de dados SAP HANA, o plug-in do SnapCenter para UNIX é instalado automaticamente.

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

Item	Requisitos
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	• Microsoft .NET Framework 4.7.2 ou posterior • Windows Management Framework (WMF) 4,0 ou posterior • PowerShell 4,0 ou posterior Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conectividade com a Internet."

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

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

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) 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

Item	Requisitos
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 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	Java 1,8.x (64-bit) Oracle Java e OpenJDK sabores Se você atualizou O JAVA para a versão mais recente, você deve garantir que a opção <code>JAVA_HOME</code> localizada em <code>/var/opt/SnapCenter/spl/etc/spl.properties</code> esteja definida para a versão JAVA correta e o caminho correto. Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Configurar credenciais para o plug-in SnapCenter para banco de dados SAP HANA

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.

Sobre esta tarefa

- Hosts Linux

Você deve configurar credenciais para instalar plug-ins em hosts Linux.

Você deve configurar as credenciais para o usuário raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

Prática recomendada: embora você tenha permissão para criar credenciais para Linux após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

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.

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

Passos

- 1. No painel de navegação esquerdo, clique em **Configurações**.
- 2. Na página Configurações, clique em **Credential**.
- 3. Clique em **nov**.

Credential

Provide information for the Credential you want to add

Credential Name

Name

Username

Username

Password

Password

Authentication

Linux

☐ Use sudo privileges

Cancel

OK

- 4. Na página Credential (credencial), especifique as informações necessárias para configurar credenciais:

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

Para este campo...	Faça isso...
Nome de utilizador	Introduza o nome de utilizador e a palavra-passe a utilizar para a autenticação. - Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são: <i>NetBIOS_username</i> <i>Domain FQDN_username</i> - Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: <i>Nome de usuário</i> 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.
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar.
Use sudo Privileges	Marque a caixa de seleção Use sudo Privileges se estiver criando credenciais para um usuário que não seja root.  Aplicável apenas a usuários Linux.

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.

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.

- Reinicie o host.
 - Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`
 - Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`
- Atribua o Privileges administrativo ao gMSA configurado no host.
 - 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 login de serviço durante a instalação do plug-in.

Instalar o plug-in do SnapCenter para bancos de dados SAP HANA

Adicione hosts e instale pacotes plug-in em hosts remotos

Você deve usar a página Adicionar host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos. Você pode adicionar um host e instalar pacotes de plug-in para um host individual ou para um cluster.

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 está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- A documentação de administração contém informações sobre o gerenciamento de hosts.

- 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 SAP HANA"](#)

Sobre esta tarefa

- Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.
- Para que a replicação do sistema SAP HANA descubra recursos em sistemas primários e secundários, recomenda-se adicionar os sistemas primário e secundário usando o usuário raiz ou sudo.

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, execute as seguintes ações:

Para este campo...	Faça isso...
Tipo de host	Selecione o tipo de host: • Windows • Linux  O plug-in para SAP HANA é instalado no host cliente HDBSQL, e esse host pode estar em um sistema Windows ou em um sistema Linux.
Nome do host	Insira o nome do host de comunicação. Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no FQDN. Você deve configurar o cliente HDBSQL e o HDBUserStore neste host.

Para este campo...	Faça isso...
Credenciais	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. Você pode exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você forneceu.  O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a instalar.

6. (Opcional) clique em **mais opções**.

Para este campo...	Faça isso...
Porta	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.  Se você instalou manualmente os plug-ins e especificou uma porta personalizada, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O plug-in para SAP HANA é instalado no host cliente HDBSQL, e esse host pode estar em um sistema Windows ou em um sistema Linux. • Para o pacote de plug-ins do SnapCenter para Windows, o caminho padrão é C: Arquivos de programas/NetApp/SnapCenter. Opcionalmente, você pode personalizar o caminho. • Para o pacote de plug-ins do SnapCenter para Linux, o caminho padrão é /opt/NetApp/SnapCenter. Opcionalmente, você pode personalizar o caminho.

Para este campo...	Faça isso...
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.
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Para o host Windows, marque essa caixa de seleção se desejar usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in.  Forneça o nome do gMSA no seguinte formato:  O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

Se você não tiver selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se o host atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .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.

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirm and Submit**.

Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.



A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitore o progresso da instalação.

Os arquivos de log específicos da instalação estão localizados em /custom_location/SnapCenter/logs.

Instale pacotes de plug-ins do SnapCenter para Linux ou Windows em vários hosts remotos usando cmdlets

Você pode instalar os Pacotes de plug-in do SnapCenter para Linux ou Windows 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 em vários hosts 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 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 o banco de dados SAP HANA em hosts Linux usando a interface de linha de comando

Você deve instalar o plug-in do SnapCenter para banco de dados SAP HANA usando a interface de usuário (UI) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in a partir da IU do SnapCenter, você pode instalar o plug-in para banco de dados SAP HANA no modo console ou no modo silencioso usando a interface de linha de comando (CLI).

O que você vai precisar

- Você deve instalar o Plug-in para o banco de dados SAP HANA em cada host Linux onde reside o cliente HDBSQL.
- O host Linux no qual você está instalando o plug-in do SnapCenter para banco de dados SAP HANA deve atender aos requisitos de software, banco de dados e sistema operacional dependentes.

A ferramenta de Matriz de interoperabilidade (IMT) contém as informações mais recentes sobre as configurações suportadas.

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

- O plug-in do SnapCenter para banco de dados SAP HANA faz parte do pacote de plug-ins do SnapCenter para Linux. Antes de instalar o pacote de plug-ins do SnapCenter para Linux, você já deve ter instalado o SnapCenter em um host do Windows.

Passos

1. Copie o pacote de plug-ins do SnapCenter para o arquivo de instalação do Linux (SnapCenter_linux_host_plugin.bin) do repositório C:/NetApp/SnapCenter para o host onde você deseja instalar o plug-in para o banco de dados SAP HANA.

Você pode acessar esse caminho a partir do host onde o servidor SnapCenter está instalado.

2. No prompt de comando, navegue até o diretório onde você copiou o arquivo de instalação.
3. Instale o plug-in: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
 - -DPORT especifica a porta de comunicação HTTPS SMCore.
 - -DSERVER_IP especifica o endereço IP do servidor SnapCenter.
 - -DSERVER_HTTPS_PORT especifica a porta HTTPS do servidor SnapCenter.
 - -DUSER_install_DIR especifica o diretório onde você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
 - DINSTALL_LOG_NAME especifica o nome do arquivo de log.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Edite o arquivo `/<installation directory>/NetApp/SnapCenter/scc/etc/SC_SMS_Services.properties` e, em seguida, adicione o parâmetro `PLUGINS_ENABLED: HANA:3,0`.
5. Adicione o host ao servidor SnapCenter usando o cmdlet `Add-Smhost` e os parâmetros necessários.

As informações sobre os parâmetros que podem ser usados com o comando 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"](#).

Monitore o status da instalação do plug-in para SAP HANA

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:

- Clique duas vezes no certificado.
- Na caixa de diálogo certificado, clique na guia **Detalhes**.
- Percorra a lista de campos e clique em **thumbprint**.
- Copie os caracteres hexadecimais da caixa.
- 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:

- 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

- Copie a impressão digital.

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

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

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

Passos

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

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

Por exemplo:

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

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

Por exemplo:

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

Configure o certificado de CA para o serviço de plug-ins SAP HANA do SnapCenter no host Linux

Você deve gerenciar a senha do armazenamento de chaves de plug-ins personalizados e seu certificado, configurar o certificado de CA, configurar certificados raiz ou intermediários para o armazenamento de confiança de plug-ins personalizados e configurar o par de chaves assinadas de CA para armazenamento de confiança de plug-ins personalizados com o serviço de plug-ins personalizados SnapCenter para ativar o certificado digital instalado.

Plug-ins personalizados usam o arquivo 'keystore.jks', que está localizado em `/opt/NetApp/SnapCenter/scc/etc` tanto como seu armazenamento de confiança e armazenamento de chaves.

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in personalizado do arquivo de propriedade do agente do plug-in personalizado.

É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Altere a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks  
. Altere a senha para todos os aliases de entradas de chave privada no  
keystore para a mesma senha usada para o keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

3. Reinicie o serviço depois de alterar a senha.



A palavra-passe para o armazenamento de chaves plug-in personalizado e para todas as palavras-passe de alias associadas da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para armazenamento de confiança de plug-in personalizado

Você deve configurar os certificados raiz ou intermediários sem a chave privada para armazenamento de confiança de plug-in personalizado.

Passos

1. Navegue até a pasta que contém o keystore de plug-in personalizado: /Opt/NetApp/SnapCenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Reinicie o serviço depois de configurar os certificados raiz ou  
intermediários para o armazenamento de confiança de plug-in personalizado.
```



Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Configure o par de chaves assinadas da CA para o armazenamento de confiança de plug-in personalizado

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança do plug-in personalizado.

Passos

1. Navegue até a pasta que contém o keystore de plug-in personalizado /opt/NetApp/SnapCenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione o certificado da CA com chave privada e pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Liste os certificados adicionados no keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

A senha padrão do keystore do plug-in personalizado é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. Se o nome do alias no certificado da CA for longo e contiver espaço ou caracteres especiais ("*", ",", "), altere o nome do alias para um nome simples:

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Configure o nome do alias do certificado CA no arquivo agent.properties.

Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança de plug-in personalizado.

Configurar a lista de revogação de certificados (CRL) para plug-ins personalizados do SnapCenter

Sobre esta tarefa

- Os plug-ins personalizados do SnapCenter pesquisarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para plug-ins personalizados do SnapCenter é '`opt/NetApp/SnapCenter/scc/etc/crl`'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo `agent.properties` contra a chave `CRL_PATH`.

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

Configure o certificado de CA para o serviço de plug-ins SAP HANA do SnapCenter no host do Windows

Você deve gerenciar a senha do armazenamento de chaves de plug-ins personalizados e seu certificado, configurar o certificado de CA, configurar certificados raiz ou intermediários para o armazenamento de confiança de plug-ins personalizados e configurar o par de chaves assinadas de CA para armazenamento de confiança de plug-ins personalizados com o serviço de plug-ins personalizados SnapCenter para ativar o certificado digital instalado.

Plug-ins personalizados usam o arquivo `keystore.jks`, que está localizado em `_C: Arquivos de programas, NetApp, SnapCenter, SnapCenter Plug-in Creator`, tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para armazenamento de chaves plug-in personalizado e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in personalizado do arquivo de propriedade do agente do plug-in personalizado.

É o valor correspondente à chave `KEYSTORE_PASS`.

2. Altere a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks
```



Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool por seu caminho completo.

```
C: Arquivos de programas/<jdk_version>/keytool.exe" -storepasswd -keystore keystore.jks
```

3. Altere a senha para todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Atualize o mesmo para a chave `KEYSTORE_PASS` no arquivo `agent.properties`.

4. Reinicie o serviço depois de alterar a senha.



A palavra-passe para o armazenamento de chaves plug-in personalizado e para todas as palavras-passe de alias associadas da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para armazenamento de confiança de plug-in personalizado

Você deve configurar os certificados raiz ou intermediários sem a chave privada para armazenamento de confiança de plug-in personalizado.

Passos

1. Navegue até a pasta que contém o armazenamento de chaves de plug-in personalizado C: *Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc*
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
Keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_root.cer -keystore keystore.jks
```

5. Reinicie o serviço depois de configurar os certificados raiz ou intermediários para o armazenamento de confiança de plug-in personalizado.



Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Configure o par de chaves assinadas da CA para o armazenamento de confiança de plug-in personalizado

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança do plug-in personalizado.

Passos

1. Navegue até a pasta que contém o armazenamento de chaves de plug-in personalizado C: *Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc*
2. Localize o arquivo *keystore.jks*.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione o certificado da CA com chave privada e pública.

```
Keytool -importkeystore -srckeystore /root/SnapCenter.ssl.test.NetApp.com.pfx -srcstoretype PKCS12 -destinkeystore keystore.jks -deststoretype JKS
```

5. Liste os certificados adicionados no keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.

7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

A senha padrão do keystore do plug-in personalizado é o valor da chave KEYSTORE_PASS no arquivo *agent.properties*.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks
```

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança de plug-in personalizado.

Configurar a lista de revogação de certificados (CRL) para plug-ins personalizados do SnapCenter

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "[Como atualizar o arquivo de lista de revogação de certificados no certificado da CA do SnapCenter](#)" consulte .
- Os plug-ins personalizados do SnapCenter pesquisarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para os plug-ins personalizados do SnapCenter é 'C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo *agent.properties* contra a chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

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.

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 banco de dados SAP HANA

Antes de usar o plug-in do SnapCenter para banco de dados SAP HANA, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no servidor SnapCenter.

- Configure o ambiente SnapCenter adicionando conexões do sistema de storage e criando credenciais, se aplicável.
- Instale o Java 1,7 ou Java 1,8 em seu host Linux ou Windows.

Você deve definir o caminho Java na variável caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault, se quiser replicação de backup.
- Instale o cliente HDBSQL no host onde você instalará o Plug-in para o banco de dados SAP HANA.

Configure as chaves do armazenamento de usuários para os nós do SAP HANA que você gerenciará por meio desse host.

- Para o banco de dados SAP HANA 2.0SPS05, se você estiver usando uma conta de usuário do banco de dados SAP HANA, verifique se você tem as seguintes permissões para executar operações de backup, restauração e clone no servidor SnapCenter:
 - Administrador de backup
 - Catálogo lido
 - Administrador de backup de banco de dados
 - Operador de recuperação de banco de dados

Como os recursos, grupos de recursos e políticas são usados para proteger bancos de dados do SAP HANA

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 SAP HANA que você faz backup ou clonar com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

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 do backup, a replicação, os 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.

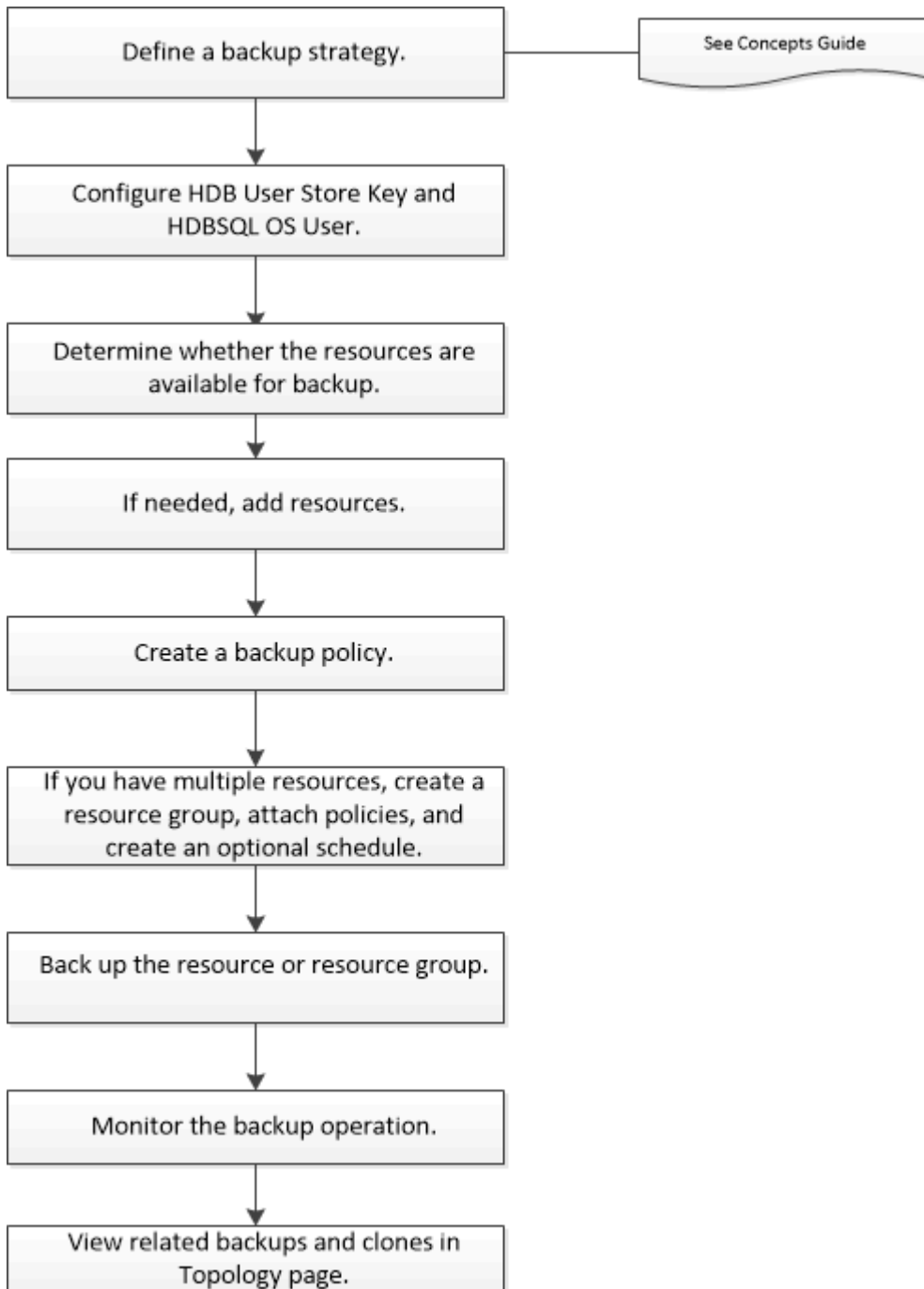
Pense em um grupo de recursos como definindo o que você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definir como você deseja protegê-la. Se você estiver fazendo backup de todos os bancos de dados, por exemplo, poderá criar um grupo de recursos que inclua todos os bancos de dados 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 diariamente.

Fazer backup dos recursos do SAP HANA

Fazer backup dos recursos do SAP HANA

Você pode criar um backup de um recurso (banco de dados) ou grupo de recursos. O fluxo de trabalho de backup inclui Planejamento, identificação de bancos de dados para backup, gerenciamento de políticas de backup, criação de grupos de recursos e inclusão de políticas, criação de backups e monitoramento das operações.

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



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de

backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "[Guia de referência de cmdlet do software SnapCenter](#)".

Configure a chave do armazenamento de usuários HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA

Você deve configurar a chave do armazenamento de usuário HDB e o usuário do sistema operacional HDBSQL para executar operações de proteção de dados em bancos de dados SAP HANA.

O que você vai precisar

- Se o banco de dados SAP HANA não tiver a chave de armazenamento de usuário seguro HDB e o usuário SQL do HDB configurado, um ícone de cadeado vermelho será exibido apenas para os recursos autodescobertos. Se, durante uma operação de descoberta subsequente, a chave de armazenamento de usuário segura HDB configurada estiver incorreta ou não tiver fornecido acesso ao próprio banco de dados, o ícone de cadeado vermelho será reexibido.
- Você deve configurar a chave de armazenamento de usuário seguro HDB e o usuário SQL do HDB para poder proteger o banco de dados ou adicioná-lo a um grupo de recursos para executar operações de proteção de dados.
- Você deve configurar HDB SQL os User para acessar o banco de dados do sistema. Se o HDB SQL os User estiver configurado para acessar somente o banco de dados de locatário, a operação de descoberta falhará.

Passos

1. No painel de navegação à esquerda, clique em **Resources** e selecione Plug-in SnapCenter para banco de dados SAP HANA na lista.
2. Na página recursos, selecione o tipo de recurso na lista **Exibir**.
3. (Opcional) clique  e selecione o nome do host.

Em seguida, pode clicar  para fechar o painel de filtro.

4. Selecione o banco de dados e clique em **Configurar banco de dados**.
5. Na seção Configurar configurações da base de dados, digite HDB Secure User Store Key.



O nome do host do plug-in é exibido e o usuário do HDB SQL os é preenchido automaticamente para o <sid>.

6. Clique em **OK**.

Pode modificar a configuração da base de dados a partir da página topologia.

Descubra recursos e prepare contentores de banco de dados multitenant para proteção de dados

Descubra os bancos de dados automaticamente

Os recursos são bancos de dados SAP HANA e volume não-dados no host Linux gerenciado pelo SnapCenter. Você pode adicionar esses recursos a grupos de recursos

para executar operações de proteção de dados depois de descobrir os bancos de dados do SAP HANA que estão disponíveis.

O que você vai precisar

- Você já deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar a chave de armazenamento de usuários HDB, adicionar hosts e configurar as conexões do sistema de armazenamento.
- Você deve ter configurado o HDB Secure User Store Key e o usuário HDB SQL no host Linux.
 - Tem de configurar a chave de armazenamento de utilizadores HDB com o utilizador SID adm. Por exemplo, para o sistema HANA com A22 como SID, a chave de armazenamento de usuário HDB deve ser configurada com a22adm.
- O plug-in do SnapCenter para banco de dados SAP HANA não oferece suporte à descoberta automática dos recursos residentes em ambientes virtuais RDM/VMDK. Você deve fornecer as informações de storage para ambientes virtuais e adicionar os bancos de dados manualmente.

Sobre esta tarefa

Depois de instalar o plug-in, todos os recursos nesse host Linux são automaticamente descobertos e exibidos na página recursos.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação à esquerda, clique em **Resources** e selecione o Plug-in para banco de dados SAP HANA na lista.
2. Na página recursos, selecione o tipo de recurso na lista Exibir.
3. (Opcional) clique em  e selecione o nome do host.

Em seguida, pode clicar em  * para fechar o painel do filtro.

4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

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

- Se o banco de dados estiver em um armazenamento NetApp e não estiver protegido, então não protegido será exibido na coluna Estado geral.
- Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, e se não houver operação de backup executada, o Backup não executado será exibido na coluna Estado geral. O status mudará para Backup failed ou Backup successful com base no último status de backup.



Se o banco de dados SAP HANA não tiver uma chave de armazenamento de usuário segura HDB configurada, um ícone de cadeado vermelho será exibido ao lado do recurso. Se, durante uma operação de descoberta subsequente, a chave de armazenamento de usuário segura HDB configurada estiver incorreta ou não tiver fornecido acesso ao próprio banco de dados, o ícone de cadeado vermelho será reexibido.



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

Depois de terminar

Você deve configurar a chave de armazenamento de usuário seguro HDB e o usuário HDBSQL os para poder proteger o banco de dados ou adicioná-lo ao grupo de recursos para executar operações de proteção de dados.

["Configure a chave do armazenamento de usuários HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA"](#)

Preparar contentores de banco de dados multitenant para proteção de dados

Para hosts SAP HANA diretamente registrados no SnapCenter, a instalação ou atualização do plug-in do SnapCenter para o banco de dados SAP HANA acionará uma descoberta automática de recursos no host. Depois de instalar ou atualizar o plug-in, para cada recurso de contentores de banco de dados multitenant (MDC) localizado no host do plug-in, outro recurso MDC será automaticamente descoberto com um formato GUID diferente e registrado no SnapCenter. O novo recurso estará no estado "bloqueado".

Sobre esta tarefa

Por exemplo, no SnapCenter 4,2, se o recurso E90 MDC estava localizado no host do plug-in e registrado manualmente, após a atualização para o SnapCenter 4,3, outro recurso E90 MDC com um GUID diferente será descoberto e registrado no SnapCenter.



Os backups associados ao recurso do SnapCenter 4,2 e versões anteriores devem ser mantidos até o final do período de retenção. Após o período de retenção expirar, você pode excluir o recurso MDC antigo e continuar a gerenciar o novo recurso MDC descoberto automaticamente.

`Old MDC resource` É o recurso MDC para um host de plug-in que foi adicionado manualmente no SnapCenter 4,2 ou versões anteriores.

Execute as etapas a seguir para começar a usar o novo recurso descoberto no SnapCenter 4,3 para operações de proteção de dados:

Passos

1. Na página recursos, selecione o recurso MDC antigo com backups adicionados à versão anterior do SnapCenter e coloque-o em "modo de manutenção" na página topologia.

Se o recurso for parte de um grupo de recursos, coloque o grupo de recursos em "modo de manutenção".

2. Configure o novo recurso MDC descoberto após a atualização para o SnapCenter 4,3 selecionando o novo recurso na página recursos.

"Novo recurso MDC" é o recurso MDC recém-descoberto que foi descoberto quando o servidor SnapCenter e o host do plug-in foram atualizados para 4,3. O novo recurso MDC pode ser identificado como um recurso com o mesmo SID que o antigo recurso MDC, para um determinado host, e com um ícone de cadeado vermelho ao lado dele na página recursos.

3. Proteja o novo recurso MDC descoberto após a atualização para o SnapCenter 4,3 selecionando políticas de proteção, horários e configurações de notificação.

4. Exclua os backups feitos no SnapCenter 4,2 ou versões anteriores com base nas configurações de retenção.
5. Exclua o grupo de recursos da página topologia.
6. Exclua o recurso MDC antigo da página recursos.

Por exemplo, se o período de retenção das cópias Snapshot principais for de 7 dias e a retenção de cópias Snapshot secundárias for de 45 dias, após 45 dias serem concluídos e após todos os backups serem excluídos, você precisará excluir o grupo de recursos e o recurso MDC antigo.

Encontre mais informações

["Configure a chave do armazenamento de usuários HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA"](#)

["Veja os backups e clones do banco de dados SAP HANA na página topologia"](#)

Adicione recursos manualmente ao host do plug-in

A detecção automática não é compatível com determinadas instâncias HANA. Você deve adicionar esses recursos manualmente.

O que você vai precisar

- Você deve ter concluído tarefas, como instalar o servidor SnapCenter, adicionar hosts, configurar conexões do sistema de armazenamento e adicionar a chave de armazenamento de usuários HDB.
- Para a replicação do sistema SAP HANA, recomenda-se adicionar todos os recursos desse sistema HANA a um grupo de recursos e fazer um backup em grupo de recursos. Isso garante um backup contínuo durante o modo de recuperação de falhas.

["Crie grupos de recursos e anexe políticas"](#).

Sobre esta tarefa

A detecção automática não é suportada para as seguintes configurações:

- Layouts RDM e VMDK



Caso os recursos acima sejam descobertos, as operações de proteção de dados não são suportadas por esses recursos.

- Configuração de vários host HANA
- Várias instâncias no mesmo host
- Replicação do SISTEMA HANA com escalabilidade horizontal de várias camadas
- Ambiente de replicação em cascata no modo de replicação do sistema

Passos

1. No painel de navegação à esquerda, selecione o plug-in do SnapCenter para banco de dados SAP HANA na lista suspensa e clique em **recursos**.
2. Na página recursos, clique em **Adicionar banco de dados SAP HANA**.

3. Na página fornecer detalhes do recurso, execute as seguintes ações:

Para este campo...	Faça isso...
Tipo recurso	Introduza o tipo de recurso. Os tipos de recursos são recipiente único, recipiente de banco de dados multitenant (MDC) e volume não-dados.
Nome do sistema HANA	Introduza o nome descritivo do sistema SAP HANA. Esta opção está disponível apenas se você selecionou tipos de recurso Single Container ou MDC.
SID	Introduza a ID do sistema (SID). O sistema SAP HANA instalado é identificado por um único SID.
Host de plug-in	Selecione o host do plug-in.
Chaves de armazenamento de usuário seguro HDB	Digite a chave para se conectar ao sistema SAP HANA. A chave contém as informações de login para se conectar ao banco de dados. Para a replicação do sistema SAP HANA, a chave de usuário secundária não é validada. Isso será usado durante a aquisição.
Usuário HDBSQL os	Introduza o nome de utilizador para o qual a chave de armazenamento de utilizador seguro HDB está configurada. Para o Windows, é obrigatório que o usuário do sistema HDBSQL os seja o usuário DO SISTEMA. Portanto, você deve configurar a chave de armazenamento de usuário seguro HDB para o usuário DO SISTEMA.

4. Na página fornecer espaço físico de armazenamento, selecione um sistema de armazenamento e escolha um ou mais volumes, LUNs e qtrees e clique em **Salvar**.

Opcional: Você pode clicar no  ícone * para adicionar mais volumes, LUNs e qtrees de outros sistemas de armazenamento.

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

Os bancos de dados são exibidos juntamente com informações como SID, host de plug-in, grupos e políticas de recursos associados e status geral

Se você quiser fornecer aos usuários acesso a recursos, você deve atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são atribuídos a eles.

"Adicione um usuário ou grupo e atribua funções e ativos"

Depois de adicionar os bancos de dados, você pode modificar os detalhes do banco de dados do SAP HANA.

Não é possível modificar o seguinte se houver backups associados ao recurso SAP HANA:

- Contentores de banco de dados multitenant (MDC): SID, ou HDBSQL Client (plug-in) Host
- Contentor único: SID ou HDBSQL Client (plug-in) Host
- Volume não-dados: Nome do recurso, SID associado ou anfitrião Plug-in

Criar políticas de backup para bancos de dados SAP HANA

Antes de usar o SnapCenter para fazer backup dos recursos do banco de dados do SAP HANA, você precisa criar uma política de backup para o recurso ou grupo de recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e retém backups.

O que você vai precisar

- Você precisa ter definido sua estratégia de backup.

Para obter detalhes, consulte as informações sobre como definir uma estratégia de proteção de dados para bancos de dados SAP HANA.

- Você precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de storage e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído as SVMs para os volumes de origem e destino a você se estiver replicando cópias Snapshot em um espelho ou cofre.

Além disso, você pode especificar as configurações de replicação, script e aplicativo na política. Essas opções economizam tempo quando você deseja reutilizar a política para outro grupo de recursos.

Sobre esta tarefa

- Replicação do sistema SAP HANA
 - Você pode proteger o sistema principal do SAP HANA e todas as operações de proteção de dados podem ser executadas.
 - Você pode proteger o sistema SAP HANA secundário, mas os backups não podem ser criados.

Após o failover, toda a operação de proteção de dados pode ser executada à medida que o sistema SAP HANA secundário se torna o sistema SAP HANA primário.

Você não pode criar um backup para o volume de dados do SAP HANA, mas o SnapCenter continua a proteger os volumes que não são de dados (NDV).

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 Configurações, execute as seguintes etapas:

- Escolha o tipo de cópia de segurança:

Se você quiser...	Faça isso...
Efetue uma verificação de integridade da base de dados	Selecione Backup baseado em arquivos . Somente os locatários ativos são copiados.
Crie um backup usando a tecnologia de cópia Snapshot	Selecione Snapshot based .

- Especifique o tipo de agendamento selecionando **on demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.



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



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

- Na seção **Configurações personalizadas de backup**, forneça quaisquer configurações específicas de backup que tenham que ser passadas para o formato de valor de chave do plug-in.

Você pode fornecer vários valores-chave a serem passados para o plug-in.

6. Na página retenção, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página tipo de backup:

Se você quiser...	Então...
Mantenha um certo número de cópias Snapshot	Selecione Total de cópias snapshot a serem mantidas e especifique o número de cópias snapshot que você deseja manter. Se o número de cópias Snapshot exceder o número especificado, as cópias snapshot serão excluídas com as cópias mais antigas excluídas primeiro.  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.  Para backups baseados em cópias Snapshot, defina a contagem de retenção para 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.  Para replicação do sistema SAP HANA, recomenda-se adicionar todos os recursos do sistema SAP HANA a um grupo de recursos. Isso garante que o número certo de backups seja retido.  Para a replicação do sistema SAP HANA, o total de cópias Snapshot obtidas será igual ao conjunto de retenção para o grupo de recursos. A remoção da cópia Snapshot mais antiga é baseada em qual nó a cópia Snapshot mais antiga está localizada. Por exemplo, a retenção está definida como 7 para um grupo de recursos com SAP HANA System Replication primário e SAP HANA System Replication secundário. Você pode tirar um máximo de 7 cópias Snapshot de cada vez, incluindo SAP HANA System Replication primário e SAP HANA System Replication secundário.

Se você quiser...	Então...
Mantenha as cópias Snapshot por um determinado número de dias	Selecione manter cópias Snapshot para e especifique o número de dias para os quais deseja manter as cópias Snapshot antes de excluí-las.

7. Para backups baseados em cópia Snapshot, especifique as configurações de replicação na página replicação:

Para este campo...	Faça isso...
Atualizar SnapMirror depois de criar uma cópia Snapshot local	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Se a relação de proteção no ONTAP for do tipo espelho e Cofre e se você selecionar somente essa opção, a cópia Snapshot criada no primário não será transferida para o destino, mas será listada no destino. Se esta cópia Snapshot for selecionada no destino para executar uma operação de restauração, o local secundário não estará disponível para a mensagem de erro de backup abobadado/espelhado selecionada será exibida.
Atualizar SnapVault depois de criar uma cópia Snapshot local	Selecione esta opção para executar a replicação de backup disco a disco (backups SnapVault).
Etiqueta de política secundária	Selecione uma etiqueta Snapshot. Dependendo do rótulo da cópia Snapshot selecionado, o ONTAP aplica a política de retenção da cópia snapshot secundária que corresponde ao rótulo.  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.
Contagem de tentativas de erro	Introduza o número máximo de tentativas de replicação que podem ser permitidas antes de a operação parar.



Você deve configurar a política de retenção do SnapMirror no ONTAP para o storage secundário para evitar alcançar o limite máximo de cópias Snapshot no storage secundário.

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

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contendor ao qual você deve adicionar recursos que deseja fazer backup e proteger. 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.

Sobre esta tarefa

Para criar backups de replicação do sistema SAP HANA, recomenda-se adicionar todos os recursos do sistema SAP HANA a um grupo de recursos. Isso garante um backup contínuo durante o modo de recuperação de falhas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, clique em **novo Grupo de recursos**.
3. Na página Nome, execute as seguintes ações:

Para este campo...	Faça isso...
Nome	Introduza um nome para o 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	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da cópia Instantânea. Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um carimbo de data/hora é anexado ao nome da cópia Snapshot.

4. Na página recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Resource Type**.

Isso ajuda a filtrar informações na tela.

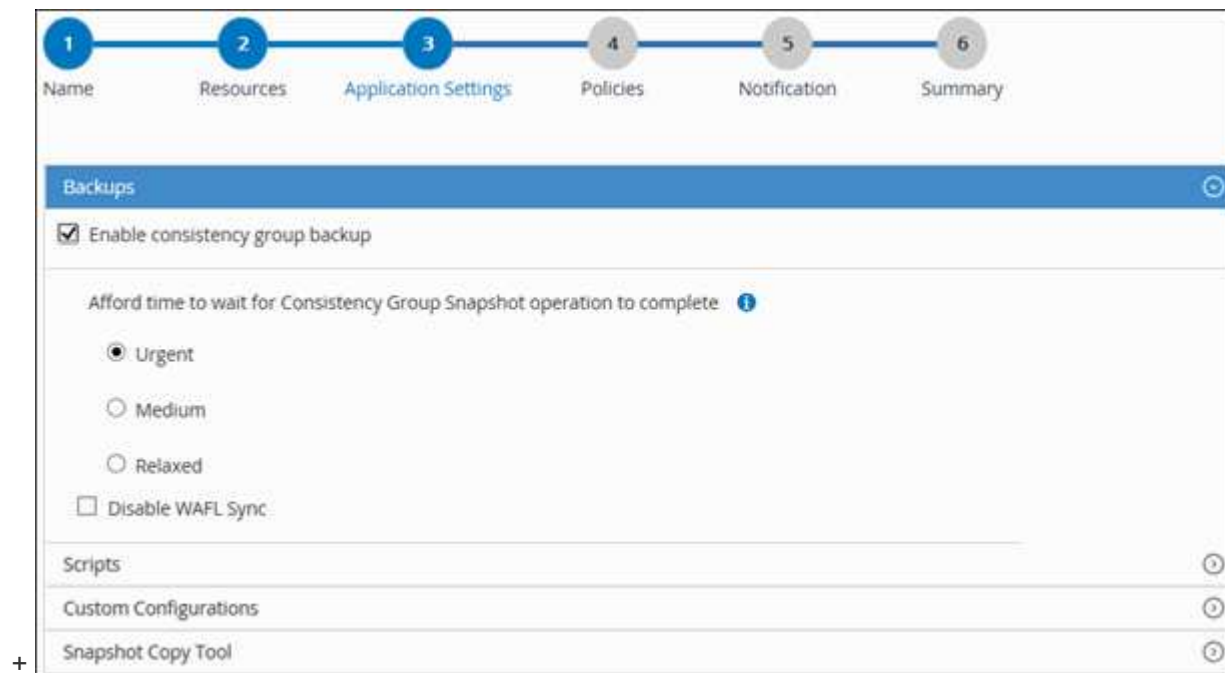
5. Selecione os recursos na seção **recursos disponíveis** e clique na seta para a direita para movê-los para a seção **recursos selecionados**.

6. Na página Configurações do aplicativo, faça o seguinte:

- a. Clique na seta **backups** para definir opções adicionais de backup:

Ative o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo...	Faça isso...
Tenha tempo para esperar que a operação de snapshot do grupo de consistência seja concluída	Selecione urgente , Médio ou relaxado para especificar o tempo de espera para que a operação de cópia Snapshot seja concluída. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL.



- a. Clique na seta **Scripts** e insira os comandos pre e POST para operações quiesce, cópia Snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.
- b. Clique na seta **Custom Configurations** (Configurações personalizadas) e insira os pares de valor de chave personalizados necessários para todas as operações de proteção de dados usando esse recurso.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_ENABLE	(Y/N)	Permite que a gestão do registo de arquivo elimine os registos de arquivo.
ARCHIVE_LOG_RETENÇÃO	number_of_days	Especifica o número de dias em que os logs de arquivo são mantidos. Esta definição tem de ser igual ou superior a NTAP_SNAPSHOT_RETENÇÕES.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs do arquivo.
ARCHIVE_LOG_EXT	extensão_ficheiro	Especifica o comprimento da extensão do arquivo de log do arquivo. Por exemplo, se o log de arquivo for log_backup_0_0_0_0,161518551942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARCH ARCHIVE_LOG_RECURSIVE_ SE	(Y/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs do arquivo estiverem localizados em subdiretórios.



Os pares de valor de chave personalizados são compatíveis com sistemas plug-in SAP HANA Linux e não são compatíveis com banco de dados SAP HANA registrado como um plug-in centralizado do Windows.

- c. Clique na seta **Snapshot Copy Tool** para selecionar a ferramenta para criar cópias snapshot:

Se você quiser...	Então...
SnapCenter para usar o plug-in para Windows e colocar o sistema de arquivos em um estado consistente antes de criar uma cópia Snapshot. Para recursos do Linux, essa opção não é aplicável.	Selecione SnapCenter com consistência do sistema de arquivos . Esta opção não é aplicável ao plug-in SnapCenter para banco de dados SAP HANA.
SnapCenter para criar uma cópia Snapshot no nível de storage	Selecione SnapCenter sem consistência do sistema de arquivos .
Para inserir o comando a ser executado no host para criar cópias Snapshot.	Selecione Other e digite o comando a ser executado no host para criar uma cópia Snapshot.

7. Na página políticas, execute as seguintes etapas:

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



Você também pode criar uma política clicando em .

As políticas são listadas na seção Configurar programações para políticas selecionadas.

- b. Na coluna Configurar agendas, clique em para a política que deseja configurar.
- c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.

Onde, *policy_name* é o nome da política selecionada.

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

As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas de backup do SnapCenter.

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. O servidor SMTP deve ser configurado em **Configurações > Configurações globais**.

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

Fazer backup de bancos de dados do SAP HANA

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

O que você vai precisar

- 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.
- Para a operação de backup baseada em cópia Snapshot, verifique se todos os bancos de dados do locatário são válidos e ativos.
- Para criar backups de replicação do sistema SAP HANA, recomenda-se adicionar todos os recursos do sistema SAP HANA a um grupo de recursos. Isso garante um backup contínuo durante o modo de recuperação de falhas.

["Crie grupos de recursos e anexe políticas".](#)

["Fazer backup de grupos de recursos"](#)

- Se você quiser criar um backup baseado em arquivo quando um ou mais bancos de dados de locatário estiverem inativos, defina o parâmetro `ALLOW_FILE_BASED_BACKUP_IFINACTIVO_TENANTS_PRESENT` como **YES** no arquivo de propriedades HANA usando `Set-SmConfigSettings cmdlet`.

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 ["Guia de referência de cmdlet do software SnapCenter"](#)

- Para os comandos pré e POST para operações do quiesce, cópia Snapshot e unquiesce, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in dos seguintes caminhos:

Para o Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands_list.txt*

Para Linux: */var/opt/SnapCenter/scc/allowed_commands_list.txt*



Se os comandos não existirem na lista de comandos, a operação falhará.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recurso, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

Clique em  e selecione o nome do host e o tipo de recurso para filtrar os recursos. Em seguida, pode clicar  para fechar o painel de filtro.

3. Clique no recurso que você deseja fazer backup.
4. Na página recurso, selecione **Use o 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.

5. Na página Configurações do aplicativo, faça o seguinte:
 - Clique na seta **backups** para definir opções adicionais de backup:

Ative o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

Para este campo...	Faça isso...
Tenha tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione urgente , Médio ou relaxado para especificar o tempo de espera para que a operação de cópia Instantânea termine. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL.

- Clique na seta **Scripts** para executar comandos pré e POST para operações quiesce, cópia Snapshot e unquiesce.

Você também pode executar pré-comandos antes de sair da operação de backup. Os Prescripts e postscripts são executados no servidor SnapCenter.

- Clique na seta ****Custom Configurations (Configurações personalizadas)** e, em seguida, insira os pares de valores personalizados necessários para todos os trabalhos que usam esse recurso.
- Clique na seta **Snapshot Copy Tool** para selecionar a ferramenta para criar cópias snapshot:

Se você quiser...	Então...
SnapCenter para criar uma cópia Snapshot no nível de storage	Selecione SnapCenter sem consistência do sistema de arquivos .
SnapCenter para usar o plug-in para Windows para colocar o sistema de arquivos em um estado consistente e, em seguida, criar uma cópia Snapshot	Selecione SnapCenter com consistência do sistema de arquivos .
Para inserir o comando para criar uma cópia Snapshot	Selecione Other e digite o comando para criar uma cópia Snapshot.

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. 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 é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas.

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. O SMTP também deve ser configurado em **Configurações > Configurações globais**.

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

A página de topologia de recursos é exibida.

9. Clique em **fazer backup agora**.

10. Na página Backup, execute as seguintes etapas:

- a. Se você aplicou 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. Clique em **Backup**.

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

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

Para obter informações, consulte: ["Não é possível detectar 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 comando `do_start Method` inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M`

Fazer backup de grupos de recursos

Um grupo de recursos é uma coleção de recursos em um host. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

O que você vai precisar

- Você deve ter criado um grupo de recursos com uma política anexada.
- 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.

Sobre esta tarefa

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 selecionando a tag. Em seguida, pode clicar  para fechar o painel de 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. Clique em **Backup**.

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

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para banco de dados SAP HANA

Você deve criar uma conexão de máquina virtual de storage (SVM) e uma credencial antes de usar cmdlets do PowerShell para fazer backup, restaurar ou clonar bancos de dados SAP HANA.

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 dados exclusivo.

Passos

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

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

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

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

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

Este exemplo mostra como criar uma nova credencial chamada FinanceAdmin com credenciais do Windows:

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

4. Adicione o host de comunicação SAP HANA ao servidor SnapCenter.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode hana
```

5. Instale o pacote e o plug-in do SnapCenter para o banco de dados SAP HANA no host.

Para Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
hana
```

Para Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana  
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Defina o caminho para o cliente HDBSQL.

Para Windows:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode  
hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program  
Files\sap\hdbclient\hdbsql.exe"}
```

Para Linux:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com  
-PluginCode hana -configSettings  
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

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 bancos de dados usando cmdlets do PowerShell

Fazer backup de um banco de dados inclui estabelecer uma conexão com o servidor

SnapCenter, adicionar recursos, adicionar uma política, criar um grupo de recursos de backup e fazer 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.

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. Adicione recursos usando o cmdlet `Add-SmResources`.

Este exemplo mostra como adicionar um banco de dados SAP HANA do tipo `SingleContainer`:

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"})
-SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys 'HS10'
-osdbuser 'h10adm' -filebackupprefix 'H10_'
```

Este exemplo mostra como adicionar um banco de dados SAP HANA do tipo `MultipleContainers`:

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType MultipleContainers
-StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.netapp.
com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType 'MultiTenant'
```

Este exemplo mostra como criar um recurso de volume que não seja de dados:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sscore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

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

Este exemplo cria uma política de backup para um backup baseado em cópia Snapshot:

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType Backup
-PluginPolicyType hana -BackupType SnapShotBasedBackup
```

Este exemplo cria uma política de backup para um backup baseado em arquivos:

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. Proteja o recurso ou adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.

Este exemplo protege um único recurso de contentor:

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="SID"} -Description test
-usesnapcenterwithoutfilesystemconsistency
```

Este exemplo protege um recurso de vários contêineres:

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="MDC\SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

Este exemplo cria um novo grupo de recursos com a política e os recursos especificados:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="sccore
linux62.sccore.test.com";"Uid"="MDC\SID"})
-Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency -plugincode 'HANA'
```

Este exemplo cria um grupo de recursos de volume não-dados:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="H11";"PluginName"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="MDC\H31";"PluginName"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="NonDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies hanaprimary
```

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

Este exemplo mostra como fazer backup de um grupo de recursos:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

Este exemplo faz backup de um recurso protegido:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"} -Policy
hana_Filebased
```

6. Monitore o status da tarefa (em execução, concluída ou com falha) usando o cmdlet Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Monitore os detalhes da tarefa de backup, como ID do backup, nome do backup para executar a operação de restauração ou clone usando o cmdlet Get-SmBackupReport.

```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId               : 269
SmJobId                  : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime              : 10/4/2016 11:21:32 PM
Duration                 : 00:00:46.2536470
CreatedDateTime          : 10/4/2016 11:21:09 PM
Status                   : Completed
ProtectionGroupName      : Verify_ASUP_Message_windows
SmProtectionGroupId      : 211
PolicyName               : test2
SmPolicyId               : 20
BackupName               : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus       : NotVerified
VerificationStatuses     :
SmJobError               :
BackupType               : SCC_BACKUP
CatalogingStatus        : NotApplicable
CatalogingStatuses      :
ReportDataCreatedDateTime :

```

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 backup

Monitore operações de backup de bancos de dados SAP HANA

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 bancos de dados SAP HANA 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.

Cancelar operações de backup para SAP HANA

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

O que você vai precisar

- Você deve estar logado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de cópia de segurança em execução.
- Você pode usar os comandos GUI, cmdlets do SnapCenter ou CLI para cancelar as operações de backup.
- 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.

Passos

1. Execute uma das seguintes ações:

A partir do...	Ação
Página do monitor	a. No painel de navegação esquerdo, clique em Monitor > trabalhos. b. Selecione a operação e clique em Cancelar trabalho.
Painel da atividade	a. Depois de iniciar a operação de backup, clique em  no painel atividade para exibir as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes da tarefa, clique em Cancelar tarefa.

A operação é cancelada e o recurso é revertido para o estado anterior.

Veja os backups e clones do banco de dados SAP HANA 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

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.



Para os recursos primários de replicação do sistema SAP HANA, as operações de restauração e exclusão são compatíveis e, para recursos secundários, a operação de clone é compatível.

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.

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 estiver protegido, a página de topologia do recurso selecionado será exibida.

4. Revise o **cartão de resumo** para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

A seção **cartão de resumo** exibe o número total de backups baseados em arquivos, backups de cópia Snapshot e clones.

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

5. No modo de 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 e exclusão.



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

7. Se quiser excluir um clone, selecione-o na tabela e clique  em .

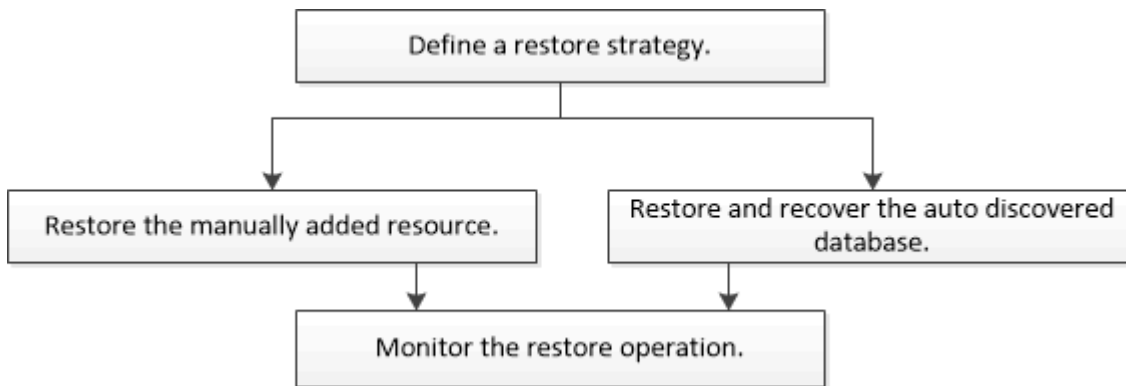
8. Se quiser dividir um clone, selecione-o na tabela e clique  em .

Restaure os bancos de dados do SAP HANA

Restaure o fluxo de trabalho

O fluxo de trabalho de restauração e recuperação inclui Planejamento, execução das operações de restauração e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de restauração:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

["Guia de referência de cmdlet do software SnapCenter"](#).

Restaure e recupere um backup de recursos adicionado manualmente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

O que você vai precisar

- Você deve ter feito backup dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:

Para o Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands_list.txt*

Para Linux: */var/opt/SnapCenter/scc/allowed_commands_list.txt*



Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- As cópias de backup baseadas em arquivo não podem ser restauradas a partir do SnapCenter.

- Após a atualização para o SnapCenter 4,3, os backups feitos no SnapCenter 4,2 podem ser restaurados, mas não podem ser recuperados. Você precisa usar scripts de recuperação HANA ou estúdio externos ao SnapCenter para recuperar os backups feitos no SnapCenter 4,2.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.



Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e, em seguida, selecione um recurso nesse grupo.

A página de topologia do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).

5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em ** .

Primary Backup(s)	
search 	  
Backup Name	End Date
rg1_scpr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. Na página Restaurar escopo, selecione **recurso completo** ou **nível de arquivo**.

- a. Se você selecionar **Complete Resource**, todos os volumes de dados configurados do banco de dados SAP HANA serão restaurados.

Se o recurso contiver volumes ou qtrees, as cópias Snapshot obtidas após a cópia Snapshot selecionada para restauração nesses volumes ou qtrees serão excluídas e não poderão ser recuperadas. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

- b. Se você selecionar **File Level**, poderá selecionar **All** ou selecionar os volumes ou qtrees específicos e, em seguida, inserir o caminho relacionado a esses volumes ou qtrees, separados por vírgulas
 - Você pode selecionar vários volumes e qtrees.
 - Se o tipo de recurso for LUN, todo o LUN será restaurado.

Pode selecionar vários LUNs.



Se você selecionar **All**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar um trabalho de restauração.

Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

8. Na página Post OPS, insira os comandos mount e POST Restore para serem executados após a execução de um trabalho de restauração.

Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

9. 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. O SMTP também deve ser configurado na página **Configurações > Configurações globais**.

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

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

Restaure e recupere um backup de banco de dados descoberto automaticamente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

O que você vai precisar

- Você deve ter feito backup dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:

Para o Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands_list.txt*

Para Linux: */var/opt/SnapCenter/scc/allowed_commands_list.txt*



Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- As cópias de backup baseadas em arquivo não podem ser restauradas a partir do SnapCenter.
- Após a atualização para o SnapCenter 4,3, os backups feitos no SnapCenter 4,2 podem ser restaurados, mas não podem ser recuperados. Você precisa usar scripts de recuperação HANA ou estúdio externos ao SnapCenter para recuperar os backups feitos no SnapCenter 4,2.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.



Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e, em seguida, selecione um recurso nesse grupo.

A página de topologia do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).

5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em ** .

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scsp0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. Na página Restaurar escopo, selecione **recurso completo** para restaurar os volumes de dados configurados do banco de dados SAP HANA.



Você pode selecionar **Complete Resource** (com ou sem **volume Revert**) ou **Tenant Database**.

A operação de recuperação não é suportada pelo servidor SnapCenter para vários locatários quando o usuário seleciona a opção **Banco de dados do locatário** ou **Restauração completa**. Você deve usar O HANA Studio ou o script HANA Python para executar a operação de recuperação.

- a. Selecione **Reverter volume** se quiser restaurar todo o volume.

Essa opção está disponível para backups feitos no SnapCenter 4,3 em ambientes NFS.

Se o recurso contiver volumes ou qtrees, as cópias Snapshot obtidas após a cópia Snapshot selecionada para restauração nesses volumes ou qtrees serão excluídas e não poderão ser recuperadas. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído. Isso é aplicável quando a opção **Complete Resource** com **volume Revert** estiver selecionada para restauração.

- b. Selecione **Banco de dados do locatário**.

Esta opção está disponível apenas para recursos MDC.

Certifique-se de parar o banco de dados do locatário antes de executar a operação de restauração.

Se você selecionar a opção **Banco de dados do locatário**, use O estúdio HANA ou use scripts de recuperação HANA externos ao SnapCenter para executar a operação de recuperação.

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

Se você...	Faça isso...
Deseja recuperar o mais próximo possível da hora atual	Selecione Recover to most recent State (recuperar para o estado mais recente). Para recursos de contentor único, especifique um ou mais locais de backup de log e catálogo. Para recursos de contentor de banco de dados multitenant (MDC), especifique um ou mais locais de backup de log e o local do catálogo de backup. Para recursos MDC, o caminho deve conter Registros de banco de dados de sistema e banco de dados de locatário.

Se você...	Faça isso...
Deseja recuperar para o ponto especificado no tempo	Selecione Recover to point in time. a. Selecione o fuso horário. O fuso horário do navegador é preenchido por padrão. O fuso horário selecionado juntamente com a hora de entrada é convertido para GMT absoluto. b. Introduza a data e a hora. Por exemplo, o host HANA Linux está localizado em Sunnyvale, CA e o usuário em Raleigh, NC está recuperando os logs no SnapCenter. A diferença de horário entre ambos os locais é de 3 horas, e como o usuário fez login em Raleigh, NC, o fuso horário padrão do navegador que será selecionado na GUI é GMT-04:00. Se o usuário quiser executar uma recuperação para 5 a.m. Sunnyvale, CA, então o usuário deve definir o fuso horário do navegador para o fuso horário do host DO HANA Linux, que é GMT-07:00 e especificar a data e a hora como 5:00 a.m. Para recursos de contentor único, especifique um ou mais locais de backup de log e catálogo. Para recursos do MDC, especifique um ou mais locais de backup de log e o local do catálogo de backup. Para recursos MDC, o caminho deve conter Registros de banco de dados de sistema e banco de dados de locatário.
Deseja recuperar para um backup de dados específico	Selecione Recover to specified data backup .
Não quero recuperar	Selecione sem recuperação . Você deve executar a operação de recuperação manualmente a partir do estúdio HANA.

Você pode recuperar apenas os backups que são feitos após a atualização para o SnapCenter 4,3, desde que o host e o plug-in sejam atualizados para o SnapCenter 4,3, e os backups selecionados para restauração sejam feitos após a conversão ou descoberta do recurso como recurso descoberta automática.

8. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar um trabalho de restauração.

Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

9. Na página Post OPS, insira os comandos mount e POST Restore para serem executados após a execução de um trabalho de restauração.

Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

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. O SMTP também deve ser configurado na página **Configurações > Configurações globais**.

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

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

Restaure o banco de dados SAP HANA usando cmdlets do PowerShell

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

O que você vai precisar

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. Identifique o backup que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

Este exemplo mostra que existem dois backups disponíveis para a restauração:

```
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. Inicie o processo de recuperação no estúdio HANA.

O banco de dados é encerrado.

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



AppObjectId é "Host Você pode obter o ResourceID do cmdlet Get-smResources.

```
Get-smResources -HostName cn24.sscore.test.com -PluginCode HANA
```

Este exemplo mostra como restaurar o banco de dados do armazenamento primário:

```
Restore-SmBackup -PluginCode HANA -AppObjectId  
cn24.sscore.test.com\hana\H10 -BackupId 3
```

Este exemplo mostra como restaurar o banco de dados do armazenamento secundário:

```
Restore-SmBackup -PluginCode 'HANA' -AppObjectId  
cn24.sscore.test.com\hana\H10 -BackupId 399 -Confirm:$false -Archive @(  
@{"Primary"="<Primary Vserver>:<PrimaryVolume>";"Secondary"="<Secondary  
Vserver>:<SecondaryVolume>"}))
```

Os backups estarão disponíveis no estúdio HANA para recuperação.

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"](#).

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"](#).

Monitore as operações de restauração de bancos de dados SAP HANA

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.

Clonar backups de recursos do SAP HANA

Fluxo de trabalho clone

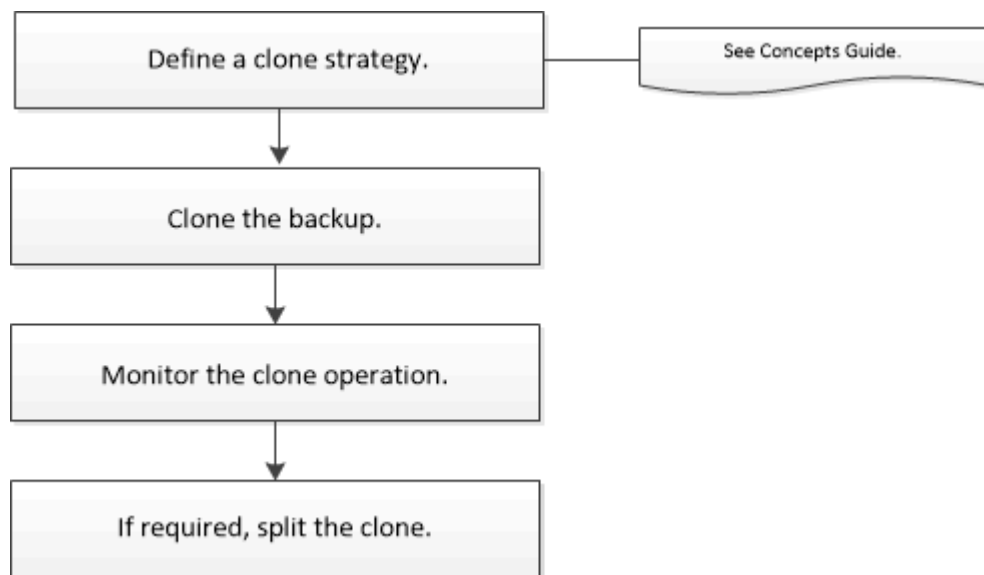
O fluxo de trabalho do clone inclui a execução da operação de clone e o monitoramento da operação.

Sobre esta tarefa

- Você pode clonar no servidor SAP HANA de origem.
- Você pode clonar backups de recursos pelos seguintes motivos:
 - Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais dos recursos durante os ciclos de desenvolvimento de aplicativos
 - Para ferramentas de extração e manipulação de dados ao preencher data warehouses

- Para recuperar dados que foram excluídos ou alterados por engano

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação clone:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

Clone um backup de banco de dados SAP HANA

Você pode usar o SnapCenter para clonar um backup. Você pode clonar do backup primário ou secundário.

O que você vai precisar

- Você deve ter feito backup dos recursos ou do grupo de recursos.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de storage (SVM).
- Não é possível clonar backups baseados em arquivo.
- O servidor clone de destino deve ter o mesmo SID de instância do SAP HANA que é fornecido no campo SID Clone de destino.
- Para comandos pré-clone ou pós-clone, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:

Para o Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands_list.txt*

Para Linux: */var/opt/SnapCenter/scc/allowed_commands_list.txt*



Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

Para obter informações sobre limitações de operação de divisão de clones, "[Guia de gerenciamento de](#)

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

Os recursos são exibidos juntamente com informações como tipo, host, grupos e políticas de recursos associados e status.

3. Selecione o grupo de recursos ou recursos.

Você deve selecionar um recurso se selecionar um grupo de recursos.

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

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Selecione o backup de dados na tabela e clique  em .
6. Na página localização, execute as seguintes ações:

Para este campo...	Faça isso...
Host plug-in	Selecione o host no qual o clone deve ser montado e o plug-in está instalado.
SID Clone alvo	Insira o ID da instância do SAP HANA para clonar dos backups existentes.
Endereço IP de exportação NFS	Insira endereços IP ou os nomes de host nos quais os volumes clonados serão exportados.
Iniciador iSCSI	Insira o nome do iniciador iSCSI do host para o qual os LUNs são exportados. Esta opção só está disponível se você selecionou o tipo de recurso LUN.
Protocolo	Introduza o protocolo LUN. Esta opção só está disponível se você selecionou o tipo de recurso LUN.

Se o recurso selecionado for um LUN e você estiver clonando de um backup secundário, os volumes de destino serão listados. Uma única fonte pode ter vários volumes de destino.



Antes da clonagem, você deve garantir que o iniciador iSCSI ou o FCP estejam presentes e configurados e conectados em hosts alternativos.

7. Na página Scripts, execute as seguintes etapas:



Os scripts são executados no host do plug-in.

a. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.

- Comando pre clone: Exclua bancos de dados existentes com o mesmo nome
- Comando Post clone: Verifique um banco de dados ou inicie um banco de dados.

b. Digite o comando mount para montar um sistema de arquivos em um host.

Monte o comando para um volume ou qtree em uma máquina Linux:

Exemplo para NFS:

```
mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt
```

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.

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

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

Clonar backups de bancos de dados do SAP HANA 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.

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. Recupere os backups para executar a operação de clone usando o cmdlet Get-SmBackup.

Este exemplo mostra que dois backups estão disponíveis para clonagem:

```
C:\PS> 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	

3. Inicie uma operação de clone a partir de um backup existente e especifique os endereços IP de exportação NFS nos quais os volumes clonados são exportados.

Este exemplo mostra que o backup a ser clonado tem um endereço NFSEXPOTIPs de 10.232.206.169:

```
New-SmClone -AppPluginCode hana -BackupName  
scscscore1_sccore_test_com_hana_H73_scscscore1_06-07-2017_02.54.29.3817  
-Resources @{"Host"="scscscore1.sccore.test.com";"Uid"="H73"}  
-CloneToInstance shivsc4.sccore.test.com -mountcommand 'mount  
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands  
'/home/scripts/scpre_clone.sh' -postclonecreatecommands  
'/home/scripts/scpost_clone.sh'
```



Se NFSEXPOTIPs não for especificado, o padrão será exportado para o host de destino clone.

4. Verifique se os backups foram clonados com sucesso usando o cmdlet Get-SmCloneReport para exibir os detalhes da tarefa clone.

Você pode exibir detalhes como ID do clone, data e hora de início, data e hora de término.

```
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}
SmJobError           :
```

Monitorar operações de clone de banco de dados SAP HANA

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**.

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"](#)

Exclua ou divida clones do banco de dados do SAP HANA após a atualização do SnapCenter

Após a atualização para o SnapCenter 4,3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones da página topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar o espaço físico de armazenamento dos clones ocultos, execute o seguinte comando:

```
Get-SmClone -ListStorageFootprint
```

Passos

1. Exclua os backups dos recursos clonados usando o cmdlet remove-smbbackup.
2. Exclua o grupo de recursos dos recursos clonados usando o cmdlet remove-smresourcegroup.
3. Remova a proteção do recurso clonado usando o cmdlet remove-sprotectresource.
4. Selecione o recurso pai na página recursos.

A página de topologia do recurso é exibida.

5. Na visualização Gerenciar cópias, selecione os clones nos sistemas de storage primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique  para excluir clones ou clique para  dividir os clones.

7. Clique em **OK**.

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 SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO 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.