



Backup e recuperação do SAP HANA com o SnapCenter

NetApp solutions for SAP

NetApp
February 25, 2026

Índice

Backup e recuperação do SAP HANA com o SnapCenter	1
Proteja sistemas SAP HANA com o SnapCenter em ONTAP, Azure NetApp Files e FSx para ONTAP.....	1
Saiba mais sobre proteção de dados SAP HANA com a tecnologia NetApp Snapshot.....	1
Backup e recuperação usando backups de instantâneo	2
Tempo de execução das operações de backup e restauração do Snapshot	3
Comparação do objetivo de tempo de recuperação	3
Casos de uso e valores de operações de clonagem e backup acelerados	4
Saiba mais sobre a arquitetura do SnapCenter.....	5
Saiba mais sobre backup e recuperação do SnapCenter para SAP HANA.....	5
Saiba mais sobre as configurações compatíveis com o SnapCenter para SAP HANA.....	7
Configurações SAP HANA suportadas	7
Configurações de plataforma e infraestrutura suportadas	8
Funcionalidades e operações suportadas	8
Saiba mais sobre os conceitos e as melhores práticas de proteção de dados do SnapCenter.....	12
Opções de implantação para o plug-in SnapCenter para SAP HANA.....	12
verificação de consistência de bloco do SAP HANA	14
Estratégia de proteção de dados	15
Cópia de segurança das chaves raiz de criptografia	16
Operações de backup	17
Gerenciamento de retenção de backups	18
Saiba mais sobre como configurar o SnapCenter para ambientes SAP HANA.....	19
Configure as definições iniciais do SnapCenter para SAP HANA.....	20
Configuração de credenciais	21
Configuração do sistema de storage	24
Configuração de políticas	25
Configure os recursos do SnapCenter para bancos de dados SAP HANA individuais.....	27
Configuração do usuário de backup do SAP HANA e do repositório de usuários do SAP HANA.....	28
Configuração de replicação de armazenamento	30
Configuração de backup ANF	30
Implantação do plug-in SnapCenter para SAP HANA.....	30
Descoberta automática do HANA	31
Configuração de proteção de recursos	31
Configure o SnapCenter para fazer backup de volumes que não contenham dados.....	32
Configure o host do plug-in central do SnapCenter para SAP HANA.....	33
Implantação do plug-in SnapCenter HANA	33
Instalação e configuração do software cliente SAP HANA hdbsql	34
Configuração do repositório de usuários do SAP HANA para um host de plug-in central.....	34
Configuração manual de recursos do HANA	35
Saiba mais sobre operações de backup para snapshots do SAP HANA no SnapCenter.....	36
Backups de snapshots do SAP HANA no SnapCenter	36
Cópias de segurança de snapshots do SAP HANA no SAP HANA Studio	37
Cópias de segurança de snapshots do SAP HANA na camada de armazenamento	37
Backups de snapshots do SAP HANA com ANF	37

Cópias de segurança instantâneas de volumes que não são de dados	38
Fluxo de trabalho de backup para backups de banco de dados HANA	38
Fluxo de trabalho de backup para volumes que não são de dados.	38
Limpeza de backups secundários	39
Execute verificações de consistência de blocos do SAP HANA com o SnapCenter.	41
Verificações de consistência com hdbpersdiag usando o diretório de snapshots local.	42
Verificações de consistência com hdbpersdiag usando um host de verificação central.	45
Backup baseado em arquivos	53
Restaurar e recuperar bancos de dados SAP HANA com o SnapCenter.	55
Restauração e recuperação automatizadas para sistemas SAP HANA MDC com um único locatário. . .	55
Recuperação manual com o HANA Studio	57
Recuperação manual com comandos SQL	61
Restauração e recuperação de inquilino único	61
Restauração de volumes não relacionados a dados	62
Configure as opções avançadas do SnapCenter para SAP HANA.	62
Mensagem de aviso em ambientes virtualizados e montagens no sistema operacional convidado. . . .	62
Desativar a limpeza automática de cópias de segurança de registros	62
Habilitar a comunicação segura com o banco de dados HANA	63
Desative a detecção automática no host do plug-in HANA	63

Backup e recuperação do SAP HANA com o SnapCenter

Proteja sistemas SAP HANA com o SnapCenter em ONTAP, Azure NetApp Files e FSx para ONTAP.

Proteja sistemas SAP HANA com o NetApp SnapCenter usando backups baseados em snapshots e replicação de dados. Esta solução abrange as melhores práticas de configuração e operação do SnapCenter para sistemas SAP HANA em sistemas ONTAP AFF e ASA, Azure NetApp Files e Amazon FSx para ONTAP, incluindo estratégias de backup, verificações de consistência e fluxos de trabalho de recuperação.

Autor: Nils Bauer, NetApp

Detalhes adicionais específicos sobre casos de uso relacionados a operações de atualização do sistema SAP e replicação do sistema SAP HANA podem ser encontrados em:

- ["Automatizando as operações de clonagem e cópia do sistema SAP HANA com o SnapCenter"](#)
- ["Replicação do sistema SAP HANA: Backup e recuperação com o SnapCenter"](#)

As melhores práticas para combinar a proteção de dados do SnapCenter com a sincronização ativa do NetApp SnapMirror são descritas em

- ["Proteção de dados SAP HANA e alta disponibilidade com sincronização ativa SnapCenter, SnapMirror e VMware Metro Storage Cluster"](#)

Documentação adicional sobre as melhores práticas específicas da plataforma está disponível em

- ["Proteção de dados SAP HANA com SnapCenter com sistemas VMware VMFS e NetApp ASA"](#)
- ["SAP HANA no Amazon FSX for NetApp ONTAP - Backup e recuperação com o SnapCenter"](#)
- ["Proteção de dados SAP HANA no Azure NetApp Files com SnapCenter \(blog e vídeo\)"](#)
- ["Operações de clonagem e atualização do sistema SAP no Azure NetApp Files com o SnapCenter \(blog e vídeo\)"](#)

Saiba mais sobre proteção de dados SAP HANA com a tecnologia NetApp Snapshot.

Descubra como a tecnologia NetApp Snapshot protege bancos de dados SAP HANA com backups concluídos em minutos, independentemente do tamanho do banco de dados. Saiba mais sobre estratégias de backup e recuperação usando cópias de Snapshot, SnapRestore para recuperação rápida e replicação com SnapVault ou backup do Azure NetApp Files para proteção secundária.

Atualmente, as empresas exigem disponibilidade contínua e ininterrupta para seus aplicativos SAP. Eles esperam níveis de desempenho consistentes e precisam de operações diárias automatizadas diante de volumes de dados cada vez maiores e da necessidade de tarefas de manutenção de rotina, como backups do sistema. Realizar backups de bancos de dados SAP é uma tarefa crítica e pode ter um impacto significativo

no desempenho do sistema SAP de produção.

As janelas de backup estão diminuindo, enquanto a quantidade de dados a serem copiados está aumentando. Portanto, é difícil encontrar um momento em que seja possível realizar backups com o mínimo impacto nos processos de negócios. O tempo necessário para restaurar e recuperar os sistemas SAP é uma preocupação, pois o tempo de inatividade dos sistemas SAP de produção e não produção deve ser minimizado para reduzir os custos para a empresa.

Backup e recuperação usando backups de instantâneo

Você pode usar a tecnologia NetApp Snapshot para criar backups de banco de dados em minutos. O tempo necessário para criar uma cópia de Snapshot é independente do tamanho do banco de dados, pois uma cópia de Snapshot não move nenhum bloco de dados físico na plataforma de armazenamento. Além disso, o uso da tecnologia Snapshot não afeta o desempenho do sistema SAP em produção, uma vez que todas as operações são executadas no sistema de armazenamento. Portanto, você pode agendar a criação de cópias de instantâneo sem levar em consideração os períodos de pico de diálogo ou atividade em lote. Os clientes SAP on NetApp normalmente agendam vários backups de Snapshot online durante o dia; por exemplo, a cada seis horas é comum. Esses backups instantâneos são normalmente mantidos por três a cinco dias no sistema de armazenamento primário antes de serem removidos ou transferidos para um armazenamento mais barato para retenção a longo prazo.

As cópias instantâneas também oferecem vantagens importantes para operações de restauração e recuperação. Uma operação de restauração recupera os dados no sistema de arquivos com base no estado de um backup. Uma operação de recuperação é usada para restaurar o estado do banco de dados para um ponto específico no tempo, utilizando backups dos logs do banco de dados.

A tecnologia NetApp SnapRestore permite a restauração de um banco de dados inteiro ou, alternativamente, apenas de uma parte dele, com base nos backups Snapshot disponíveis no momento. O processo de restauração é concluído em poucos segundos, independentemente do tamanho do banco de dados. Como vários backups instantâneos online podem ser criados durante o dia, o tempo necessário para o processo de recuperação é significativamente reduzido em comparação com a abordagem tradicional de backup uma vez por dia. Como é possível realizar uma restauração com uma cópia de Snapshot que tenha no máximo algumas horas (em vez de até 24 horas), menos registros de transação precisam ser aplicados durante a recuperação. O tempo necessário para restauração e recuperação é significativamente reduzido em comparação com os backups de streaming tradicionais.

Como os backups de Snapshot são armazenados no mesmo sistema de disco que os dados online ativos, a NetApp recomenda usar as cópias de backup de Snapshot como um complemento, e não como uma substituição, para backups em um local secundário. A maioria das ações de restauração e recuperação são gerenciadas usando o SnapRestore no sistema de armazenamento primário. A restauração a partir de um local secundário só é necessária se o sistema de armazenamento primário que contém as cópias do Snapshot não estiver disponível. Você também pode usar o backup secundário caso seja necessário restaurar um backup que não esteja mais disponível no armazenamento primário.

O backup para um local secundário é baseado em cópias de snapshot criadas no armazenamento primário. Dessa forma, os dados são lidos diretamente do sistema de armazenamento primário sem gerar carga no servidor de banco de dados SAP e em sua rede. O armazenamento primário comunica-se diretamente com o armazenamento secundário e replica os dados de backup para o destino usando a funcionalidade de backup SnapVault ou ANF.

O SnapVault e o backup ANF oferecem vantagens significativas em comparação com os backups tradicionais. Após uma transferência inicial de dados, onde todos os dados são transferidos da origem para o destino, todos os backups subsequentes replicam apenas os blocos alterados para o armazenamento secundário. Portanto, a carga no sistema de armazenamento primário e o tempo necessário para um backup completo são significativamente reduzidos. Como apenas os blocos alterados são armazenados no destino, qualquer

backup completo adicional do banco de dados consome significativamente menos espaço em disco.

Tempo de execução das operações de backup e restauração do Snapshot

A figura a seguir mostra o HANA Studio de um cliente usando operações de backup de Snapshot. A imagem mostra que o banco de dados HANA (com aproximadamente 4 TB de tamanho) é copiado em 1 minuto e 20 segundos usando a tecnologia de backup Snapshot e em mais de 4 horas com uma operação de backup baseada em arquivos.

A maior parte do tempo total de execução do fluxo de trabalho de backup é o tempo necessário para executar a operação de Snapshot do banco de dados HANA. O backup do snapshot de armazenamento em si é concluído em poucos segundos, independentemente do tamanho do banco de dados HANA.

[largura=624, altura=267]

Comparação do objetivo de tempo de recuperação

Esta seção apresenta uma comparação do objetivo de tempo de recuperação (RTO) de backups de Snapshot baseados em arquivos e backups de Snapshot baseados em armazenamento. O RTO é definido pela soma do tempo necessário para restaurar, recuperar e, em seguida, iniciar o banco de dados.

Tempo necessário para restaurar o banco de dados

Com um backup baseado em arquivo, o tempo de restauração depende do tamanho do banco de dados e da infraestrutura de backup, que define a velocidade de restauração em megabytes por segundo. Por exemplo, se a infraestrutura oferecer suporte a uma operação de restauração a uma velocidade de 250MBps Gbps, levará aproximadamente 4,5 horas para restaurar um banco de dados de tamanho 4TB na persistência.

Com os backups Snapshot da NetApp, o tempo de restauração é independente do tamanho do banco de dados e está sempre na faixa de alguns segundos.

Tempo necessário para recuperar o banco de dados

O tempo de recuperação depende do número de logs que devem ser aplicados após a restauração. Este número é determinado pela frequência em que os backups de dados são feitos.

Com backups de dados baseados em arquivos, o agendamento de backup geralmente é uma vez por dia. Uma frequência de backup maior normalmente não é possível, porque o backup degrada o desempenho de produção. Portanto, no pior dos casos, todos os logs que foram escritos durante o dia devem ser aplicados durante a recuperação futura.

Os backups de snapshots são normalmente agendados com maior frequência, pois não têm impacto no desempenho do banco de dados SAP HANA. Por exemplo, se os backups de Snapshot estiverem agendados a cada seis horas, os logs precisarão ser aplicados, no pior cenário, referentes às últimas seis horas, caso a falha ocorra imediatamente antes da criação do próximo Snapshot. Para um backup diário baseado em arquivos, os logs das últimas 24 horas precisariam ser aplicados, no pior dos casos.

Tempo necessário para iniciar o banco de dados

A hora de início do banco de dados depende do tamanho do banco de dados e do tempo necessário para carregar os dados na memória. Nos exemplos a seguir, presume-se que os dados podem ser carregados com 1000Mbps. Carregar 4TB GB na memória demora cerca de 1hour e 10 minutos. O horário de início é o mesmo para operações de restauração e recuperação baseadas em Snapshot e arquivo.

Cálculo de amostra de restauração e recuperação

A figura a seguir mostra uma comparação entre operações de restauração e recuperação com backup diário baseado em arquivos e backups de snapshot com diferentes programações.

As duas primeiras barras mostram que, mesmo com um único backup de Snapshot por dia, a restauração e a recuperação são reduzidas para 43% devido à velocidade da operação de restauração a partir de um backup de Snapshot. Se forem criados vários backups Snapshot por dia, o tempo de execução poderá ser reduzido ainda mais, pois menos logs precisam ser aplicados durante a recuperação avançada.

A figura a seguir também mostra que quatro a seis backups Snapshot por dia faz mais sentido, porque uma frequência mais alta não tem mais uma grande influência no tempo de execução geral.

[largura=624, altura=326]

Casos de uso e valores de operações de clonagem e backup acelerados

A execução de backups é uma parte essencial de qualquer estratégia de proteção de dados. Os backups são programados regularmente para garantir que você possa se recuperar de falhas do sistema. Esse é o caso de uso mais óbvio, mas também há outras tarefas de gerenciamento de ciclo de vida do SAP, onde acelerar as operações de backup e recuperação é crucial.

A atualização do sistema SAP HANA é um exemplo em que um backup sob demanda antes da atualização e uma possível operação de restauração, caso a atualização falhe, têm um impacto significativo no tempo de inatividade planejado. Com o exemplo de um banco de dados de 4 TB, você pode reduzir o tempo de inatividade planejado em 8 horas, ou seja, terá mais 8 horas para analisar e corrigir erros usando as operações de backup e restauração baseadas em snapshots.

Outro caso de uso seria um ciclo de teste típico, onde os testes devem ser realizados em múltiplas iterações com diferentes conjuntos de dados ou parâmetros. Ao aproveitar as operações rápidas de backup e restauração, você pode facilmente criar pontos de salvamento dentro do seu ciclo de teste e redefinir o sistema para qualquer um desses pontos de salvamento anteriores caso um teste falhe ou precise ser repetido. Isso permite que os testes terminem mais cedo ou que mais testes sejam realizados simultaneamente, melhorando os resultados.

[largura=618, altura=279]

Após a implementação dos backups de snapshot, eles podem ser usados para atender a diversos outros casos de uso que exigem cópias de um banco de dados HANA. Você pode criar um novo volume com base no conteúdo de qualquer backup de Snapshot disponível. O tempo de execução desta operação é de alguns segundos, independentemente do tamanho do volume.

O caso de uso mais comum é a atualização do sistema SAP, onde os dados do sistema de produção precisam ser copiados para o sistema de teste ou de controle de qualidade. Ao aproveitar o recurso de clonagem do ONTAP ou ANF, você pode provisionar o volume para o sistema de teste a partir de qualquer cópia Snapshot do sistema de produção em questão de segundos. O novo volume deve então ser anexado ao sistema de teste e o banco de dados HANA deve ser recuperado.

O segundo caso de uso é a criação de um sistema de reparo, utilizado para solucionar problemas de corrupção lógica no sistema de produção. Neste caso, um backup Snapshot mais antigo do sistema de produção é usado para iniciar um sistema de reparo, que é um clone idêntico do sistema de produção com os dados anteriores à ocorrência da corrupção. Em seguida, o sistema de reparo é usado para analisar o problema e exportar os dados necessários antes que sejam corrompidos.

O último caso de uso é a capacidade de executar um teste de failover de recuperação de desastres sem

interromper a replicação e, portanto, sem influenciar o RTO (Objetivo de Tempo de Recuperação) e o RPO (Objetivo de Ponto de Recuperação) da configuração de recuperação de desastres. Quando a replicação ONTAP SnapMirror ou a replicação entre regiões ANF é usada para replicar os dados para o site de recuperação de desastres, os backups de Snapshot de produção também ficam disponíveis no site de recuperação de desastres e podem ser usados para criar um novo volume para testes de recuperação de desastres.

[largura=627, altura=328]

Saiba mais sobre a arquitetura do SnapCenter.

Saiba mais sobre a arquitetura do SnapCenter para proteção de dados SAP HANA, incluindo o servidor SnapCenter, os componentes de plug-in e as plataformas de armazenamento compatíveis. O SnapCenter oferece gerenciamento centralizado de backup, restauração e clonagem para bancos de dados SAP HANA em sistemas ONTAP, Azure NetApp Files e FSx para ONTAP.

O SnapCenter é uma plataforma unificada para proteção de dados consistente com a aplicação. O SnapCenter oferece controle e supervisão centralizados, ao mesmo tempo que delega aos usuários a capacidade de gerenciar operações de backup, restauração e clonagem específicas de cada aplicativo. O NetApp SnapCenter é uma ferramenta única que pode ser usada por administradores de banco de dados e armazenamento para gerenciar operações de backup, restauração e clonagem para uma variedade de aplicativos e bancos de dados. O SnapCenter oferece suporte a sistemas de armazenamento NetApp ONTAP, bem como ao Azure NetApp Files e ao FSx para ONTAP. Você também pode usar o SnapCenter para replicar dados entre ambientes locais; entre ambientes locais e a nuvem; e entre nuvens privadas, híbridas ou públicas.

O SnapCenter inclui o servidor SnapCenter e os plug-ins do SnapCenter. Os plug-ins estão disponíveis para diversas aplicações e componentes de infraestrutura. O servidor SnapCenter pode ser executado tanto em Windows quanto em Linux.

[largura=601, altura=275]

Saiba mais sobre backup e recuperação do SnapCenter para SAP HANA.

O SnapCenter oferece recursos abrangentes de backup e recuperação para bancos de dados SAP HANA, utilizando cópias de snapshot baseadas em armazenamento, gerenciamento automatizado de retenção e integração com NetApp ONTAP, Azure NetApp Files e FSx para NetApp ONTAP. A solução oferece suporte a backups de banco de dados consistentes com o aplicativo, proteção de volumes não relacionados a dados, verificações de integridade de blocos e replicação para armazenamento secundário usando o SnapVault ou o backup ANF.

A solução de backup da SnapCenter para SAP HANA abrange as seguintes áreas:

- Operações de backup, agendamento e gerenciamento de retenção
- Backup de dados do SAP HANA com cópias Snapshot baseadas em storage
- Backup de volumes não relacionados a dados com cópias de snapshot baseadas em armazenamento (por

exemplo, /hana/shared)

- operações de verificação de integridade de blocos de banco de dados
 - usando um backup baseado em arquivos
 - usando a ferramenta SAP HANA hdbpersdiag
- Replicação de backup de snapshot para um local de backup secundário
 - usando SnapVault/ SnapMirror
 - usando o backup do Azure NetApp Files ANF
- Manutenção do catálogo de backup do SAP HANA
 - para backups de dados HANA (snapshot e baseado em arquivo)
 - para backups de logs do HANA
- Operações de restauração e recuperação
 - Restauração e recuperação automatizadas
 - operações de restauração de inquilino único

Os backups de dados do banco de dados são executados pelo SnapCenter em conjunto com o plug-in do SnapCenter para SAP HANA. O plug-in aciona um snapshot interno do banco de dados SAP HANA, de forma que os snapshots criados no sistema de armazenamento sejam baseados em uma imagem consistente do banco de dados SAP HANA para cada aplicação.

O SnapCenter permite a replicação de imagens de banco de dados consistentes para um local de backup secundário ou de recuperação de desastres usando o SnapVault ou o recurso SnapMirror. Normalmente, são definidas políticas de retenção diferentes para backups no armazenamento primário e no armazenamento secundário. O SnapCenter gerencia a retenção no armazenamento primário, e o ONTAP gerencia a retenção no armazenamento de backup secundário.

Para permitir um backup completo de todos os recursos relacionados ao SAP HANA, o SnapCenter também permite fazer backup de todos os volumes que não são de dados usando o plug-in SAP HANA com cópias Snapshot baseadas em storage. Você pode agendar volumes que não sejam de dados de forma independente do backup de dados do banco de dados para habilitar políticas individuais de retenção e proteção.

A SAP recomenda combinar backups de snapshots baseados em armazenamento com uma verificação semanal de consistência da camada de persistência. Você pode executar a verificação de consistência de blocos diretamente do SnapCenter, seja executando um backup baseado em arquivo ou utilizando a ferramenta SAP hdbpersdiag.

Com base nas políticas de retenção configuradas, o SnapCenter gerencia a manutenção dos backups de arquivos de dados no armazenamento primário, dos backups de arquivos de log e do catálogo de backups do SAP HANA.

O SnapCenter manipula a retenção no storage primário, enquanto o ONTAP gerencia a retenção de backup secundário.

A figura a seguir mostra uma visão geral das operações de gerenciamento de retenção e backup do SnapCenter.

Ao executar um backup Snapshot baseado em storage do banco de dados SAP HANA, o SnapCenter realiza as seguintes tarefas:

- Operação de backup:
 - Aciona um snapshot interno do banco de dados HANA para obter uma imagem consistente da aplicação na camada de persistência.
 - Cria um backup instantâneo baseado em armazenamento do volume de dados.
 - Fecha o snapshot interno do banco de dados HANA, confirmando ou abandonando a operação de backup. Esta etapa registra o backup no catálogo de backups do HANA.
- Gestão de retenção:
 - Exclui backups de snapshots de armazenamento com base no período de retenção definido.
 - Exclui snapshots na camada de armazenamento.
 - Exclui entradas do catálogo de backup do SAP HANA
 - Exclui todos os backups de log que sejam mais antigos que o backup de dados mais antigo. Os backups de log são excluídos do sistema de arquivos e do catálogo de backups do SAP HANA.

[largura=601, altura=285]

Se um backup secundário estiver configurado, seja com SnapVault/ SnapMirror ou com backup ANF, o Snapshot criado no volume primário será replicado para o armazenamento de backup secundário. O SnapCenter gerencia o catálogo de backups do HANA, bem como a retenção de backups de log, de acordo com a disponibilidade de backups secundários.

[largura=601, altura=278]

Saiba mais sobre as configurações compatíveis com o SnapCenter para SAP HANA.

O SnapCenter oferece suporte a uma ampla gama de arquiteturas de sistema SAP HANA e cenários de implantação em plataformas de armazenamento locais e em nuvem. Saiba mais sobre as configurações do SAP HANA suportadas, combinações de plataforma, protocolos de armazenamento e operações de backup e restauração disponíveis para cada ambiente.

Configurações SAP HANA suportadas

O SnapCenter é compatível com as seguintes configurações e recursos do HANA:

- Sistemas de host único SAP HANA
- Sistemas de múltiplos hosts SAP HANA
 - Requer uma implantação central de plug-in conforme descrito em ["Opções de implantação para o plug-in SnapCenter para SAP HANA"](#).
- Sistemas SAP HANA MDC
 - com um único inquilino ou com vários inquilinos
- Sistemas SAP HANA com múltiplas partições
- Replicação do sistema SAP HANA
- Criptografia SAP HANA (dados, logs, backups)

Configurações de plataforma e infraestrutura suportadas

O SnapCenter suporta as seguintes combinações de plataformas de host, sistemas de arquivos e plataformas de armazenamento.

Plataforma de hospedagem	Conexão de armazenamento e sistema de arquivos SAP HANA	Plataforma de armazenamento
VMware	Montagens NFS no sistema operacional convidado	ONTAP AFF
VMware	Armazenamento de dados FC com VMFS + VM com XFS com ou sem Linux LVM	ONTAP AFF ou ASA
KVM	Montagens NFS no sistema operacional convidado	ONTAP AFF
Servidor bare metal	Montagens NFS	ONTAP AFF
Servidor bare metal	FC SAN + e XFS com ou sem Linux LVM	ONTAP AFF ou ASA (*)
Máquina virtual do Azure	Montagens NFS	Azure NetApp Files
AWS EC2	Montagens NFS	FSx para ONTAP

(*): Suporte para ASA disponível a partir da versão 6.2 do SnapCenter



Os plug-ins HANA e Linux estão disponíveis apenas para a plataforma de CPU Intel. Para Linux em IBM Power, é necessário configurar uma implantação central de plug-in HANA, conforme descrito em ["Opções de implantação para o plug-in SnapCenter para SAP HANA"](#).

Funcionalidades e operações suportadas

Explicação da abreviação

- VBSR: SnapRestore baseado em volume + Um SnapRestore baseado em volume reverte o volume para o estado do Snapshot.
- SFSR: SnapRestore de Arquivo Único + A SnapRestore de Arquivo Único pode ser usada para restaurar arquivos ou LUNs específicos dentro de um volume.

Veja também ["Tipos de operações de restauração para bancos de dados SAP HANA descobertos automaticamente"](#)

ONTAP AFF e FSx para ONTAP



Apenas a coluna 1 (montagens NFS) da tabela abaixo é relevante para o FSx para ONTAP.

Operação	Montagens NFS em hardware dedicado ou em máquinas virtuais com VMware ou KVM.	FC SAN + Metal nu	Armazenamento de dados FC VMware VMFS
Operações de backup e restauração de snapshots para o banco de dados HANA			
Backup de instantâneo	Sim	Sim	Sim
Instantâneo à prova de adulteração	Sim	Sim	Sim
Restauração completa	VBSR ou SFSR (selecionável)	SFSR de LUN completo	Clonar, montar, copiar
Restauração de inquilino único	SFSR	Clonar, montar, copiar	Clonar, montar, copiar
* Operações de backup e restauração do SnapVault para banco de dados HANA*			
Replicação SnapVault	Sim	Sim	Sim
Instantâneo à prova de adulteração	Sim	Sim	Sim
Restauração completa	Sim	Sim	Clonar, montar, copiar
Restauração de inquilino único	Sim	Clonar, montar, copiar	Clonar, montar, copiar
Operação de recuperação do HANA a partir do destino Snapshot ou SnapVault primário			
Recuperação automatizada MDC para locatário único	Sim	Sim	Sim
Recuperação automatizada MDC para múltiplos locatários	Não	Não	Não
Fazer backup e restaurar volumes que não sejam de dados			
Backup de instantâneo	Sim	Sim	Sim (*)
Restaurar do Snapshot	VBSR ou SFSR (selecionável)	SFSR de LUN completo	VBSR (*)
Replicação SnapVault	Sim	Sim	Sim (*)
Restaurar a partir do destino SnapVault	Sim	Sim	Sim (*)
Atualização do Sistema SAP			
A partir do instantâneo primário	Sim	Sim (**)	Sim (**)
Do destino SnapVault	Sim	Sim (**)	Sim (**)
HA e DR			

Operação	Montagens NFS em hardware dedicado ou em máquinas virtuais com VMware ou KVM.	FC SAN + Metal nu	Armazenamento de dados FC VMware VMFS
Suporte a Snapshots e SnapVault do HSR	Sim	Sim	Sim
Atualizações de replicação do SnapMirror com SC	Sim	Sim	Sim
Sincronização ativa do SnapMirror	NA	Sim	Sim

(*): Sem integração com VMware - Snapshot de imagem de falha e restauração completa do volume

(**): Soluções alternativas necessárias para versões do SnapCenter anteriores à 6.2

ONTAP ASA

Operação	FC SAN + Bare metal (*)	Armazenamento de dados FC VMware VMFS
Operações de backup e restauração de snapshots para o banco de dados HANA		
Backup de instantâneo	Sim	Sim
Instantâneo à prova de adulteração	Não	Não
Restauração completa	SFSR de LUN completo	Clonar, montar, copiar
Restauração de inquilino único	Clonar, montar, copiar	Clonar, montar, copiar
* Operações de backup e restauração do SnapVault para banco de dados HANA*		
Replicação SnapVault	Sim	Sim
Instantâneo à prova de adulteração	Não	Não
Restauração completa	Sim	Clonar, montar, copiar
Restauração de inquilino único	Clonar, montar, copiar	Clonar, montar, copiar
Operação de recuperação do HANA a partir do destino Snapshot ou SnapVault primário		
Recuperação automatizada MDC para locatário único	Sim	Sim
Recuperação automatizada MDC para múltiplos locatários	Não	Não
Fazer backup e restaurar volumes que não sejam de dados		
Backup de instantâneo	Sim	Sim (*)
Restaurar do Snapshot	SFSR de LUN completo	SFSR de LUN completo (*)

Operação	FC SAN + Bare metal (*)	Armazenamento de dados FC VMware VMFS
Replicação SnapVault	Sim	Sim (*)
Restaurar a partir do destino SnapVault	Sim	Sim (*)
Atualização do Sistema SAP		
A partir do instantâneo primário	Sim	Sim (**)
Do destino SnapVault	Sim	Sim (**)
HA e DR		
Suporte a Snapshots e SnapVault do HSR	Sim	Sim
Atualizações de replicação do SnapMirror acionadas pelo SnapCenter	Sim	Sim
Sincronização ativa do SnapMirror	Sim	Sim

(*): Suporte a partir da versão 6.2 do SnapCenter

(**): Soluções alternativas necessárias para versões do SnapCenter anteriores à 6.2

Azure NetApp Files

Operação	Montagens NFS
Operações de backup e restauração de snapshots para o banco de dados HANA	
Backup de instantâneo	Sim
Instantâneo à prova de adulteração	Não
Restauração completa no local	Reversão de volume ou SFSR (selecionável)
Restauração de inquilino único	SFSR
Operações de backup e restauração ANF para banco de dados HANA	
Replicação de backup ANF	Sim
Instantâneo à prova de adulteração	Não
Restauração completa no local	Sim
Restauração de inquilino único	Sim
Operação de recuperação do HANA a partir do Snapshot primário ou do backup ANF	
Recuperação automatizada MDC para locatário único	Sim
Recuperação automatizada MDC para múltiplos locatários	Não
Fazer backup e restaurar volumes que não sejam de dados	
Backup de instantâneo	Sim

Operação	Montagens NFS
Restaurar do Snapshot	Reversão de volume
Replicação de backup ANF	Sim
Restauração completa no local a partir do backup ANF	Não (*)
Atualização do Sistema SAP	
A partir do instantâneo primário	Sim
Do backup ANF	Sim
HA e DR	
Suporte a snapshots HSR e backup ANF	Sim
Atualização de replicação entre regiões acionada pelo SnapCenter	Não

(*): Na versão atual, a operação de restauração deve ser feita usando o portal do Azure ou a CLI.

Saiba mais sobre os conceitos e as melhores práticas de proteção de dados do SnapCenter.

Saiba mais sobre as opções de implantação do SnapCenter , estratégias de proteção de dados e gerenciamento de retenção de backups para ambientes SAP HANA. O SnapCenter oferece suporte à implantação de plug-ins em hosts de banco de dados ou hosts centrais, descoberta automática e configuração manual, verificações de consistência de blocos usando backups baseados em arquivos ou hdbpersdiag e gerenciamento abrangente de retenção em armazenamento primário e secundário.

Opções de implantação para o plug-in SnapCenter para SAP HANA

A figura a seguir mostra a visão lógica da comunicação entre o servidor SnapCenter , o banco de dados SAP HANA e o sistema de armazenamento. O servidor SnapCenter utiliza o HANA e os plug-ins do Linux para se comunicar com o banco de dados HANA e os sistemas operacionais Linux.

[largura=601, altura=199]

A opção de implantação recomendada e padrão para os plug-ins do SnapCenter é a instalação no host do banco de dados HANA. Com essa opção de implantação, todas as configurações e recursos descritos no capítulo Configuração compatível com o SnapCenter são válidos. Existem algumas exceções em que os plug-ins do SnapCenter não podem ser instalados no host do banco de dados HANA, mas precisam ser configurados em um host central de plug-ins, que pode ser o próprio servidor SnapCenter . É necessário um host central de plug-in para sistemas HANA com múltiplos hosts ou sistemas HANA executados na plataforma IBM Power. Ambas as opções de implantação também podem ser combinadas, por exemplo, usando o servidor SnapCenter como um host central de plug-ins para um sistema com vários hosts e implantando os plug-ins nos hosts do banco de dados HANA para todos os outros sistemas HANA de host único.

No SnapCenter, um recurso HANA pode ser descoberto automaticamente ou configurado manualmente. Por padrão, um sistema HANA é descoberto automaticamente assim que os plug-ins HANA e Linux são implantados no host do banco de dados. A descoberta automática do SnapCenter não suporta várias instalações do HANA no mesmo host. Os sistemas HANA gerenciados por meio de um host plug-in central

devem ser configurados manualmente no SnapCenter. Além disso, os volumes que não contêm dados são, por padrão, recursos configurados manualmente.

	Plug-in implantado em	Recurso SnapCenter
Banco de dados HANA	Hospedagem do banco de dados	Autodescoberto
Banco de dados HANA	Host central de plug-ins	Configuração manual
Volume de dados não	N/A.	Configuração manual

Embora o SnapCenter ofereça suporte a uma implantação centralizada de plug-ins para sistemas HANA, existem limitações em termos de suporte a plataformas e recursos. As seguintes configurações e operações de infraestrutura não são suportadas para sistemas HANA configurados com um host plug-in central:

- VMware com datastores FC
- Sincronização ativa do SnapMirror
- O servidor SnapCenter oferece alta disponibilidade quando usado como um host central de plug-ins.
- Descoberta automática do sistema HANA
- Recuperação automatizada de banco de dados HANA
- Atualização automatizada do sistema SAP
- Restauração de inquilino único

Plug-in SnapCenter para HANA implantado no host do banco de dados SAP HANA

O servidor SnapCenter comunica-se com os bancos de dados HANA através do plug-in HANA. O plug-in HANA utiliza o software cliente hdbsql do HANA para executar comandos SQL nos bancos de dados HANA. O repositório de usuários hdb do HANA é usado para fornecer as credenciais do usuário, o nome do host e as informações da porta para acessar os bancos de dados HANA. O plug-in SnapCenter para Linux é usado para abranger quaisquer operações do sistema de arquivos do host, bem como a descoberta automática de recursos de armazenamento e do sistema de arquivos.

Quando o plug-in HANA é implantado no host do banco de dados HANA, o sistema HANA é descoberto automaticamente pelo SnapCenter e sinalizado como um recurso descoberto automaticamente no SnapCenter.

[largura=601, altura=304]

Alta disponibilidade do servidor SnapCenter

O SnapCenter pode ser configurado em uma configuração de alta disponibilidade (HA) de dois nós. Nessa configuração, um balanceador de carga (por exemplo, F5) é usado para acessar os hosts do SnapCenter. O repositório do SnapCenter (o banco de dados MySQL) é replicado pelo SnapCenter entre os dois hosts, de forma que os dados do SnapCenter estejam sempre sincronizados.

A alta disponibilidade (HA) do servidor SnapCenter não é suportada se o plug-in HANA estiver instalado no servidor SnapCenter. Mais detalhes sobre o SnapCenter HA podem ser encontrados em ["Configurar servidores SnapCenter para alta disponibilidade"](#).

[largura=601, altura=307]

Host central de plug-ins

Conforme discutido no capítulo anterior, um plug-in central é necessário para

- Sistemas de múltiplos hosts HANA
- Sistemas HANA executados em IBM Power

Com um host de plug-in central, o plug-in HANA e o cliente SAP HANA hdbsql devem ser instalados em um host fora dos hosts do banco de dados HANA. Esse host pode ser qualquer host Windows ou Linux, por exemplo, o servidor SnapCenter .



Ao executar o servidor SnapCenter no Windows, você pode usar o sistema Windows como host central de plug-ins. Ao executar o servidor SnapCenter no Linux, você deve usar um host diferente como host central de plug-ins.

Para um sistema HANA com múltiplos hosts, as chaves do repositório de usuários SAP HANA para todos os hosts de trabalho e de espera devem ser configuradas no host central do plug-in. O SnapCenter tenta se conectar ao banco de dados usando cada uma das chaves fornecidas e, portanto, pode operar independentemente de uma falha do banco de dados do sistema (servidor de nomes HANA) para um host diferente.

[largura=601, altura=314]

Para vários sistemas HANA de host único gerenciados por um host plug-in central, todas as chaves individuais do repositório de usuários SAP HANA dos sistemas HANA devem ser configuradas no host plug-in central.

[largura=601, altura=338]

verificação de consistência de bloco do SAP HANA

A SAP recomenda incluir verificações regulares de consistência de blocos do HANA na estratégia geral de backup. Com backups tradicionais baseados em arquivos, essa verificação é feita a cada operação de backup. Com backups de snapshot, a verificação de consistência deve ser executada além das operações de backup de snapshot, por exemplo, uma vez por semana.

Tecnicamente, existem duas opções para executar a verificação de consistência de bloco.

- Executando um backup padrão baseado em arquivos ou em backin.
- Executando a ferramenta HANA hdbpersdiag, veja também "[Verificação de consistência de persistência | Portal de Ajuda SAP](#)"

A ferramenta hdbpersdiag do HANA faz parte da instalação do HANA e permite executar operações de verificação de consistência de blocos em um banco de dados HANA offline. Portanto, é ideal para ser usado em conjunto com backups de Snapshot, onde os backups de Snapshot existentes podem ser apresentados ao hdbpersdiag.

Ao comparar as duas abordagens, o hdbpersdiag apresenta vantagens significativas em relação ao backup baseado em arquivos para verificações de consistência de blocos do HANA. Uma das dimensões é a capacidade de armazenamento necessária. Com backups baseados em arquivos, é necessário que haja espaço disponível pelo menos no tamanho de um backup para cada sistema HANA. Se você tiver, por exemplo, 15 sistemas HANA com um tamanho de persistência de 3 TB, precisará de mais 45 TB apenas para as verificações de consistência. Com o hdbpersdiag, não é necessária capacidade de armazenamento adicional, pois a operação é executada em um backup Snapshot existente ou em um FlexClone de um backup

Snapshot existente. A segunda dimensão é a carga da CPU no host HANA durante a operação de verificação de consistência. Um backup baseado em arquivos exigirá ciclos de CPU no host do banco de dados HANA, enquanto o processamento do hdbpersdiag pode ser totalmente descarregado do host HANA quando usado em combinação com um host de verificação central. A tabela abaixo resume as principais características.

	Capacidade de armazenamento necessária	Carga de CPU e de rede no host HANA
Backup baseado em arquivos	Tamanho mínimo de backup de dados de 1 unidade para cada sistema HANA.	Alto
hdbpersdiag usando diretório de Snapshot no host HANA (somente NFS)	Nenhum	Médio
Host de verificação central usado para executar o hdbpersdiag com volumes FlexClone.	Nenhum	Nenhum

A NetApp recomenda o uso do hdbpersdiag para executar verificações de consistência de blocos do HANA. Mais detalhes sobre a implementação estão disponíveis no capítulo ["Verificações de consistência de blocos com o SnapCenter"](#).

Estratégia de proteção de dados

Antes de configurar o SnapCenter e o plug-in SAP HANA, a estratégia de proteção de dados deve ser definida com base nos requisitos de rto e RPO dos vários sistemas SAP.

Uma abordagem comum é definir tipos de sistemas como produção, desenvolvimento, teste ou sistemas sandbox. Todos os sistemas SAP do mesmo tipo de sistema normalmente têm os mesmos parâmetros de proteção de dados.

Os parâmetros que devem ser definidos são:

- Com que frequência um backup Snapshot deve ser executado?
- Por quanto tempo os backups de cópias Snapshot devem ser mantidos no sistema de storage primário?
- Com que frequência deve ser executada uma verificação de integridade de bloco?
- Os backups primários devem ser replicados para um site de backup secundário?
- Por quanto tempo os backups devem ser mantidos no armazenamento de backup secundário?

A tabela a seguir mostra um exemplo de parâmetros de proteção de dados para os tipos de sistema produção, desenvolvimento e teste. Para o sistema de produção, foi definida uma alta frequência de backup, e os backups são replicados para um site de backup secundário uma vez por dia. Os sistemas de teste têm requisitos mais baixos e não realizam replicação dos backups.

Parâmetros	Sistemas de produção	Sistemas de desenvolvimento	Sistemas de teste
Frequência de backup	A cada 6 horas	A cada 6 horas	A cada 12 horas
Retenção primária	3 dias	3 dias	6 dias

Parâmetros	Sistemas de produção	Sistemas de desenvolvimento	Sistemas de teste
Verificação de integridade do bloco	Uma vez por semana	Uma vez por semana	Não
Replicação para site de backup secundário	Uma vez por dia	Uma vez por dia	Não
retenção de backup secundário	2 semanas	2 semanas	Não

A tabela a seguir mostra as políticas e os agendamentos que precisariam ser configurados para os parâmetros de proteção de dados acima.

Política	Tipo de cópia de segurança	Frequência de programação	Retenção primária	Replicação SnapVault	Retenção secundária
LocalSnap	Baseado em snapshot	A cada 6 horas	Contagem = 12	Não	NA
LocalSnapAndSnapVault	Baseado em snapshot	Uma vez por dia	Contagem = 2	Sim	Contagem = 14
SnapAndCallHdbpersdiag	Baseado em snapshot	Uma vez por semana	Contagem = 2	Não	NA



Para o sistema ONTAP ou FSx para ONTAP, uma relação de proteção de dados deve ser configurada no ONTAP para a replicação do SnapVault, antes que o SnapCenter possa executar operações de atualização do SnapVault. A retenção secundária é definida na política de proteção do ONTAP.



Para backup do ANF, nenhuma configuração adicional é necessária fora do SnapCenter. O backup secundário de retenção do ANF é gerenciado pelo SnapCenter.



Para esta configuração de exemplo, o hdbpersdiag é usado para a operação de verificação de integridade do bloco. Mais detalhes podem ser encontrados no capítulo ["Verificações de consistência de blocos com o SnapCenter"](#).

A figura abaixo resume os cronogramas e os períodos de retenção de backups. Se o SnapCenter for usado para gerenciar a retenção de backups de log, todos os backups de log mais antigos que o backup de Snapshot mais antigo serão excluídos. Em outras palavras, os backups de log são mantidos pelo tempo necessário para permitir a recuperação até o ponto atual, para cada backup disponível.

[largura=601, altura=192]

Cópia de segurança das chaves raiz de criptografia

Quando a criptografia de persistência do HANA é utilizada, é fundamental criar backups das chaves raiz, além dos backups de dados padrão. É necessário fazer backup da chave raiz para recuperar o banco de dados HANA caso o volume de dados e o sistema de arquivos de instalação do HANA sejam perdidos. Para obter mais informações, consulte ["Guia de administração do SAP HANA"](#).



Lembre-se de que, se uma chave raiz for alterada, a nova chave raiz não poderá ser usada para recuperar backups antigos do banco de dados HANA criados anteriormente. Você sempre precisa da chave raiz que estava ativa no momento da criação do backup.

Operações de backup

O SnapCenter oferece suporte a operações de backup de snapshots de sistemas HANA MDC com um único locatário ou com vários locatários. O SnapCenter também oferece suporte a duas operações de restauração diferentes de um sistema HANA MDC. Você pode restaurar o sistema completo, o banco de dados do sistema e todos os tenants, ou pode restaurar apenas um tenant. Existem alguns pré-requisitos para permitir que o SnapCenter execute essas operações.

Em um sistema MDC, a configuração do locatário não é necessariamente estática. É possível adicionar ou remover inquilinos. O SnapCenter não pode confiar na configuração descoberta quando o banco de dados HANA é adicionado ao SnapCenter. Para permitir uma operação de restauração de locatário único, o SnapCenter precisa saber quais locatários estão incluídos em cada backup de Snapshot. Além disso, precisa saber quais arquivos e diretórios pertencem a cada locatário incluído no backup do Snapshot.

Portanto, a cada operação de backup, o SnapCenter identifica as informações do locatário. Isso inclui os nomes dos inquilinos e as informações correspondentes de arquivos e diretórios. Esses dados devem ser armazenados nos metadados de backup do Snapshot para que seja possível realizar uma operação de restauração em um único locatário.

Outra etapa da descoberta automática de aplicativos é a detecção do nó primário ou secundário do HANA System Replication (HSR). Se um sistema HANA estiver configurado com HSR, o SnapCenter deve identificar o nó primário em cada operação de backup para que os comandos SQL de backup sejam executados no nó primário do HSR. Veja também ["Replicação do sistema SAP HANA: Backup e recuperação com o SnapCenter"](#).

O SnapCenter também detecta a configuração do volume de dados do HANA e a mapeia para o sistema de arquivos e recursos de armazenamento. Com essa abordagem, o SnapCenter consegue lidar com alterações na configuração de volumes do HANA, como múltiplas partições ou alterações na configuração de armazenamento, como migrações de volumes.

O próximo passo é a própria operação de backup do Snapshot. Esta etapa inclui o comando SQL para acionar o snapshot do banco de dados HANA, o backup do snapshot de armazenamento e o comando SQL para encerrar a operação de snapshot do HANA. Ao usar o comando close, o banco de dados HANA atualiza o catálogo de backup do banco de dados do sistema e de cada locatário.



O SAP não dá suporte às operações de backup Snapshot para sistemas MDC quando um ou mais locatários são interrompidos.

Para o gerenciamento da retenção de backups de dados e o gerenciamento do catálogo de backup HANA, a SnapCenter deve executar as operações de exclusão de catálogo para o banco de dados do sistema e todos os bancos de dados de locatários identificados na primeira etapa. Da mesma forma para os backups de log, o fluxo de trabalho do SnapCenter deve operar em cada locatário que fazia parte da operação de backup.

A figura a seguir mostra uma visão geral do fluxo de trabalho de backup.

[largura=601, altura=237]

Gerenciamento de retenção de backups

O gerenciamento de retenção de backup de dados e o gerenciamento de backup de log podem ser divididos em cinco áreas principais, incluindo o gerenciamento de retenção de:

- Backups locais no storage primário
- Backups baseados em arquivos
- Cópias de segurança no armazenamento secundário (SnapVault ou backup ANF)
- Backups de dados no catálogo de backup do SAP HANA
- Os backups de log são armazenados no catálogo de backups do SAP HANA e no sistema de arquivos.

A figura a seguir fornece uma visão geral dos diferentes fluxos de trabalho e das dependências de cada operação. As seções a seguir descrevem as diferentes operações em detalhes.

[largura=601, altura=309]

Gerenciamento de retenção de backups locais no storage primário

O SnapCenter gerencia os backups do banco de dados SAP HANA e os backups de volumes que não sejam de dados, excluindo as cópias de snapshots no armazenamento primário e no repositório do SnapCenter, de acordo com o período de retenção definido na política de backup do SnapCenter. O gerenciamento de retenção está incluído em cada fluxo de trabalho de backup no SnapCenter. Os backups locais no armazenamento primário também podem ser excluídos manualmente no SnapCenter.

Gerenciamento de retenção de backups baseados em arquivos

O SnapCenter gerencia a organização dos backups baseados em arquivos, excluindo-os do sistema de arquivos de acordo com o período de retenção definido na política de backup do SnapCenter. A lógica de gerenciamento de retenção é executada em cada fluxo de trabalho de backup no SnapCenter.

Gerenciamento de retenção de backups no armazenamento secundário (SnapVault)

O gerenciamento de retenção de backups no armazenamento secundário (SnapVault) é tratado pelo ONTAP com base na retenção definida na relação de proteção do ONTAP. Para sincronizar essas alterações no armazenamento secundário do repositório SnapCenter, o SnapCenter utiliza uma tarefa de limpeza agendada. Esta tarefa de limpeza sincroniza todos os backups de armazenamento secundário com o repositório do SnapCenter para todos os plug-ins e recursos do SnapCenter.

A tarefa de limpeza está agendada uma vez por semana por padrão. Essa programação semanal resulta em um atraso na exclusão de backups no SnapCenter e no SAP HANA Studio em comparação com os backups que já foram excluídos no armazenamento secundário. Para evitar essa inconsistência, os clientes podem alterar a programação para uma frequência maior, por exemplo, uma vez por dia. Para obter detalhes sobre como adaptar a programação da tarefa de limpeza ou como acionar uma atualização manual, consulte o capítulo. "[Limpeza de backups secundários](#)".

Gerenciamento de retenção de backups no armazenamento secundário (backup ANF)

A retenção dos backups do ANF é configurada e gerenciada pelo SnapCenter. O SnapCenter gerencia a organização dos backups do ANF, excluindo-os de acordo com o período de retenção definido na política de backup do SnapCenter. O gerenciamento de retenção está incluído em cada fluxo de trabalho de backup no SnapCenter.

Gerenciamento de retenção de backups de dados no catálogo de backup do SAP HANA

Quando o SnapCenter exclui qualquer backup, seja ele local (Snapshot) ou baseado em arquivo, ou se o SnapCenter identifica a exclusão de um backup no armazenamento secundário, esse backup de dados também é excluído do catálogo de backups do SAP HANA. Antes de excluir a entrada do catálogo SAP HANA para um backup Snapshot local no armazenamento primário, o SnapCenter verifica se o backup ainda existe no armazenamento secundário.

Gerenciamento de retenção de backups de log

O banco de dados SAP HANA cria backups de logs automaticamente. Essas operações criam arquivos de backup para cada serviço individual do SAP HANA em um diretório de backup configurado no SAP HANA. Os backups de logs mais antigos que o backup de dados mais recente não são mais necessários para recuperação futura e, portanto, podem ser excluídos. O SnapCenter gerencia a organização e a manutenção dos backups de arquivos de log no nível do sistema de arquivos, bem como no catálogo de backups do SAP HANA, executando as seguintes etapas:

1. O SnapCenter lê o catálogo de backups do SAP HANA para obter o ID do backup de dados mais antigo realizado com sucesso.
2. O SnapCenter exclui todos os backups de log no catálogo do SAP HANA e no sistema de arquivos mais antigos que esse ID de backup.



O SnapCenter apenas lida com o serviço de limpeza dos backups criados pelo SnapCenter. Se backups adicionais baseados em arquivos forem criados fora do SnapCenter, você deverá garantir que os backups baseados em arquivos sejam excluídos do catálogo de backup. Se esse backup de dados não for excluído manualmente do catálogo de backup, ele poderá se tornar o backup de dados mais antigo e backups de log mais antigos não serão excluídos até que esse backup baseado em arquivo seja excluído.



Embora a retenção esteja definida para backups sob demanda na configuração da política, a limpeza só é realizada quando outro backup sob demanda é executado. Portanto, os backups sob demanda normalmente precisam ser excluídos manualmente no SnapCenter para garantir que esses backups também sejam excluídos do catálogo de backups do SAP HANA e que a manutenção dos backups de log não seja baseada em um backup sob demanda antigo.



O gerenciamento de retenção de backups de logs está ativado por padrão. Caso necessário, pode ser desativado conforme descrito na seção Desativar a limpeza automática de backups de logs.

Saiba mais sobre como configurar o SnapCenter para ambientes SAP HANA.

Configure o SnapCenter para ambientes SAP HANA usando uma abordagem de duas fases: configuração inicial para recursos compartilhados (credenciais, sistemas de armazenamento e políticas) e configuração específica de recursos para sistemas HANA individuais (implantação de host, descoberta automática e configurações de proteção).

A configuração do SnapCenter para um ambiente SAP HANA com múltiplos sistemas HANA pode ser dividida em duas áreas principais:

- A configuração inicial
 - Configurações de credenciais, armazenamento e políticas. + Essas configurações ou recursos são normalmente consumidos por vários sistemas HANA.
- Configuração específica de recursos do HANA
 - A configuração de host, HANA e proteção de recursos deve ser feita individualmente para cada sistema HANA.

A figura abaixo ilustra os diferentes componentes de configuração e suas dependências.

Todas as etapas de configuração são descritas detalhadamente nos tópicos a seguir.



As descrições e capturas de tela neste documento são baseadas em sistemas HANA descobertos automaticamente SnapCenter . Etapas de configuração adicionais ou diferentes para recursos configurados manualmente com um host plug-in central são descritas em ["Configuração central do host do plug-in"](#).

[largura=601, altura=319]

Configure as definições iniciais do SnapCenter para SAP HANA.

Configure as definições iniciais do SnapCenter para ambientes SAP HANA, definindo as credenciais para entidades de serviço do Azure, adicionando sistemas de armazenamento e criando políticas para backups de snapshots, verificações de integridade de blocos e replicação secundária.

A configuração inicial do SnapCenter inclui os seguintes passos:

1. Configuração de credenciais
 - a. Para sistemas HANA configurados com o Azure NetApp Files (ANF), uma entidade de serviço deve ser preparada e, em seguida, configurada no SnapCenter.
 - b. As credenciais do host devem ser fornecidas para permitir a instalação automatizada do plug-in HANA nos hosts do banco de dados HANA.
2. Configuração do sistema de storage
 - a. Para sistemas HANA configurados com ANF, as contas NetApp necessárias podem ser selecionadas e adicionadas à configuração do SnapCenter .
 - b. Para sistemas de armazenamento ONTAP ou FSx para ONTAP , tanto as SVMs quanto o cluster de armazenamento completo podem ser adicionados ao SnapCenter.
3. Configuração de políticas
 - a. É possível configurar políticas para backups baseados em snapshots, bem como operações de verificação de integridade de blocos, tanto para ANF quanto para sistemas de armazenamento ONTAP e FSx para ONTAP .
 - b. As políticas para snapshots à prova de adulteração e backups secundários com SnapVault ou SnapMirror só podem ser configuradas para sistemas de armazenamento ONTAP e FSx para ONTAP .
 - c. Para sistemas HANA configurados com ANF, uma política pode incluir ["Backup ANF"](#).



As mesmas políticas de backup de Snapshot podem ser usadas tanto para bancos de dados HANA quanto para volumes que não contêm dados, como o volume compartilhado do HANA.

A figura abaixo resume as seções de configuração.

[largura=601, altura=158]

Os capítulos seguintes descrevem os passos iniciais de configuração.

Configuração de credenciais

Credenciais para implantação do plug-in HANA

As credenciais são configuradas na seção Configurações, selecionando a guia Credenciais. É possível adicionar credenciais clicando no ícone +.

[largura=601, altura=118]

A NetApp recomenda configurar um usuário em todos os hosts do banco de dados HANA (por exemplo, scuser) e configurar os privilégios sudo conforme descrito em ["Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para banco de dados SAP HANA"](#).

[largura=287, altura=247]

Credenciais para o Azure NetApp Files

É necessário configurar uma entidade de serviço do Azure para permitir que o SnapCenter execute as operações necessárias para os volumes do Azure Networking. O exemplo abaixo mostra as permissões mínimas necessárias, que devem ser incluídas.

```
"assignableScopes": [
  "/subscriptions/xxx"
],
"createdBy": "xxx",
"createdOn": "2025-05-07T07:12:14.451483+00:00",
"description": "Restricted Access for SnapCenter ",
"id":
"/subscriptions/xxx/providers/Microsoft.Authorization/roleDefinitions/xxx"
,
"name": "xxx",
"permissions": [
  {
    "actions": [
      "Microsoft.NetApp/register/action",
      "Microsoft.NetApp/unregister/action",
      "Microsoft.NetApp/netAppAccounts/read",
      "Microsoft.NetApp/netAppAccounts/getKeyVaultStatus/action",
      "Microsoft.NetApp/netAppAccounts/migrateEncryption/action",
      "Microsoft.NetApp/netAppAccounts/transitionToCmk/action",
      "Microsoft.NetApp/netAppAccounts/capacityPools/read",
```



```
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/revert/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/poolChange/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/finalizeRelocation/
action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/revertRelocation/ac
tion",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/breakFileLocks/acti
on",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/getGroupIdListForLd
apUser/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/backups/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/backups/restoreFile
s/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/restoreFi
les/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/getMetad
ata/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/volumeQuotaRules/re
ad",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/latestRestoreStatus
```

```

/current/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/mountTargets/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/restoreStatus/read"
,
    "Microsoft.NetApp/netAppAccounts/snapshotPolicies/read",
    "Microsoft.NetApp/netAppAccounts/snapshotPolicies/write",

"Microsoft.NetApp/netAppAccounts/snapshotPolicies/listVolumes/read",

"Microsoft.NetApp/netAppAccounts/snapshotPolicies/volumes/read",
    "Microsoft.NetApp/netAppAccounts/volumeGroups/read",
    "Microsoft.NetApp/netAppAccounts/volumeGroups/write",
    "Microsoft.NetApp/locations/checknameavailability/action",
    "Microsoft.NetApp/locations/checkfilepathavailability/action",
    "Microsoft.NetApp/locations/operationresults/read",
    "Microsoft.NetApp/Operations/read",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/write",
    "Microsoft.Network/virtualNetworks/subnets/write",
    "Microsoft.NetApp/netAppAccounts/backupVaults/read",
    "Microsoft.NetApp/netAppAccounts/backupVaults/write",
    "Microsoft.NetApp/netAppAccounts/backupVaults/backups/read",
    "Microsoft.NetApp/netAppAccounts/backupVaults/backups/write",
    "Microsoft.NetApp/netAppAccounts/backupVaults/backups/delete",

"Microsoft.NetApp/netAppAccounts/backupVaults/backups/restoreFiles/action"
    ],
    "condition": null,
    "conditionVersion": null,
    "dataActions": [],
    "notActions": [],
    "notDataActions": []
}
],
"roleName": "SnapCenter-Restricted-Access",
"roleType": "CustomRole",
"type": "Microsoft.Authorization/roleDefinitions",
"updatedBy": "xxx",
"updatedOn": "2025-05-07T07:12:14.451483+00:00"

```

```
}
```

As credenciais são configuradas na seção Configurações, selecionando a guia Credenciais. As credenciais são configuradas clicando no ícone +.

[largura=601, altura=116]

Na tela seguinte, deve ser fornecido um nome de credencial e o Modo de Autenticação "Credenciais do Azure" deve ser selecionado. Em seguida, é necessário configurar o ID do locatário, o ID do cliente e a chave secreta do cliente.

[largura=252, altura=246]

Configuração do sistema de storage

Sistemas ONTAP e FSx para ONTAP

O sistema ONTAP ou o FSx para ONTAP podem ser adicionados ao SnapCenter fornecendo credenciais de cluster ou credenciais para cada SVM necessária. Quando as credenciais do cluster são fornecidas, todas as SVMs do cluster são adicionadas ao SnapCenter.

Em nossa configuração de laboratório, adicionamos os clusters de armazenamento ao SnapCenter. Os clusters ONTAP são configurados na seção Sistemas de armazenamento, selecionando a guia Armazenamento ONTAP e o tipo de cluster ONTAP . Um novo cluster é adicionado clicando no ícone +.

[largura=601, altura=117]

Na tela seguinte, você precisa fornecer as credenciais de um usuário do cluster.



O usuário administrador do cluster não deve ser utilizado. Em vez disso, um novo usuário deve ser criado com os privilégios necessários, conforme descrito em "[Crie funções de cluster ONTAP com privilégios mínimos](#)". Os privilégios necessários para o sistema ASA podem ser encontrados em "[Criar funções de cluster ONTAP para sistemas ASA r2](#)".

[largura=299, altura=176]

Os SVMs são configurados na seção Sistemas de armazenamento, selecionando a guia Armazenamento ONTAP e o tipo ONTAP SVMS. Um novo SVM é adicionado clicando no ícone +.

Na tela seguinte, você precisa fornecer as credenciais de um usuário do cluster.



O usuário SVM vsadmin não deve ser usado. Em vez disso, um novo usuário deve ser criado com os privilégios necessários, conforme descrito em "[Crie funções SVM com privilégios mínimos](#)". Os privilégios necessários para o sistema ASA podem ser encontrados em "[Criar funções SVM para sistemas ASA r2](#)".



O nome DNS da SVM deve corresponder ao nome da SVM configurado no sistema ONTAP .

[largura=331, altura=199]

Azure NetApp Files

Após a configuração das credenciais ANF, as contas NetApp ANF podem ser adicionadas ao SnapCenter. As contas NetApp são configuradas na seção Sistemas de armazenamento, selecionando a guia Azure NetApp Files . Uma nova conta NetApp é adicionada clicando no ícone +.

[largura=601, altura=117]

Após selecionar a credencial ANF e a assinatura, uma conta NetApp pode ser adicionada ao SnapCenter.

[largura=401, altura=176]

Configuração de armazenamento ao usar o SnapMirror ActiveSync.

As etapas específicas de configuração de armazenamento são descritas em "[Configuração de armazenamento com sincronização ativa SnapMirror](#)".

Configuração de políticas

Conforme discutido na seção Políticas de estratégia de proteção de dados, elas geralmente são configuradas independentemente do recurso e podem ser usadas para vários sistemas SAP HANA.

Uma configuração mínima típica consiste nas seguintes políticas:

- Política para backups horários sem replicação
- Política para backups diários com replicação de backup SnapVault ou ANF
- Política para operação de verificação semanal da integridade do bloco
 - usando um backup baseado em arquivos
 - usando a ferramenta HANA hdbpersdiag

As seções a seguir descrevem a configuração dessas três políticas.

As políticas são configuradas na seção Configurações, selecionando a guia Políticas. Uma nova política é configurada clicando no ícone +. As duas capturas de tela abaixo mostram a lista de políticas para sistemas HANA executados com o Azure NetApp Files e uma segunda lista para sistemas HANA executados com sistemas de armazenamento ONTAP ou FSx para ONTAP.

[largura=601, altura=133]

[largura=601, altura=138]

Backups de snapshots com sistemas ONTAP e FSx para ONTAP

As políticas de backup de snapshots para o sistema ONTAP ou FSx para ONTAP podem combinar um snapshot local com operações de replicação ou bloqueio de snapshot (snapshot à prova de adulteração). Este exemplo mostra uma política com replicação para um armazenamento secundário usando o SnapVault.

Forneça um nome para a política e uma descrição opcional.

[largura=376, altura=103]

Selecione o tipo de armazenamento ONTAP e o escopo da política de snapshot.

[largura=385, altura=97]

Para esta política, foi configurado um tipo de agendamento diário. Um Snapshot diário será criado e as diferenças entre os Snapshots serão replicadas para o armazenamento secundário usando o SnapVault.



O próprio agendamento é configurado com a configuração individual de proteção de recursos do HANA.

O período de retenção configurado na política é válido apenas para os Snapshots primários. A retenção no destino SnapVault é configurada com o relacionamento de replicação ONTAP para o(s) volume(s) individual(is) do banco de dados HANA, conforme descrito no capítulo "[Operações de backup de snapshots do SAP HANA](#)". O rótulo do Snapshot configurado na política deve corresponder ao rótulo configurado na relação de replicação do ONTAP .

O bloqueio de instantâneos (instantâneos à prova de adulteração) pode ser ativado clicando nas caixas de seleção e definindo o período de bloqueio. Essa funcionalidade requer uma licença SnapLock no sistema de armazenamento e que o relógio de conformidade esteja configurado.

Uma política que permita apenas snapshots locais seria configurada com um agendamento por hora e desativando a caixa de seleção "Atualizar SnapVault" .

[largura=378, altura=352]

A tela de resumo exibe os parâmetros configurados.

[largura=385, altura=119]

Backups de instantâneos com o Azure NetApp Files

As políticas de backup de snapshots para o Azure NetApp Files podem combinar um snapshot local com um backup do ANF, que replica os dados do snapshot para o blob do Azure. Este exemplo mostra uma política usada para replicação com backup ANF.

Forneça um nome para a política e uma descrição opcional.

[largura=356, altura=95]

Selecione o tipo de armazenamento Azure NetApp Files e o escopo da política de instantâneo.

[largura=360, altura=102]

Para esta política, foi configurado um tipo de agendamento diário. Um Snapshot diário será criado e as diferenças entre os Snapshots serão replicadas para o cofre de backup usando o backup ANF.



O próprio agendamento é configurado com a configuração individual de proteção de recursos do HANA.

A retenção de snapshots configurada na política é válida para os snapshots primários no volume ANF. O período de retenção do backup do ANF é configurado de acordo com as definições de retenção de backup.

Uma política que permita apenas snapshots locais seria configurada com um agendamento por hora e desativando a caixa de seleção "Ativar backup".

[largura=373, altura=361]

A tela de resumo exibe os parâmetros configurados.

[largura=376, altura=138]

Operações de verificação de integridade de blocos para todas as plataformas

Ferramenta HANA hdbpersdiag

Os detalhes são descritos no capítulo. ["Verificações de consistência de blocos com o SnapCenter"](#).

Backup baseado em arquivos

Forneça um nome para a política e uma descrição opcional.

[largura=346, altura=95]

Selecione o tipo de armazenamento ONTAP ou Azure NetApp Files , dependendo da sua configuração, e selecione o escopo da política baseado em arquivo.

[largura=357, altura=98]

Conforme discutido, recomenda-se executar a verificação de integridade do bloco uma vez por semana. Portanto, foi selecionado um cronograma semanal.



O próprio agendamento é configurado com a configuração individual de proteção de recursos do HANA.



O sistema de arquivos onde o backup baseado em arquivos é gravado deve fornecer capacidade suficiente para um backup a mais do que o definido nas configurações de retenção, pois o SnapCenter exclui o backup antigo após a criação do novo. Neste exemplo, é necessário espaço para dois backups, com retenção de apenas um. A retenção mínima configurável é zero.

[largura=351, altura=173]

A tela de resumo exibe os parâmetros configurados.

[largura=366, altura=101]

Configuração de políticas ao usar o SnapMirror ActiveSync.

As etapas específicas de configuração da política são descritas no documento. ["Configuração de política SnapMirror ActiveSync"](#).

Configure os recursos do SnapCenter para bancos de dados SAP HANA individuais.

Configure bancos de dados SAP HANA individuais no SnapCenter criando usuários de backup e chaves de armazenamento de usuários, configurando a replicação de armazenamento para backups secundários, implantando o plug-in HANA para descoberta automática e configurando a proteção de recursos com políticas e agendamentos.

A configuração de um banco de dados HANA no SnapCenter é feita seguindo os passos abaixo:

1. Um usuário de backup do SnapCenter deve ser configurado no banco de dados do sistema HANA e uma chave de armazenamento de usuários do SAP HANA deve ser configurada no host do banco de dados HANA.
2. Caso seja necessária a replicação de dados para um armazenamento secundário, a replicação de armazenamento ONTAP para o volume de dados HANA deve ser configurada.
3. O plug-in SnapCenter HANA deve ser implantado no host do banco de dados HANA.
 - a. O processo de descoberta automática é iniciado.
 - b. A chave do repositório de usuários do SAP HANA deve ser configurada no SnapCenter.
 - c. A segunda fase da descoberta automática é iniciada e o recurso HANA é adicionado automaticamente pelo SnapCenter.
4. A proteção de recursos do HANA deve ser configurada para o novo recurso do HANA adicionado.

A configuração inicial do SnapCenter , conforme descrito no tópico anterior. "[Configuração inicial do SnapCenter](#)" Isso deve ser feito primeiro, pois credenciais, sistemas de armazenamento e políticas são necessários durante a configuração de recursos do banco de dados HANA. A figura abaixo resume as etapas e dependências.

A figura abaixo visualiza os diferentes componentes de configuração e suas dependências.

[largura=601, altura=315] As seções a seguir fornecem uma descrição detalhada das etapas de configuração necessárias.

Configuração do usuário de backup do SAP HANA e do repositório de usuários do SAP HANA

A NetApp recomenda configurar um usuário dedicado no banco de dados HANA para executar as operações de backup com o SnapCenter. Como segundo passo, uma chave de armazenamento de usuários do SAP HANA é configurada para este usuário de backup, e a chave de armazenamento de usuários do SAP HANA é fornecida na configuração do SnapCenter .

A figura a seguir mostra o SAP HANA Studio por meio do qual o usuário de backup, neste exemplo SNAPCENTER, pode ser criado.



O usuário de backup precisa ser configurado com os privilégios de administrador de backup, leitura de catálogo, administrador de backup de banco de dados e operador de recuperação de banco de dados.



O usuário de backup deve ser criado no banco de dados do sistema, pois todos os comandos de backup para o sistema e para os bancos de dados dos tenants são executados por meio do banco de dados do sistema.

[largura=601, altura=382]

Configuração do repositório de usuários do SAP HANA no host do banco de dados HANA

O SnapCenter usa o usuário <sid>adm para se comunicar com o banco de dados HANA. Portanto, a chave do repositório de usuários do SAP HANA deve ser configurada usando o usuário <sid>adm no host do banco de dados.

hdbuserstore set <nome-da-chave> <host>:<porta> <usuário-do-banco-de-dados> <senha>

Para um sistema SAP HANA MDC, a porta do banco de dados do sistema HANA é 3<instanceNo>13.

Exemplos de configuração do repositório de usuários do SAP HANA

A saída mostra a chave SS1KEY que foi configurada para o sistema HANA com número de instância = 00.

```
ssladm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY
KEY SS1SAPDBCTRL
ENV : hana-1:30013
USER: SAPDBCTRL
KEY SS1KEY
ENV : hana-1:30013
USER: SNAPCENTER
KEY SYSTEMKEY
ENV : hana-1:30013
USER: SYSTEM
ACTIVE RECORDS : 10
DELETED RECORDS : 15
NUMBER OF COMPLETE KEY: 3
Operation succeed.
ssladm@hana-1:/usr/sap/SS1/HDB00>
```

A saída mostra a chave SM1KEY que foi configurada para o sistema HANA com número de instância = 12.

```
smladm@hana-2:/usr/sap/SM1/HDB12> hdbuserstore list
DATA FILE : /usr/sap/SM1/home/.hdb/hana-2/SSFS_HDB.DAT
KEY FILE : /usr/sap/SM1/home/.hdb/hana-2/SSFS_HDB.KEY
KEY SM1SAPDBCTRL
ENV : hana-2:31213
USER: SAPDBCTRL
KEY SM1KEY
ENV : hana-2:31213
USER: SNAPCENTER
ACTIVE RECORDS : 7
DELETED RECORDS : 9
NUMBER OF COMPLETE KEY: 2
Operation succeed.
smladm@hana-2:/usr/sap/SM1/HDB12>
```


Configuração de replicação de armazenamento

A configuração da relação de proteção de dados, bem como a transferência inicial de dados, devem ser executadas antes que as atualizações de replicação possam ser gerenciadas pelo SnapCenter.

As capturas de tela a seguir mostram uma configuração usando o gerenciador de sistema ONTAP . Para sistemas FSx para ONTAP , a replicação deve ser feita usando a CLI do ONTAP , conforme descrito em ["Visão geral - Backup de replicação com o SnapVault"](#).

A figura a seguir mostra a relação de proteção configurada para o volume de dados SS1 do sistema SAP HANA. Neste exemplo, o volume de origem SS1_data_mnt00001 no SVM hana-primary é replicado para o SVM hana-backup e para o volume de destino SS1_data_mnt00001_dst.

[largura=601, altura=183]

A figura a seguir mostra a política de proteção criada para esta configuração de laboratório. A política de proteção utilizada para a relação de proteção define o rótulo do SnapMirror , bem como a retenção de backups no armazenamento secundário. Neste exemplo, o rótulo utilizado é Diário e o período de retenção está definido como 5.



O rótulo SnapMirror na política de replicação deve corresponder ao rótulo definido na configuração da política do SnapCenter .



O agendamento do relacionamento deve ser definido como Nenhum, porque o SnapCenter aciona a atualização do SnapVault como parte da operação de backup com base no Snapshot consistente do aplicativo criado anteriormente.



O período de retenção dos backups no armazenamento secundário é definido na política e controlado pelo ONTAP.

[largura=601, altura=180]

Configuração de backup ANF

Para backup ANF, nenhuma preparação específica é necessária. Assim que o primeiro backup com o recurso de backup ANF ativado for executado, um cofre de backup do Azure com o nome snapcenter-vault será criado pelo SnapCenter. Este cofre de backup é então utilizado por todas as operações de backup ANF subsequentes executadas pelo SnapCenter.

[largura=601, altura=227]

Implantação do plug-in SnapCenter para SAP HANA

Os requisitos do host estão listados em ["Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux"](#).

A implantação do plug-in HANA é feita clicando no botão Adicionar na seção Hosts da interface do usuário do SnapCenter .

[largura=601, altura=145]

Na tela Adicionar host, você precisa fornecer o tipo e o nome do host, bem como as credenciais a serem usadas no processo de implantação. Além disso, o plug-in SAP HANA deve ser selecionado. Ao clicar em

enviar, o processo de implantação é iniciado.



Para esta descrição, não adicionamos um novo host, mas mostramos a configuração dos hosts existentes no SnapCenter.

[largura=601, altura=154]

Descoberta automática do HANA

Assim que a implantação do plug-in HANA for concluída, o processo de descoberta automática será iniciado. Na primeira fase, apenas as configurações básicas são detectadas e o SnapCenter cria um novo recurso que é listado na seção Recursos da interface do usuário, marcado com um cadeado vermelho.

[largura=601, altura=169]

Ao clicar no recurso, você será solicitado a inserir a chave do repositório de usuários SAP HANA para este banco de dados HANA.

[largura=316, altura=180]

Após o fornecimento da chave, a segunda fase do processo de descoberta automática é iniciada. O processo de descoberta automática detecta todos os bancos de dados de locatários no sistema HANA, detalhes de configuração de backup de logs e catálogos e funções de replicação do sistema HANA. Além disso, os detalhes da área de armazenamento são descobertos automaticamente. Essas configurações podem ser verificadas selecionando um recurso e clicando no botão Detalhes.



Esse processo de descoberta automática é executado a cada operação de backup, de forma que quaisquer alterações feitas no sistema HANA, relevantes para a operação de backup, sejam detectadas automaticamente.

[largura=601, altura=219]

Configuração de proteção de recursos

A tela de configuração de proteção de recursos é aberta clicando em um recurso após a conclusão do processo de descoberta automática. As capturas de tela nesta documentação mostram a configuração de proteção de um recurso existente.

Configure um formato de nome personalizado para o Snapshot. A NetApp recomenda o uso de um nome de snapshot personalizado para identificar facilmente quais backups foram criados com qual política e tipo de agendamento.

Na configuração mostrada na figura a seguir, os nomes de cópia de backup e cópia Snapshot têm o seguinte formato:

- Backup agendado a cada hora: + SnapCenter_<nome-do-host>_LocalSnap_Hourly_<carimbo_de_data/hora>
- Backup diário agendado: + SnapCenter_<nome-do-host>_LocalSnapAndSnapVault_Daily_<carimbo_de_data/hora>

[largura=601, altura=294]

Na tela seguinte, é possível configurar scripts que devem ser executados em várias etapas do fluxo de

trabalho de backup.

[largura=601, altura=294]

Agora, as políticas estão associadas ao recurso e os cronogramas estão definidos.

Neste exemplo, configuramos

- Verificação semanal da integridade do bloco, todos os domingos.
- Um backup local do tipo Snapshot, a cada 4 horas.
- Um backup diário de Snapshot com replicação do SnapVault uma vez por dia.

[largura=601, altura=294]

É possível configurar o envio de notificações por e-mail.

[largura=601, altura=294]

Após a configuração da proteção de recursos, os backups agendados serão executados de acordo com as configurações definidas.

Configure o SnapCenter para fazer backup de volumes que não contenham dados.

Configure o SnapCenter para fazer backup de volumes que não contenham dados, como executáveis, arquivos de configuração, arquivos de rastreamento e dados do servidor de aplicativos.

Proteger o volume de dados do banco de dados é suficiente para restaurar e recuperar o banco de dados SAP HANA para um determinado ponto no tempo, desde que os recursos de instalação do banco de dados e os logs necessários ainda estejam disponíveis.

Para se recuperar de situações em que outros arquivos não relacionados a dados precisam ser restaurados, a NetApp recomenda o desenvolvimento de uma estratégia de backup adicional para volumes não relacionados a dados, a fim de complementar o backup do banco de dados SAP HANA. Dependendo das suas necessidades específicas, o backup de volumes que não contêm dados pode variar em termos de frequência de agendamento e configurações de retenção, e você deve considerar com que frequência os arquivos que não contêm dados são alterados. Por exemplo, o volume HANA /hana/shared contém executáveis, arquivos de configuração, mas também arquivos de rastreamento do SAP HANA. Embora os arquivos executáveis só mudem quando o banco de dados SAP HANA é atualizado, os arquivos de configuração e rastreamento do SAP HANA podem precisar de backups com maior frequência. Além disso, os volumes do servidor de aplicativos SAP podem ser protegidos com o SnapCenter usando backups de volumes que não sejam de dados.

O backup de volumes não relacionados a dados do SnapCenter permite a criação de cópias instantâneas de todos os volumes relevantes em poucos segundos, com a mesma eficiência de espaço dos backups de banco de dados SAP HANA. A diferença é que não há necessidade de interação com o banco de dados SAP HANA.

Na guia recurso, selecione não volume de dados e clique em Adicionar banco de dados SAP HANA.

[largura=601, altura=173]

[largura=601, altura=112]

Na etapa um da caixa de diálogo Adicionar banco de dados SAP HANA, na lista tipo de recurso, selecione volumes não-dados. Especifique um nome para o recurso e o SID associado e o host de plug-in SAP HANA que você deseja usar para o recurso e clique em Avançar.

[largura=332, altura=310]

Para sistemas ONTAP e FSx para ONTAP, selecione o tipo de armazenamento ONTAP e adicione a(s) SVM(s) e o(s) volume(s) de armazenamento como área de armazenamento, depois clique em Avançar.

[largura=332, altura=312]

Para o ANF, selecione o tipo de armazenamento Azure NetApp Files, selecione a conta NetApp e o pool de capacidade e adicione o(s) volume(s) do ANF como espaço de armazenamento e clique em Avançar.

[largura=350, altura=337]

Na etapa de resumo, clique em concluir para salvar as configurações.

Repita esses passos para todos os volumes que não sejam de dados. Prossiga com a configuração de proteção do novo recurso.



A configuração de proteção de dados para recursos que não sejam volumes de dados é idêntica ao fluxo de trabalho para recursos de banco de dados SAP HANA e pode ser definida em nível de recurso individual.

Configure o host do plug-in central do SnapCenter para SAP HANA.

Implante o plug-in SnapCenter HANA em um host central para oferecer suporte a sistemas SAP HANA com vários hosts ou sistemas HANA em IBM Power. Este procedimento inclui a instalação do plug-in em um host Windows ou Linux, a configuração do cliente SAP HANA hdbsql e a configuração das chaves de armazenamento de usuário para cada sistema HANA protegido.

Conforme discutido em ["Opções de implantação para o plug-in SnapCenter para SAP HANA"](#) O plug-in HANA pode ser implementado fora do banco de dados HANA para oferecer suporte a uma configuração centralizada de plug-in, necessária em ambientes SAP HANA com múltiplos hosts ou SAP HANA em IBM Power.

O host central do plug-in pode ser qualquer host Windows ou Linux, mas normalmente o próprio servidor SnapCenter é usado como host central do plug-in.

A configuração de um host central de plug-in consiste nas seguintes etapas:

- Implantação do plug-in SnapCenter HANA
- Instalação e configuração do cliente hdbsql do SAP HANA
- Configuração do repositório de usuários do SAP HANA para cada sistema HANA, protegida pelo host central do plug-in.

Implantação do plug-in SnapCenter HANA

Os requisitos do host estão listados em ["Requisitos de host para instalar o pacote de plug-ins SnapCenter"](#)

para Linux".

O host central do plug-in é adicionado como um host e o plug-in SAP HANA é instalado nesse host. A captura de tela abaixo mostra a implantação do plug-in em um servidor SnapCenter executado no Windows.

1. Vá para hosts e clique em Adicionar.
2. Forneça as informações necessárias do host. Clique em Enviar.

[largura=601, altura=166]

Instalação e configuração do software cliente SAP HANA hdbsql

O software cliente SAP HANA hdbsql deve ser instalado no mesmo host em que o plug-in SAP HANA está instalado. O software pode ser baixado do ["Portal de suporte SAP"](#).

O usuário do sistema operacional hdbsql configurado durante a configuração do recurso HANA deve ter permissão para executar o executável hdbsql. O caminho para o executável hdbsql deve ser configurado no arquivo hana.properties ou nos parâmetros de caminho de pesquisa (%PATH%, \$PATH) do usuário do sistema operacional.

Host central de plug-ins no Windows:

```
C:\More C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in  
Creator\etc\hana.properties  
  
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql.exe
```

Host central de plug-ins no Linux:

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties  
  
HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

Configuração do repositório de usuários do SAP HANA para um host de plug-in central.

Para cada sistema HANA gerenciado pelo host central do plug-in, uma chave de armazenamento de usuário SAP HANA deve ser configurada. Antes que a chave possa ser configurada no host central do plug-in, um usuário de banco de dados deve ser criado conforme descrito em ["Configuração do usuário de backup do SAP HANA e do repositório de usuários do SAP HANA"](#).

Se o plug-in SAP HANA e o cliente SAP hdbsql estiverem instalados no Windows, o usuário do sistema local executará os comandos hdbsql e estará configurado por padrão na configuração de recursos. Como o usuário do sistema não é um usuário de login, a configuração do armazenamento de usuários do SAP HANA deve ser feita com um usuário diferente usando a opção -u <Usuário>.

```
hdbuserstore.exe -u SYSTEM set <key> <host>:<port> <database user>  
<password>
```

Para uma configuração SAP HANA com vários hosts, as chaves do repositório de usuários SAP HANA para todos os hosts devem ser configuradas. O SnapCenter tenta se conectar ao banco de dados usando cada uma das chaves fornecidas e, portanto, pode operar independentemente de uma falha do banco de dados do sistema (servidor de nomes HANA) para um host diferente. Uma chave de armazenamento de usuário SAP HANA é configurada para todos os hosts de trabalho e para o host de espera. O usuário do banco de dados HANA, neste exemplo, SNAPCENTER, é o usuário que foi configurado no banco de dados do sistema.

```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE : C:\ProgramData\.hdb\SNAPCENTER-61\S-1-5-18\SSFS_HDB.DAT
KEY FILE : C:\ProgramData\.hdb\SNAPCENTER-61\S-1-5-18\SSFS_HDB.KEY
KEY MS1KEYHOST1
ENV : hana-4:30013
USER: SNAPCENTER
KEY MS1KEYHOST2
ENV : hana-5:30013
USER: SNAPCENTER
KEY MS1KEYHOST3
ENV : hana-6:30013
USER: SNAPCENTER
KEY SS2KEY
ENV : hana-3:30013
USER: SNAPCENTER

C:\Program Files\sap\hdbclient>
```

Configuração manual de recursos do HANA

Um recurso de sistema HANA configurado manualmente é criado no SnapCenter clicando no botão Adicionar na visualização de recursos.

[largura=601, altura=189]

Na próxima tela, você precisará fornecer alguns parâmetros do sistema.

- Host do plug-in: O host central do plug-in deve ser selecionado.
- Chave do repositório de usuários do SAP HANA: Para um sistema HANA de host único, deve ser fornecido o nome da chave que foi preparada no host central do plug-in. Para um sistema HANA com múltiplos hosts, deve ser fornecida uma lista de todas as chaves do sistema, separadas por vírgulas.
- Usuário do sistema operacional HDBSQL: Se o host do plug-in central estiver sendo executado no Windows, o usuário será pré-selecionado como usuário do SISTEMA. Caso contrário, deverá ser fornecido o usuário que foi utilizado para a chave do repositório de usuários do SAP HANA.

[largura=384, altura=357]

Como próximo passo, é necessário configurar o espaço de armazenamento disponível. Todos os volumes ONTAP ou ANF pertencentes ao sistema HANA devem ser adicionados aqui.

[largura=385, altura=359]

A configuração da proteção de recursos agora pode ser feita da mesma forma que para sistemas HANA descobertos automaticamente.

Saiba mais sobre operações de backup para snapshots do SAP HANA no SnapCenter.

Realize backups de snapshots do SAP HANA usando o SnapCenter. Saiba mais sobre backups de snapshots de banco de dados, verificações de integridade de blocos, backups de volumes que não sejam de dados e replicação de backups usando o SnapVault ou o backup de Azure NetApp Files .

No SnapCenter, os backups de bancos de dados geralmente são executados usando as programações definidas na configuração de proteção de recursos de cada banco de DADOS HANA.

O backup do banco de dados sob demanda pode ser feito usando a GUI do SnapCenter, uma linha de comando do PowerShell ou APIS REST.

O SnapCenter suporta as seguintes operações de backup.

- Operações de backup de snapshots do banco de dados HANA
- operações de verificação de integridade de bloco
- Cópias de segurança instantâneas de volumes que não são de dados
- Replicação de backup usando SnapVault ou backup ANF para backups de banco de dados HANA ou backups de volumes que não sejam de dados.

As seções a seguir descrevem as diferentes operações para sistemas HANA de host único que foram descobertos automaticamente pelo SnapCenter (plug-in HANA implantado no host do banco de dados HANA).

Backups de snapshots do SAP HANA no SnapCenter

A topologia de recursos do SnapCenter mostra a lista de backups criados pelo SnapCenter. A figura a seguir mostra os backups disponíveis no armazenamento primário e destaca o backup mais recente.

[largura=601, altura=293]

Os backups no armazenamento secundário podem ser listados clicando no ícone de cópias do Vault.

[largura=601, altura=294]

A captura de tela a seguir mostra a lista de backups do sistema SM1, onde snapshots à prova de adulteração foram configurados.

[largura=601, altura=293]

Cópias de segurança de snapshots do SAP HANA no SAP HANA Studio

Ao realizar um backup usando Snapshots de armazenamento para um sistema SAP HANA MDC, uma cópia Snapshot do volume de dados é criada. Este volume de dados contém os dados do banco de dados do sistema, bem como os dados de todos os bancos de dados dos locatários. Para refletir essa arquitetura física, o SAP HANA realiza internamente um snapshot combinado do banco de dados do sistema, bem como de todos os bancos de dados de locatários, sempre que o SnapCenter aciona um backup de snapshot. Isso resulta em várias entradas de backup separadas no catálogo de backup do SAP HANA: uma para o banco de dados do sistema e uma para cada banco de dados de locatário.

No catálogo de backups do SAP HANA, o nome do backup do SnapCenter é armazenado como um campo de Comentário, assim como o ID de Backup Externo (EBID). Isso é mostrado na captura de tela a seguir para o banco de dados do sistema e na captura de tela seguinte para o banco de dados do locatário SS1. Ambas as figuras destacam o nome do backup do SnapCenter armazenado no campo de comentários e o EBID.

[largura=601, altura=289]

[largura=601, altura=296]



O SnapCenter só tem conhecimento dos seus próprios backups. Os backups adicionais criados, por exemplo, com o SAP HANA Studio, são visíveis no catálogo do SAP HANA, mas não no SnapCenter. Além disso, os snapshots criados diretamente no sistema de armazenamento não ficarão visíveis no SnapCenter.

Cópias de segurança de snapshots do SAP HANA na camada de armazenamento

Para visualizar os backups na camada de armazenamento, você pode usar o NetApp System Manager e selecionar o volume do banco de dados. A captura de tela a seguir mostra os backups disponíveis para o volume de banco de dados SS1_data_mnt00001 no armazenamento primário. O backup destacado é o backup mostrado no SnapCenter e no SAP HANA Studio nas imagens anteriores e possui a mesma convenção de nomenclatura.

[largura=601, altura=294]

A captura de tela a seguir mostra os backups disponíveis para o volume de destino de replicação hana_SS1_data_mnt00001_dest no sistema de armazenamento secundário.

[largura=601, altura=294]

Backups de snapshots do SAP HANA com ANF

A captura de tela a seguir mostra a visualização da topologia de um sistema HANA usando o Azure NetApp Files. Para este sistema HANA, foram configurados backups locais de snapshots, bem como replicação de backup usando o backup ANF.

[largura=601, altura=303]

Os backups de snapshot no volume ANF podem ser listados usando o portal do Azure.

[largura=601, altura=258]

Ao clicar no ícone de backup, você pode listar os backups que foram replicados com o backup do ANF.

[largura=601, altura=304]

Os backups do ANF também podem ser listados no portal do Azure.

[largura=601, altura=216]

Cópias de segurança instantâneas de volumes que não são de dados

A topologia de recursos do SnapCenter mostra a lista de backups para volumes que não contêm dados. Na figura a seguir, estão listados os backups do volume compartilhado do HANA.

[largura=601, altura=294]

Fluxo de trabalho de backup para backups de banco de dados HANA

O fluxo de trabalho de backup para um backup de snapshot de banco de dados HANA consiste em três seções principais.

- Descoberta automática
 - Descoberta de aplicações, por exemplo
 - O SnapCenter detecta quaisquer alterações na configuração do locatário.
 - O SnapCenter detecta o nó primário de replicação do sistema HANA.
 - Descoberta de sistemas de arquivos e armazenamento, por exemplo
 - O SnapCenter detecta quaisquer alterações na configuração do volume.
 - O SnapCenter detecta configurações de múltiplas partições no HANA.
- Operações de backup HANA e Snapshot
 - Acionar snapshot do banco de dados HANA
 - Criar instantâneo de armazenamento
 - Confirme o snapshot do banco de dados HANA e registre o backup no catálogo de backups do HANA.
- Gerenciamento de retenção
 - Excluir backups de snapshot com base no período de retenção definido em
 - Repositório SnapCenter
 - Armazenar
 - Catálogo de backup do HANA
 - gerenciamento de retenção de backups de logs
 - Exclua os backups de log no sistema de arquivos e no catálogo de backup do HANA.

[largura=339, altura=475]

Fluxo de trabalho de backup para volumes que não são de dados.

Para um volume que não contenha dados, o fluxo de trabalho de backup consiste na operação de Snapshot e na operação de gerenciamento de retenção.

[largura=329, altura=404]

Limpeza de backups secundários

Conforme descrito em "[Gestão de retenção para backups secundários](#)" O gerenciamento da retenção de backups de dados para um armazenamento de backup secundário é tratado pelo ONTAP. O SnapCenter verifica periodicamente se o ONTAP excluiu backups no armazenamento de backup secundário, executando uma tarefa de limpeza com um agendamento padrão semanal.

A tarefa de limpeza do SnapCenter exclui backups no repositório do SnapCenter , bem como no catálogo de backups do SAP HANA, caso algum backup excluído no armazenamento de backup secundário tenha sido identificado.

[largura=601, altura=158]

[largura=267, altura=330]

Até que essa limpeza programada seja concluída, o SAP HANA e o SnapCenter ainda exibirão backups que já foram excluídos do armazenamento de backup secundário. Isso resultará em backups de log adicionais que serão mantidos, mesmo que os backups de Snapshot correspondentes, baseados em armazenamento, no armazenamento de backup secundário já tenham sido excluídos. A NetApp recomenda alterar a programação de semanal para diária para evitar a manutenção de backups de log, que não são mais necessários.

Altere a frequência do trabalho de limpeza do SnapCenter

Por padrão, o SnapCenter executa a tarefa de limpeza SnapCenter_RemoveSecondaryBackup para todos os recursos semanalmente. Isso pode ser alterado usando um cmdlet do PowerShell do SnapCenter .

```
SnapCenterPS C:\> Open-SmConnection

Enter username/password
User: sapcc\scadmin
Password for user sapcc\scadmin: *****

SnapCenterPS C:\> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"="1"}
-TaskName SnapCenter_RemoveSecondaryBackup

TaskName : SnapCenter_RemoveSecondaryBackup
Hosts : {}
StartTime : 8/25/2025 3:45:00 AM
DaysoftheMonth :
MonthsofTheYear :
DaysInterval : 1
DaysOfTheWeek :
AllowDefaults : False
ReplaceJobIfExists : False
UserName :
Password :
SchedulerType : Daily
RepeatTask_Every_Hour : 1
IntervalDuration :
```

```
EndTime :
LocalScheduler : False
AppType : False
AuthMode :
SchedulerSQLInstance : SMCoreContracts.SmObject
MonthlyFrequency :
Hour : 0
Minute : 0
NodeName :
ScheduleID : 0
RepeatTask_Every_Mins :
CronExpression :
CronOffsetInMinutes :
StrStartTime :
StrEndTime :
ScheduleCategory :
PolicyId : 0
PolicyName :
ProtectionGroupId : 0
ProtectionGroupName :
PluginCode : NONE
PolicyType : None
ReportTriggerName :
PolicyScheduleId : 0
HoursOfTheDay :
DayStartTime :
MinuteOffset : ZeroMinutes
SnapMirrorLabel :
BackupType :
SnapCenterPS C:\>
```

A configuração também pode ser verificada na visualização Monitor - Agendamentos na interface do usuário do SnapCenter .

[largura=601, altura=257]

Atualização manual no nível de recurso

Caso necessário, uma limpeza manual dos backups secundários também pode ser executada na visualização de topologia de um recurso. O SnapCenter exibe os backups no armazenamento de backup secundário ao selecionar os backups secundários, conforme mostrado na captura de tela a seguir. O SnapCenter executa uma operação de limpeza com o ícone Atualizar para sincronizar os backups deste recurso.

[largura=601, altura=291]

Execute verificações de consistência de blocos do SAP HANA com o SnapCenter.

Execute verificações de consistência de blocos do SAP HANA usando a ferramenta SAP hdbpersdiag ou executando backups baseados em arquivos. Saiba mais sobre as opções de configuração, incluindo acesso ao diretório de Snapshots local, hosts de verificação central com volumes FlexClone e integração com o SnapCenter para agendamento e automação.

A tabela abaixo resume os principais parâmetros que ajudam a decidir qual método de verificação de consistência de blocos é o mais adequado para o seu ambiente.

	Ferramenta HANA hdbpersdiag usando diretório de Snapshot local	Ferramenta HANA hdbpersdiag com host de verificação central	Backup baseado em arquivos
Configurações suportadas	Somente NFS Montagens em sistema operacional convidado: Bare metal, ANF, FSx ONTAP, VMware ou KVM	Todos os protocolos e plataformas	Todos os protocolos e plataformas
Carga da CPU no host HANA	Médio	Nenhum	Alto
Utilização da rede no host HANA	Alto	Nenhum	Alto
Tempo de execução	Aproveita ao máximo a capacidade de leitura do volume de armazenamento.	Aproveita ao máximo a capacidade de leitura do volume de armazenamento.	Normalmente limitado pela taxa de transferência de escrita do sistema de destino.
Requisitos de capacidade	Nenhum	Nenhum	Pelo menos 1 unidade de tamanho de backup por sistema HANA
Integração com o SnapCenter	Script de backup posterior	Script para criar e publicar clones, e para excluir clones.	Recurso integrado
Agendamento	Agendador SnapCenter	Script do PowerShell para executar fluxo de trabalho de criação e exclusão de clones, agendado externamente.	Agendador SnapCenter

Os capítulos seguintes descrevem a configuração e a execução das diferentes opções para operações de verificação de consistência de blocos.

Verificações de consistência com hdbpersdiag usando o diretório de snapshots local.

Dentro do SnapCenter, é criada uma política dedicada para operações hdbpersdiag com um agendamento diário e uma retenção de dois. Não utilizamos o agendamento semanal, pois isso nos resultaria em pelo menos 2 backups instantâneos (retenção mínima = 2), sendo que um deles teria até duas semanas de idade.

Na configuração de proteção de recursos do SnapCenter do sistema HANA, é adicionado um script pós-backup que executa a ferramenta hdbpersdiag. Como o script de pós-backup também será executado com qualquer outra política configurada para o recurso, precisamos verificar no script qual política está ativa no momento. No script, também verificamos o dia da semana atual e executamos a operação hdbpersdiag apenas uma vez por semana, aos domingos. O comando HANA hdbpersdiag é então executado para cada volume de dados no diretório hdb* correspondente do diretório de backup do Snapshot atual. Se a verificação de consistência com o hdbpersdiag reportar algum erro, a tarefa do SnapCenter será marcada como falha.



O script de exemplo call-hdbpersdiag.sh é fornecido tal como está e não é coberto pelo suporte da NetApp. Você pode solicitar o script por e-mail para ng-sapcc@netapp.com.

A figura abaixo mostra o conceito geral da implementação da verificação de consistência.

[largura=601, altura=248]

Como primeiro passo, você precisa permitir o acesso ao diretório de snapshots, para que o diretório ".snapshot" fique visível no host do banco de dados HANA.

- Sistemas ONTAP e FSX para ONTAP: Você precisa configurar o parâmetro de volume de acesso ao diretório de snapshots.
- ANF: Você precisa configurar o parâmetro de volume "Ocultar caminho do snapshot".

Como próximo passo, você deve configurar uma política que corresponda ao nome usado no script pós-backup. Para o nosso exemplo de script, o nome deve ser SnapAndCallHdbpersdiag. Conforme discutido anteriormente, utiliza-se um cronograma diário para evitar a necessidade de manter snapshots antigos com um cronograma semanal.

[largura=414, altura=103]

[largura=424, altura=108]

[largura=433, altura=336]

Na configuração de proteção de recursos, o script pós-backup é adicionado e a política é atribuída ao recurso.[largura=601, altura=294]

[largura=601, altura=281]

Por fim, o script deve ser configurado no arquivo allowed_commands.config no host HANA.

```
hana-1:/ # cat /opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/hdbpersdiag/call-hdbpersdiag.sh
```

A operação de backup do Snapshot agora será executada uma vez por dia, e o script garante que a verificação hdbpersdiag seja executada apenas uma vez por semana, aos domingos.



O script chama o hdbpersdiag com a opção de linha de comando “-e”, que é necessária para a criptografia do volume de dados. Caso a criptografia de volume de dados HANA não seja utilizada, o parâmetro deverá ser removido.

A saída abaixo mostra o arquivo de log do script:

```
20251024055824###hana-1###call-hdbpersdiag.sh: Current policy is
SnapAndCallHdbpersdiag
20251024055824###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001
20251024055827###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivercache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001/ (4.8 GB,
5100273664 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (94276 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055827###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001.
```

```

20251024055827###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003
20251024055828###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivercache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003/
(320.0 MB, 335544320 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251024055828###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003.
20251024055828###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003
20251024055833###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivercache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003/
(4.6 GB, 4898947072 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:

```

```
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (100817 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055833###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003.
20251024060048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnapAndSnapVault, consistency check is only done with Policy
SnapAndCallHdbpersdiag
20251024080048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnap, consistency check is only done with Policy SnapAndHdbpersdiag
```

Verificações de consistência com hdbpersdiag usando um host de verificação central.

A figura abaixo mostra uma visão geral da arquitetura da solução e do fluxo de trabalho. Com um host de verificação central, é possível usar esse host para verificar a consistência de vários sistemas HANA diferentes. A solução utiliza os fluxos de trabalho de criação e exclusão de clones do SnapCenter para anexar um volume clonado do sistema HANA, que deve ser verificado no host de verificação. Um script pós-clonagem é usado para executar a ferramenta hdbpersdiag do HANA. Como segundo passo, o fluxo de trabalho de exclusão de clones do SnapCenter é usado para desmontar e excluir o volume clonado.



Se os sistemas HANA estiverem configurados com criptografia de volume de dados, as chaves raiz de criptografia do sistema HANA de origem deverão ser importadas no host de verificação antes da execução do hdbpersdiag. Veja também ["Importar chaves raiz de backup antes da recuperação do banco de dados | Portal de Ajuda SAP"](#)

[largura=601, altura=257]

A ferramenta HANA hdbpersdiag está incluída em cada instalação do HANA, mas não está disponível como uma ferramenta independente. Portanto, o host de verificação central deve ser preparado com a instalação de

um sistema HANA normal.

Etapas iniciais de preparação, realizadas uma única vez:

- Instalação do sistema SAP HANA para ser usado como host de verificação central.
- Configuração do sistema SAP HANA no SnapCenter
 - Implantação do plug-in SnapCenter SAP HANA no host de verificação. O sistema SAP HANA é detectado automaticamente pelo SnapCenter.
- A primeira operação hdbpersdiag após a instalação inicial é preparada seguindo os passos abaixo:
 - Encerre o sistema SAP HANA de destino
 - Desmonte o volume de dados do SAP HANA.

Você deve adicionar os scripts que devem ser executados no sistema de destino ao arquivo de configuração de comandos permitidos do SnapCenter.

```
hana-7:/mnt/sapcc-share/hdbpersdiag # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/hdbpersdiag/call-hdbpersdiag-flexclone.sh
```



O script de exemplo call-hdbpersdiag-flexclone.sh é fornecido tal como está e não é coberto pelo suporte da NetApp . Você pode solicitar o script por e-mail para ng-sapcc@netapp.com.

Execução manual do fluxo de trabalho

Na maioria dos casos, a operação de verificação de consistência será executada como uma operação agendada, conforme descrito no próximo capítulo. No entanto, conhecer o fluxo de trabalho manual é útil para entender os parâmetros utilizados no processo automatizado.

O fluxo de trabalho de criação de clones é iniciado selecionando um backup do sistema que deve ser verificado e clicando em "Clonar do backup".

[largura=601, altura=247]

Na próxima tela, devem ser fornecidos o nome do host, o SID e a interface de rede de armazenamento do host de verificação.



É importante usar sempre o SID do sistema HANA instalado no host de verificação; caso contrário, o fluxo de trabalho falhará.

[largura=431, altura=115]

Na próxima tela, você precisa adicionar o script call-hdbpersdiag-fleclone.sh como um comando pós-clonagem.

[largura=442, altura=169]

Quando o fluxo de trabalho for iniciado, o SnapCenter criará um volume clonado com base no backup do

Snapshot selecionado e o montará no host de verificação.

Nota: O exemplo de saída abaixo é baseado em sistemas HANA que utilizam NFS como protocolo de armazenamento. Para sistemas HANA que utilizam FC ou VMDKs da VMware, o dispositivo será montado da mesma forma em /hana/data/SID/mnt00001.

```
hana-7:/mnt/sapcc-share/hdbpersdiag # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 16G 8.0K 16G 1% /dev
tmpfs 25G 0 25G 0% /dev/shm
tmpfs 16G 474M 16G 3% /run
tmpfs 16G 0 16G 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 9.0G 48G 16% /
/dev/mapper/system-root 60G 9.0G 48G 16% /home
/dev/mapper/system-root 60G 9.0G 48G 16% /.snapshots
/dev/mapper/system-root 60G 9.0G 48G 16% /root
/dev/mapper/system-root 60G 9.0G 48G 16% /opt
/dev/mapper/system-root 60G 9.0G 48G 16% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 9.0G 48G 16% /srv
/dev/mapper/system-root 60G 9.0G 48G 16% /usr/local
/dev/mapper/system-root 60G 9.0G 48G 16% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 9.0G 48G 16% /var
/dev/mapper/system-root 60G 9.0G 48G 16% /tmp
/dev/sda1 500M 5.1M 495M 2% /boot/efi
192.168.175.117:/QS1_shared/usr-sap 251G 15G 236G 6% /usr/sap/QS1
192.168.175.86:/sapcc_share 1.4T 858G 568G 61% /mnt/sapcc-share
192.168.175.117:/QS1_log_mnt00001 251G 335M 250G 1% /hana/log/QS1/mnt00001
192.168.175.117:/QS1_shared/shared 251G 15G 236G 6% /hana/shared
tmpfs 3.2G 20K 3.2G 1% /run/user/467
tmpfs 3.2G 0 3.2G 0% /run/user/0
192.168.175.117:/SS2_data_mnt00001_Clone_10292511250337819 250G 6.4G 244G
3% /hana/data/QS1/mnt00001
```

A saída abaixo mostra o arquivo de log do comando pós-clonagem call-hdbpersdiag-flexclone.sh.

```
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag for source system SS2.
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Clone mounted at
/hana/data/QS1/mnt00001.
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00001
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivercache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
```

```

#0 /hana/data/QS1/mnt00001/hdb00001/ (3.1 GB, 3361128448 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (65388 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00001.
20251029112601###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00002.00003
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivercache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00002.00003/ (288.0 MB, 301989888 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00002.00003.

```

```

20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00003.00003
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivercache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00003.00003/ (3.7 GB, 3942645760 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (79333 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00003.00003.

```



O script chama o hdbpersdiag com a opção de linha de comando “-e”, que é necessária para a criptografia do volume de dados. Caso a criptografia de volume de dados HANA não seja utilizada, o parâmetro deverá ser removido. Quando o script pós-clonagem for concluído, a tarefa do SnapCenter também será finalizada.

[largura=279, altura=344]

Como próximo passo, executaremos o fluxo de trabalho de exclusão de clones do SnapCenter para limpar o host de verificação e excluir o volume FlexClone .

Na visualização de topologia do sistema de origem, selecionamos o clone e clicamos no botão excluir.

[largura=601, altura=165]

O SnapCenter irá agora desmontar o volume clonado do host de verificação e excluir o volume clonado do sistema de armazenamento.

Automação do fluxo de trabalho do SnapCenter usando scripts do PowerShell

Na seção anterior, os fluxos de trabalho de criação e exclusão de clones foram executados usando a interface do usuário do SnapCenter . Todos os fluxos de trabalho também podem ser executados com scripts do PowerShell ou chamadas à API REST, permitindo maior automação. A seção a seguir descreve um exemplo básico de script do PowerShell para executar os fluxos de trabalho de criação e exclusão de clones do SnapCenter .



Os scripts de exemplo `call-hdbpersdiag-flexclone.sh` e `clone-hdbpersdiag.ps1` são fornecidos "como estão" e não são cobertos pelo suporte da NetApp . Você pode solicitar os scripts por e-mail para ng-sapcc@netapp.com.

O script de exemplo do PowerShell executa o seguinte fluxo de trabalho.

- Procure o backup Snapshot mais recente de acordo com o parâmetro de linha de comando `SID` e o host de origem.
- Executa o fluxo de trabalho de criação de clone do SnapCenter usando o backup do Snapshot definido na etapa anterior. As informações do host de destino e as informações do `hdbpersdiag` são definidas no script. O script `call-hdbpersdiag-flexclone.sh` é definido como um script pós-clonagem e é executado no host de destino.
 - `$result = New-SmClone -AppPluginCode hana -BackupName $backupName -Resources @{"Host"="$sourceHost";"UID"="$uid"} -CloneToInstance "$verificationHost" -NFSEExportIPs $exportIpTarget -CloneUid $targetUid -PostCloneCreateCommands $postCloneScript`
- Executa o fluxo de trabalho de exclusão de clones do SnapCenter. O texto abaixo mostra a saída do script de exemplo executado no servidor SnapCenter .

O texto abaixo mostra a saída do script de exemplo executado no servidor SnapCenter .

```

C:\Users\scadmin>pwsh -command "c:\netapp\clone-hdbpersdiag.ps1 -sid SS2
-sourceHost hana-3.sapcc.stl.netapp.com"
Starting verification
Connecting to SnapCenter
Validating clone/verification request - check for already existing clones
Get latest back for [SS2] on host [hana-3.sapcc.stl.netapp.com]
Found backup name [SnapCenter_hana-3_LocalSnapKeep2_Hourly_11-21-
2025_07.56.27.5547]
Creating clone from backup [hana-
3.sapcc.stl.netapp.com/SS2/SnapCenter_hana-3_LocalSnapKeep2_Hourly_11-21-
2025_07.56.27.5547]: [hana-7.sapcc.stl.netapp.com/QS1]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Completed]
Removing clone [SS2 - HANA System Replication__clone__169851_MDC_SS2_07-
09-2025_07.44.09]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Completed]
Verification completed

C:\Users\scadmin>

```



O script chama o hdbpersdiag com a opção de linha de comando “-e”, que é necessária para a criptografia do volume de dados. Caso a criptografia de volume de dados HANA não seja utilizada, o parâmetro deverá ser removido.

A saída abaixo mostra o arquivo de log do script call-hdbpersdiag-flexclone.sh.

```

20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag for source system SS2.
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Clone mounted at
/hana/data/QS1/mnt00001.

```

```

20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00001
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivercache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00001/ (3.1 GB, 3361128448 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
      Default Anchor Page OK
      Restart Page OK
      Default Converter Pages OK
      RowStore Converter Pages OK
      Logical Pages (65415 pages) OK
      Logical Pages Linkage OK
Checking entries from restart page...
      ContainerDirectory OK
      ContainerNameDirectory OK
      FileIDMappingContainer OK
      UndoContainerDirectory OK
      LobDirectory OK
      MidSizeLobDirectory OK
      LobFileIDMap OK
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00001.
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00002.00003
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivercache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00002.00003/ (288.0 MB, 301989888 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
      Default Anchor Page OK
      Restart Page OK
      Default Converter Pages OK
      RowStore Converter Pages OK

```

```

        Logical Pages (4099 pages) OK
        Logical Pages Linkage OK
Checking entries from restart page...
        UndoContainerDirectory OK
        DRLoadedTable OK
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00002.00003.
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00003.00003
20251121085729###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivercache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
    #0 /hana/data/QS1/mnt00001/hdb00003.00003/ (3.7 GB, 3942645760 bytes)
Tips:
    Type 'help' for help on the available commands
    Use 'TAB' for command auto-completion
    Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
        Default Anchor Page OK
        Restart Page OK
        Default Converter Pages OK
        Static Converter Pages OK
        RowStore Converter Pages OK
        Logical Pages (79243 pages) OK
        Logical Pages Linkage OK
Checking entries from restart page...
        ContainerDirectory OK
        ContainerNameDirectory OK
        FileIDMappingContainer OK
        UndoContainerDirectory OK
        LobDirectory OK
        DRLoadedTable OK
        MidSizeLobDirectory OK
        LobFileIDMap OK
20251121085729###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00003.00003.
hana-7:/mnt/sapcc-share/hdbpersdiag #

```

Backup baseado em arquivos

O SnapCenter suporta a execução de uma verificação de integridade de bloco usando uma política na qual o backup baseado em arquivo é selecionado como o tipo de backup.

Ao agendar backups usando essa política, o SnapCenter cria um backup de arquivo padrão do SAP HANA para o sistema e todos os bancos de dados do locatário.

O SnapCenter não exibe a verificação de integridade de bloco da mesma maneira que os backups baseados em cópia Snapshot. Em vez disso, o cartão de resumo mostra o número de backups baseados em arquivos e o status do backup anterior.

[largura=601, altura=293]

O catálogo de backup do SAP HANA mostra entradas para os bancos de dados do sistema e do locatário. A figura a seguir mostra uma verificação de integridade de bloco SnapCenter no catálogo de backup do banco de dados do sistema.

[largura=601, altura=293]

Uma verificação de integridade de bloco bem-sucedida cria arquivos de backup de dados padrão do SAP HANA.

[largura=351, altura=433]

O SnapCenter utiliza o caminho de backup que foi configurado no banco de dados HANA para operações de backup de dados baseadas em arquivos.

```
hana-1:/hana/shared/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 3717564
drwxr-xr-- 2 ssladm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ssladm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ssladm sapsys 159744 Aug 17 05:32 SnapCenter_SnapCenter_hana-
1_BlockIntegrityCheck_Weekly_08-17-2025_05.32.00.4493_databackup_0_1
-rw-r----- 1 ssladm sapsys 83898368 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_2_1
-rw-r----- 1 ssladm sapsys 3707777024 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_3_1
SYSTEMDB:
total 3339236
drwxr-xr-- 2 ssladm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ssladm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ssladm sapsys 163840 Aug 17 05:32 SnapCenter_SnapCenter_hana-
1_BlockIntegrityCheck_Weekly_08-17-2025_05.32.00.4493_databackup_0_1

-rw-r----- 1 ssladm sapsys 3405787136 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_1_1
```

Restaure e recupere bancos de dados SAP HANA com o SnapCenter.

Restaure e recupere sistemas SAP HANA usando o SnapCenter com opções de recuperação automatizada ou manual. Isso inclui restaurações completas do sistema, restaurações de localitário único para bancos de dados HANA no ONTAP, Azure NetApp Files e FSx para ONTAP.

O SnapCenter oferece suporte às seguintes operações de restauração e recuperação.

- Sistemas SAP HANA MDC com um único localitário
 - Restauração e recuperação automatizadas de ponta a ponta
 - Restauração automatizada de ponta a ponta e recuperação manual (selecionável)
- Sistemas SAP HANA MDC com múltiplos localitários
 - Restauração automatizada de ponta a ponta; a recuperação precisa ser feita manualmente.
- Restauração de um único localitário
 - Restauração automatizada de ponta a ponta; a recuperação precisa ser feita manualmente.



A recuperação automatizada só é suportada quando o plug-in HANA é implantado no host do banco de dados HANA e o sistema HANA é descoberto automaticamente pelo SnapCenter. Com uma configuração centralizada de host plug-in, a recuperação precisa ser feita manualmente após a operação de restauração com o SnapCenter.



Com o Azure NetApp Files, as operações de restauração são suportadas para volumes ANF primários ou backups ANF. Para volumes ANF primários, uma reversão de volume será executada; para backups ANF, uma restauração no local com restauração de arquivo único será executada. Em ambos os casos, as configurações do grupo de volume do aplicativo serão mantidas.



Se a criptografia de volume estiver habilitada e o SAP local secure store (LSS) for utilizado, uma recuperação com SnapCenter é suportada desde que a senha de backup da chave raiz no LSS não tenha sido alterada desde que o backup foi realizado. Se a senha for alterada e uma restauração e recuperação forem realizadas usando um Snapshot mais antigo com uma senha diferente, a recuperação precisará ser feita manualmente e a senha antiga precisará ser fornecida com a instrução de recuperação: "RECOVER DATA USING SNAPSHOT CLEAR LOG ENCRYPTION ROOT KEYS BACKUP PASSWORD 'old-password'"

Restauração e recuperação automatizadas para sistemas SAP HANA MDC com um único localitário.

Uma operação de restauração é iniciada selecionando um backup de Snapshot na visualização da topologia de recursos e clicando em Restaurar.

[largura=601, altura=294]

Para sistemas HANA que utilizam NFS em ANF, FSx para ONTAP ou sistemas de armazenamento ONTAP, você pode selecionar a restauração completa com ou sem uma operação de reversão de volume para snapshots do volume primário.

- O recurso completo sem reversão de volume usa o Single File SnapRestore (SFSR) para restaurar todos os arquivos do banco de dados.
- A restauração completa do volume com reversão utiliza uma operação de restauração baseada em volume (VBSR) para reverter todo o volume ao estado do Snapshot selecionado.



A reversão de volume não pode ser usada se você precisar restaurar para um Snapshot que seja mais antigo do que o Snapshot de replicação ativo do SnapVault ou SnapMirror .



Uma operação de reversão de volume excluirá todos os backups de Snapshot mais recentes que o Snapshot selecionado para a operação de reversão.



Uma restauração com o SFSR é quase tão rápida quanto uma operação de reversão de volume, mas bloqueia qualquer operação de Snapshot até que o processo em segundo plano conclua as operações de metadados.

[largura=300]

Para sistemas HANA em hosts bare metal usando FC SAN, a reversão de volume (VBSR) não é suportada; em vez disso, o SFSR é sempre usado para a operação de restauração. Para sistemas HANA executados em VMware com VMFS, será utilizada uma operação de clonagem, montagem e cópia.

[largura=345, altura=325]

Para restaurar a partir de um backup secundário, você precisa selecionar o local do arquivo.

[largura=345, altura=323]

Com o escopo de recuperação, você pode selecionar uma recuperação 'para o estado mais recente', 'para um ponto específico no tempo' ou para um ponto de salvamento, sem usar backups de log. Se você selecionar "sem recuperação", o SnapCenter executará apenas a operação de restauração e a recuperação precisará ser feita manualmente, conforme descrito. "[Recuperação manual com o HANA Studio](#)".



O SnapCenter utiliza os caminhos configurados no SAP HANA para os locais de backup de logs e de catálogos. Se você tiver backups em camadas em um local adicional, poderá adicionar esses caminhos adicionais.

[largura=346, altura=324]

Opcionalmente, você pode adicionar scripts de pré e pós-restauração.

[largura=348, altura=326]

[largura=359, altura=335]

Ao clicar em Concluir na tela de resumo, a operação de restauração e recuperação é iniciada.

[largura=361, altura=336]

O fluxo de trabalho de restauração e recuperação pode ser dividido em três seções principais.

- Desligamento do sistema HANA
- Operação de restauro

- Preparativos específicos do sistema de arquivos, por exemplo, operação de desmontagem.
- Operação de restauração de instantâneo
- Operações pós-montagem específicas do sistema de arquivos, por exemplo, operação de montagem.
- Recuperação HANA
 - Recuperação de banco de dados do sistema
 - Recuperação de banco de dados do locatário

[largura=357, altura=439]

Recuperação manual com o HANA Studio

Para restaurar e recuperar um sistema SAP HANA MDC com um ou vários tenants usando o SAP HANA Studio e o SnapCenter, siga os passos abaixo:

1. Prepare o processo de restauração e recuperação com o SAP HANA Studio:
 - a. Selecione recuperar banco de dados do sistema e confirme o desligamento do sistema SAP HANA.
 - b. Selecione o tipo de recuperação e forneça o local do catálogo de backup.
 - c. É apresentada a lista de cópias de segurança de dados. Selecione Backup (cópia de segurança) para ver a ID de cópia de segurança externa.
2. Execute o processo de restauração com o SnapCenter:
 - a. Na visualização de topologia do recurso, selecione Cópias Locais para restaurar do armazenamento primário ou Cópias do Vault se desejar restaurar de um armazenamento de backup secundário.
 - b. Selecione o backup do SnapCenter que corresponde ao ID ou campo de comentário do backup externo do SAP HANA Studio.
 - c. Inicie o processo de restauração.
3. Execute o processo de recuperação do banco de dados do sistema com o SAP HANA Studio:
 - a. Clique em Atualizar na lista de cópias de segurança e selecione a cópia de segurança disponível para recuperação (indicada com um ícone verde).
 - b. Inicie o processo de recuperação. Após o processo de recuperação ser concluído, o banco de dados do sistema é iniciado.
4. Execute o processo de recuperação do banco de dados do locatário com o SAP HANA Studio:
 - a. Selecione recuperar banco de dados do locatário e selecione o locatário a ser recuperado.
 - b. Selecione o tipo de recuperação e a localização da cópia de segurança do registro.
 - c. É apresentada uma lista de cópias de segurança de dados. Como o volume de dados já foi restaurado, o backup do locatário é indicado como disponível (em verde).
 - d. Selecione este backup e inicie o processo de recuperação. Depois que o processo de recuperação for concluído, o banco de dados do locatário é iniciado automaticamente.
5. Para um sistema HANA com vários tenants, repita o passo 4 para cada tenant.



A recuperação manual com o SAP HANA Cockpit é feita seguindo os mesmos passos.

A seção a seguir descreve as etapas das operações de restauração e recuperação de um sistema SAP HANA MDC com um único locatário.

No HANA Studio, selecione Backup e Recuperação e Recuperar Banco de Dados do Sistema.

[largura=450, altura=368]

Confirme a operação de desligamento; necessário apenas se o sistema HANA ainda estiver em execução.

[largura=349, altura=83]

Selecione a operação de recuperação. Neste exemplo, queremos retornar ao estado mais recente.

[largura=345, altura=359]

Forneça o local de backup do catálogo.

[largura=343, altura=356]

O HANA Studio lista os backups mais recentes armazenados no catálogo de backups do HANA.

É exibida uma lista de backups disponíveis com base no conteúdo do catálogo de backups. Selecione o backup desejado e anote o ID do backup externo: neste exemplo, o backup mais recente.

[largura=391, altura=283]

Na interface gráfica do SnapCenter , selecione a visualização da topologia de recursos e escolha o backup que deve ser restaurado; neste exemplo, o backup primário mais recente. Clique no ícone Restaurar para iniciar a restauração.

[largura=601, altura=294]

O assistente de restauração do SnapCenter será iniciado. Selecione o tipo de restauração "Reversão completa de recursos e volumes" para usar uma restauração baseada em volume.

[largura=346, altura=325]

Selecione 'Sem recuperação' para excluir as operações de recuperação do fluxo de trabalho do SnapCenter .

[largura=358, altura=336]

Clique em Concluir para iniciar a operação de restauração.

[largura=361, altura=339]

O SnapCenter está executando a operação de restauração.

- Preparativos específicos do sistema de arquivos, por exemplo, operação de desmontagem.
- Operação de restauração de instantâneo
- Operações pós-instalação específicas do sistema de arquivos, por exemplo, operação de montagem.

[largura=322, altura=398]

Quando o Snapshot é restaurado pelo SnapCenter , um arquivo snapshot_databackup_0_1 fica disponível no subdiretório do banco de dados do sistema e do locatário do volume de dados HANA. Este arquivo foi criado pelo banco de dados HANA durante a criação do Snapshot do banco de dados HANA. O HANA exclui o arquivo quando a operação de backup é concluída, de forma que os arquivos fiquem visíveis apenas no backup de Snapshot. Esses arquivos são necessários para qualquer operação de recuperação. Após a

recuperação, os arquivos são excluídos pelo banco de dados HANA.

```
hana-1:~ # cd /hana/data/SS1/mnt00001/
hana-1:/hana/data/SS1/mnt00001 # ls -al *
-rw-r--r-- 1 ssladm sapsys 16 Aug 26 06:00 nameserver.lck
hdb00001:
total 4992236
drwxr-x--- 2 ssladm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ssladm sapsys 4096 Aug 26 06:00 ..
-rw-r----- 1 ssladm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 ssladm sapsys 5100273664 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ssladm sapsys 36 Aug 25 10:30 landscape.id
-rw-r----- 1 ssladm sapsys 163840 Aug 26 06:00 snapshot_databackup_0_1
hdb00002.00003:
total 201420
drwxr-xr-- 2 ssladm sapsys 4096 Nov 3 2020 .
drwxr-x--- 5 ssladm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ssladm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ssladm sapsys 335544320 Aug 26 06:00 datavolume_0000.dat
hdb00003.00003:
total 4803140
drwxr-xr-- 2 ssladm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ssladm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ssladm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ssladm sapsys 4898947072 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ssladm sapsys 159744 Aug 26 06:00 snapshot_databackup_0_1
hana-1:/hana/data/SS1/mnt00001 #
```

Acesse o SAP HANA Studio e clique em Atualizar para atualizar a lista de backups disponíveis. O backup restaurado com o SnapCenter agora é exibido com um ícone verde na lista de backups. Selecione o backup e clique em Avançar.

[largura=400, altura=290]

Forneça a localização dos backups de log. Clique em seguinte.



O SAP HANA Studio utiliza os caminhos configurados no SAP HANA para os locais de backup de logs e de catálogos. Se você tiver backups em camadas em um local adicional, poderá adicionar esses caminhos adicionais.

[largura=465, altura=296]

Selecione outras definições, conforme necessário. Certifique-se de que a opção usar backups Delta não está selecionada. Clique em seguinte.

[largura=466, altura=296]

Reveja as definições de recuperação e clique em concluir.

Ao clicar em "Exibir instrução SQL", o HANA Studio mostra o comando SQL que é executado para a operação de recuperação.

[largura=464, altura=295]

O processo de recuperação começa. Aguarde até que a recuperação do banco de dados do sistema seja concluída.

[largura=376, altura=239]

No SAP HANA Studio, selecione a entrada para o banco de dados do sistema e inicie Backup Recovery - Recover Tenant Database.

[largura=476, altura=315]

Selecione o locatário a recuperar e clique em Avançar.

[largura=342, altura=355]

Especifique o tipo de recuperação e clique em Avançar.

[largura=343, altura=356]

Confirme a localização do catálogo de backup e clique em Avançar.

[largura=342, altura=355]

Confirme o desligamento do banco de dados do locatário.

[largura=348, altura=85]

Como a restauração do volume de dados foi realizada antes da recuperação do banco de dados do sistema, o backup do locatário fica imediatamente disponível. Selecione o backup destacado em verde e clique em Avançar.

[largura=433, altura=349]

Forneça a localização dos backups de log. Clique em seguinte.



O SAP HANA Studio utiliza os caminhos configurados no SAP HANA para os locais de backup de logs e de catálogos. Se você tiver backups em camadas em um local adicional, poderá adicionar esses caminhos adicionais.

[largura=384, altura=310]

Selecione outras definições, conforme necessário. Certifique-se de que a opção usar backups Delta não está selecionada. Clique em seguinte.

[largura=384, altura=310]

Reveja as definições de recuperação e clique em concluir.

Ao clicar em "Exibir instrução SQL", o HANA Studio mostra o comando SQL que é executado para a operação de recuperação.

[largura=380, altura=307]

Aguarde até que a recuperação tenha terminado e o banco de dados do locatário seja iniciado.

[largura=378, altura=305]

Quando a recuperação do locatário for concluída, o sistema SAP HANA estará operacional.



Para um sistema SAP HANA MDC com vários tenants, você deve repetir a recuperação de tenant para cada tenant.

Recuperação manual com comandos SQL

Você também pode usar instruções SQL para a recuperação do sistema HANA.

Primeiro você precisa recuperar o banco de dados do sistema.

```
HDBSettings.sh recoverSys.py --command="RECOVER DATABASE UNTIL TIMESTAMP  
'2026-08-26 10:55:49' USING CATALOG PATH ('mnt/log-backup/SYSTEMDB') USING  
LOG PATH ('mnt/log-backup/SYSTEMDB') USING SNAPSHOT"
```

Como segundo passo, você precisa se conectar ao banco de dados do sistema e iniciar a recuperação do(s) banco(s) de dados do locatário. Neste exemplo, o banco de dados do locatário é SS1.

```
hdbsql SYSTEMDB=> RECOVER DATABASE FOR SS1 UNTIL TIMESTAMP '2026-08-26  
10:55:49' USING CATALOG PATH ('mnt/log-backup/DB_SS1') USING LOG PATH  
('mnt/log-backup/DB_SS1') USING SNAPSHOT
```

Restauração e recuperação de inquilino único

Uma operação de restauração e recuperação de locatário único com o SnapCenter é muito semelhante ao fluxo de trabalho descrito no tópico anterior. ["Recuperação manual com o HANA Studio"](#).

Para restaurar e recuperar um sistema de alocação única SAP HANA MDC usando o SAP HANA Studio e o SnapCenter, siga estas etapas:

1. Prepare o processo de restauração e recuperação com o SAP HANA Studio:
 - a. Selecione "Recuperar banco de dados do locatário" e confirme o desligamento do banco de dados do locatário.
 - b. Selecione o tipo de recuperação e forneça o local do catálogo de backup.
 - c. É apresentada a lista de cópias de segurança de dados. Selecione Backup (cópia de segurança) para ver a ID de cópia de segurança externa.
2. Execute o processo de restauração com o SnapCenter:
 - a. Na visualização de topologia do recurso, selecione Cópias Locais para restaurar do armazenamento

primário ou Cópias do Vault se desejar restaurar de um armazenamento de backup secundário.

b. Selecione o backup do SnapCenter que corresponde ao ID ou campo de comentário do backup externo do SAP HANA Studio.

c. Inicie o processo de restauração do inquilino.

3. Execute o processo de recuperação do banco de dados do locatário com o SAP HANA Studio:

a. Clique em Atualizar na lista de cópias de segurança e selecione a cópia de segurança disponível para recuperação (indicada com um ícone verde).

b. Inicie o processo de recuperação. Após a conclusão do processo de recuperação, o banco de dados do locatário é iniciado.

Restauração de volumes não relacionados a dados

A operação de restauração de um volume que não contém dados é iniciada selecionando um backup de Snapshot na visualização de topologia do recurso de volume que não contém dados e clicando em Restaurar.

[largura=601, altura=294]

Para volumes que não sejam de dados com NFS, pode-se selecionar uma operação de restauração completa de recursos (VBSR) ou uma operação de restauração em nível de arquivo (SFSR). Para a restauração em nível de arquivo, é possível definir todos os arquivos ou arquivos individuais para a operação de restauração.

[largura=369, altura=344]

Configure as opções avançadas do SnapCenter para SAP HANA.

Configure as definições avançadas do SnapCenter para ambientes SAP HANA, incluindo a supressão de mensagens de aviso do VMware para montagens NFS no sistema operacional convidado, a desativação da limpeza automática de backups de logs e a ativação da criptografia SSL para conexões de banco de dados HANA.

Mensagem de aviso em ambientes virtualizados e montagens no sistema operacional convidado.

Ao usar, por exemplo, o VMware com montagens NFS no sistema operacional convidado, o SnapCenter exibirá uma mensagem de aviso informando que o plug-in do SnapCenter para VMware deve ser usado. Como o plug-in do VMware não é necessário para montagens no sistema operacional convidado, a mensagem de aviso pode ser ignorada e desativada. Para configurar o SnapCenter para suprimir este aviso, a seguinte configuração deve ser aplicada:

1. Na guia Configurações, selecione Configurações globais.
2. Para as configurações do hipervisor, selecione VMs com discos conectados iSCSI Direct ou NFS para todos os hosts e atualize as configurações.

[largura=601, altura=176]

Desativar a limpeza automática de cópias de segurança de registros

A limpeza e o backup de logs estão ativados por padrão e podem ser desativados no nível do host do plug-in

HANA. Utilize o comando do PowerShell:

O comando `Set-SmConfigSettings -Plugin -HostName <nome_do_host_plugin> -PluginCode hana -configSettings @"LOG_CLEANUP_DISABLE" = "Y"` desativa a limpeza de backup de logs para este host SAP HANA.

Habilitar a comunicação segura com o banco de dados HANA

Se os bancos de dados HANA estiverem configurados com comunicação segura, o comando `hdbsql` executado pelo SnapCenter deverá usar opções adicionais de linha de comando.

Existem várias opções para configurar a comunicação SSL. Por padrão, o SnapCenter usa a opção de linha de comando `-e ssltrustcert hdbsql`. Com essa opção, a comunicação SSL é realizada sem a validação do certificado do servidor, e essa opção também funciona para sistemas HANA onde o SSL não está habilitado.

Caso seja necessária a validação de certificados no servidor e/ou no cliente, serão necessárias opções diferentes na linha de comando do `hdbsql`, e você deverá configurar o ambiente PSE de acordo com as instruções do Guia de Segurança do SAP HANA.

Isso pode ser conseguido usando um script auxiliar que chama o `hdbsql` com as opções necessárias. Em vez de configurar o executável `hdbsql` nos arquivos `hana.properties`, o script wrapper é adicionado.

```
HANA_HDBSQL_CMD = /usr/sap/SM1/HDB12/exe/hdbsqls
```

O script wrapper `hdbsqls` chama o `hdbsql` com as opções de linha de comando necessárias.

```
#!/bin/bash
/usr/sap/SM1/HDB12/exe/hdbsql <command line options> $*
```

Desative a detecção automática no host do plug-in HANA

Para desativar a descoberta automática no host do plug-in HANA, siga os passos abaixo:

1. No servidor SnapCenter, abra o PowerShell. Conecte-se ao servidor SnapCenter executando o comando `Open-SmConnection` e especifique o nome de usuário e a senha na janela de login que será aberta.
2. Para desativar a descoberta automática, execute o comando `Set-SmConfigSettings`.

Para um host HANA `hana-2`, o comando é o seguinte:

```
PS C:\Users\administrator.SAPCC> Set-SmConfigSettings -Agent -Hostname
hana-2 -configSettings @{"DISABLE_AUTO_DISCOVERY"="true"}
```

```
Name Value
```

```
-----
```

```
DISABLE_AUTO_DISCOVERY true
```

```
PS C:\Users\administrator.SAPCC>
```

Verify the configuration by running the Get- SmConfigSettings command.

```
PS C:\Users\administrator.SAPCC> Get-SmConfigSettings -Agent -Hostname
hana-2 -key all
```

```
Key: CUSTOMPLUGINS_OPERATION_TIMEOUT_IN_MSEC Value: 3600000 Details: Plug-
in API operation Timeout
```

```
Key: CUSTOMPLUGINS_HOSTAGENT_TO_SERVER_TIMEOUT_IN_SEC Value: 1800 Details:
Web Service API Timeout
```

```
Key: CUSTOMPLUGINS_ALLOWED_CMDS Value: *; Details: Allowed Host OS
Commands
```

```
Key: DISABLE_AUTO_DISCOVERY Value: true Details:
```

```
Key: PORT Value: 8145 Details: Port for server communication
```

```
PS C:\Users\administrator.SAPCC>
```

A configuração é gravada no arquivo de configuração do agente no host e ainda está disponível após uma atualização do plug-in com o SnapCenter.

```
hana-2:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/agent.properties | grep DISCOVERY
DISABLE_AUTO_DISCOVERY = true
hana-2:/opt/NetApp/snapcenter/scc/etc #
```

Informações sobre direitos autorais

Copyright © 2026 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 SOBRESSALENTE; 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.