



Backup, restauração e recuperação de desastres

NetApp solutions for SAP

NetApp
February 25, 2026

Índice

Backup, restauração e recuperação de desastres	1
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
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
Saiba mais sobre os conceitos e as melhores práticas de proteção de dados do SnapCenter.	12
Saiba mais sobre como configurar o SnapCenter para ambientes SAP HANA.	19
Configure as definições iniciais do SnapCenter para SAP HANA.	20
Configure os recursos do SnapCenter para bancos de dados SAP HANA individuais.	27
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
Saiba mais sobre operações de backup para snapshots do SAP HANA no SnapCenter.	36
Execute verificações de consistência de blocos do SAP HANA com o SnapCenter.	40
Restaure e recupere bancos de dados SAP HANA com o SnapCenter.	54
Configure as opções avançadas do SnapCenter para SAP HANA.	62
SAP HANA no Amazon FSX for NetApp ONTAP - Backup e recuperação com o SnapCenter.	64
SAP HANA no Amazon FSX for NetApp ONTAP - Backup e recuperação com o SnapCenter	65
Backup e recuperação usando o Amazon FSX for ONTAP.	65
Arquitetura da SnapCenter	70
Configuração do SnapCenter	76
Operações de backup do SnapCenter.	92
Backup de volumes que não são de dados.	102
Restaurar e recuperar	109
Faça backup da replicação com o SnapVault	117
Onde encontrar informações adicionais	131
Proteção de dados do SAP HANA e alta disponibilidade com o SnapCenter, o SnapMirror active Sync e o cluster de storage VMware Metro	132
Proteção de dados do SAP HANA e alta disponibilidade com o SnapCenter, o SnapMirror active Sync e o cluster de storage VMware Metro	132
Visão geral SAP HANA de alta disponibilidade	133
Exemplo de visão geral da configuração	136
Provisionamento e instalação do SISTEMA HANA	137
Configuração de sincronização ativa do SnapMirror	145
Configuração do SnapCenter	151
Operações de backup do SnapCenter.	156
Restauração e recuperação do SnapCenter	159
Operação de atualização do sistema SAP	161
Volumes SnapCenter que não são de dados	162
Cenários de failover	163
Informações adicionais e histórico de versões	167
Proteção de dados SAP HANA com SnapCenter com sistemas VMware VMFS e NetApp ASA	168

Proteção de dados SAP HANA com SnapCenter com sistemas VMware VMFS e NetApp ASA	168
Configuração de laboratório usada para este documento	169
Provisionamento e instalação do SISTEMA HANA	170
Configuração HANA	177
Configuração do SnapCenter	178
Operações de backup	185
Operações de restauração e recuperação	188
Atualização do sistema SAP	192
Informações adicionais e histórico de versões	202
Backup e recuperação de replicação do sistema SAP HANA com o SnapCenter	203
Replicação do sistema SAP HANA: Backup e recuperação com o SnapCenter	203
Backups de Snapshot de storage e replicação do sistema SAP	204
Opções de configuração do SnapCenter para replicação do sistema SAP	205
Configuração do SnapCenter 4,6 usando um grupo de recursos	207
Configuração do SnapCenter com um único recurso	218
Restauração e recuperação a partir de um backup criado no outro host	231
Onde encontrar informações adicionais	235
Histórico de versões	235
Recuperação de desastres do SAP HANA com o Azure NetApp Files	236
Recuperação de desastres do SAP HANA com o Azure NetApp Files	236
Comparação da solução de recuperação de desastres	238
Replicação entre regiões do ANF com SAP HANA	242
Teste de recuperação de desastres	254
Failover de recuperação de desastres	267
Histórico de atualizações	279
Recuperação de desastres do SAP HANA com replicação de storage	279
Backup e recuperação do SAP HANA usando NetApp Storage Systems e o software Commvault	280
Integração SnapCenter para banco de dados SAP ASE	280
Introdução	280
Informações adicionais e histórico de versões	293
Integração do SnapCenter para o banco de dados IBM DB2	294
Introdução	294
Exemplo de visão geral da configuração	295
Ambiente de demonstração	295
Informações adicionais e histórico de versões	302
Integração SnapCenter para o banco de dados SAP MaxDB	303
Introdução	303
Exemplo de visão geral da configuração	303
Ambiente de demonstração	304
Versões de software	304
MaxDB volume Design	304
Passos para proteger banco de dados M02	305
Pré-requisitos no Host	305
Pré-requisitos para o banco de dados – criar modelos de backup, ativar Logbackup	306
Implante o agente do SnapCenter para hospedar o sap-lnx25HANA	306

Criar Configuração de recursos do SnapCenter para Banco de dados M02	307
Sequência para recuperar o sistema M02.....	314
Recuperar instância M02.....	314
Informações adicionais e histórico de versões	320

Backup, restauração e recuperação de desastres

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

Operação	Montagens NFS em hardware dedicado ou em máquinas virtuais com VMware ou KVM.	FC SAN + Metal nu	Armazenamento de dados FC VMware VMFS
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			
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 (*)
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

Operação	FC SAN + Bare metal (*)	Armazenamento de dados FC VMware VMFS
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
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

Operação	Montagens NFS
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

	Capacidade de armazenamento necessária	Carga de CPU e de rede no host HANA
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
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

- Para sistemas HANA configurados com o Azure NetApp Files (ANF), uma entidade de serviço deve ser preparada e, em seguida, configurada no SnapCenter.
- 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

- Para sistemas HANA configurados com ANF, as contas NetApp necessárias podem ser selecionadas e adicionadas à configuração do SnapCenter .
- 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

- 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 .
- 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 .
- 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"](#).

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/restoreFiles/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/restoreFiles/action",

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

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

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/getMetadata/action",

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

"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",
"updatedAt": "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
DaysOfMonth :
MonthsOfYear :
DaysInterval : 1
DaysOfWeek :
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" -NFSExportIPs $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 #
```

SAP HANA no Amazon FSX for NetApp ONTAP - Backup e recuperação com o SnapCenter

SAP HANA no Amazon FSX for NetApp ONTAP - Backup e recuperação com o SnapCenter

Este relatório técnico fornece as práticas recomendadas para proteção de dados SAP HANA no Amazon FSX for NetApp ONTAP e NetApp SnapCenter. Este documento abrange os conceitos do SnapCenter, as recomendações de configuração e os fluxos de trabalho operacionais, incluindo configurações, operações de backup e operações de restauração e recuperação.

Autor: Nils Bauer, NetApp

Hoje, as empresas exigem disponibilidade contínua e ininterrupta para suas aplicações SAP. Elas esperam níveis de performance consistentes diante de volumes cada vez maiores de dados e da necessidade de tarefas de manutenção de rotina, como backups do sistema. Realizar backups de bancos de dados SAP é uma tarefa essencial e pode ter um impacto significativo no desempenho do sistema SAP de produção.

As janelas de backup estão encolhendo enquanto a quantidade de dados a serem copiados está aumentando. Portanto, é difícil encontrar um momento em que você pode executar backups com efeito mínimo nos processos de negócios. O tempo necessário para restaurar e recuperar os sistemas SAP é uma preocupação porque o tempo de inatividade para sistemas de produção e não produção SAP deve ser minimizado para reduzir os custos para os negócios.

Backup e recuperação usando o Amazon FSX for ONTAP

Você pode usar a tecnologia Snapshot do NetApp para criar backups de bancos de dados em minutos.

O tempo necessário para criar uma cópia Snapshot não depende do tamanho do banco de dados, pois a cópia Snapshot não move blocos de dados físicos na plataforma de storage. Além disso, o uso da tecnologia Snapshot não afeta a performance do sistema SAP ao vivo. Portanto, você pode agendar a criação de cópias Snapshot sem considerar períodos de atividade em lote ou diálogos de pico. Em geral, os clientes da SAP e da NetApp agendam vários backups de Snapshot on-line durante o dia; por exemplo, a cada seis horas é comum. Esses backups Snapshot costumam ser mantidos por três a cinco dias no sistema de storage primário antes de serem removidos ou dispostos em camadas em um storage mais barato para retenção a longo prazo.

As cópias Snapshot também oferecem vantagens importantes para operações de restauração e recuperação. A tecnologia NetApp SnapRestore permite a restauração de um banco de dados inteiro ou, como alternativa, apenas uma parte de um banco de dados a qualquer momento, com base nas cópias Snapshot disponíveis atualmente. Esses processos de restauração são concluídos em poucos segundos, independentemente do tamanho do banco de dados. Como vários backups Snapshot online podem ser criados durante o dia, o tempo necessário para o processo de recuperação é significativamente reduzido em relação a uma abordagem tradicional de backup uma vez por dia. Como você pode executar uma restauração com uma cópia Snapshot que tenha no máximo apenas algumas horas (em vez de até 24 horas), menos logs de transações devem ser aplicados durante a recuperação avançada. Portanto, o RTO é reduzido para vários minutos, em vez das várias horas necessárias para backups de streaming convencionais.

Os backups de cópias snapshot são armazenados no mesmo sistema de disco que os dados on-line ativos. Portanto, a NetApp recomenda o uso de backups de cópias Snapshot como um suplemento, em vez de um substituto para backups em um local secundário. A maioria das ações de restauração e recuperação é gerenciada usando o SnapRestore no sistema de storage primário. As restaurações de um local secundário só serão necessárias se o sistema de storage primário que contém as cópias Snapshot estiver danificado. Você também pode usar o local secundário se for necessário restaurar um backup que não esteja mais

disponível no local principal.

Um backup em um local secundário é baseado nas cópias Snapshot criadas no storage primário. Portanto, os dados são lidos diretamente do sistema de armazenamento primário sem gerar carga no servidor de banco de dados SAP. O storage primário se comunica diretamente com o storage secundário e replica os dados de backup para o destino usando o recurso NetApp SnapVault.

O SnapVault oferece vantagens significativas em comparação com os backups tradicionais. Após uma transferência inicial de dados, na qual todos os dados foram transferidos da origem para o destino, todos os backups subsequentes só migram os blocos alterados para o armazenamento secundário. Portanto, a carga no sistema de storage primário e o tempo necessário para um backup completo são reduzidos significativamente. Como o SnapVault armazena apenas os blocos alterados no destino, todos os backups completos adicionais do banco de dados consomem muito 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 Snapshot. A imagem mostra que o backup do banco de DADOS HANA (de tamanho aproximado de 4TB TB) é feito em 1 minuto e 20 segundos usando a tecnologia de backup Snapshot e mais de 4 horas com uma operação de backup baseada em arquivo.

A maior parte do tempo de execução geral do fluxo de trabalho de backup é o tempo necessário para executar a operação de ponto de salvamento DO BACKUP HANA, e essa etapa depende da carga no banco de DADOS HANA. O backup do Snapshot de armazenamento em si sempre termina em alguns segundos.

Backup Catalog					
☐ Show Log Backups ☐ Show Delta Backups					
Stat...	Started	Duration	Size	Backup Ty...	Destinati...
■	Jan 11, 2022 10:26:59 AM	00h 01m 17s	4.51 TB	Data Back...	Snapshot
■	Jan 11, 2022 8:40:02 AM	00h 27m 11s	4.51 TB	Data Back...	Snapshot
■	Jan 11, 2022 1:00:58 AM	04h 05m 39s	3.82 TB	Data Back...	File
■	Jan 9, 2022 4:40:03 PM	00h 01m 23s	4.51 TB	Data Back...	Snapshot
■	Jan 9, 2022 8:00:02 AM	02h 39m 04s	3.82 TB	Data Back...	File
■	Jan 9, 2022 12:40:03 AM	00h 01m 18s	4.51 TB	Data Back...	Snapshot
■	Jan 8, 2022 4:40:03 PM	00h 01m 18s	4.51 TB	Data Back...	Snapshot
■	Jan 8, 2022 8:40:03 AM	00h 01m 22s	4.51 TB	Data Back...	Snapshot
■	Jan 8, 2022 12:40:03 AM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 7, 2022 4:40:03 PM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 7, 2022 8:40:02 AM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 7, 2022 12:40:02 AM	00h 01m 20s	4.51 TB	Data Back...	Snapshot
■	Jan 6, 2022 4:40:02 PM	00h 01m 18s	4.51 TB	Data Back...	Snapshot
■	Jan 6, 2022 8:40:03 AM	00h 01m 17s	4.51 TB	Data Back...	Snapshot
■	Jan 6, 2022 12:40:03 AM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 5, 2022 4:40:03 PM	00h 01m 19s	4.51 TB	Data Back...	Snapshot

File-based backup: 4 hours 05 min
(~270 MB/s throughput)

04h 05m 39s	3.82 TB	Data Back...	File
-------------	---------	--------------	------

Snapshot backup: 1 min 20 sec

00h 01m 18s	4.51 TB	Data Back...	Snapshot
00h 01m 22s	4.51 TB	Data Back...	Snapshot
00h 01m 19s	4.51 TB	Data Back...	Snapshot

Backup runtime reduced by 99%

Comparação do objetivo de tempo de recuperação

Esta seção fornece uma comparação entre o objetivo de tempo de recuperação (rto) de backups Snapshot baseados em arquivo e baseados em storage. 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 de cópia Snapshot do storage, o tempo de restauração é independente do tamanho do banco de dados e está sempre dentro de alguns segundos.

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.

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.

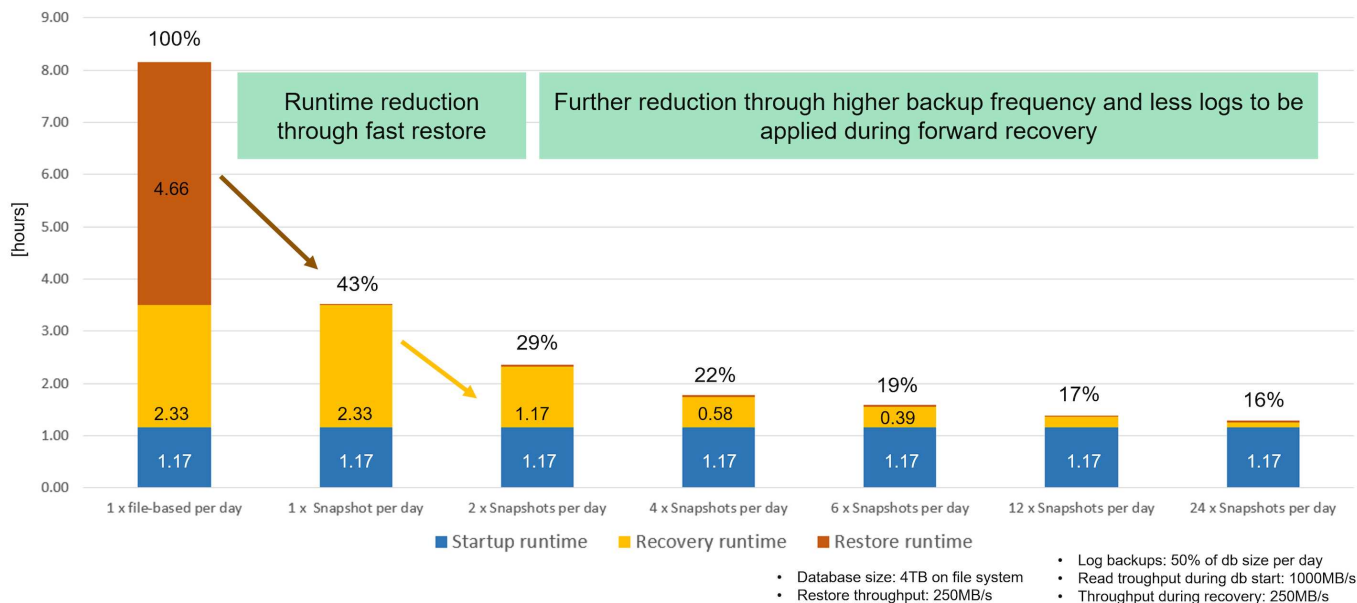
Os backups de snapshot geralmente são programados com uma frequência maior, porque não influenciam o desempenho do banco de dados SAP HANA. Por exemplo, se os backups Snapshot forem agendados a cada seis horas, o tempo de recuperação seria, no pior dos casos, um quarto do tempo de recuperação para um backup baseado em arquivo (6 horas / 24 horas, ou seja, 25%).

A figura a seguir mostra uma comparação das operações de restauração e recuperação com um backup diário baseado em arquivos e backups 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.

Restore and Recovery of a 4TB HANA Database (8TB RAM)



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.

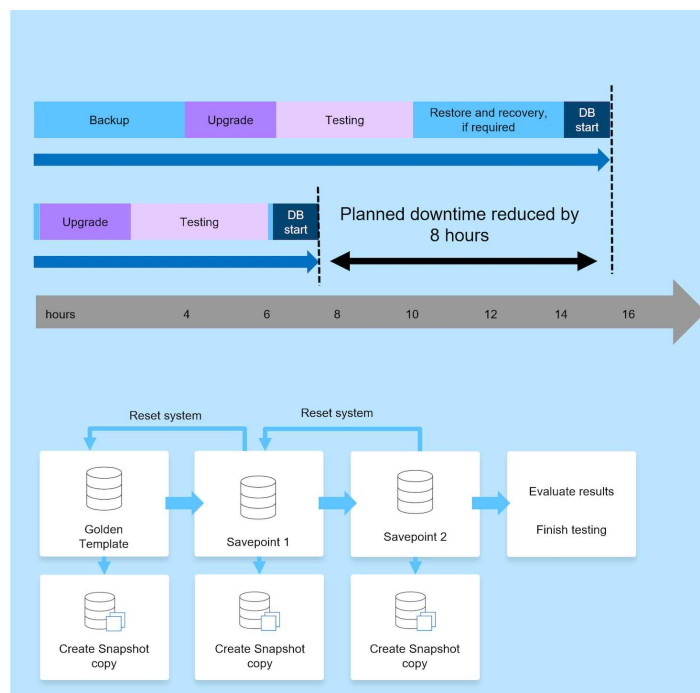
A atualização do sistema do SAP HANA é um exemplo de onde um backup sob demanda antes da atualização e uma possível operação de restauração se a atualização falhar tem um impactos significativo sobre o tempo de inatividade planejado geral. Com o exemplo de um banco de dados 4TB, você pode reduzir o tempo de inatividade planejado em 8 horas usando as operações de backup e restauração baseadas no Snapshot.

Outro exemplo de caso de uso seria um ciclo de teste típico, em que o teste deve ser feito em várias 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 se um teste falhar ou precisar ser repetido. Isso permite que o teste termine mais cedo ou permite mais testes ao mesmo tempo e melhora os resultados do teste.

Use Cases for Backup and Recovery Operations

- Accelerate HANA system upgrade operations
 - Fast on-demand backup before HANA system upgrade
 - Fast restore operation in case of an upgrade failure
 - Reduction of planned downtime

- Accelerate test cycles
 - Fast creation of savepoints after a successful step
 - Fast reset of system to any savepoint
 - Repeat step until successful



Quando os backups Snapshot são implementados, eles podem ser usados para lidar com vários outros casos de uso, o que exige cópias de um banco de DADOS HANA. Com o FSX for ONTAP, você pode criar um novo volume com base no conteúdo de qualquer backup instantâneo disponível. O tempo de execução desta operação é de alguns segundos, independente do tamanho do volume.

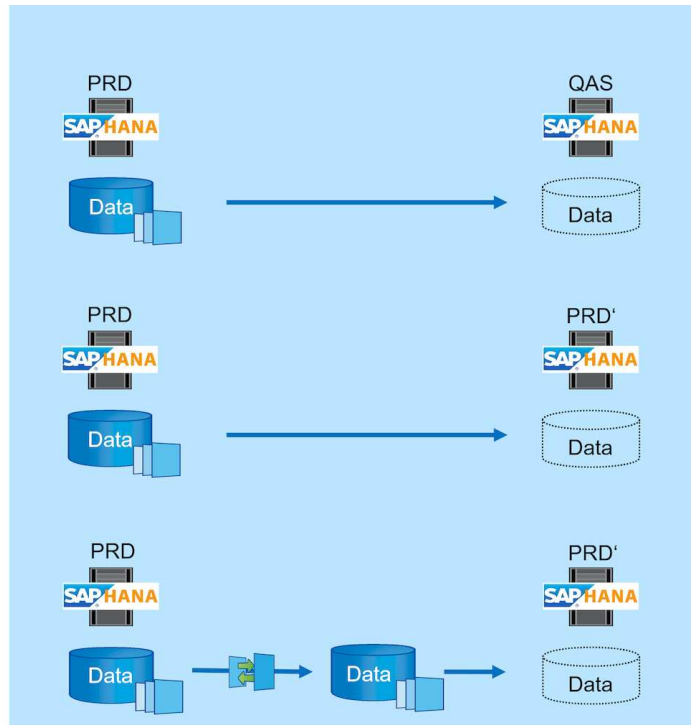
O caso de uso mais popular é o SAP System Refresh, onde os dados do sistema de produção precisam ser copiados para o sistema de teste ou QA. Ao aproveitar o recurso de clonagem do FSX for ONTAP, você pode provisionar o volume do sistema de teste a partir de qualquer cópia Snapshot do sistema de produção em questão de segundos. Então, o novo volume precisa ser anexado ao sistema de teste e o banco de dados HANA será recuperado.

O segundo caso de uso é a criação de um sistema de reparo, que é usado para resolver uma corrupção lógica no sistema de produção. Nesse 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 antes que a corrupção ocorra. O sistema de reparação é então utilizado para analisar o problema e exportar os dados necessários antes de ser corrompido.

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 e o objetivo do ponto de recuperação (RPO) da configuração de recuperação de desastres. Quando a replicação do FSX for ONTAP NetApp SnapMirror é usada para replicar os dados para o local de recuperação de desastres, os backups do Snapshot de produção também estão disponíveis no local de recuperação de desastres e podem ser usados para criar um novo volume para testes de recuperação de desastres.

Use Cases for Cloning Operations

- SAP System Refresh
 - Fast creation of a new volume based on a production Snapshot backup
 - Attach volume to the test system and recover HANA database with SID change
- Repair System creation to address logical corruption
 - Fast creation of a new volume based on a production Snapshot backup
 - Attach volume to the repair system and recover HANA database w/o SID change
- Disaster Recovery testing
 - Combined with SnapMirror Replication
 - Attach storage clone from a replicated production Snapshot backup to a DR test system



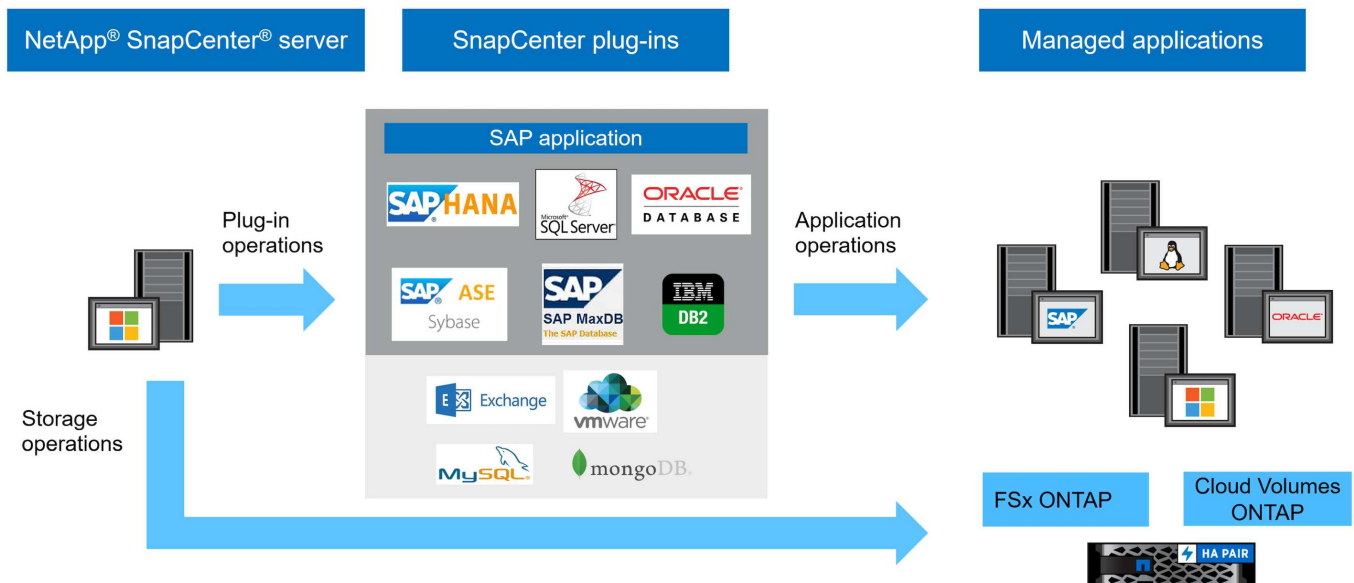
Arquitetura da SnapCenter

O SnapCenter é uma plataforma unificada e dimensionável para proteção de dados consistente com aplicações. O SnapCenter fornece controle e supervisão centralizados, enquanto delega a capacidade de os usuários gerenciarem tarefas de backup, restauração e clonagem específicas de aplicações. Com o SnapCenter, os administradores de banco de dados e storage aprendem uma única ferramenta para gerenciar operações de backup, restauração e clonagem de uma variedade de aplicações e bancos de dados.

O SnapCenter gerencia dados em pontos de extremidade no data fabric com tecnologia NetApp. Use o SnapCenter para replicar dados entre ambientes locais, entre ambientes locais e a nuvem e entre nuvens privadas, híbridas ou públicas.

Componentes do SnapCenter

O SnapCenter inclui o servidor SnapCenter, o pacote de plug-ins SnapCenter para Windows e o pacote de plug-ins SnapCenter para Linux. Cada pacote contém plug-ins do SnapCenter para vários aplicativos e componentes de infraestrutura.



Solução de backup SAP HANA da SnapCenter

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 volume que não é de dados com cópias Snapshot baseadas em storage (por exemplo /hana/shared,)
 - Verificações de integridade de bloco de banco de dados usando um backup baseado em arquivo
 - Replicação para um local de backup ou recuperação de desastres externo
- Manutenção do catálogo de backup do SAP HANA
 - Para backups de DADOS HANA (Snapshot e baseados em arquivo)
 - Para backups de log DO HANA
- Operações de restauração e recuperação
 - Restauração e recuperação automatizadas
 - Operações de restauração de localitário único para sistemas SAP HANA (MDC)

Os backups de arquivos de dados de banco de dados são executados pelo SnapCenter em combinação com o plug-in para SAP HANA. O plug-in aciona o ponto salvo do backup do banco de dados SAP HANA. Assim, as cópias Snapshot, criadas no sistema de storage primário, baseiam-se em uma imagem consistente do banco de dados SAP HANA.

O SnapCenter permite a replicação de imagens consistentes de bancos de dados para um local de backup ou recuperação de desastres externo usando o SnapVault ou o recurso SnapMirror. Em geral, diferentes políticas de retenção são definidas para backups no storage primário e externo. O SnapCenter manipula a retenção no storage primário, e o ONTAP manipula a retenção no storage de backup externo.

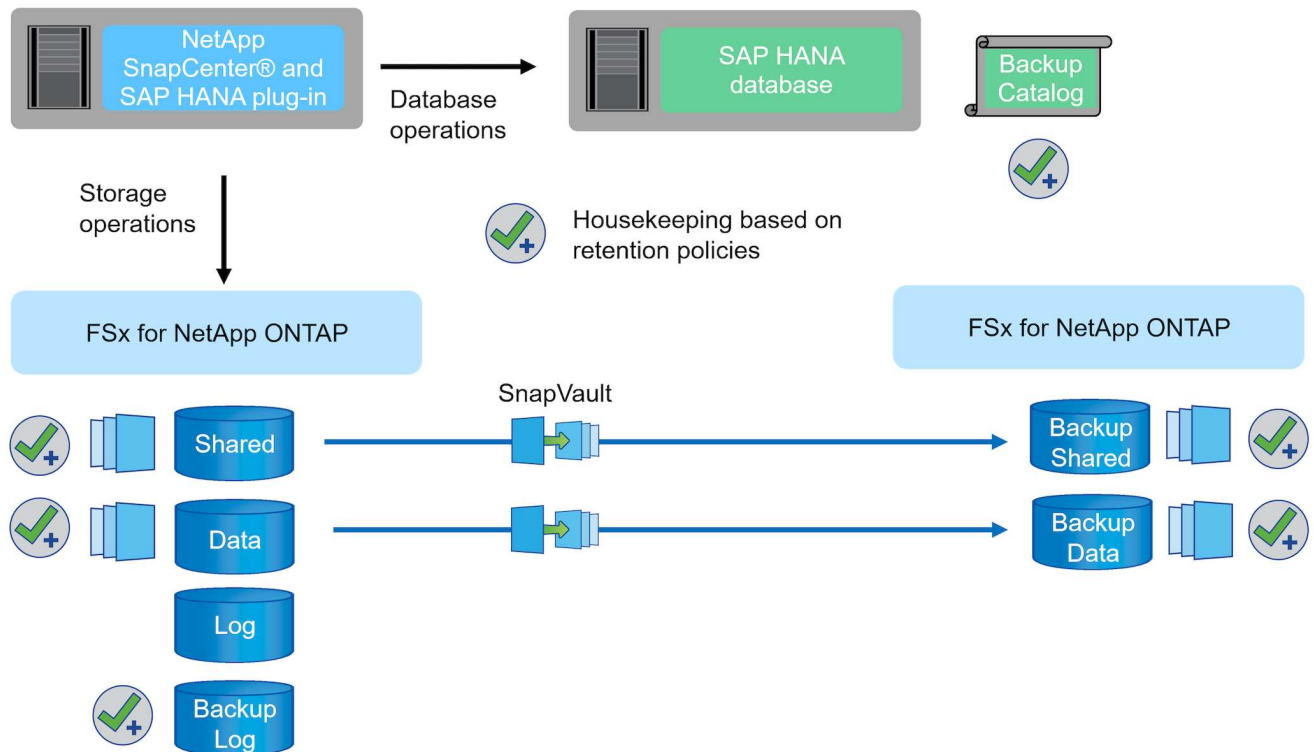
Para permitir um backup completo de todos os recursos relacionados ao SAP HANA, o SnapCenter também permite fazer backup de todos os volumes que não são de dados usando o plug-in SAP HANA com cópias Snapshot baseadas em storage. Você pode agendar volumes que não sejam de dados de forma independente do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

proteção.

A SAP recomenda combinar backups Snapshot baseados em storage com um backup semanal baseado em arquivo para executar uma verificação de integridade de bloco. Você pode executar a verificação de integridade de bloco a partir do SnapCenter. Com base em suas políticas de retenção configuradas, o SnapCenter gerencia o serviço de manutenção dos backups de arquivos de dados no storage primário, backups de arquivos de log e no catálogo de backup do SAP HANA.

O SnapCenter lida com a retenção no armazenamento primário, enquanto o FSX for 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:

1. Cria um ponto salvo do backup do SAP HANA para criar uma imagem consistente na camada de persistência.
2. Cria uma cópia Snapshot baseada em storage do volume de dados.
3. Registra o backup do Snapshot baseado em storage no catálogo de backup do SAP HANA.
4. Libera o ponto salvo do backup do SAP HANA.
5. Executa uma atualização do SnapVault ou do SnapMirror para o volume de dados, se configurado.
6. Exclui cópias Snapshot de storage no storage primário com base nas políticas de retenção definidas.
7. Exclui entradas do catálogo de backup do SAP HANA se os backups não existirem mais no storage de backup primário ou externo.
8. Sempre que um backup foi excluído com base na política de retenção ou manualmente, o SnapCenter também exclui todos os backups de log mais antigos do que o backup de dados mais antigo. Os backups

de log são excluídos no sistema de arquivos e no catálogo de backup do SAP HANA.

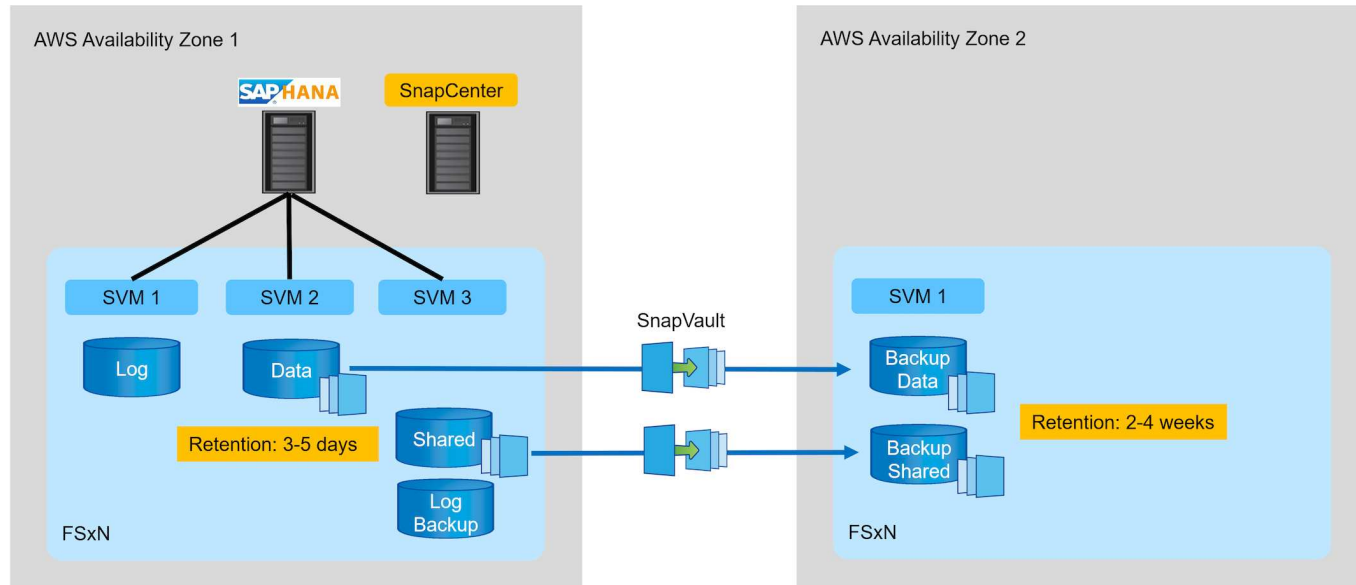
Âmbito deste documento

Este documento descreve a opção de configuração mais comum do SnapCenter para um sistema SAP HANA MDC de host único com um único locatário no FSx para ONTAP. Outras opções de configuração são possíveis e, em alguns casos, necessárias para sistemas SAP HANA específicos, por exemplo, para um sistema com múltiplos hosts. Para obter uma descrição detalhada sobre outras opções de configuração, consulte ["Conceitos e melhores práticas da SnapCenter \(NetApp.com\)"](#).

Neste documento, usamos o console do Amazon Web Services (AWS) e a CLI do FSX for ONTAP para executar as etapas de configuração necessárias na camada de armazenamento. Você também pode usar o Gerenciador de nuvem do NetApp para gerenciar o FSX for ONTAP, mas isso está fora do escopo deste documento. Para obter informações sobre como usar o Gerenciador de nuvem do NetApp para o FSX for ONTAP, ["Saiba mais sobre o Amazon FSX for ONTAP \(NetApp.com\)"](#) consulte .

Estratégia de proteção de dados

A figura a seguir mostra uma arquitetura típica de backup para SAP HANA no FSX for ONTAP. O sistema HANA está localizado na zona de disponibilidade da AWS 1 e está usando um sistema de arquivos FSX for ONTAP dentro da mesma zona de disponibilidade. As operações de backup Snapshot são executadas para os dados e o volume compartilhado do banco de DADOS HANA. Além dos backups Snapshot locais, mantidos por 3-5 dias, os backups também são replicados para um storage externo para retenção de longo prazo. O armazenamento de backup externo é um segundo sistema de arquivos FSX for ONTAP localizado em uma zona de disponibilidade diferente da AWS. Os backups dos DADOS HANA e do volume compartilhado são replicados com o SnapVault para o segundo sistema de arquivos FSX for ONTAP e são mantidos por 2-3 semanas.



Antes de configurar o SnapCenter, 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 seguintes parâmetros devem ser definidos:

- 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 principais devem ser replicados para um local de backup externo?
- Por quanto tempo os backups devem ser mantidos no armazenamento de backup externo?

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, uma alta frequência de backup foi definida e os backups são replicados para um local de backup externo uma vez por dia. Os sistemas de teste têm requisitos menores e nenhuma 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 6 horas
Retenção primária	3 dias	3 dias	3 dias
Verificação de integridade do bloco	Uma vez por semana	Uma vez por semana	Não
Replicação para um local de backup externo	Uma vez por dia	Uma vez por dia	Não
Retenção de backup externo	2 semanas	2 semanas	Não aplicável

A tabela a seguir mostra as políticas que devem ser configuradas para os parâmetros de proteção de dados.

Parâmetros	Política LocalSnap	Política LocalSnapAndSnapVault	Bloqueio de políticas IntegrityCheck
Tipo de cópia de segurança	Baseado em snapshot	Baseado em snapshot	Baseado em arquivo
Frequência de programação	Por hora	Diariamente	Semanalmente
Retenção primária	Contagem: 12	Contagem: 3	Contagem: 1
Replicação SnapVault	Não	Sim	Não aplicável

A política `LocalSnapshot` é usada nos sistemas de produção, desenvolvimento e teste para cobrir os backups Snapshot locais com uma retenção de dois dias.

Na configuração de proteção de recursos, a programação é definida de forma diferente para os tipos de sistema:

- Produção: Cronograma a cada 4 horas.
- Desenvolvimento: Agendar a cada 4 horas.
- Teste: Agendar a cada 4 horas.

A política `LocalSnapAndSnapVault` é usada para os sistemas de produção e desenvolvimento para cobrir a replicação diária para o storage de backup externo.

Na configuração de proteção de recursos, o cronograma é definido para produção e desenvolvimento:

- Produção: Cronograma todos os dias.
- Desenvolvimento: Programe todos os dias. A política `BlockIntegrityCheck` é usada para os sistemas de produção e desenvolvimento para cobrir a verificação semanal da integridade do bloco usando um backup baseado em arquivo.

Na configuração de proteção de recursos, o cronograma é definido para produção e desenvolvimento:

- Produção: Cronograma a cada semana.
- Desenvolvimento: Agendar todas as semanas.

Para cada banco de dados SAP HANA individual que usa a política de backup externo, é necessário configurar uma relação de proteção na camada de storage. A relação de proteção define quais volumes são replicados e a retenção de backups no storage de backup externo.

Com o exemplo a seguir, para cada sistema de produção e desenvolvimento, uma retenção de duas semanas é definida no storage de backup externo.

Neste exemplo, as políticas de proteção e a retenção para recursos de banco de dados do SAP HANA e recursos de volume não são diferentes.

Exemplo de configuração do laboratório

A configuração do laboratório a seguir foi usada como um exemplo de configuração para o restante deste documento.

PFX do sistema HANA:

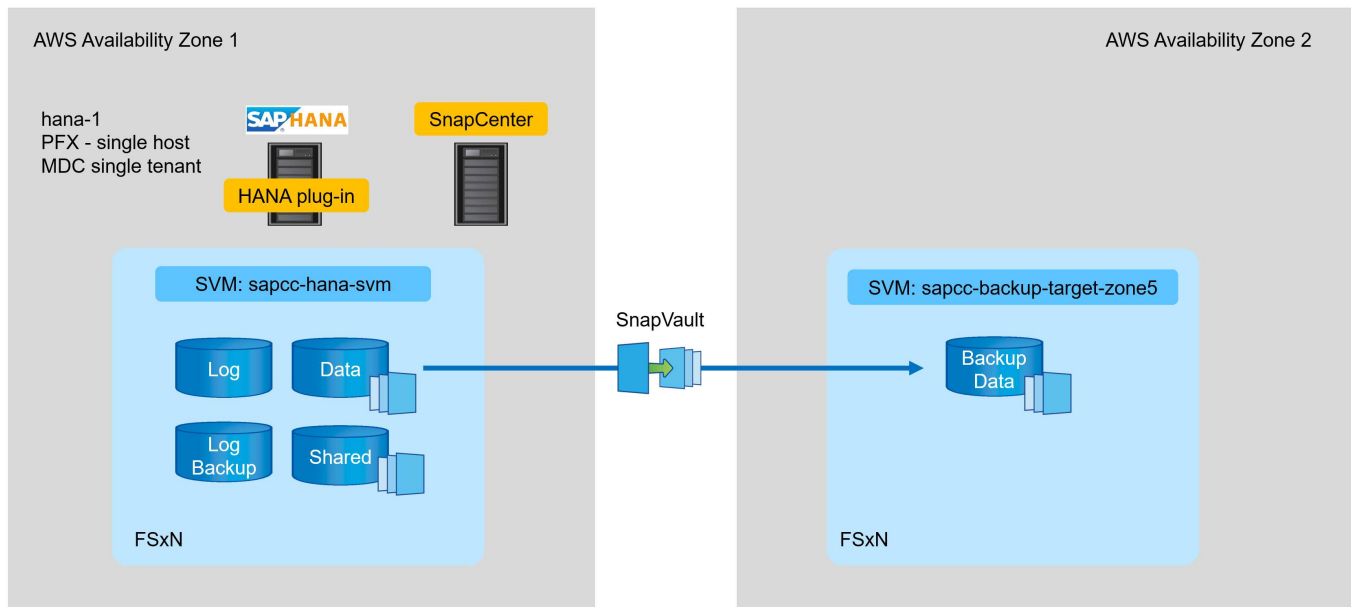
- Sistema MDC de host único com um único locatário
- HANA 2,0 SPS 6 revisão 60
- SLES PARA SAP 15SP3

SnapCenter -

- Versão 4,6
- Plug-in HANA e Linux implantado em um host de banco de dados HANA

FSX para sistemas de arquivos ONTAP:

- Dois sistemas de arquivos FSX para ONTAP com uma única máquina virtual de armazenamento (SVM)
- Cada sistema FSX for ONTAP em uma zona de disponibilidade da AWS diferente
- Volume de DADOS HANA replicado para o segundo sistema de arquivos FSX for ONTAP



Configuração do SnapCenter

Siga as etapas nesta seção para a configuração de SnapCenter de base e a proteção do recurso HANA.

Visão geral das etapas de configuração

Siga as etapas a seguir para a configuração de SnapCenter de base e a proteção do recurso HANA. Cada passo é descrito em detalhes nos capítulos seguintes.

1. Configurar o usuário de backup do SAP HANA e a chave hdbuserstore. Usado para acessar o banco de dados HANA com o cliente hdbsql.
2. Configurar o armazenamento no SnapCenter. Credenciais para acessar os SVMs do FSX para ONTAP a partir do SnapCenter
3. Configurar credenciais para implantação de plug-in. Usado para implantar e instalar automaticamente os plug-ins do SnapCenter necessários no host do banco de dados HANA.
4. Adicionar host HANA ao SnapCenter. Implanta e instala os plug-ins do SnapCenter necessários.
5. Configurar políticas. Define o tipo de operação de backup (Snapshot, arquivo), as retenções, bem como a replicação opcional de backup do Snapshot.
6. Configurar a proteção de recursos DO HANA. Forneça a chave do hdbuserstore e anexe políticas e programações ao recurso HANA.

Configuração do usuário de backup do SAP HANA e do hdbuserstore

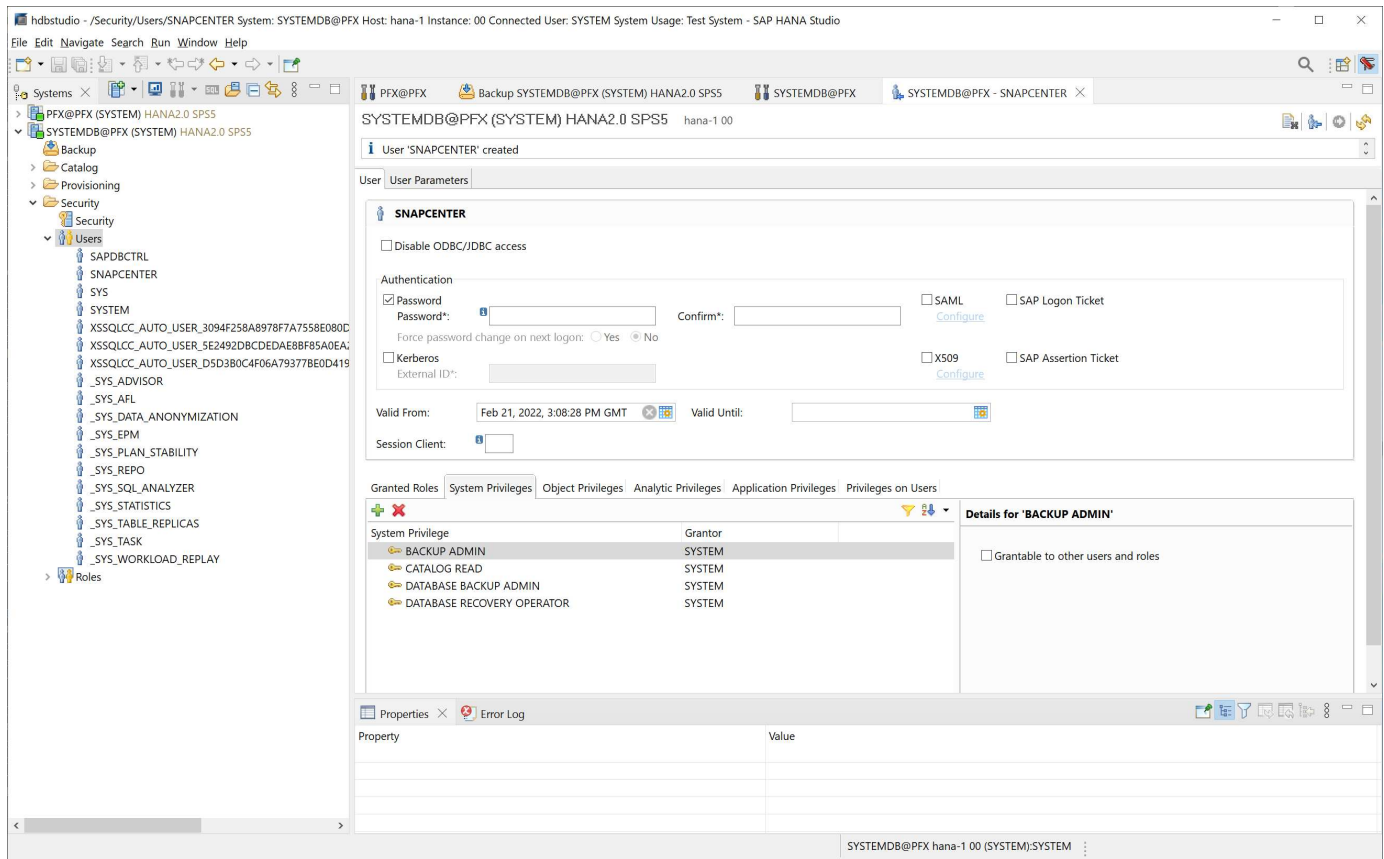
A NetApp recomenda configurar um usuário de banco de dados dedicado no banco de DADOS HANA para executar as operações de backup com o SnapCenter. Na segunda etapa, uma chave de armazenamento de usuário SAP HANA é configurada para esse usuário de backup e essa chave de armazenamento de usuário é usada na configuração do plug-in SAP HANA do SnapCenter.

A figura a seguir mostra o SAP HANA Studio através do qual você pode criar o usuário de backup

Os Privileges necessários são alterados com a versão HANA 2,0 SPS5: Administração de backup, leitura de

catálogo, administração de backup de banco de dados e operador de recuperação de banco de dados. Para versões anteriores, o administrador de backup e a leitura do catálogo são suficientes.

Para um sistema SAP HANA MDC, você deve criar o usuário no banco de dados do sistema porque todos os comandos de backup para o sistema e os bancos de dados de locatário são executados usando o banco de dados do sistema.



O comando a seguir é usado para a configuração do armazenamento do usuário com o <sid>adm usuário:

```
hdbuserstore set <key> <host>:<port> <database user> <password>
```

O SnapCenter usa o <sid>adm usuário para se comunicar com o banco de DADOS HANA. Portanto, você deve configurar a chave de armazenamento de usuário usando o usuário 'id>adm' no host do banco de dados. Normalmente, o software cliente SAP HANA hdbsql é instalado juntamente com a instalação do servidor de banco de dados. Se este não for o caso, você deve instalar o hdbclient primeiro.

Em uma configuração SAP HANA MDC, a porta 3<instanceNo>13 é a porta padrão para o acesso SQL ao banco de dados do sistema e deve ser usada na configuração hdbuserstore.

Para uma configuração de vários hosts do SAP HANA, você deve configurar chaves de armazenamento de usuários para todos os hosts. O SnapCenter tenta se conectar ao banco de dados usando cada uma das chaves fornecidas e, portanto, pode operar independentemente de um failover de um serviço SAP HANA para um host diferente. Em nossa configuração de laboratório, nós configuramos uma chave de armazenamento de usuário para o usuário pfxadm para nosso sistema PFX, que é um único sistema HANA MDC de host com um único locatário.

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore set PFXKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore list
DATA FILE      : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE       : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.KEY
ACTIVE RECORDS : 7
DELETED RECORDS : 0
KEY PFXKEY
  ENV : hana-1:30013
  USER: SNAPCENTER
KEY PFXSAPDBCTRL
  ENV : hana-1:30013
  USER: SAPDBCTRL
Operation succeed.
```

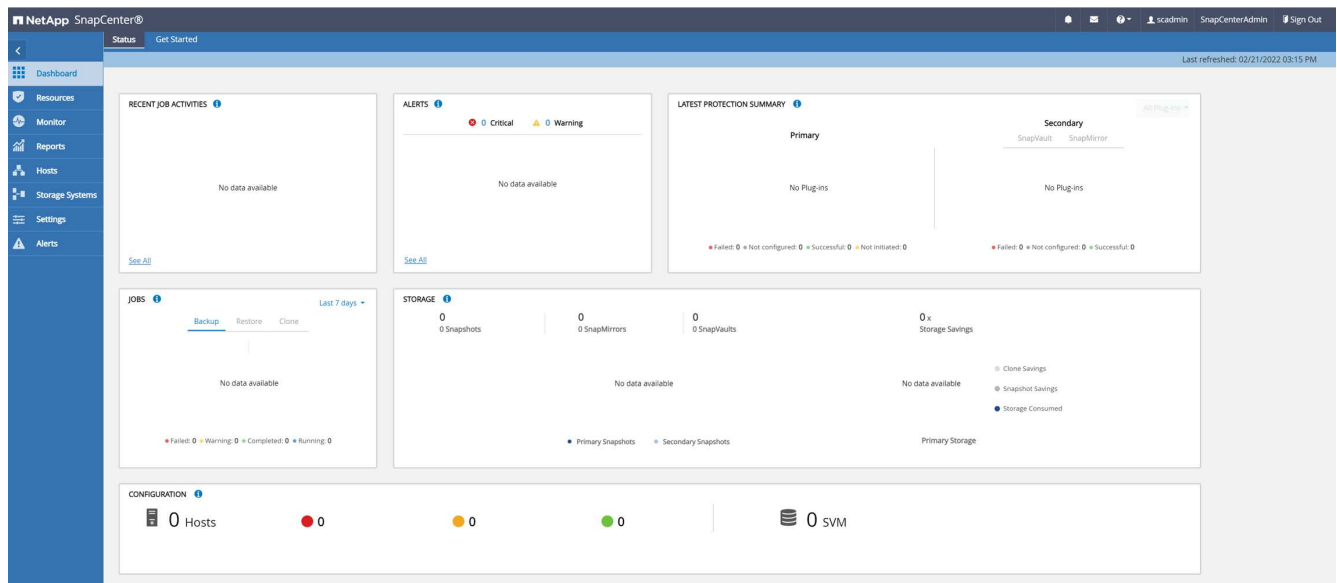
Você pode verificar o acesso ao banco de dados do sistema HANA que usa a chave com o `hdbsql` comando.

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbsql -U PFXKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=>
```

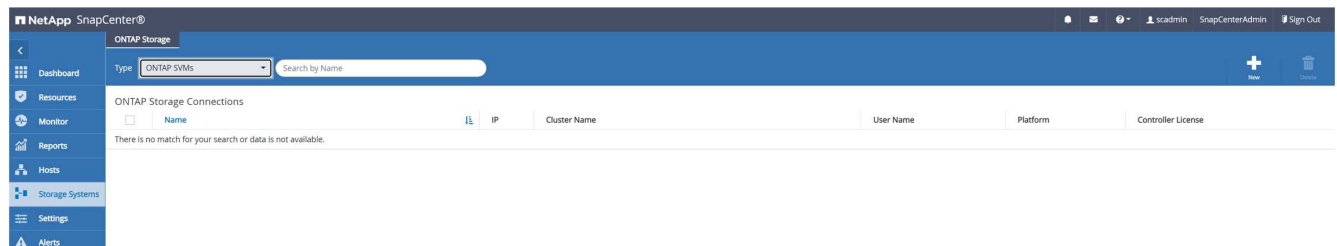
Configurar o armazenamento

Siga estas etapas para configurar o armazenamento no SnapCenter.

1. Na IU do SnapCenter, selecione sistemas de armazenamento.

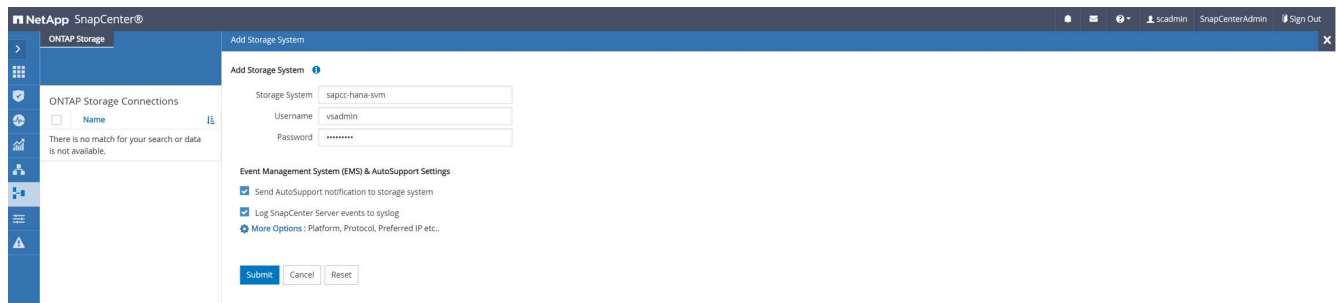


Você pode selecionar o tipo de sistema de storage, que pode ser ONTAP SVMs ou clusters ONTAP. No exemplo a seguir, o gerenciamento da SVM é selecionado.



2. Para adicionar um sistema de storage e fornecer o nome de host e as credenciais necessárias, clique em novo.

O usuário SVM não precisa ser o usuário vsadmin, como mostrado na figura a seguir. Normalmente, um usuário é configurado no SVM e recebe as permissões necessárias para executar operações de backup e restauração. Para obter informações sobre o Privileges necessário, "[Guia de instalação do SnapCenter](#)" consulte a seção intitulada "ONTAP Privileges mínimo necessário".



3. Para configurar a plataforma de armazenamento, clique em mais opções.
4. Selecione All Flash FAS como o sistema de armazenamento para garantir que a licença, que faz parte do FSX for ONTAP, esteja disponível para SnapCenter.

More Options

Platform
All Flash FAS
Secondary
Protocol
HTTPS
Port
443
Timeout
60
seconds
Preferred IP
Save
Cancel

O SVM `sapcc-hana-svm` agora está configurado no SnapCenter.

NetApp SnapCenter®

ONTAP Storage
Type: ONTAP SVMs
Search by Name

ONTAP Storage Connections

Name	IP	IP	Cluster Name	User Name	Platform	Controller License
sapcc-hana-svm		198.19.255.9		vsadmin	AFF	✓

Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts

Crie credenciais para a implantação do plugin

Para permitir que o SnapCenter implante os plug-ins necessários nos HOSTS HANA, você deve configurar as credenciais do usuário.

- Vá para Configurações, selecione credenciais e clique em novo.

NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

Search by Credential Name

Credential Name	Authentication Mode	Details
There is no match for your search or data is not available.		

Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts

- Na configuração do laboratório, configuramos um novo usuário, `snapcenter`, no host HANA que é usado para a implantação do plug-in. Você deve ativar os privilégios de sudo, como mostrado na figura a seguir.

Credential

Credential Name

PluginOnLinux

Authentication Mode

Linux

Username

snapcenter

Password

☒ Use sudo privileges

Cancel

OK

```
hana-1:/etc/sudoers.d # cat /etc/sudoers.d/90-cloud-init-users
# Created by cloud-init v. 20.2-8.48.1 on Mon, 14 Feb 2022 10:36:40 +0000
# User rules for ec2-user
ec2-user ALL=(ALL) NOPASSWD:ALL
# User rules for snapcenter user
snapcenter ALL=(ALL) NOPASSWD:ALL
hana-1:/etc/sudoers.d #
```

Adicionar um host SAP HANA

Ao adicionar um host SAP HANA, o SnapCenter implanta os plug-ins necessários no host do banco de dados e executa operações de descoberta automática.

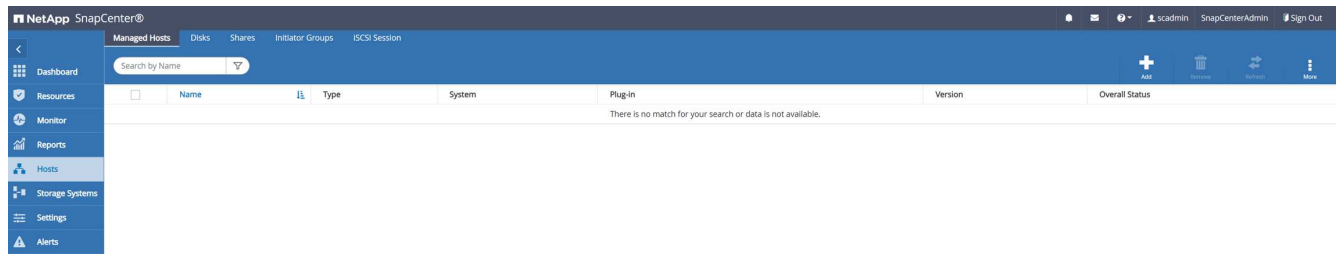
O plug-in SAP HANA requer Java versão 1,8 de 64 bits. O Java deve ser instalado no host antes que o host seja adicionado ao SnapCenter.

```
hana-1:/etc/ssh # java -version
openjdk version "1.8.0_312"
OpenJDK Runtime Environment (IcedTea 3.21.0) (build 1.8.0_312-b07 suse-
3.61.3-x86_64)
OpenJDK 64-Bit Server VM (build 25.312-b07, mixed mode)
hana-1:/etc/ssh #
```

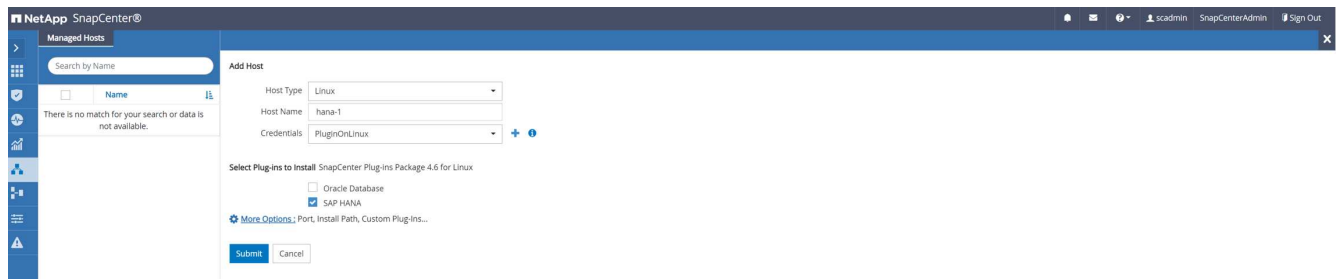
OpenJDK ou Oracle Java é suportado com SnapCenter.

Para adicionar o host SAP HANA, siga estas etapas:

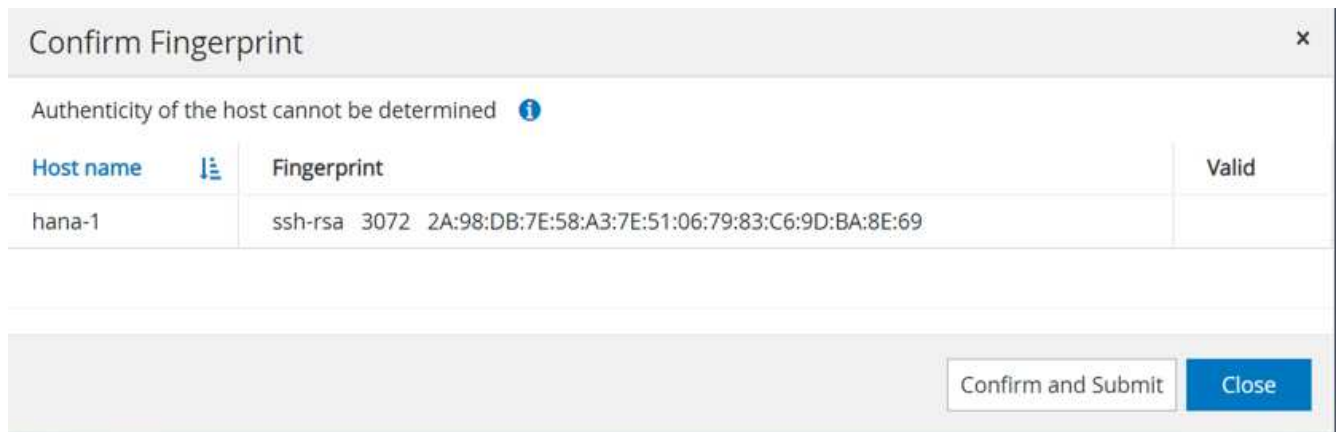
1. Na guia host, clique em Adicionar.



2. Forneça informações do host e selecione o plug-in SAP HANA a ser instalado. Clique em Enviar.

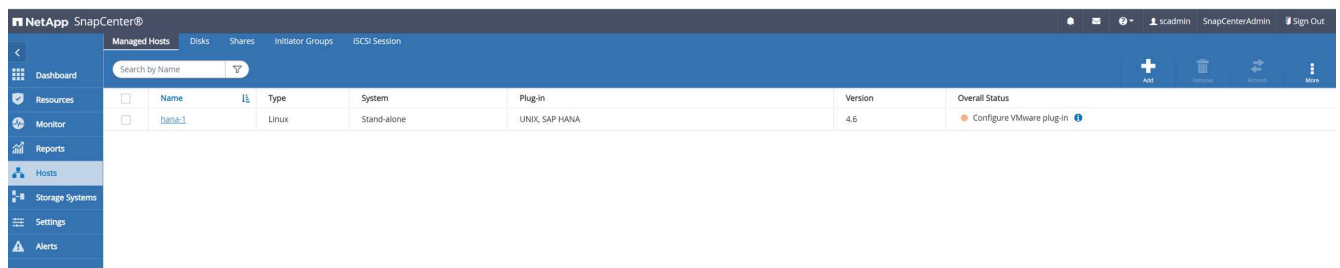


3. Confirme a impressão digital.

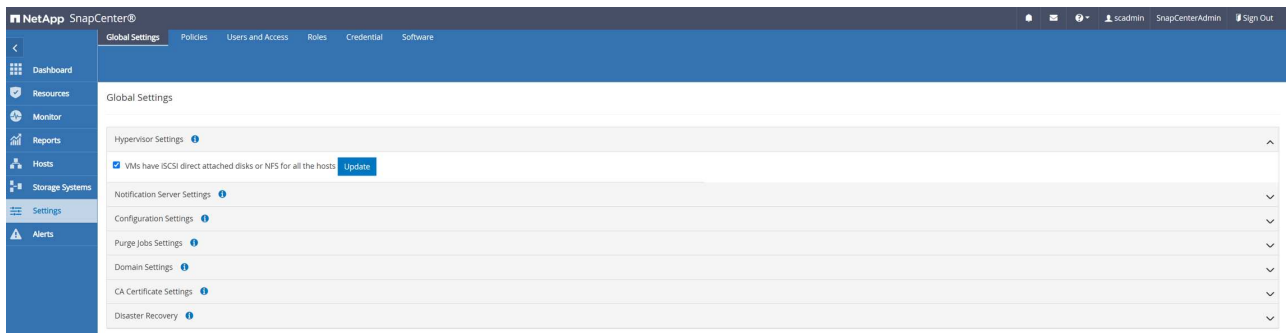


A instalação DO HANA e do plug-in Linux é iniciada automaticamente. Quando a instalação for concluída, a coluna de status do host mostra Configurar plug-in VMware. O SnapCenter detecta se o plug-in SAP HANA está instalado em um ambiente virtualizado. Esse pode ser um ambiente VMware ou um ambiente em um provedor de nuvem pública. Nesse caso, o SnapCenter exibe um aviso para configurar o hipervisor.

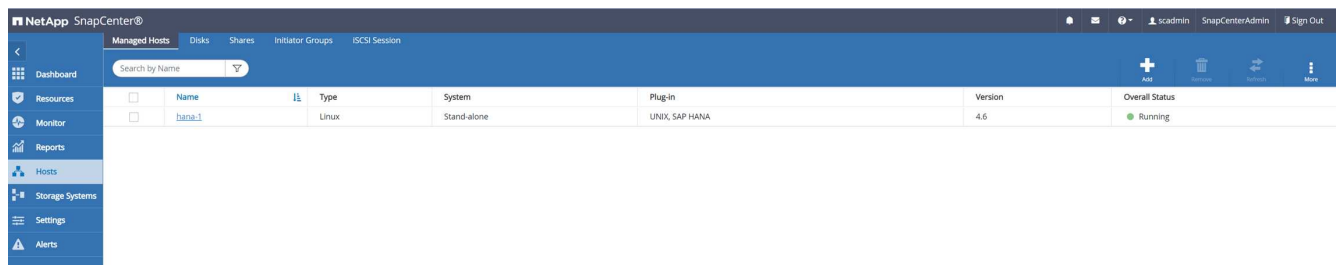
Você pode remover a mensagem de aviso usando as etapas a seguir.



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



A tela agora mostra o plug-in Linux e o plug-in HANA com o status em execução.



Configurar políticas

As políticas geralmente são configuradas independentemente do recurso e podem ser usadas por vários bancos de dados SAP HANA.

Uma configuração mínima típica consiste nas seguintes políticas:

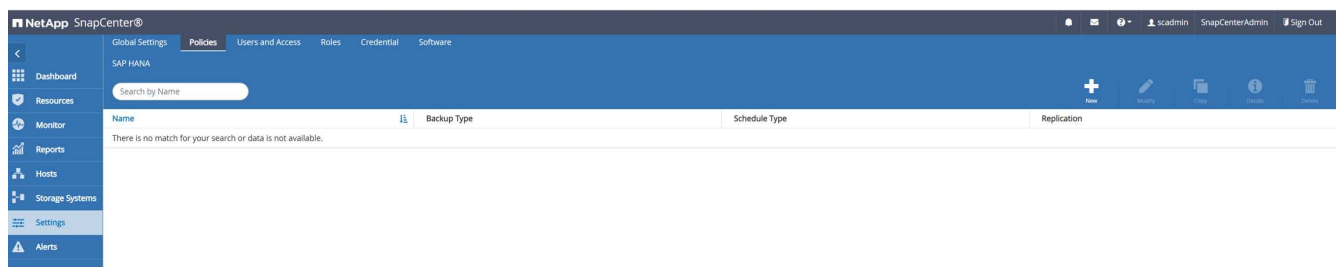
- Política para backups por hora sem replicação LocalSnap: .
- Política para verificação semanal de integridade de bloco usando um backup baseado em arquivo BlockIntegrityCheck: .

As seções a seguir descrevem a configuração dessas políticas.

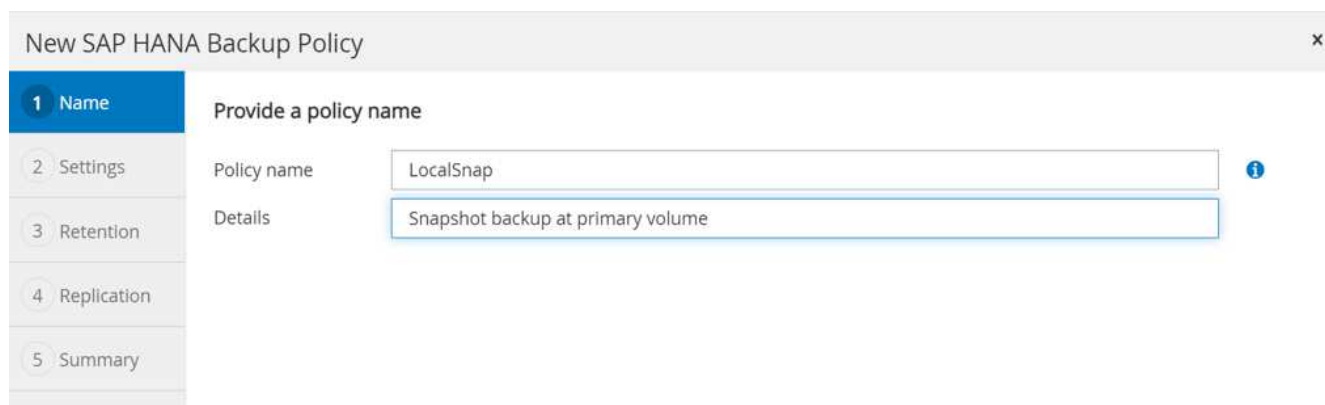
Política para backups Snapshot

Siga estas etapas para configurar políticas de backup do Snapshot.

1. Acesse a Definições > políticas e clique em novo.



2. Introduza o nome e a descrição da política. Clique em seguinte.



New SAP HANA Backup Policy

1 Name

Provide a policy name

Policy name: LocalSnap

Details: Snapshot backup at primary volume

2 Settings

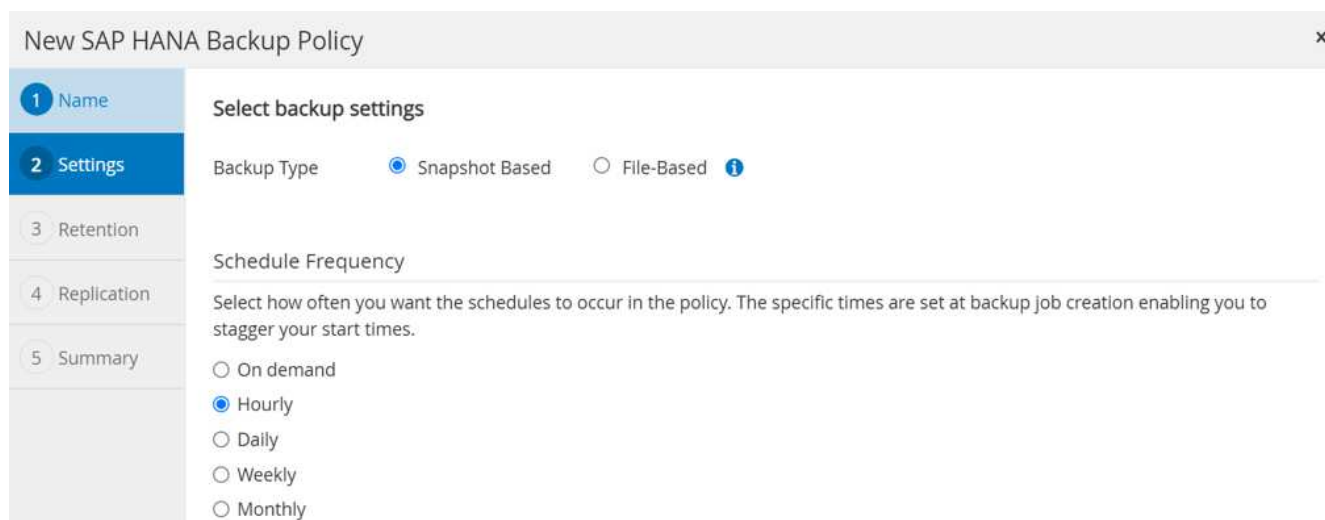
3 Retention

4 Replication

5 Summary

3. Selecione o tipo de cópia de segurança como Instantâneo e selecione hora para a frequência de programação.

A programação em si é configurada posteriormente com a configuração de proteção de recursos HANA.



New SAP HANA Backup Policy

1 Name

2 Settings

Select backup settings

Backup Type: ☒ Snapshot Based ☐ File-Based

Schedule Frequency

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

☐ On demand

☒ Hourly

☐ Daily

☐ Weekly

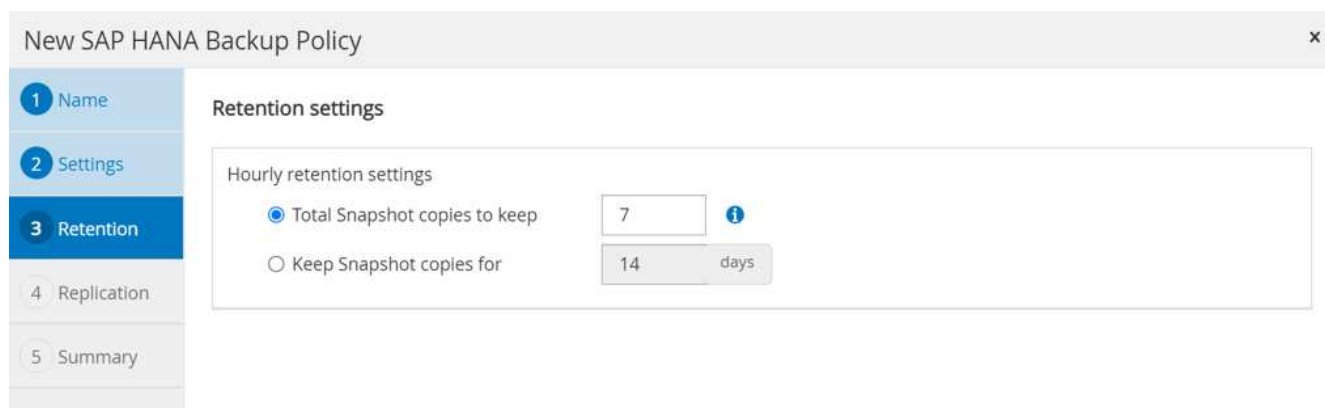
☐ Monthly

3 Retention

4 Replication

5 Summary

4. Configure as configurações de retenção para backups sob demanda.



New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

Retention settings

Hourly retention settings

☒ Total Snapshot copies to keep: 7

☐ Keep Snapshot copies for: 14 days

4 Replication

5 Summary

5. Configure as opções de replicação. Neste caso, não está selecionada nenhuma atualização do SnapVault ou do SnapMirror.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select secondary replication options i

☐ Update SnapMirror after creating a local Snapshot copy.
 ☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Choose i

Error retry count

3 i

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Summary

Policy name	LocalSnap
Details	Snapshot backup at primary volume
Backup Type	Snapshot Based Backup
Schedule Type	Hourly
Hourly backup retention	Total backup copies to retain : 7
Replication	none

A nova política está agora configurada.

NetApp SnapCenter®				
Global Settings Policies Users and Access Roles Credential Software SAP HANA Search by Name + ✎ 📄 ℹ 🗑				
Name	Backup Type	Schedule Type	Replication	
LocalSnap	Data Backup	Hourly		

Política para verificação de integridade de bloco

Siga estas etapas para configurar a política de verificação de integridade de bloco.

1. Aceda a Definições > políticas e clique em novo.
2. Introduza o nome e a descrição da política. Clique em seguinte.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name

BlockIntegrityCheck

Details

Check HANA DB blocks using file-based backup

3. Defina o tipo de cópia de segurança para File-Based e programe a frequência para Weekly (semanal). A programação em si é configurada posteriormente com a configuração de proteção de recursos HANA.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Select backup settings

Backup Type

☐ Snapshot Based
☒ File-Based

Schedule Frequency

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

☐ On demand
☐ Hourly
☐ Daily
☒ Weekly
☐ Monthly

4. Configure as configurações de retenção para backups sob demanda.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Retention settings

Weekly retention settings

☒ Total backup copies to keep

1

☐ Keep backup copies for

14

days

5. Na página Resumo, clique em concluir.

New SAP HANA Backup Policy ✕

1 Name

2 Settings

3 Retention

4 Summary

Summary

Policy name

BlockIntegrityCheck

Details

Check HANA DB blocks using file-based backup

Backup Type

File-Based Backup

Schedule Type

Weekly

Weekly backup retention

Total backup copies to retain : 1

NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

SAP HANA

Search by Name

Name	Backup Type	Schedule Type	Replication
BlockIntegrityCheck	File Based Backup	Weekly	
LocalSnap	Data Backup	Hourly	

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

Free Modify Copy Details Delete

Configurar e proteger um recurso HANA

Após a instalação do plug-in, o processo de descoberta automática do recurso HANA é iniciado automaticamente. Na tela recursos, um novo recurso é criado, que é marcado como bloqueado com o ícone de cadeado vermelho. Para configurar e proteger o novo recurso HANA, siga estas etapas:

1. Selecione e clique no recurso para continuar a configuração.

Você também pode acionar o processo de descoberta automática manualmente na tela recursos clicando em Atualizar recursos.

NetApp SnapCenter®

SAP HANA

View Multitenant Database Container Search databases

System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
PFX	PFX	PFX	None	hana-1				Not protected

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

Refresh Resources Add SAP HANA Database New Resource Group

2. Forneça a chave de armazenamento de usuários para o banco de dados HANA.

Configure Database

Plug-in host

hana-1

HDBSQL OS User

pfxadm

HDB Secure User Store Key

PFXKEY

Cancel

OK

O processo de descoberta automática de segundo nível começa no qual os dados do locatário e as informações de espaço físico do storage são descobertos.

NetApp SnapCenter®

SAP HANA

Search databases

System

PFX

Resource - Details

Details for selected resource

Type	Multitenant Database Container		
HANA System Name	PFX		
SID	PFX		
Tenant Databases	PFX		
Plug-in Host	hana-1		
HDB Secure User Store Key	PFXKEY		
HDBSQL OS User	pfxadm		
Log backup location	/backup/log		
Backup catalog location	/backup/log		
System Replication	None		
plug-in name	SAP HANA		
Last backup	None		
Resource Groups	None		
Policy	None		
Discovery Type	Auto		
Storage Footprint			
SVM	Volume	Junction Path	LUN/Qtree
sapcc-hana-svm	PFX_data_mnt00001	/PFX_data_mnt00001	

3. Na guia recursos, clique duas vezes no recurso para configurar a proteção de recursos.

NetApp SnapCenter®

SAP HANA

Search databases

Resources

System

System ID (SID)

Tenant Databases

Replication

Plug-in Host

Resource Groups

Policies

Last backup

Overall Status

PFX

PFX

PFX

None

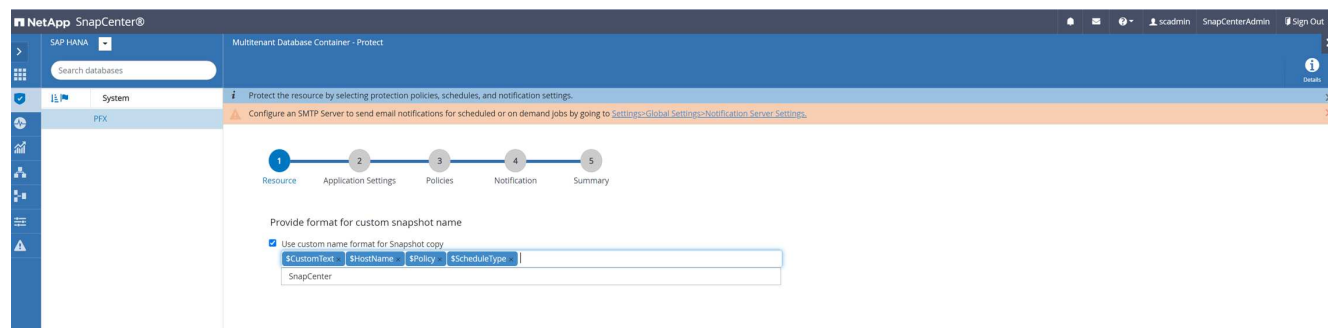
hana-1

Not protected

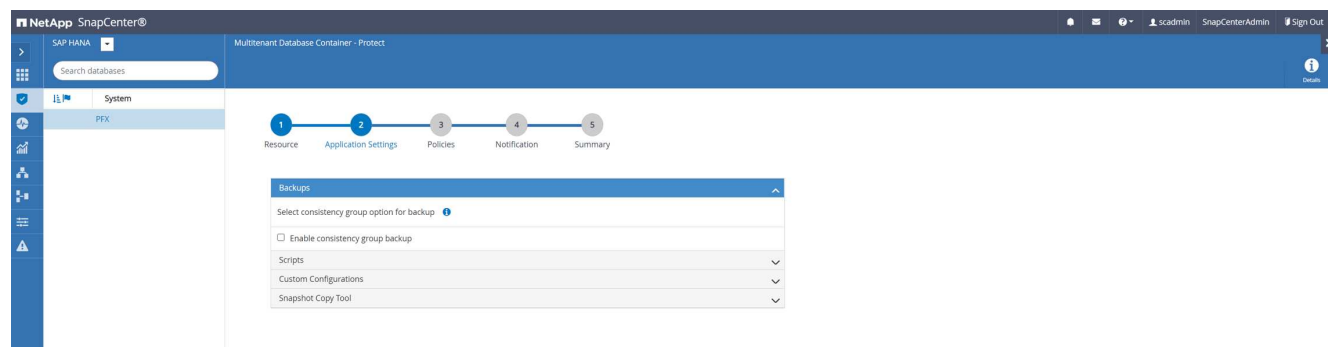
4. Configure um formato de nome personalizado para a cópia Snapshot.

A NetApp recomenda o uso de um nome de cópia Snapshot personalizado para identificar facilmente

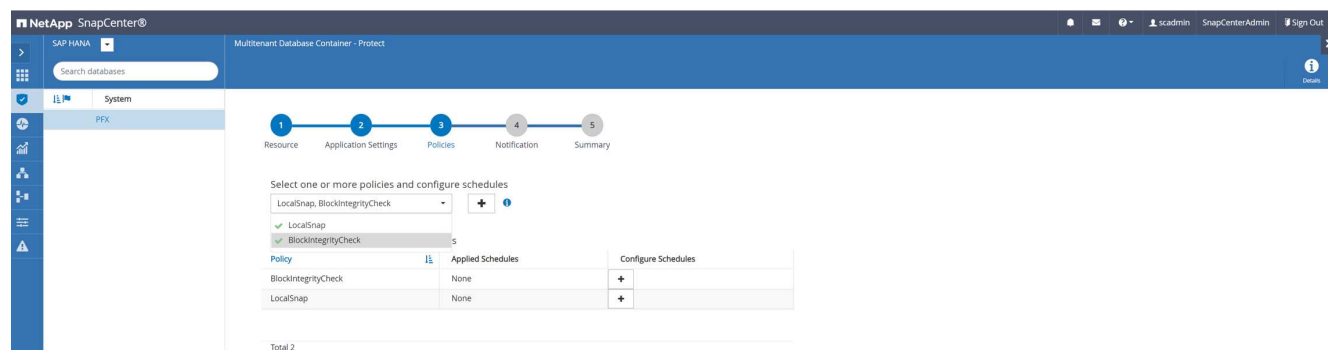
quais backups foram criados com qual tipo de política e agendamento. Ao adicionar o tipo de agendamento no nome da cópia Snapshot, você pode distinguir entre backups programados e sob demanda. A `schedule` name cadeia de caracteres para backups sob demanda está vazia, enquanto os backups programados incluem a cadeia `Hourly`, `Daily`, or `Weekly`.



5. Nenhuma configuração específica precisa ser feita na página Configurações do aplicativo. Clique em seguinte.



6. Selecione as políticas a serem adicionadas ao recurso.



7. Defina o agendamento para a política de verificação de integridade do bloco.

Neste exemplo, ele é definido para uma vez por semana.

Add schedules for policy BlockIntegrityCheck



Weekly

Start date

02/22/2022 12:00 pm



☐ Expires on

03/22/2022 12:00 pm



Days

Sunday

✓ Sunday

Monday

Tuesday

Wednesday

Thursday

Friday



The schedules are triggered in the SnapCenter Server time zone.



Cancel

OK

8. Defina o agendamento para a política Snapshot local.

Neste exemplo, ele é definido para cada 6 horas.

Modify schedules for policy LocalSnap



Hourly

Start date

02/22/2022 02:00 pm



☐ Expires on

04/28/2022 11:57 am



Repeat every

6

hours

0

mins



The schedules are triggered in the SnapCenter Server time zone.



Cancel

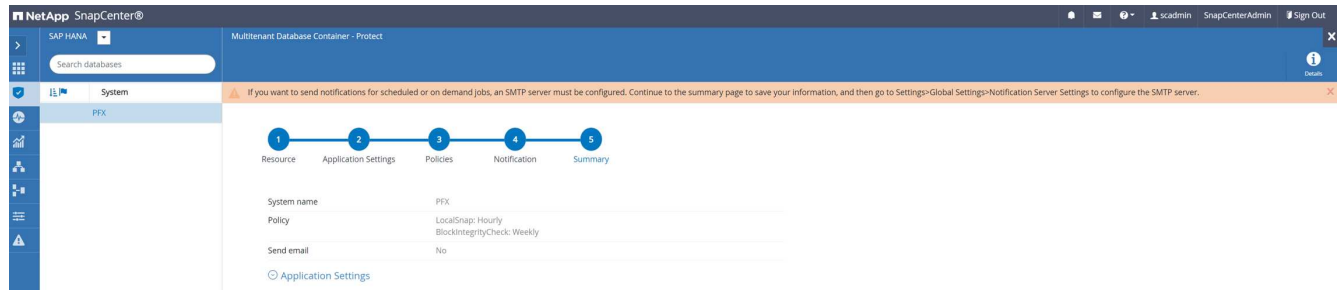
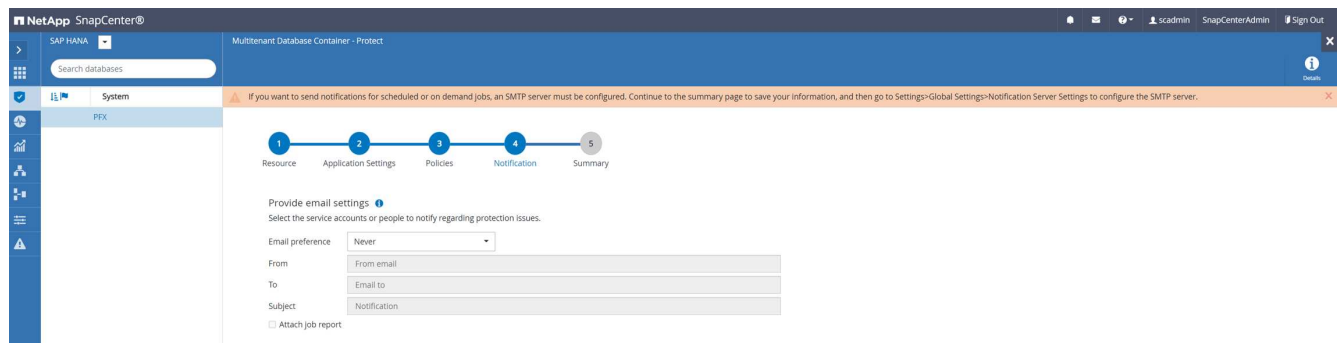
OK

The screenshot shows the NetApp SnapCenter interface. The left sidebar contains navigation icons for System, PFX, and other resources. The main area displays the configuration for the 'LocalSnap' policy. A progress bar at the top indicates the steps: 1. Resource, 2. Application Settings, 3. Policies, 4. Notification, 5. Summary. The 'Policies' step is currently active. Below the progress bar, there is a section titled 'Select one or more policies and configure schedules' with a dropdown menu showing 'LocalSnap, BlockIntegrityCheck'. Below this, there is a table titled 'Configure schedules for selected policies'.

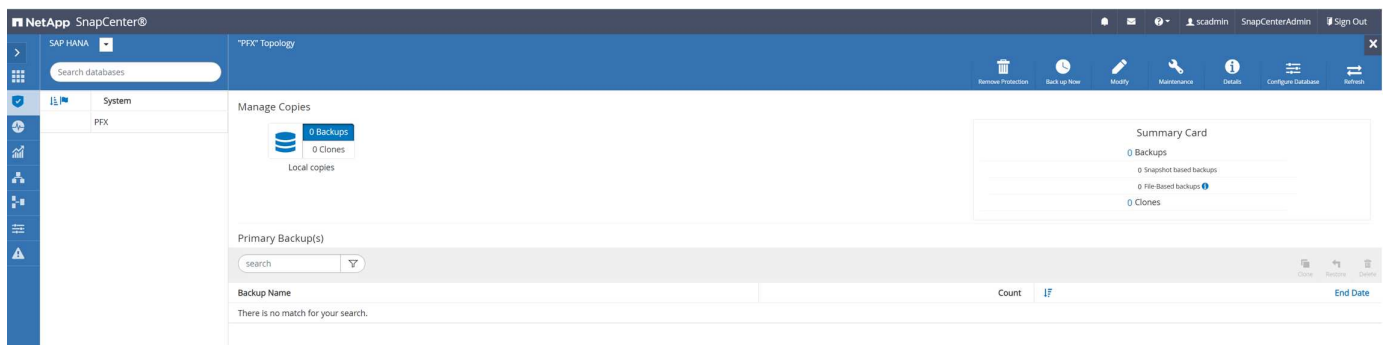
Policy	Applied Schedules	Configure Schedules
BlockIntegrityCheck	Weekly; Run on days: Sunday	
LocalSnap	Hourly; Repeat every 6 hours	

Total 2

9. Forneça informações sobre a notificação por e-mail.



A configuração do recurso HANA agora está concluída e você pode executar backups.



Operações de backup do SnapCenter

Você pode criar um backup Snapshot sob demanda e uma operação de verificação de integridade de bloco sob demanda.

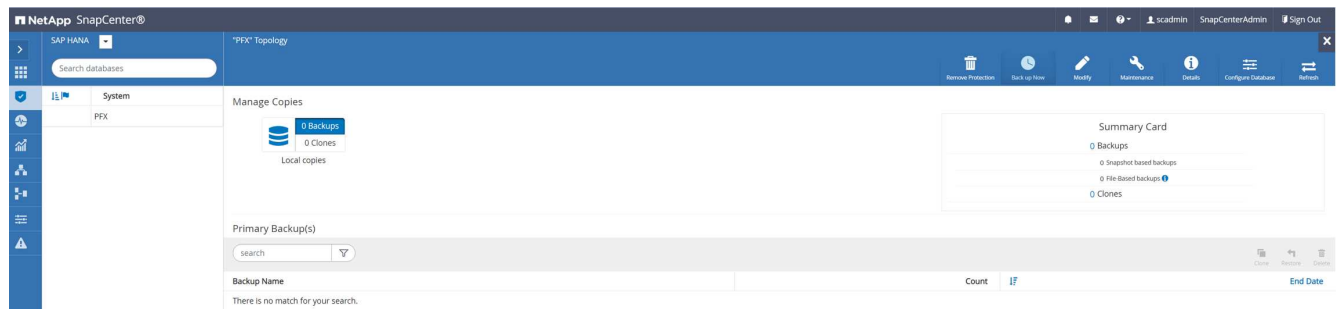
Crie um backup Snapshot sob demanda

Siga estas etapas para criar backups Snapshot sob demanda.

1. No modo de exibição recurso, selecione o recurso e clique duas vezes na linha para alternar para a exibição topologia.

A visualização topologia de recursos fornece uma visão geral de todos os backups disponíveis que foram criados usando o SnapCenter. A área superior dessa visualização exibe a topologia de backup mostrando os backups no storage primário (cópias locais) e, se disponível, no storage de backup externo (cópias do Vault).

2. Na linha superior, selecione o ícone fazer backup agora para iniciar um backup sob demanda.



3. Na lista suspensa, selecione a política de backup LocalSnap e clique em Backup para iniciar o backup sob demanda.

Backup

Create a backup for the selected resource

Resource Name

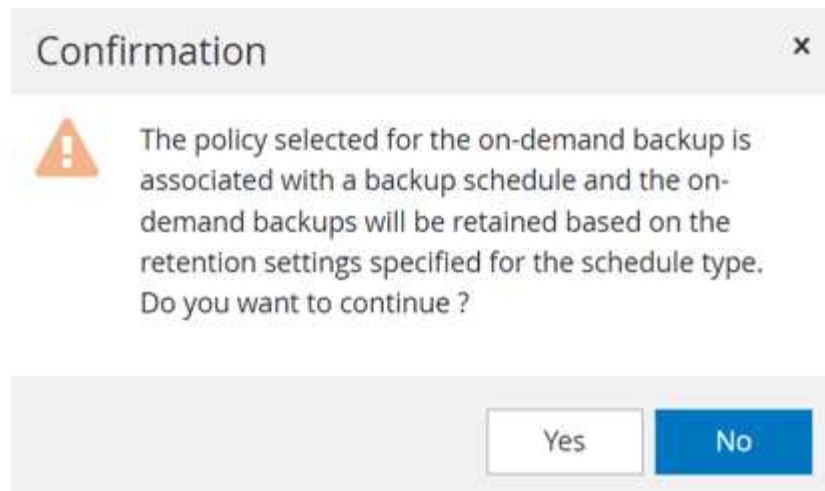
PFX

Policy

LocalSnap

Cancel

Backup



É apresentado um registo dos cinco trabalhos anteriores na área atividade na parte inferior da vista topologia.

- Os detalhes do trabalho são apresentados ao clicar na linha de atividade do trabalho na área atividade. Você pode abrir um log de trabalho detalhado clicando em Exibir logs

Job Details

Backup of Resource Group 'hana-1_hana_MDC_PFX' with policy 'LocalSnap'

✓ ▾ Backup of Resource Group 'hana-1_hana_MDC_PFX' with policy 'LocalSnap'

✓ ▾ hana-1

✓ Backup

✓ ▶ Validate Dataset Parameters

✓ ▶ Validate Plugin Parameters

✓ ▶ Complete Application Discovery

✓ ▶ Initialize Filesystem Plugin

✓ ▶ Discover Filesystem Resources

✓ ▶ Validate Retention Settings

✓ ▶ Quiesce Application

✓ ▶ Quiesce Filesystem

✓ ▶ Create Snapshot

✓ ▶ UnQuiesce Filesystem

✓ ▶ UnQuiesce Application

✓ ▶ Get Snapshot Details

✓ ▶ Get Filesystem Meta Data

✓ ▶ Finalize Filesystem Plugin

✓ ▶ Collect Autosupport data

✓ ▶ Register Backup and Apply Retention

✓ ▶ Register Snapshot attributes

✓ ▶ Application Clean-Up

✓ ▶ Data Collection

✓ ▶ Agent Finalize Workflow

Task Name: Backup Start Time: 02/22/2022 12:08:58 PM End Time: 02/22/2022 12:10:21 PM

View Logs

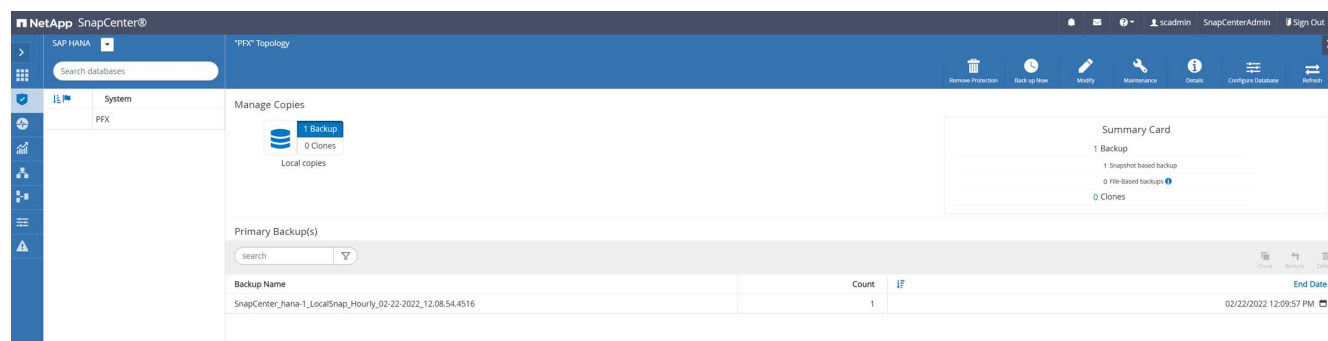
Cancel Job

Close

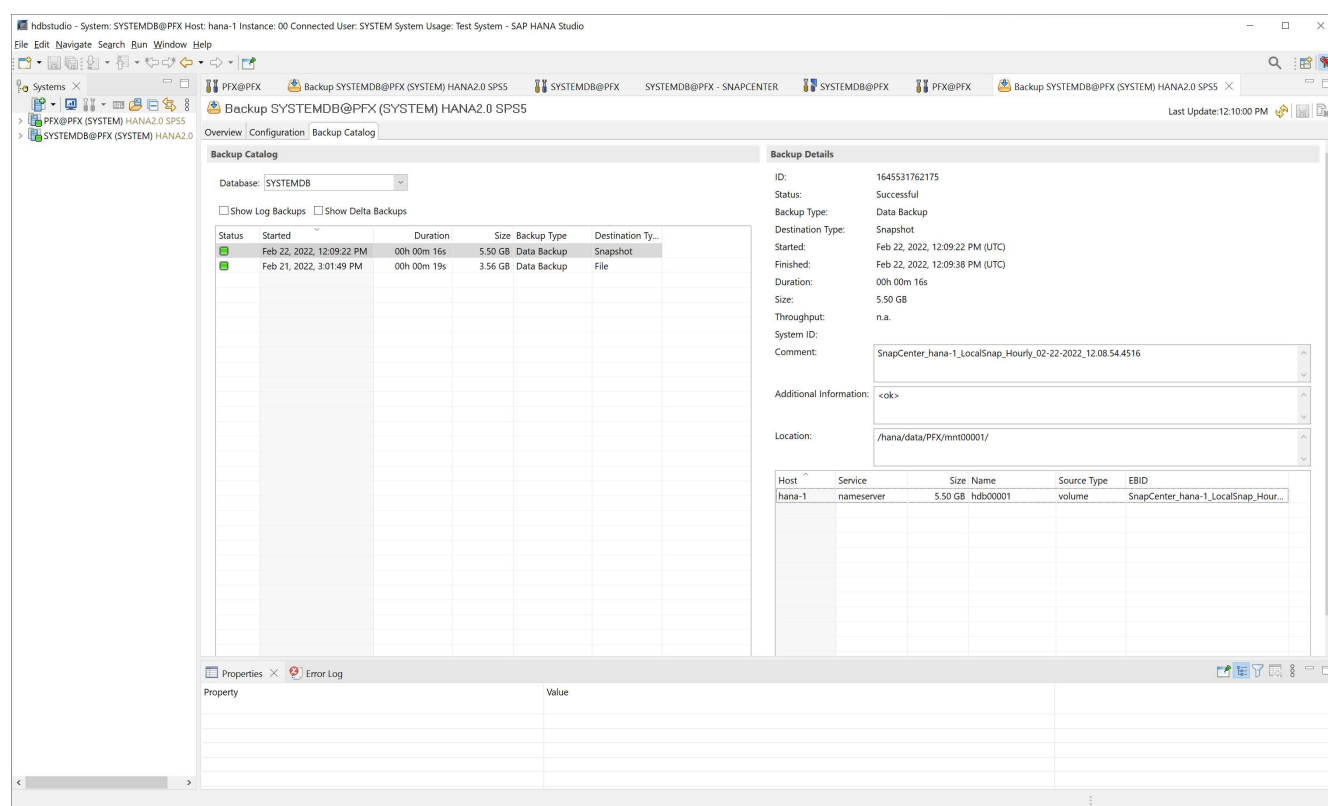
Quando o backup for concluído, uma nova entrada é mostrada na visualização de topologia. Os nomes de backup seguem a mesma convenção de nomenclatura que o nome de captura instantânea definido na seção ["Configurar e proteger um recurso HANA"](#).

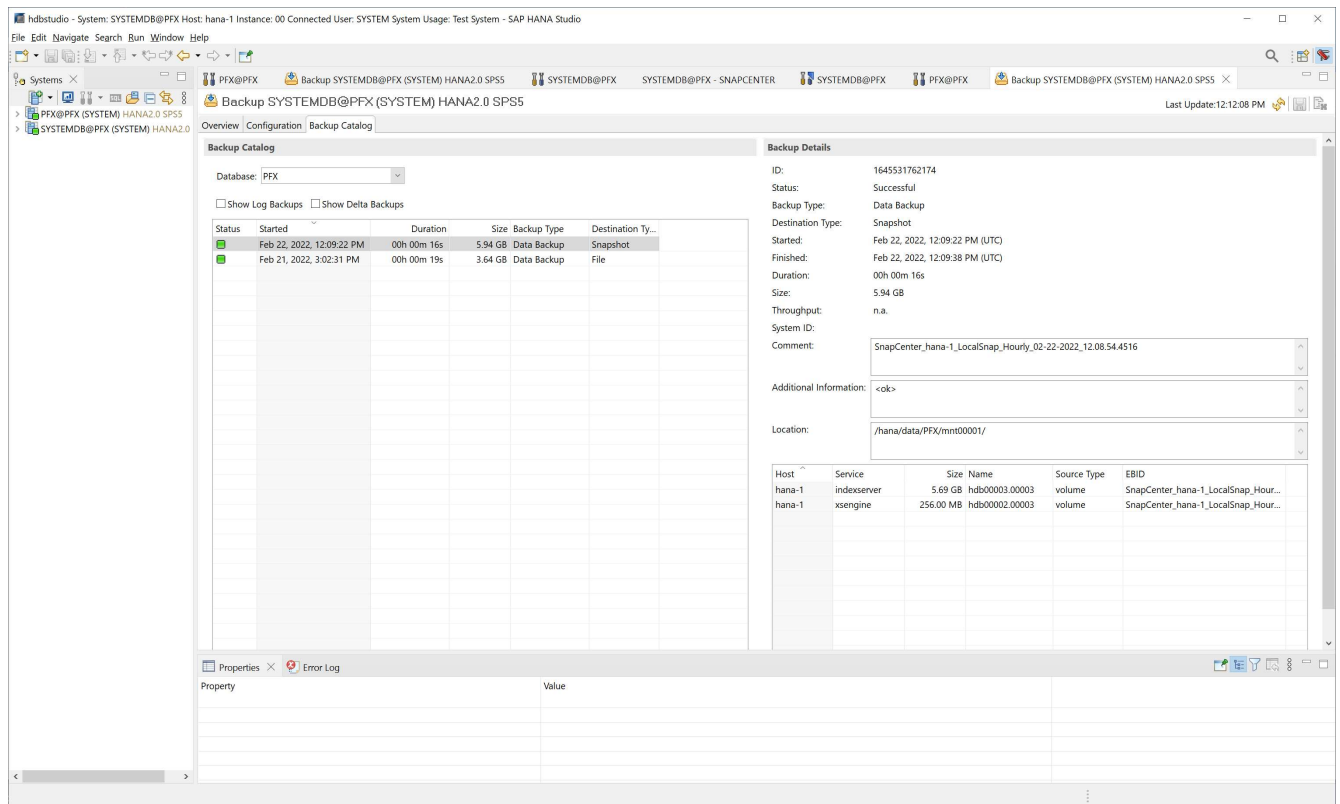
95

Você deve fechar e reabrir a exibição de topologia para ver a lista de backup atualizada.



No catálogo de backup do SAP HANA, o nome do backup do SnapCenter é armazenado como um campo de comentário e o ID de Backup Externo (EBID) também. Isso é mostrado na figura a seguir para o banco de dados do sistema e na figura seguinte para o banco de dados do locatário PFX.





No sistema de arquivos FSX for ONTAP, você pode listar os backups Snapshot conectando-se ao console do SVM.

```
sapcc-hana-svm::> snapshot show -volume PFX_data_mnt00001
---Blocks---
Vserver   Volume      Snapshot                                     Size Total%
Used%
-----
sapcc-hana-svm
          PFX_data_mnt00001
          SnapCenter_hana-1_LocalSnap_Hourly_02-22-
2022_12.08.54.4516
                                     126.6MB      0%
2%
sapcc-hana-svm::>
```

Crie uma operação de verificação de integridade de bloco sob demanda

Uma operação de verificação de integridade de bloco sob demanda é executada da mesma forma que uma tarefa de backup Snapshot, selecionando a política BlockIntegrityCheck. Ao agendar backups usando essa política, o SnapCenter cria um backup de arquivos padrão do SAP HANA para os bancos de dados do sistema e do locatário.

Backup



Create a backup for the selected resource

Resource Name

PFX

Policy

BlockIntegrityCheck



Cancel

Backup

Job Details

Backup of Resource Group 'hana-1_hana_MDC_PFX' with policy 'BlockIntegrityCheck'

✓ ▾ Backup of Resource Group 'hana-1_hana_MDC_PFX' with policy 'BlockIntegrityCheck'

✓ ▾ hana-1

✓ ▾ File-Based Backup

✓ ▶ Validate Plugin Parameters

✓ ▶ Start File-Based Backup

✓ ▶ Check File-Based Backup

✓ ▶ Register Backup and Apply Retention

✓ ▶ Data Collection

Task Name: File-Based Backup Start Time: 02/22/2022 12:55:21 PM End Time: 02/22/2022 12:56:36 PM

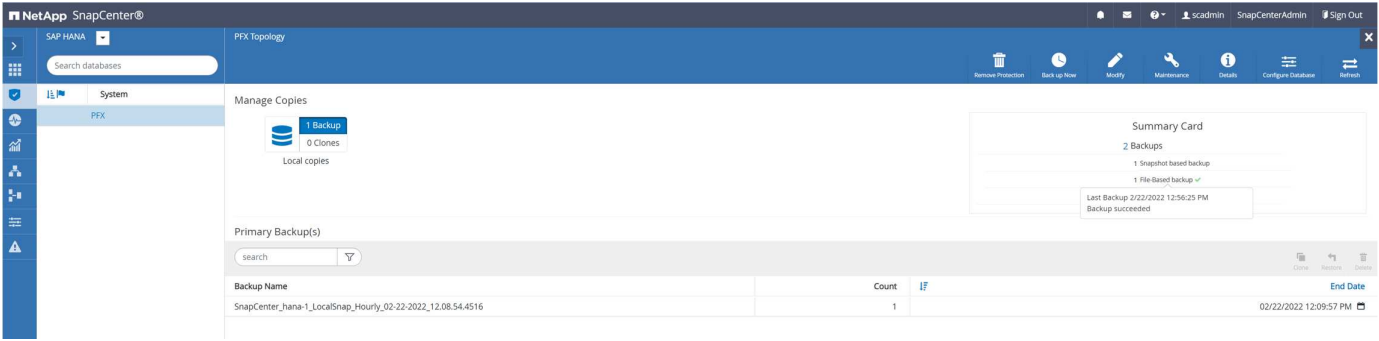
View Logs

Cancel Job

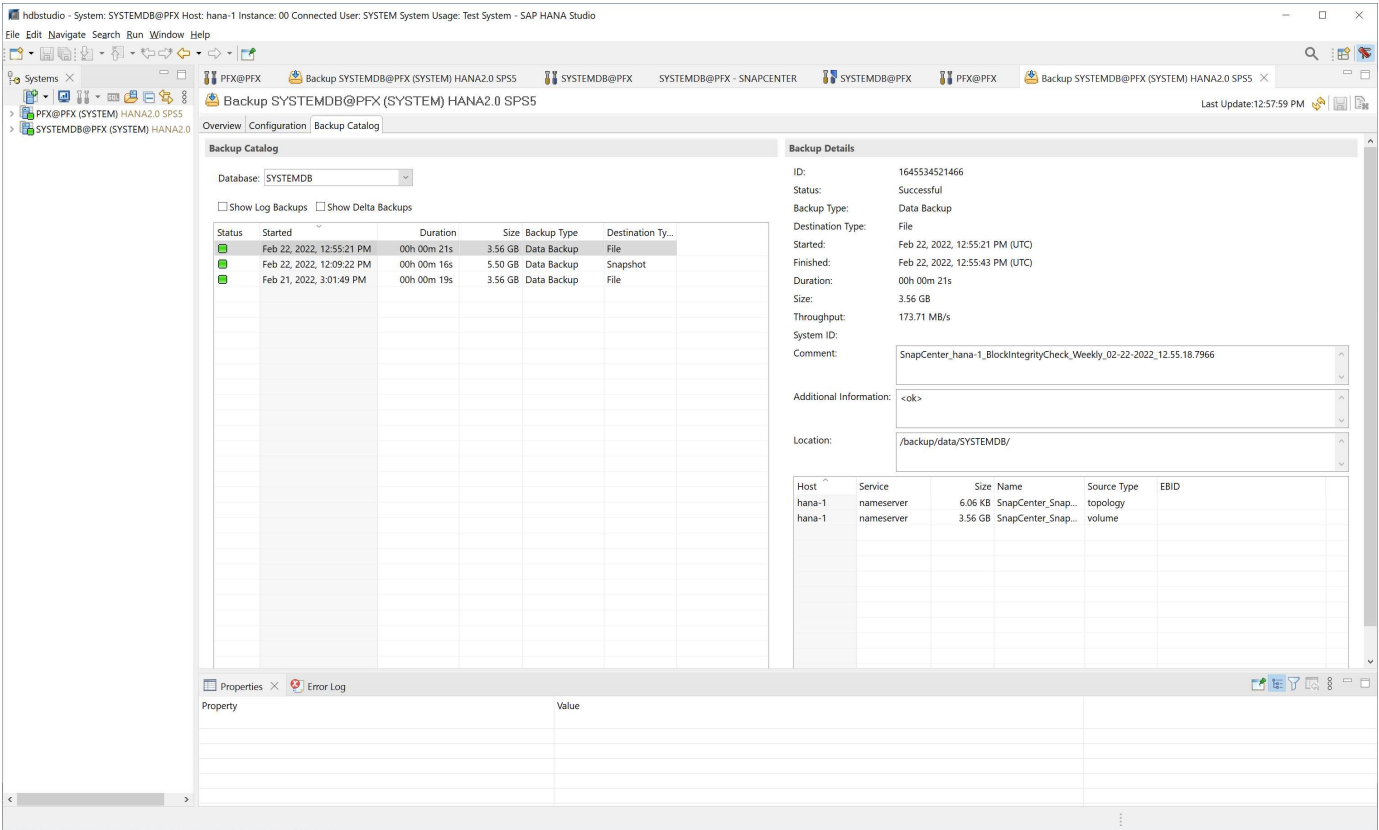
Close

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.



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



hdbstudio - System: SYSTEMDB@PFX Host: hana-1 Instance: 00 Connected User: SYSTEM System Usage: Test System - SAP HANA Studio

File Edit Navigate Search Run Window Help

Systems

Backup SYSTEMDB@PFX (SYSTEM) HANA2.0 SPS5

Last Update: 12:58:19 PM

Overview Configuration Backup Catalog

Database: PFX

☐ Show Log Backups ☐ Show Delta Backups

Status	Started	Duration	Size	Backup Type	Destination Ty...
✓	Feb 22, 2022, 12:55:34 PM	00h 00m 27s	3.64 GB	Data Backup	File
✓	Feb 22, 2022, 12:09:22 PM	00h 00m 16s	5.94 GB	Data Backup	Snapshot
✓	Feb 21, 2022, 3:02:31 PM	00h 00m 19s	3.64 GB	Data Backup	File

Backup Details

ID: 1645534534230

Status: Successful

Backup Type: Data Backup

Destination Type: File

Started: Feb 22, 2022, 12:55:34 PM (UTC)

Finished: Feb 22, 2022, 12:56:01 PM (UTC)

Duration: 00h 00m 27s

Size: 3.64 GB

Throughput: 138.07 MB/s

System ID:

Comment: SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-2022_12:55:18.7966

Additional Information: <ok>

Location: /backup/data/DB_PFX/

Host	Service	Size	Name	Source Type	EBID
hana-1	indexserver	1.58 KB	SnapCenter_Snap...	topology	
hana-1	xsengine	80.00 MB	SnapCenter_Snap...	volume	
hana-1	indexserver	3.56 GB	SnapCenter_Snap...	volume	

Properties Error Log

Property Value

Uma verificação de integridade de bloco bem-sucedida cria arquivos padrão de backup de dados SAP HANA. O SnapCenter usa o caminho de backup que foi configurado com o banco de DADOS HANA para operações de backup de dados baseadas em arquivo.

```

hana-1:~ # ls -al /backup/data/*
/backup/data/DB_PFX:
total 7665384
drwxr-xr-- 2 pfxadm sapsys      4096 Feb 22 12:56 .
drwxr-xr-x 4 pfxadm sapsys      4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys    155648 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys    83894272 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_2_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_3_1
-rw-r----- 1 pfxadm sapsys      155648 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys    83894272 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_2_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 22 12:56
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_3_1
/backup/data/SYSTEMDB:
total 7500880
drwxr-xr-- 2 pfxadm sapsys      4096 Feb 22 12:55 .
drwxr-xr-x 4 pfxadm sapsys      4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys    159744 Feb 21 15:01
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_1_1
-rw-r----- 1 pfxadm sapsys    159744 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_1_1
hana-1:~ #

```

Backup de volumes que não são de dados

O backup de volumes que não são de dados é uma parte integrada do SnapCenter e do plug-in SAP HANA.

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 que não sejam de dados devem ser restaurados, a

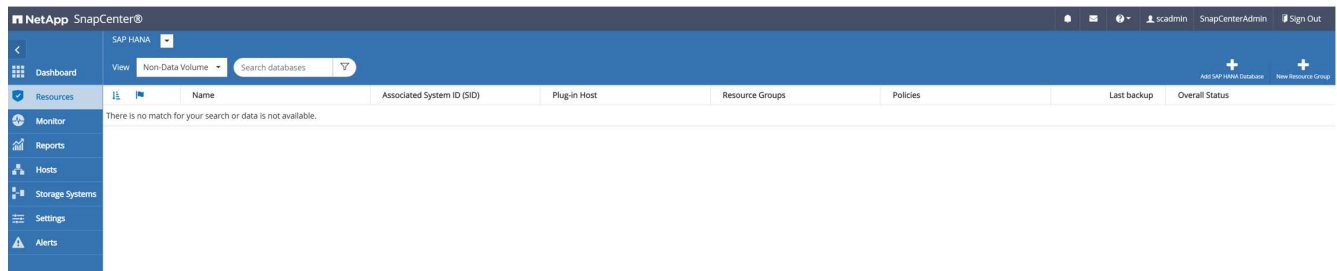
NetApp recomenda o desenvolvimento de uma estratégia de backup adicional para volumes que não sejam de dados para aumentar o backup do banco de dados SAP HANA. Dependendo de seus requisitos específicos, o backup de volumes que não sejam de dados pode diferir na frequência de agendamento e nas configurações de retenção, e você deve considerar a frequência com que os arquivos que não são de dados são alterados. Por exemplo, o volume HANA `/hana/shared` contém executáveis, mas também arquivos de rastreamento SAP HANA. Embora os executáveis só sejam alterados quando o banco de dados SAP HANA é atualizado, os arquivos de rastreamento do SAP HANA podem precisar de uma frequência de backup mais alta para oferecer suporte à análise de situações de problema com o SAP HANA.

O backup em volume que não é de dados da SnapCenter permite que cópias Snapshot de todos os volumes relevantes sejam criadas em poucos segundos com a mesma eficiência de espaço que os backups de bancos de dados do SAP HANA. A diferença é que não há necessidade de comunicação SQL com o banco de dados SAP HANA.

Configurar recursos de volume que não sejam de dados

Siga estas etapas para configurar recursos de volume que não sejam de dados:

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



2. Na etapa um da caixa de diálogo Adicionar banco de dados SAP HANA, na lista tipo de recurso, selecione volumes não de 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.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Resource Details

Resource Type

Non-data Volume

Resource Name

PFX-Shared-Volume

Associated SID

PFX

Plug-In Host

hana-1

Previous

Next

3. Adicione o SVM e o volume de storage como espaço físico do storage e clique em Avançar.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Storage Footprint Details

Storage Type

☒ ONTAP

Add Storage Footprint

Storage System

sapcc-hana-svm

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name

PFX_shared

LUNs or Qtrees

Default is 'None' or type to find

Save

Previous

Next

4. Para salvar as configurações, na etapa de resumo, clique em concluir.

105

Add SAP HANA Database

1 Name
2 Storage Footprint
3 Summary

Summary

Resource Type	Non-data Volume
Resource Name	PFX-Shared-Volume
Associated SID	PFX
Plug-in Host	hana-1

Storage Footprint

Storage System	Volume	LUN/Qtree
sapcc-hana-svm	PFX_shared	

Previous
Finish

O novo volume não-dados é agora adicionado ao SnapCenter. Clique duas vezes no novo recurso para executar a proteção de recursos.

NetApp SnapCenter®

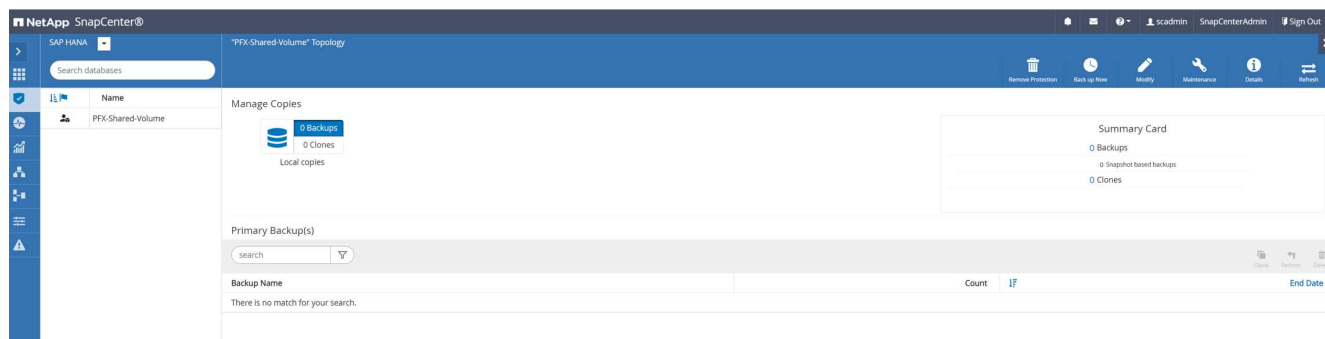
Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts

SAP HANA
View
Non-Data Volume
Search databases

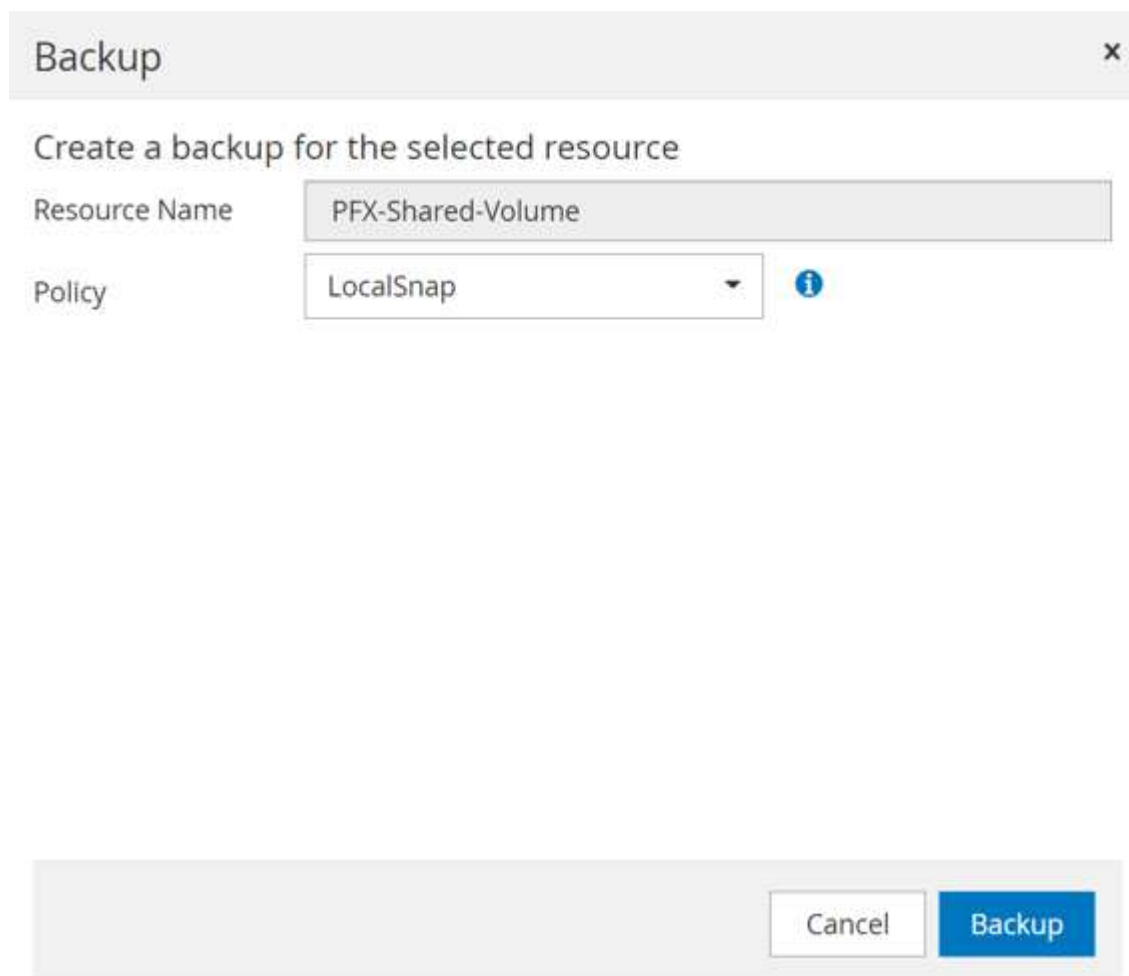
Name	Associated System ID (SID)	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
PFX-Shared-Volume	PFX	hana-1				Not protected

A proteção de recursos é feita da mesma maneira que descrito anteriormente com um recurso de banco de DADOS HANA.

5. Agora você pode executar um backup clicando em Backup Now.



6. Selecione a política e inicie a operação de backup.



O log de tarefas do SnapCenter mostra as etapas individuais do fluxo de trabalho.

Job Details

Backup of Resource Group 'hana-1_hana_NonDataVolume_PFX_PFX-Shared-Volume' with policy 'LocalSnap'

▼ Backup of Resource Group 'hana-1_hana_NonDataVolume_PFX_PFX-Shared-Volume' with policy 'LocalSnap'

▼ hana-1

▼ Backup

▶ Validate Dataset Parameters

▶ Validate Plugin Parameters

▶ Validate Retention Settings

▶ Create Snapshot

▶ Get Snapshot Details

▶ Collect Autosupport data

▶ Register Backup and Apply Retention

▶ Register Snapshot attributes

▶ Data Collection

▶ Agent Finalize Workflow

Task Name: Backup Start Time: 02/22/2022 3:27:48 PM End Time:

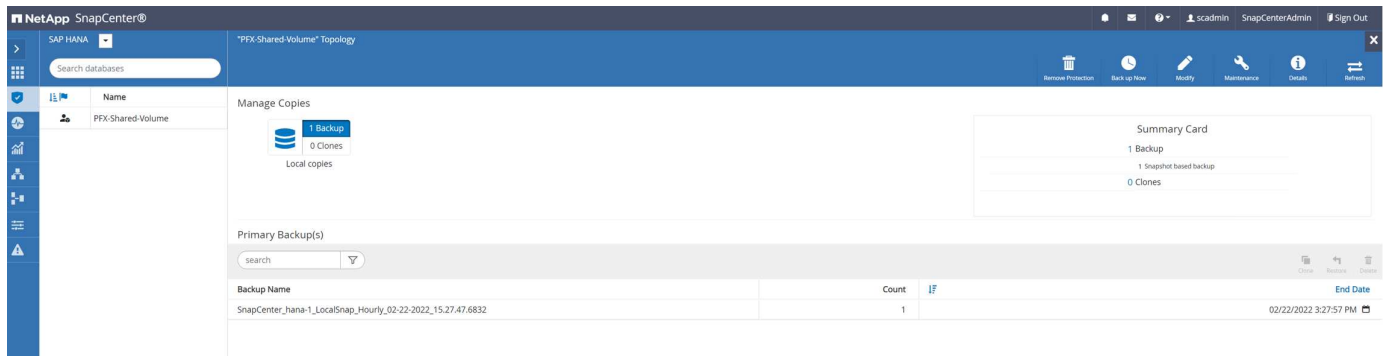
View Logs

Cancel Job

Close

O novo backup agora está visível na exibição de recursos do recurso de volume não-dados.

108



Restaurar e recuperar

Com o SnapCenter, as operações de restauração e recuperação automatizadas são compatíveis com sistemas MDC de host único HANA com um único locatário. Para sistemas de vários hosts ou sistemas MDC com vários locatários, o SnapCenter só executa a operação de restauração e você precisa executar a recuperação manualmente.

Você pode executar uma operação de restauração e recuperação automatizada com as seguintes etapas:

1. Selecione o backup a ser usado para a operação de restauração.
2. Selecione o tipo de restauração. Selecione Restaurar completo com Reverter volume ou sem Reverter volume.
3. Selecione o tipo de recuperação das seguintes opções:
 - Ao estado mais recente
 - Ponto no tempo
 - Para backup de dados específico
 - Sem recuperação

O tipo de recuperação selecionado é usado para a recuperação do sistema e do banco de dados do locatário.

Em seguida, o SnapCenter realiza as seguintes operações:

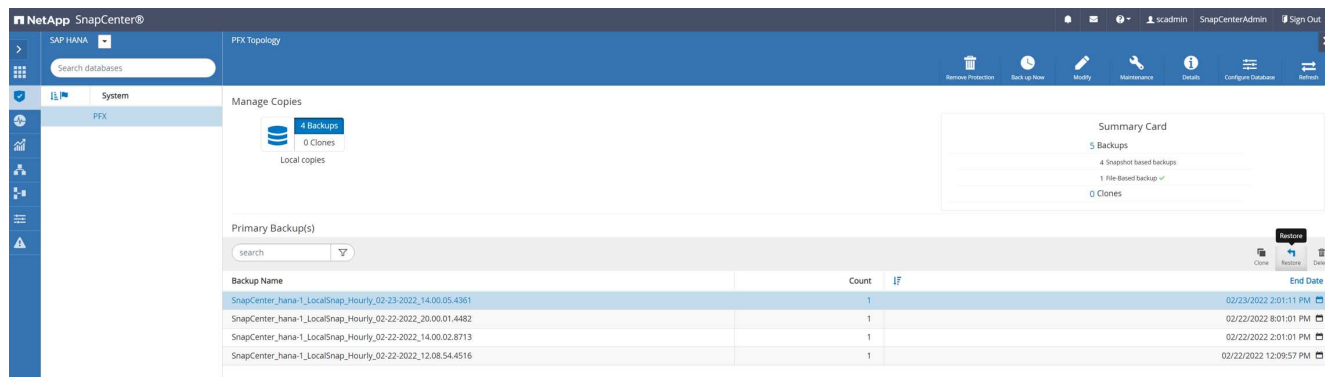
1. Ele interrompe o banco de dados HANA.
2. Restaura o banco de dados. Dependendo do tipo de restauração selecionado, diferentes operações são executadas.
 - Se a opção Reverter volume estiver selecionada, o SnapCenter removerá o volume, restaurará o volume usando o SnapRestore baseado em volume na camada de armazenamento e montará o volume.
 - Se a opção Reverter volume não estiver selecionada, o SnapCenter restaurará todos os arquivos usando operações de SnapRestore de arquivo único na camada de storage.
3. Recupera o banco de dados:
 - a. Recuperando o banco de dados do sistema
 - b. recuperando o banco de dados do locatário
 - c. Iniciar o banco de DADOS HANA

Se nenhuma recuperação estiver selecionada, o SnapCenter será encerrado e você deverá executar a

operação de restauração do sistema e do banco de dados do locatário manualmente.

Para executar uma operação de restauração manual, siga estas etapas:

1. Selecione um backup no SnapCenter a ser usado para a operação de restauração.



2. Selecione o escopo e o tipo de restauração.

O cenário padrão para sistemas HANA MDC de locatário único é usar o recurso completo com reversão de volume. Para um sistema HANA MDC com vários tenants, talvez você queira restaurar apenas um único tenant. Para obter mais informações sobre a restauração de locatário único, consulte ["Restauração e recuperação \(NetApp.com\)"](#).

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361 ×

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ?

☒ Volume Revert

⚠ As part of Complete Resource restore, if a resource contains volumes as Storage Footprint, then the latest Snapshot copies on such volumes will be deleted permanently. Also, if there are other resources hosted on the same volumes, then it will result in data loss for such resources.

☐ Tenant Database

⚠ The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation.

⚠ Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

3. Selecione Recovery Scope e forneça o local para backup de log e backup de catálogo.

O SnapCenter usa o caminho padrão ou os caminhos alterados no arquivo HANA global.ini para preencher previamente os locais de backup de log e catálogo.

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Recover database files using

☒ Recover to most recent state

☐ Recover to point in time

☐ Recover to specified data backup

☐ No recovery

Specify log backup locations

Add

/backup/log

Specify backup catalog location

/backup/log

Recovery options are applicable to both system database and tenant database.

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

4. Introduza os comandos opcionais de pré-restauro.

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run before performing a restore operation

Pre restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

PreviousNext

5. Insira os comandos opcionais pós-restauração.

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run after performing a restore operation

Post restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

PreviousNext

6. Para iniciar a operação de restauração e recuperação, clique em concluir.

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

Backup Name	SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361
Backup date	02/23/2022 2:01:11 PM
Restore scope	Complete Resource with Volume Revert
Recovery scope	Recover to most recent state
Log backup locations	/backup/log
Backup catalog location	/backup/log
Pre restore command	
Post restore command	
Send email	No

If you want to send notifications for Restore Jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Finish

O SnapCenter executa a operação de restauração e recuperação. Este exemplo mostra os detalhes do trabalho de restauro e recuperação.

Job Details



Restore 'hana-1\hana\MDC\PFX'

- ✓ ▼ Restore 'hana-1\hana\MDC\PFX'
- ✓ ▼ hana-1
 - ✓ ▼ Restore
 - ✓ ▶ Validate Plugin Parameters
 - ✓ ▼ Pre Restore Application
 - ✓ ▶ Stopping HANA instance
 - ✓ ▶ Filesystem Pre Restore
 - ✓ ▼ Restore Filesystem
 - ✓ ▶ Filesystem Post Restore
 - ✓ ▼ Recover Application
 - ✓ ▶ Recovering system database
 - ✓ ▶ Checking HDB services status
 - ✓ ▶ Recovering tenant database 'PFX'
 - ✓ ▶ Starting HANA instance
 - ✓ ▶ Clear Catalog on Server
 - ✓ ▶ Application Clean-Up
 - ✓ ▶ Data Collection
 - ✓ ▶ Agent Finalize Workflow

Task Name: Recover Application Start Time: 02/23/2022 2:07:31 PM End Time:

View Logs

Cancel Job

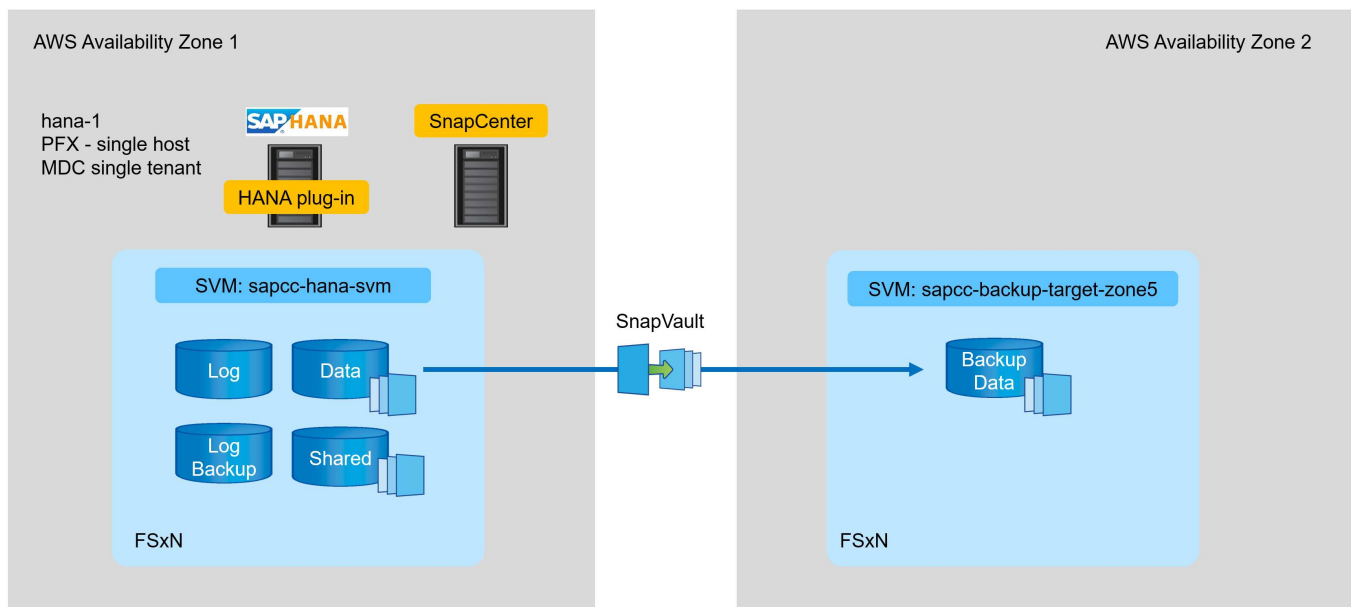
Close

Faça backup da replicação com o SnapVault

Visão geral - Backup de replicação com o SnapVault

Em nossa configuração de laboratório, usamos um segundo sistema de arquivos FSX for ONTAP em uma segunda zona de disponibilidade da AWS para mostrar a replicação de backup para o volume de dados HANA.

Como discutido no ["Estratégia de proteção de dados"](#) capítulo , o destino de replicação deve ser um segundo sistema de arquivos FSX for ONTAP em outra zona de disponibilidade para ser protegido contra uma falha do sistema de arquivos FSX for ONTAP primário. Além disso, o volume compartilhado HANA deve ser replicado para o sistema de arquivos FSX for ONTAP secundário.



Visão geral das etapas de configuração

Existem algumas etapas de configuração que você deve executar na camada FSX for ONTAP. Você pode fazer isso com o Gerenciador de nuvem do NetApp ou a linha de comando FSX for ONTAP.

1. Peer FSX para sistemas de arquivos ONTAP. Os sistemas de arquivos FSX para ONTAP devem ser peered para permitir replicação entre si.
2. SVMs pares. Os SVMs devem ser peered para permitir a replicação entre si.
3. Crie um volume de destino. Crie um volume no SVM de destino com tipo de volume `DP`. O tipo `DP` é necessário para ser usado como um volume de destino de replicação.
4. Crie uma política do SnapMirror. Isso é usado para criar uma diretiva para replicação com o tipo `vault`.
 - a. Adicione uma regra à política. A regra contém o rótulo `SnapMirror` e a retenção de backups no local secundário. Você deve configurar o mesmo rótulo do SnapMirror posteriormente na política do SnapCenter para que o SnapCenter crie backups do Snapshot no volume de origem que contém esse rótulo.
5. Crie uma relação SnapMirror. Defina a relação de replicação entre o volume de origem e destino e anexe uma política.
6. Inicialize o SnapMirror. Isso inicia a replicação inicial na qual os dados de origem completos são

transferidos para o volume de destino.

Quando a configuração de replicação de volume estiver concluída, você deverá configurar a replicação de backup no SnapCenter da seguinte forma:

1. Adicione o SVM de destino ao SnapCenter.
2. Criar uma nova política do SnapCenter para backup instantâneo e replicação do SnapVault.
3. Adicionar a política à proteção de recursos DO HANA.
4. Agora você pode executar backups com a nova política.

Os capítulos a seguir descrevem os passos individuais com mais detalhes.

Configurar relações de replicação no FSX para sistemas de arquivos ONTAP

Você pode encontrar informações adicionais sobre as opções de configuração do SnapMirror na documentação do ONTAP em "[Fluxo de trabalho de replicação do SnapMirror \(NetApp.com\)](#)".

- Fonte FSX para sistema de arquivos ONTAP: FsxId00fa9e3c784b6abbb
- Fonte SVM: sapcc-hana-svm
- Escolha o sistema de arquivos FSX for ONTAP: FsxId05f7f00af49dc7a3e
- SVM-alvo: sapcc-backup-target-zone5

Peer FSX para sistemas de arquivos ONTAP

```
FsxId00fa9e3c784b6abbb::> network interface show -role intercluster
      Logical      Status      Network      Current      Current
Is
Vserver      Interface  Admin/Oper  Address/Mask      Node      Port
Home
-----
----
FsxId00fa9e3c784b6abbb
      inter_1      up/up      10.1.1.57/24
FsxId00fa9e3c784b6abbb-01
                                     e0e
true
      inter_2      up/up      10.1.2.7/24
FsxId00fa9e3c784b6abbb-02
                                     e0e
true
2 entries were displayed.
```

```
FsxId05f7f00af49dc7a3e::> network interface show -role intercluster
```

	Logical	Status	Network	Current	Current
Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----

FsxId05f7f00af49dc7a3e	inter_1	up/up	10.1.2.144/24		
FsxId05f7f00af49dc7a3e-01					e0e
true					
	inter_2	up/up	10.1.2.69/24		
FsxId05f7f00af49dc7a3e-02					e0e
true					

2 entries were displayed.

```
FsxId05f7f00af49dc7a3e::> cluster peer create -address-family ipv4 -peer
-peer-addr 10.1.1.57, 10.1.2.7
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters. To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:

Confirm the passphrase:

Notice: Now use the same passphrase in the "cluster peer create" command in the other cluster.



peer-addr São IPs de cluster do cluster de destino.

```
FsxId00fa9e3c784b6abbb::> cluster peer create -address-family ipv4 -peer
-addrs 10.1.2.144, 10.1.2.69
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
FsxId00fa9e3c784b6abbb::>
FsxId00fa9e3c784b6abbb::> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
Authentication
-----
FsxId05f7f00af49dc7a3e    1-80-000011             Available      ok
```

SVMs pares

```
FsxId05f7f00af49dc7a3e::> vserver peer create -vserver sapcc-backup-
target-zone5 -peer-vserver sapcc-hana-svm -peer-cluster
FsxId00fa9e3c784b6abbb -applications snapmirror
Info: [Job 41] 'vserver peer create' job queued
```

```
FsxId00fa9e3c784b6abbb::> vserver peer accept -vserver sapcc-hana-svm
-peer-vserver sapcc-backup-target-zone5
Info: [Job 960] 'vserver peer accept' job queued
```

```
FsxId05f7f00af49dc7a3e::> vserver peer show
Peer          Peer          Peering
Remote
Vserver      Vserver      State      Peer Cluster      Applications
Vserver
-----
sapcc-backup-target-zone5
peer-source-cluster
peered      FsxId00fa9e3c784b6abbb
snapmirror
sapcc-hana-svm
```

Crie um volume de destino

Você deve criar o volume de destino com o tipo DP para sinalizá-lo como um destino de replicação.


```
FsxId05f7f00af49dc7a3e::> volume create -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -aggregate aggr1 -size 100GB -state online
-policy default -type DP -autosize-mode grow_shrink -snapshot-policy none
-foreground true -tiering-policy all -anti-ransomware-state disabled
[Job 42] Job succeeded: Successful
```

Crie uma política do SnapMirror

A política SnapMirror e a regra adicionada definem a retenção e o rótulo SnapMirror para identificar snapshots que devem ser replicados. Ao criar a política SnapCenter mais tarde, você deve usar o mesmo rótulo.

```
FsxId05f7f00af49dc7a3e::> snapmirror policy create -policy snapcenter-
policy -tries 8 -transfer-priority normal -ignore-atime false -restart
always -type vault -vserver sapcc-backup-target-zone5
```

```
FsxId05f7f00af49dc7a3e::> snapmirror policy add-rule -vserver sapcc-
backup-target-zone5 -policy snapcenter-policy -snapmirror-label
snapcenter -keep 14
```

```
FsxId00fa9e3c784b6abbb::> snapmirror policy showVserver Policy
```

Policy Number	Transfer						
Name	Name	Type	Of Rules	Tries	Priority	Comment	

FsxId00fa9e3c784b6abbb							
	snapcenter-policy	vault	1	8	normal	-	
	SnapMirror Label: snapcenter					Keep:	14
						Total Keep:	14

Criar relacionamento SnapMirror

Agora, a relação entre o volume de origem e destino é definida, bem como o tipo XDP e a política que criamos anteriormente.

```
FsxId05f7f00af49dc7a3e::> snapmirror create -source-path sapcc-hana-
svm:PFX_data_mnt00001 -destination-path sapcc-backup-target-
zone5:PFX_data_mnt00001 -vserver sapcc-backup-target-zone5 -throttle
unlimited -identity-preserve false -type XDP -policy snapcenter-policy
Operation succeeded: snapmirror create for the relationship with
destination "sapcc-backup-target-zone5:PFX_data_mnt00001".
```

Inicialize o SnapMirror

Com este comando, a replicação inicial é iniciada. Esta é uma transferência completa de todos os dados do volume de origem para o volume de destino.

```
FsxId05f7f00af49dc7a3e::> snapmirror initialize -destination-path sapcc-backup-target-zone5:PFX_data_mnt00001 -source-path sapcc-hana-svm:PFX_data_mnt00001
Operation is queued: snapmirror initialize of destination "sapcc-backup-target-zone5:PFX_data_mnt00001".
```

Você pode verificar o status da replicação com o `snapmirror show` comando.

```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source          Destination Mirror Relationship Total
Last
Path            Type  Path            State  Status          Progress Healthy
Updated
-----
-----
sapcc-hana-svm:PFX_data_mnt00001
                XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                                Uninitialized
                                Transferring  1009MB  true
02/24 12:34:28
```

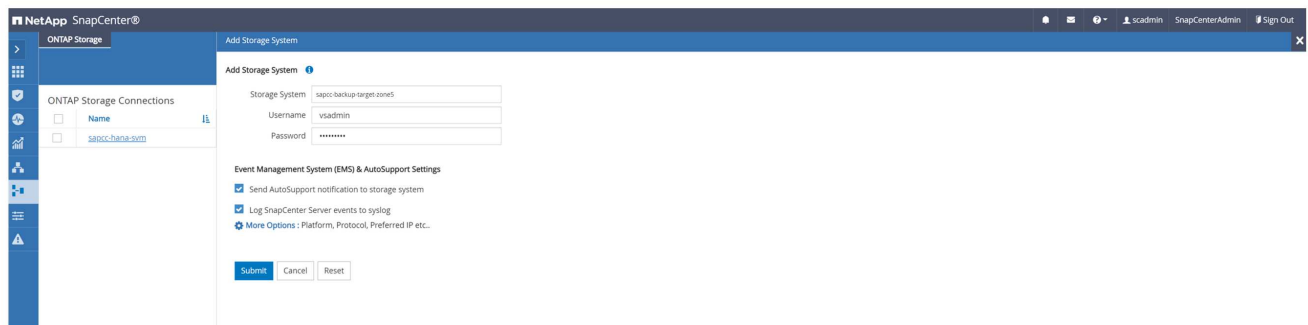
```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source          Destination Mirror Relationship Total
Last
Path            Type  Path            State  Status          Progress Healthy
Updated
-----
-----
sapcc-hana-svm:PFX_data_mnt00001
                XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                                Snapmirrored
                                Idle          -      true  -
```

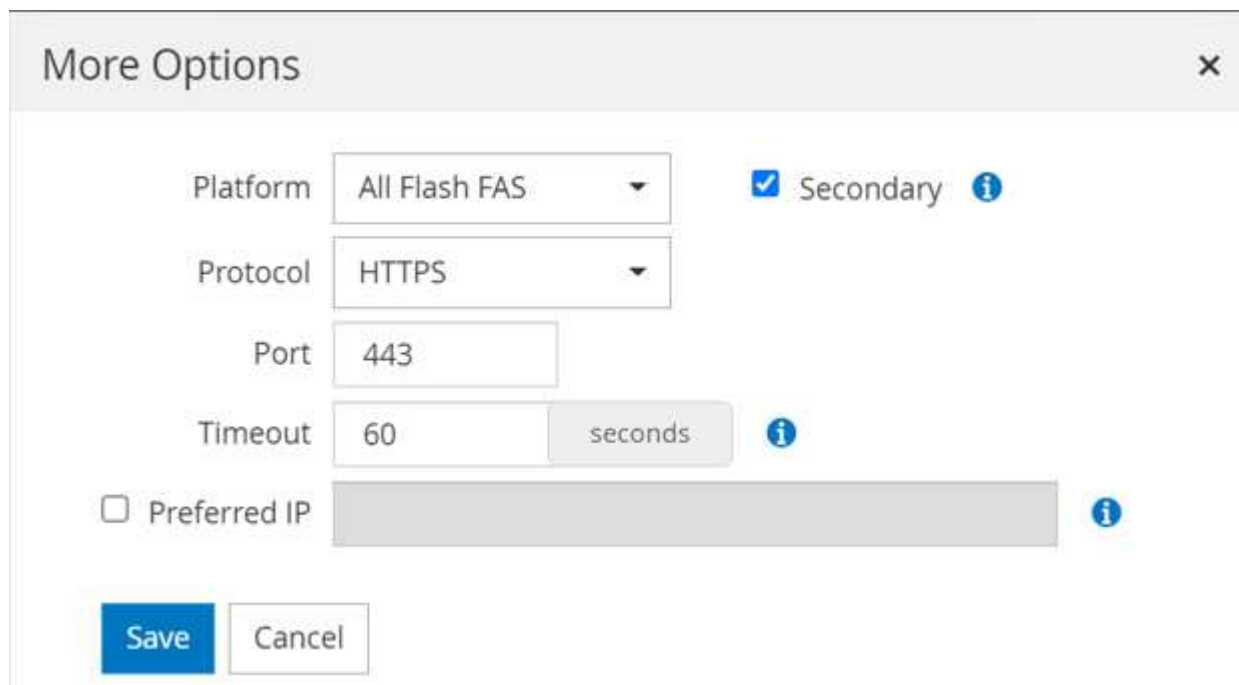
Adicionar um SVM de backup ao SnapCenter

Para adicionar um SVM de backup ao SnapCenter, siga estas etapas:

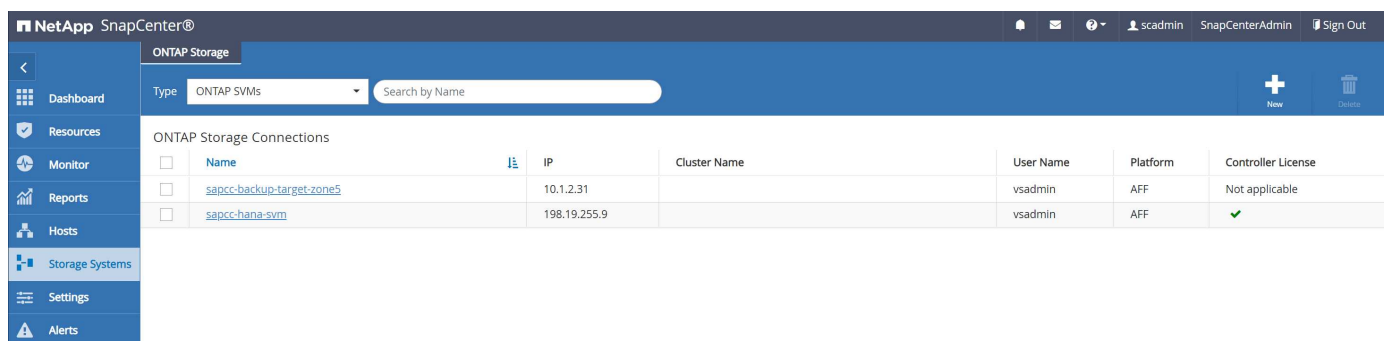
1. Configurar o SVM onde o volume de destino do SnapVault está localizado no SnapCenter.



2. Na janela mais opções, selecione All Flash FAS como a plataforma e selecione secundário.



O SVM agora está disponível no SnapCenter.

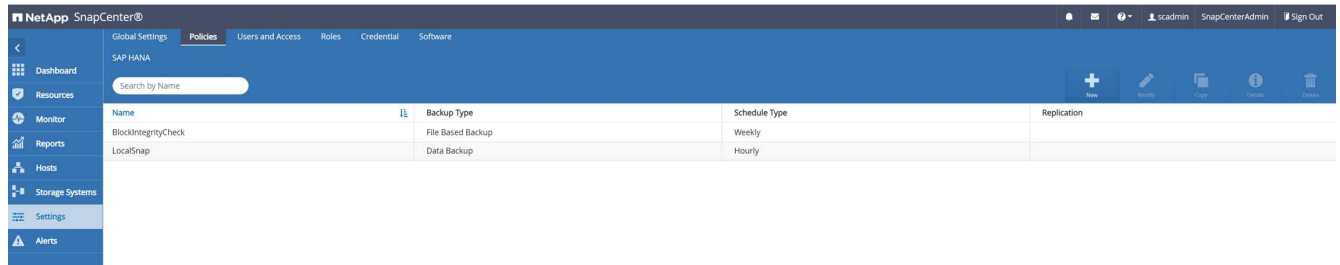


ONTAP Storage Connections	IP	Cluster Name	User Name	Platform	Controller License
☐ sapcc-backup-target-zone5	10.1.2.31		vsadmin	AFF	Not applicable
☐ sapcc-hana-svm	198.19.255.9		vsadmin	AFF	✓

Crie uma nova política do SnapCenter para replicação de backup

Você deve configurar uma política para a replicação de backup da seguinte forma:

1. Forneça um nome para a política.



2. Selecione cópia de segurança instantânea e uma frequência de programação. Diariamente é normalmente usado para replicação de backup.

New SAP HANA Backup Policy

1 Name Provide a policy name

2 Settings Policy name LocalSnapAndSnapVault

3 Retention Details Replication to backup volume

4 Replication

5 Summary

3. Selecione a retenção para os backups Snapshot.

New SAP HANA Backup Policy

1 Name

2 Settings Select backup settings

Backup Type ☒ Snapshot Based ☐ File-Based

Schedule Frequency

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

☐ On demand

☐ Hourly

☒ Daily

☐ Weekly

☐ Monthly

3 Retention

4 Replication

5 Summary

Essa é a retenção dos backups diários do Snapshot feitos no storage primário. A retenção para backups secundários no destino SnapVault já foi configurada anteriormente usando o comando add rule no nível ONTAP. Consulte "Configurar relações de replicação no FSX para sistemas de arquivos ONTAP" (xref).

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

Daily retention settings

☒ Total Snapshot copies to keep

3

☐ Keep Snapshot copies for

14

days

4. Selecione o campo Atualizar SnapVault e forneça uma etiqueta personalizada.

Esse rótulo deve corresponder ao rótulo SnapMirror fornecido no `add rule` comando no nível ONTAP.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select secondary replication options

☐ Update SnapMirror after creating a local Snapshot copy.
 ☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Custom Label

snapcenter

Error retry count

3

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Summary

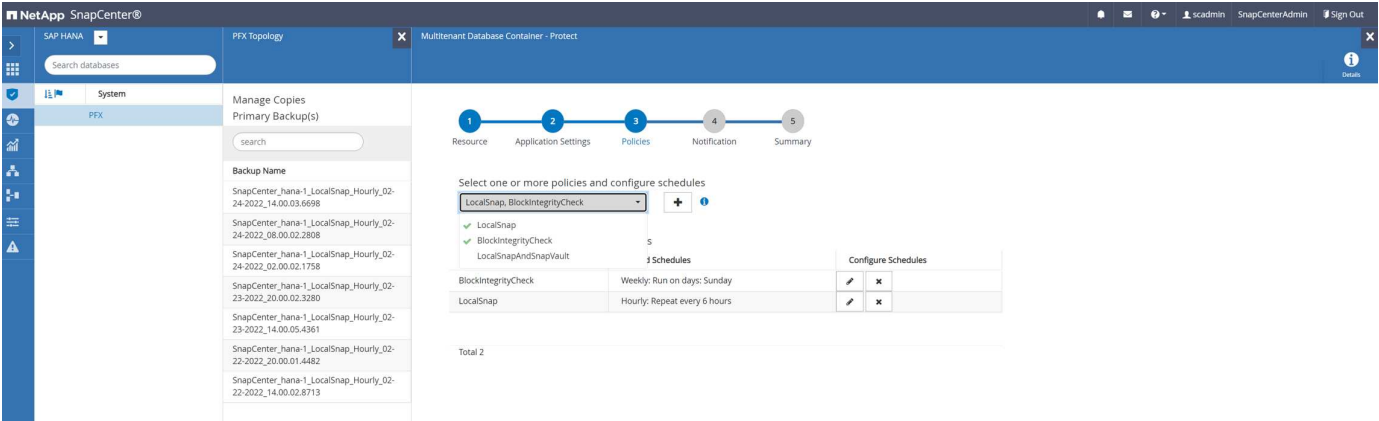
Policy name	LocalSnapAndSnapVault
Details	Replication to backup volume
Backup Type	Snapshot Based Backup
Schedule Type	Daily
Daily backup retention	Total backup copies to retain : 3
Replication	SnapVault enabled , Secondary policy label: Custom Label : snapcenter , Error retry count: 3

A nova política SnapCenter está agora configurada.

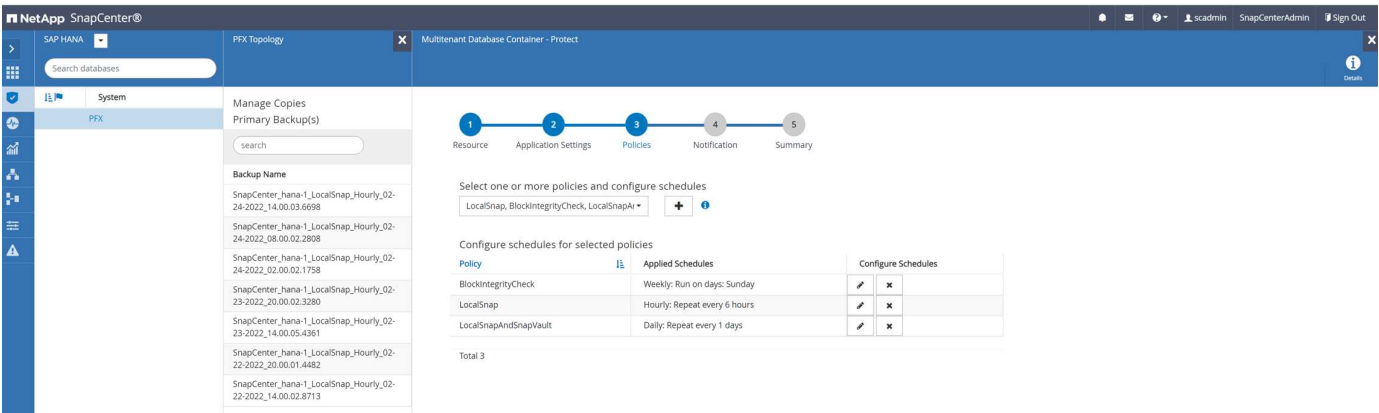
NetApp SnapCenter®				
Global Settings Policies Users and Access Roles Credential Software				
SAP HANA				
Search by Name				
Name	Backup Type	Schedule Type	Replication	
BlockIntegrityCheck	File Based Backup	Weekly		
LocalSnap	Data Backup	Hourly		
LocalSnapAndSnapVault	Data Backup	Daily	SnapVault	

Adicione uma política à proteção de recursos

Você precisa adicionar a nova política à configuração de proteção de recursos DO HANA, conforme mostrado na figura a seguir.



Uma programação diária é definida em nossa configuração.



Crie um backup com replicação

Um backup é criado da mesma forma que com uma cópia Snapshot local.

Para criar um backup com replicação, selecione a política que inclui a replicação de backup e clique em Backup.

Backup

x

Create a backup for the selected resource

Resource Name

PFX

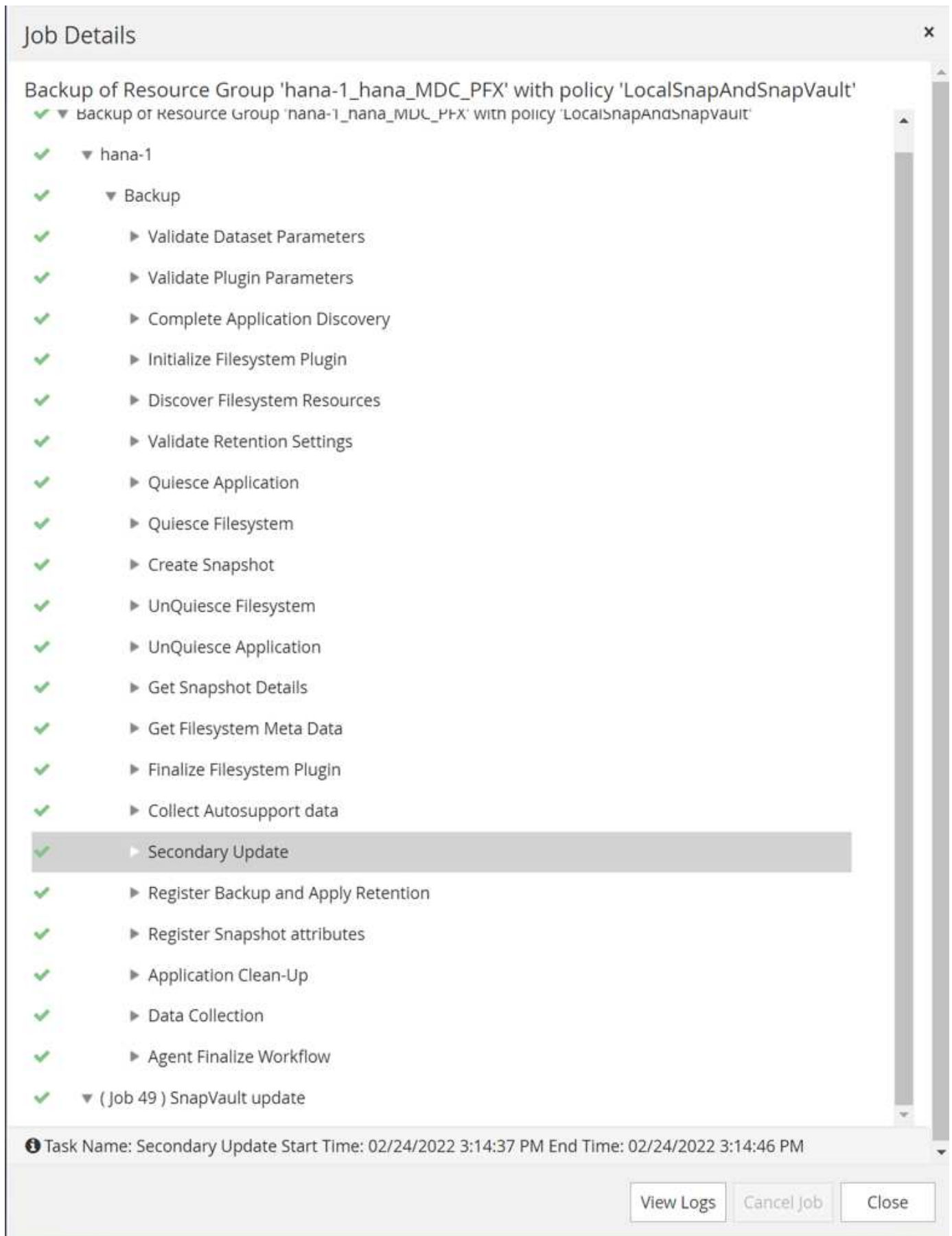
Policy

LocalSnapAndSnapVault

Cancel

Backup

No log de tarefas do SnapCenter, você pode ver a etapa Atualização secundária, que inicia uma operação de atualização do SnapVault. A replicação alterou blocos do volume de origem para o volume de destino.



No sistema de arquivos FSX for ONTAP, uma captura instantânea no volume de origem é criada usando o

rótulo SnapMirror snapcenter , conforme configurado na política SnapCenter.

```
FsxId00fa9e3c784b6abbb:> snapshot show -vserver sapcc-hana-svm -volume
PFX_data_mnt00001 -fields snapmirror-label
vserver          volume          snapshot
snapmirror-label
-----
-----
-----
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_13.10.26.5482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_14.00.05.2023 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_08.00.06.3380 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_14.00.01.6482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-14-
2022_20.00.05.0316 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_08.00.06.3629 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_14.00.01.7275 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853

snapcenter
8 entries were displayed.
```

No volume de destino, uma cópia Snapshot com o mesmo nome é criada.

```
FsxId05f7f00af49dc7a3e:> snapshot show -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -fields snapmirror-label
vserver          volume          snapshot
snapmirror-label
-----
-----
-----
sapcc-backup-target-zone5 PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853 snapcenter
FsxId05f7f00af49dc7a3e:>
```

O novo backup Snapshot também está listado no catálogo de backup DO HANA.

Backup Catalog						Backup Details					
Database: SYSTEMDB						ID: 1651162926424					
☐ Show Log Backups ☐ Show Delta Backups						Status: Successful					
Status	Started	Duration	Size	Backup Type	Destination Ty...	Backup Type: Data Backup					
	Apr 28, 2022, 4:22:06 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Destination Type: Snapshot					
	Apr 28, 2022, 2:00:26 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Started: Apr 28, 2022, 4:22:06 PM (UTC)					
	Apr 28, 2022, 8:00:35 AM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Finished: Apr 28, 2022, 4:22:21 PM (UTC)					
	Apr 15, 2022, 5:00:44 PM	00h 06m 59s	5.50 GB	Data Backup	Snapshot	Duration: 00h 00m 15s					
	Apr 14, 2022, 8:00:32 PM	00h 00m 16s	5.50 GB	Data Backup	Snapshot	Size: 5.50 GB					
	Apr 5, 2022, 2:00:29 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Throughput: n.a.					
	Apr 5, 2022, 8:00:39 AM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	System ID:					
	Mar 31, 2022, 2:00:29 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Comment: SnapCenter_hana-1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853					
	Mar 31, 2022, 1:10:57 PM	00h 00m 16s	5.50 GB	Data Backup	Snapshot	Additional Information: <ok>					
	Feb 22, 2022, 12:55:21 PM	00h 00m 21s	3.56 GB	Data Backup	File	Location: /hana/data/PFX/mnt00001/					
						Host	Service	Size	Name	Source Type	EBID
						hana-1	nameserver	5.50 GB	hdb00001	volume	SnapCent...

No SnapCenter, você pode listar os backups replicados clicando em cópias do Vault na exibição de topologia.

Restaure e recupere do storage secundário

Para restaurar e recuperar do armazenamento secundário, siga estas etapas:

Para recuperar a lista de todos os backups no armazenamento secundário, no modo de exibição topologia do SnapCenter, clique em cópias do cofre, selecione um backup e clique em Restaurar.

A caixa de diálogo Restore (Restaurar) mostra as localizações secundárias.

Restore from SnapCenter_hana-1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853 ×

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ?

☐ Tenant Database

Choose archive location

sapcc-hana-svm:PFX_data_mnt00001

sapcc-backup-target-zone5:PFX_data_mnt00 ▼

⚠ The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation. ×

⚠ Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#). ×

Previous

Next

As etapas de restauração e recuperação adicionais são idênticas às anteriormente abordadas para um backup Snapshot no storage primário.

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Guia do usuário do FSX for NetApp ONTAP: O que é o Amazon FSX para NetApp ONTAP?

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html>

- Página de recursos do SnapCenter

["https://www.netapp.com/us/documentation/snapcenter-software.aspx"](https://www.netapp.com/us/documentation/snapcenter-software.aspx)

- Documentação do software SnapCenter

["https://docs.netapp.com/us-en/snapcenter/index.html"](https://docs.netapp.com/us-en/snapcenter/index.html)

- Automatizando as operações de clonagem e cópia do sistema SAP HANA com o SnapCenter

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

- Replicação do sistema SAP HANA — backup e recuperação com SnapCenter

["Backup e recuperação com o SnapCenter"](#)

Histórico de versões

Versão	Data	Histórico de versões do documento
Versão 1,0	Maio de 2022	Lançamento inicial.

Proteção de dados do SAP HANA e alta disponibilidade com o SnapCenter, o SnapMirror active Sync e o cluster de storage VMware Metro

Proteção de dados do SAP HANA e alta disponibilidade com o SnapCenter, o SnapMirror active Sync e o cluster de storage VMware Metro

Este documento fornece as práticas recomendadas de proteção de dados com o SnapCenter em um ambiente VMware combinado ao SnapMirror active Sync como uma solução de alta disponibilidade para os recursos de STORAGE HANA.

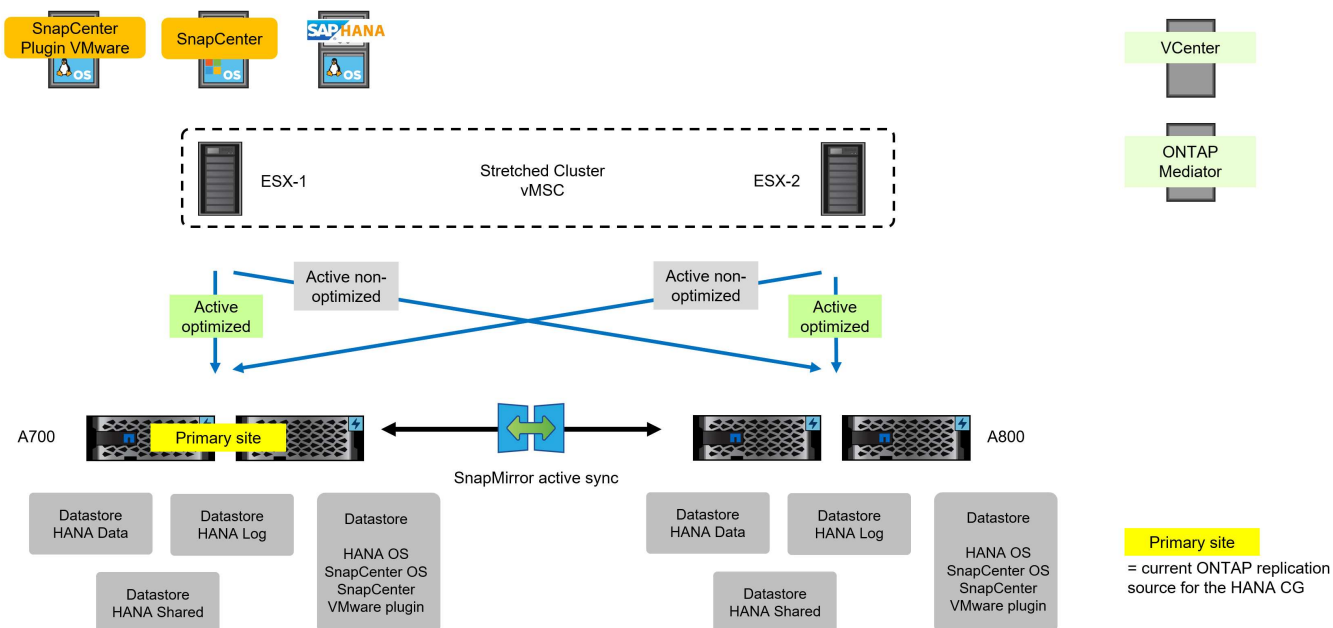
Autor: Nils Bauer, NetApp

Âmbito deste documento

O documento não se destina a ser uma descrição passo a passo de como configurar o ambiente completo, mas abrange conceitos e detalhes relevantes relacionados com:

- Configuração de sistemas SAP HANA com VMware VMFS
- Configuração de sincronização ativa do SnapMirror para SAP HANA
- Configuração do SnapCenter para HANA no VMware com VMFS
- Configuração do SnapCenter para sincronização ativa do SnapMirror
- Operações do SnapCenter com HANA em sincronização ativa do VMware e do SnapMirror

Vamos nos concentrar em uma configuração vMSC (VMware Metro Storage Cluster) usando uma configuração de acesso uniforme do SnapMirror ativo Sync, como mostrado na figura abaixo, mas também tocaremos brevemente em bare metal, bem como configurações de acesso não uniformes.



Visão geral SAP HANA de alta disponibilidade

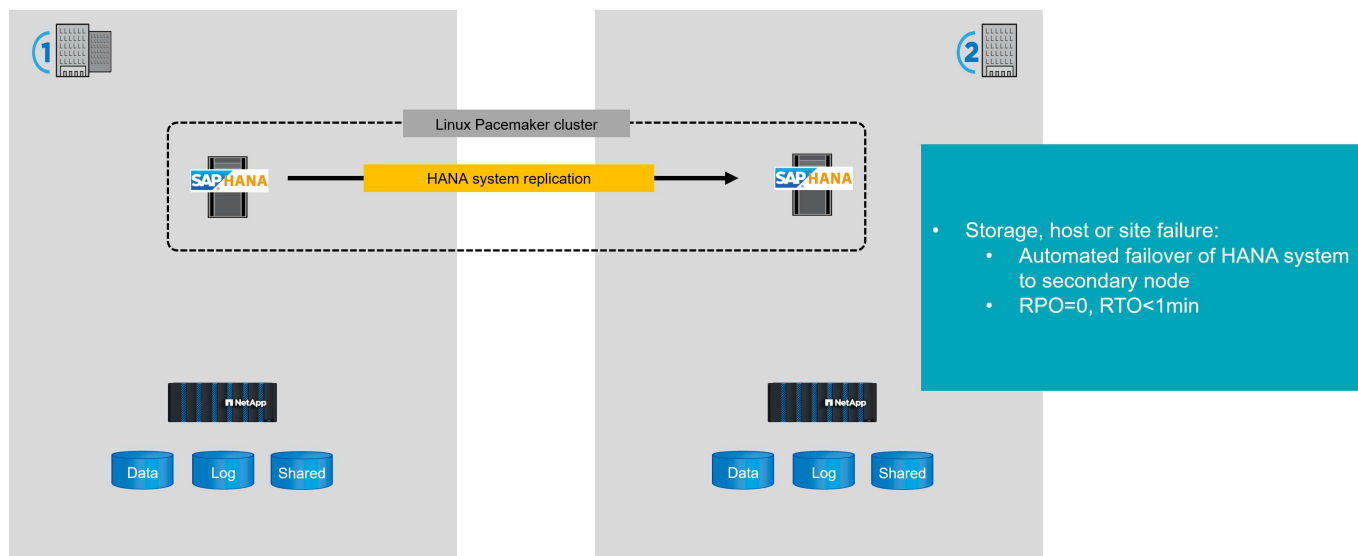
Este capítulo fornece uma visão geral das opções de alta disponibilidade para o SAP HANA que compara a replicação na camada de aplicação com a replicação de storage.

Replicação do sistema SAP HANA (HSR)

A replicação do sistema SAP HANA oferece um modo de operação no qual os dados são replicados de forma síncrona, pré-carregados na memória e atualizados continuamente no host secundário. Este modo permite valores de rto muito baixos, aproximadamente 1 minuto ou menos, mas também requer um servidor dedicado que é usado apenas para receber os dados de replicação do sistema de origem. Devido ao baixo tempo de failover, a replicação do sistema SAP HANA também costuma ser usada para operações de manutenção de inatividade quase zero, como atualizações de software HANA. As soluções de cluster do Linux Pacemaker são normalmente usadas para automatizar operações de failover.

Em caso de qualquer falha no local principal, no storage, no host ou no local completo, o sistema HANA faz failover automaticamente para o local secundário controlado pelo cluster do Linux Pacemaker.

Para obter uma descrição completa de todas as opções de configuração e cenários de replicação, "[SAP HANA System Replication e SAP Help Portal](#)" consulte .



Sincronização ativa do NetApp SnapMirror

O SnapMirror active Sync permite que os serviços empresariais continuem operando mesmo em uma falha completa do local, com suporte ao failover de aplicações de forma transparente, usando uma cópia secundária. Não há necessidade de intervenção manual ou script personalizado para acionar um failover com a sincronização ativa do SnapMirror. O SnapMirror active Sync é compatível com clusters AFF, clusters All-Flash SAN Array (ASA) e C-Series (AFF ou ASA). A sincronização ativa do SnapMirror protege aplicações com LUNs iSCSI ou FCP.

A partir do ONTAP 9.15.1, o SnapMirror active Sync é compatível com uma funcionalidade ativo-ativo simétrica. Ativo-ativo simétrico habilita operações de e/S de leitura e gravação de ambas as cópias de um LUN protegido com replicação síncrona bidirecional, de modo que ambas as cópias LUN possam servir operações de e/S localmente.

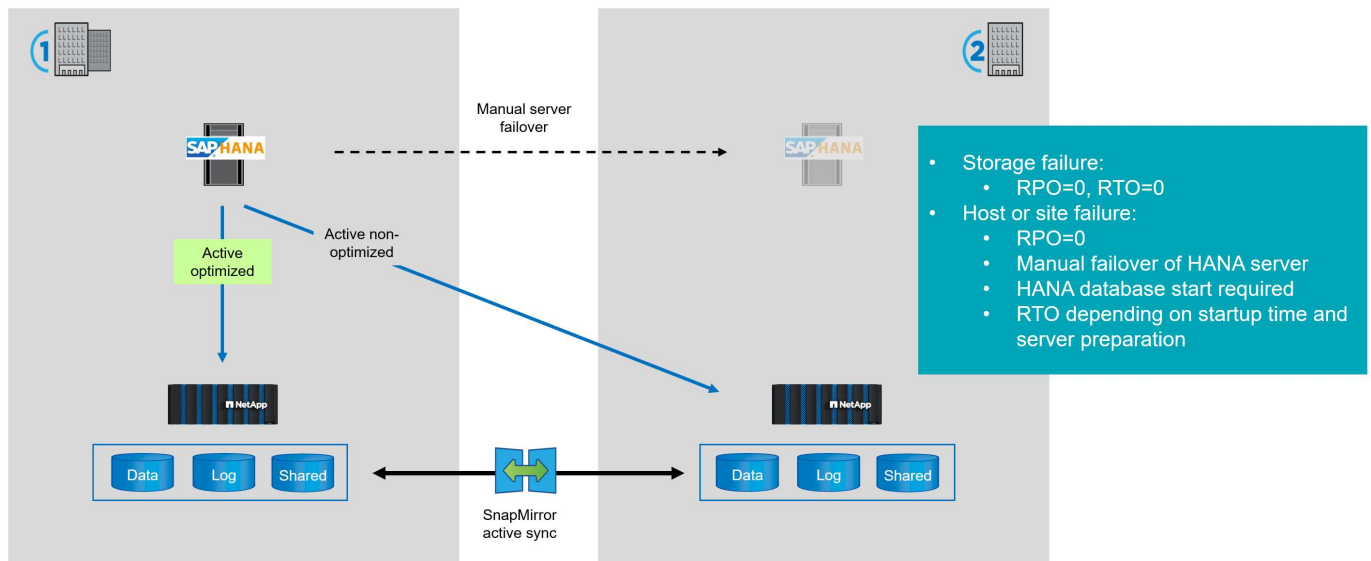
Mais detalhes podem ser encontrados em ["Descrição geral da sincronização ativa do SnapMirror no ONTAP"](#).

HANA bare metal

Ao executar o SAP HANA em um servidor bare metal, você pode usar o SnapMirror active Sync para fornecer uma solução de storage altamente disponível. Os dados são replicados de forma síncrona, fornecendo um RPO igual a 0.

No caso de uma falha de storage, o SISTEMA HANA acessará de forma transparente a cópia espelhada no local secundário usando o segundo caminho FCP que fornece rto de 0.

Em caso de falha de um host ou de um local completo, um novo servidor no local secundário precisa ser fornecido para acessar os dados do host com falha. Normalmente, este seria um sistema de teste ou QA do mesmo tamanho que a produção, que agora será desligado e será usado para executar o sistema de produção. Depois que os LUNs no local secundário forem conectados ao novo host, o banco de dados HANA precisa ser iniciado. Portanto, o rto total depende do tempo necessário para provisionar o host e o tempo de inicialização do banco de DADOS HANA.

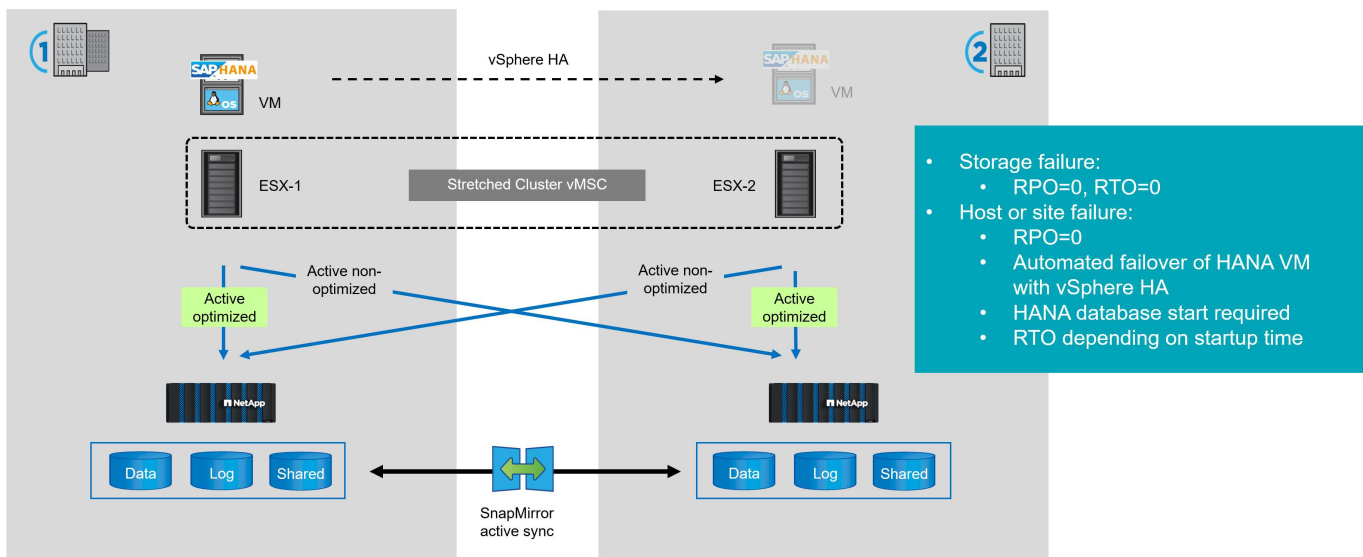


VSphere Metro Storage Cluster (vMSC)

Ao executar o SAP HANA em um ambiente VMware usando datastores anexados ao FCP, você pode usar a sincronização ativa do SnapMirror para criar um cluster de storage do VMware Metro. Em tal configuração, os armazenamentos de dados usados pelo sistema HANA são replicados de forma síncrona para o local secundário.

Em caso de falha de storage, o host ESX acessará automaticamente a cópia espelhada no local secundário fornecendo um rto de 0.

No caso de uma falha completa do host ou do local, o vSphere HA é usado para iniciar a VM HANA no host ESX secundário. Quando a VM HANA está em execução, o banco de DADOS HANA precisa ser iniciado. O rto total, portanto, depende principalmente do tempo de inicialização do banco de DADOS HANA.



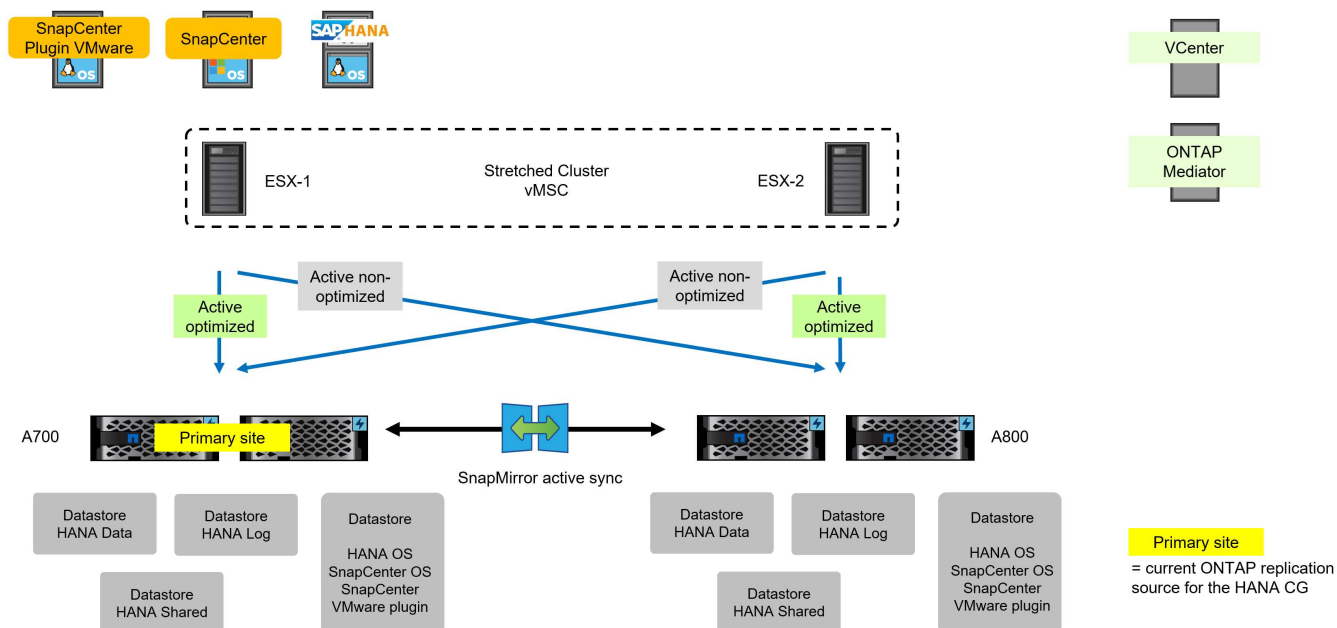
Comparação de soluções

A tabela a seguir fornece um resumo das principais características das soluções descritas acima.

	Replicação do sistema HANA	SnapMirror ativo Sync – bare metal	SnapMirror ativo Sync – VMware vMSC
RPO com qualquer falha	RPO igual a 0 e replicação síncrona		
Rto com falha de storage	Rto superior a 1min	Rto superior a 0 ms com failover de storage transparente	
Rto com falha do local ou do host	Rto superior a 1min	Rto: Dependendo do tempo necessário para a preparação do servidor e inicialização do banco de dados HANA.	Rto: Dependendo do tempo necessário para a inicialização do banco de dados HANA.
Automação de failover	Sim, Failover automatizado em host HSR secundário controlado pelo conjunto de pacemakers.	Sim, para falha de armazenamento Não, para falha do host ou do local (Provisionamento de host, conexão de recursos de storage, início do banco de dados HANA)	Sim, para falha de armazenamento Sim, para falha do host ou do local (Failover da VM para outro local automatizado com o vSphere HA, início do banco de dados HANA)
É necessário um servidor dedicado no local secundário	Sim, necessário para pré-carregar dados na memória e habilitar failover rápido com inicialização do banco de dados.	Não, o servidor só é necessário em caso de failover. Normalmente, o servidor usado para QA seria usado para produção.	Não, Os recursos no host ESX são necessários apenas em caso de failover. Normalmente, os recursos de QA seriam usados para produção.

Exemplo de visão geral da configuração

Na configuração do laboratório, estamos usando uma configuração de acesso uniforme, onde ambos os hosts ESX têm acesso a ambos os clusters de armazenamento. Nas próximas seções, descrevemos a configuração de acesso uniforme, mas também destacamos as diferenças para uma configuração não uniforme.



Versões de software

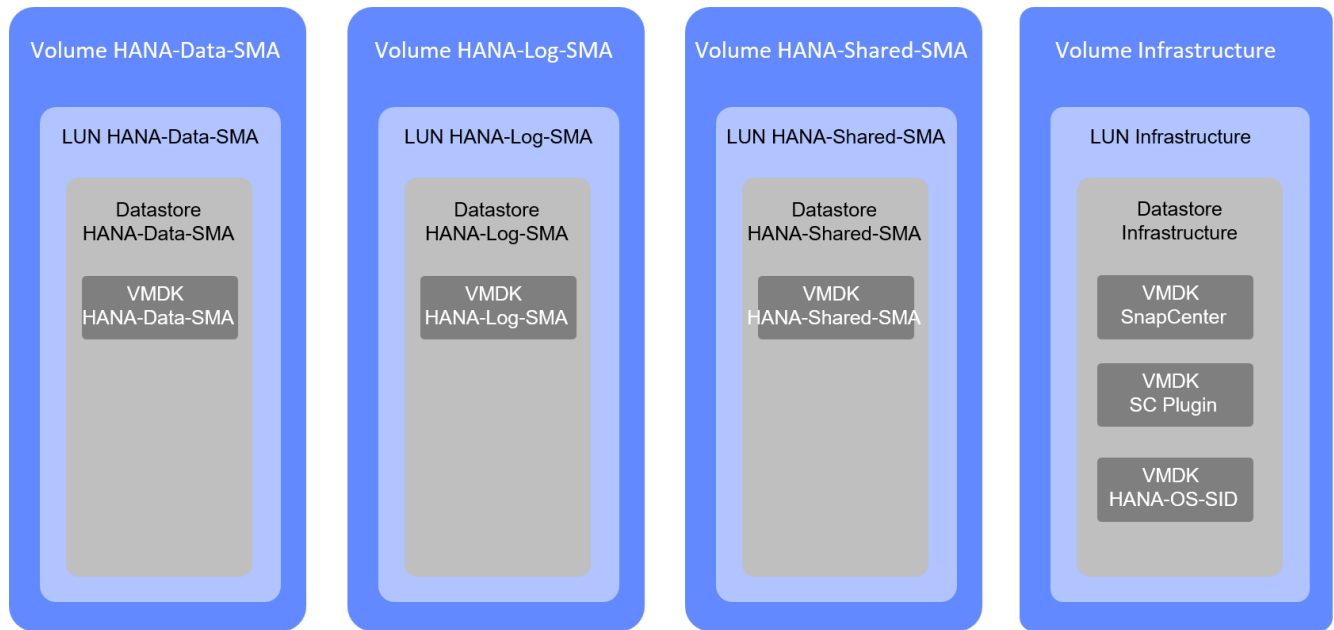
Software	Versão
ONTAP	A700: 9.15.1P7, A800: 9.16.1RC1
Cliente vSphere	8.0.3
ESXi	8.0.3
Plug-in do SnapCenter para vSphere	6.0.1
OS do Linux	SLES PARA SAP 15 SP5
SAP HANA	2,0 SPS8
SnapCenter	6.0.1

Provisionamento e instalação do SISTEMA HANA

Este capítulo descreve a instalação e configuração do sistema SAP HANA específico para uma configuração VMware usando VMFS. As melhores práticas genéricas adicionais podem ser encontradas em "[SAP HANA em sistemas NetApp AFF com protocolo Fibre Channel](#)".

Configuração de armazenamento

A figura abaixo mostra a configuração de storage e armazenamento de dados para o sistema HANA. Você deve configurar um volume dedicado, LUN, datastore para cada sistema de arquivos do sistema HANA. Os armazenamentos de dados não devem ser compartilhados em vários SISTEMAS HANA ou outros workloads.



Todos os três LUNs do SISTEMA HANA (HANA e HANA), bem como o LUN para as imagens do sistema operacional e os componentes do SnapCenter, foram provisionados no cluster de storage A700.



Todos os volumes do SISTEMA HANA devem ser provisionados no mesmo SVM. Na configuração de sincronização ativa do SnapMirror descrita posteriormente, criaremos um grupo de consistência em todos os três VOLUMES HANA, o que exige que os volumes estejam no mesmo SVM. O volume de infraestrutura estará em um grupo de consistência diferente e, portanto, poderá estar em um SVM diferente.

ONTAP System Manager

Search actions, objects, and pages

LUNs

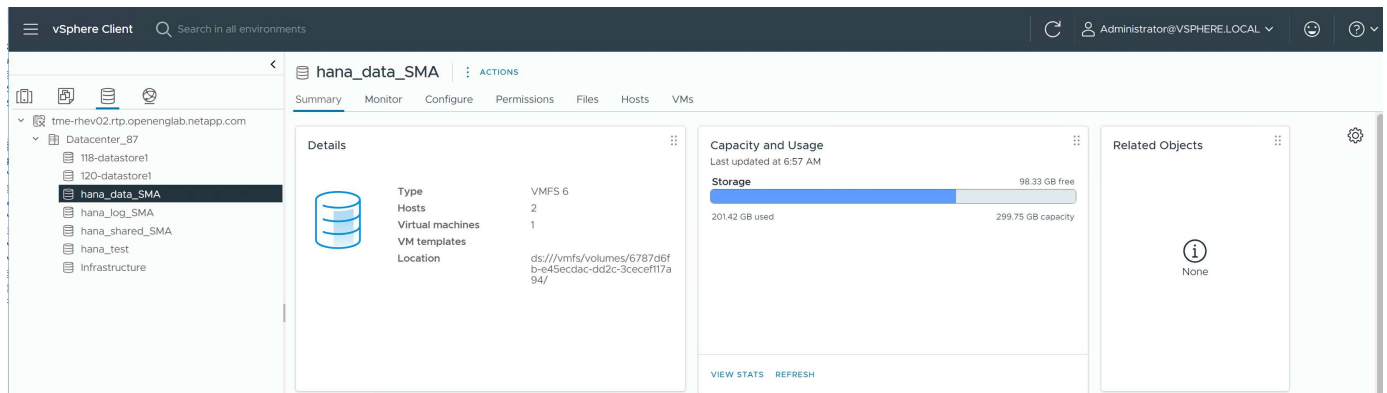
Name	Storage VM	Volume	Size	IOPS	Latency (ms)	Throughput (MB/s)
vvolPE-1724163990635	svm200_blueexpdr_a700s	vvol_FCoE_2	4 MiB	0	0	0
vvolPE-1724163990633	svm200_blueexpdr_a700s	vvol_FCoE_1	4 MiB	0	0	0
DraaS_qa_lun1	svm200_blueexpdr_a700s	DraaS_qa_lun1	200 GiB	0	0	0
DraaS_qa_lun2	svm200_blueexpdr_a700s	DraaS_qa_lun2	100 GiB	0	0	0
Infrastructure	svm200_blueexpdr_a700s	Infrastructure	2 TiB	50	0.31	0.58
hana_data_SMA	svm200_blueexpdr_a700s	hana_data_SMA	300 GiB	0	0.24	0
hana_log_SMA	svm200_blueexpdr_a700s	hana_log_SMA	158 GiB	0	0.24	0
hana_shared_SMA	svm200_blueexpdr_a700s	hana_shared_SMA	210 GiB	1	0.16	0.01
hana_test_lun	svm200_blueexpdr_a700s	hana_test_lun	1 TiB	0	0.39	0

Showing 1 - 9 of 9 LUNs

Um grupo de iniciadores deve ser configurado e os LUNs acima devem ser mapeados para o host ESX-1, que está próximo ao sistema de armazenamento A700 em nossa configuração de laboratório.

Provisionamento de datastore

Criamos três armazenamentos de dados para o sistema HANA usando os três LUNs provisionados anteriormente. Além disso, criamos um datastore de infraestrutura usando o LUN de infraestrutura.

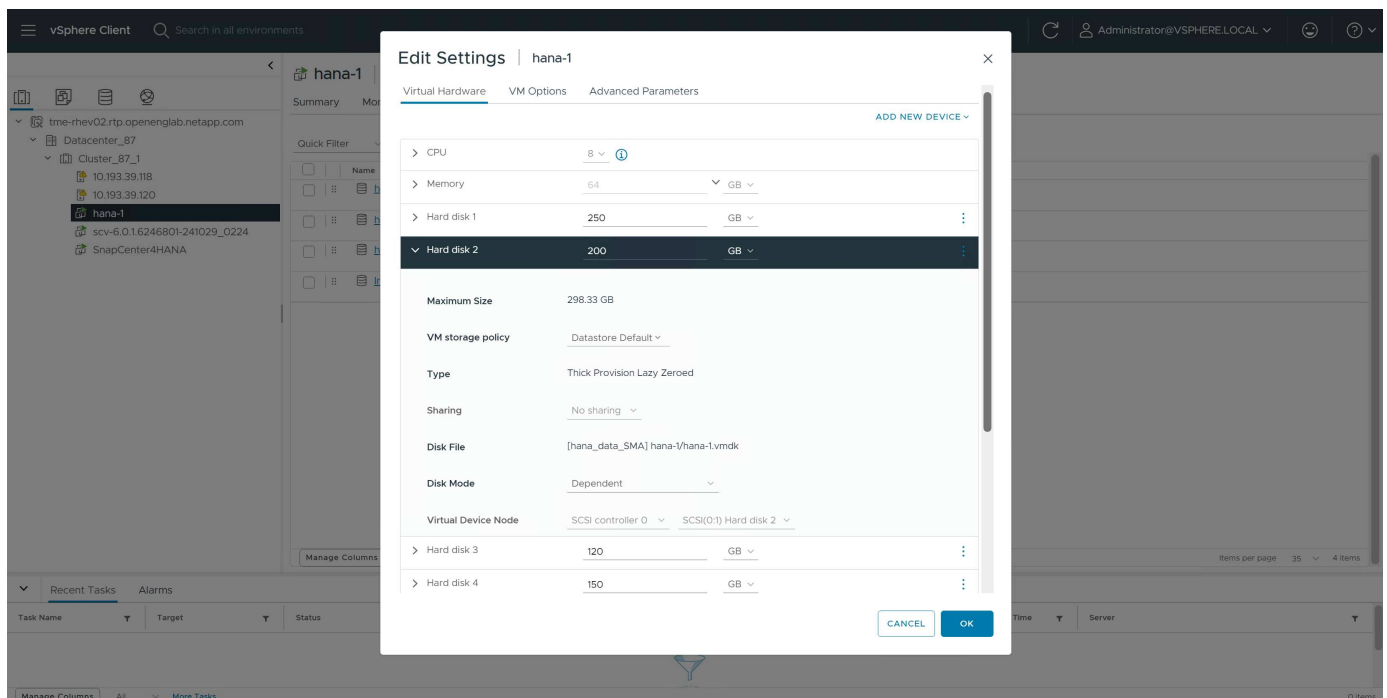


Provisionamento de VM e instalação do sistema operacional

Em nossa configuração de laboratório, implantamos uma nova VM e colocamos o VMDK para o sistema operacional Linux no datastore da infraestrutura.

Configuração de disco de VM

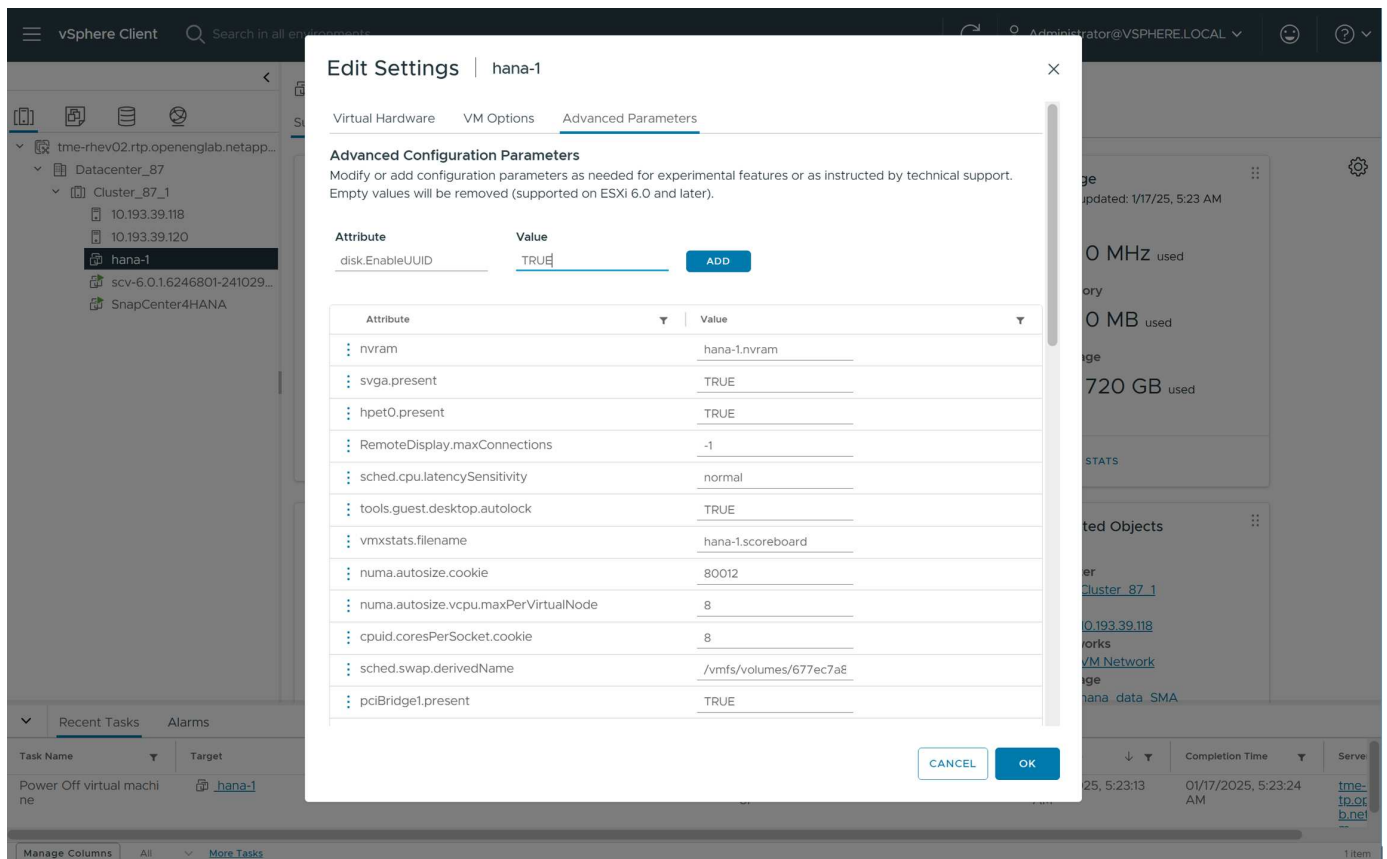
Três novos discos foram adicionados à VM HANA, cada disco em um dos datastores criados para o sistema HANA.



Configuração do parâmetro da VM

O parâmetro disk.EnableUID deve ser adicionado e definido como true . O parâmetro é exigido pelo SnapCenter. Se não definir a operação "descobrir recurso virtual" do SnapCenter falhará.

A VM deve ser parada antes que o parâmetro possa ser adicionado.



A funcionalidade pode ser verificada com o comando abaixo.

```
hana-1:~ # sg_inq /dev/sdd
standard INQUIRY:
PQual=0 PDT=0 RMB=0 LU_CONG=0 hot_pluggable=0 version=0x06 [SPC-4]
[AERC=0] [TrmTsk=] NormACA=0 HiSUP=0 Resp_data_format=2
SCCS=0 ACC=0 TPGS=0 3PC=0 Protect=0 [BQue=0]
EncServ=0 MultiP=0 [MChngr=0] [ACKREQQ=0] Addr16=0
[RelAdr=0] WBus16=1 Sync=1 [Linked=0] [TranDis=0] CmdQue=1
length=36 (0x24) Peripheral device type: disk
Vendor identification: VMware
Product identification: Virtual disk
Product revision level: 2.0
Unit serial number: 6000c293fecf25ac6bc457af67fe1f54
```

Preparação do sistema de arquivos no host Linux

Criação do sistema de arquivos xfs em novos discos

Os nomes dos dispositivos novos os novos discos podem ser verificados com o comando abaixo.

```

hana-1:/install # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 250G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
   ├─system-root 254:0 0 60G 0 lvm /root
   │ /var
   │ /usr/local
   │ /tmp
   │ /srv
   │ /opt
   │ /home
   │ /boot/grub2/x86++_++64-efi
   │ /boot/grub2/i386-pc
   │ /.snapshots
   │ /
   └─system-swap 254:1 0 2G 0 lvm SWAP
sdb 8:16 0 200G 0 disk
sdc 8:32 0 120G 0 disk
sdd 8:48 0 150G 0 disk
sr0 11:0 1 1024M 0 rom
hana-1:/install #

```

Um sistema de arquivos xfs foi criado em cada um dos três novos discos.

```

hana-1:/install # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=9830400 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=39321600, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=19200, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
hana-1:/install #

```

Criação de pontos de montagem

```
hana-1:/ # mkdir -p /hana/data/SMA/mnt00001
hana-1:/ # mkdir -p /hana/log/SMA/mnt00001
hana-1:/ # mkdir -p /hana/shared
hana-1:/ # chmod -R 777 /hana/log/SMA
hana-1:/ # chmod -R 777 /hana/data/SMA
hana-1:/ # chmod -R 777 /hana/shared
```

Configuração do /etc/fstab

```

hana-1:/install # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=@/var 0 0
/dev/system/root /usr/local btrfs subvol=@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=@/tmp 0 0
/dev/system/root /srv btrfs subvol=@/srv 0 0
/dev/system/root /root btrfs subvol=@/root 0 0
/dev/system/root /opt btrfs subvol=@/opt 0 0
/dev/system/root /home btrfs subvol=@/home 0 0
/dev/system/root /boot/grub2/x86_64-efi btrfs subvol=@/boot/grub2/x86_64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=@/boot/grub2/i386-pc 0 0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=@/.snapshots 0 0
UUID=2E8C-48E1 /boot/efi vfat utf8 0 2
/dev/sdb /hana/data/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-1:/install #

hana-1:/install # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 26M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 35G 25G 58% /
/dev/mapper/system-root 60G 35G 25G 58% /.snapshots
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 35G 25G 58% /home
/dev/mapper/system-root 60G 35G 25G 58% /opt
/dev/mapper/system-root 60G 35G 25G 58% /srv
/dev/mapper/system-root 60G 35G 25G 58% /tmp
/dev/mapper/system-root 60G 35G 25G 58% /usr/local
/dev/mapper/system-root 60G 35G 25G 58% /var
/dev/mapper/system-root 60G 35G 25G 58% /root
/dev/sda1 253M 5.1M 247M 3% /boot/efi
tmpfs 6.3G 56K 6.3G 1% /run/user/0
/dev/sdb 200G 237M 200G 1% /hana/data/SMA/mnt00001
/dev/sdc 120G 155M 120G 1% /hana/log/SMA/mnt00001
/dev/sdd 150G 186M 150G 1% /hana/shared
hana-1:/install #

```


INSTALAÇÃO HANA

A instalação HANA agora pode ser executada.



Com a configuração descrita, o diretório /usr/sap/SMA estará no VMDK do os. Se /usr/sap/SMA deve ser armazenado no VMDK compartilhado, o disco compartilhado HANA pode ser particionado para fornecer outro sistema de arquivos para /usr/sap/SMA.

Chave de armazenamento de usuários para SnapCenter

É necessário criar um arquivo de usuário para um usuário de banco de dados do sistema, que deve ser usado pelo SnapCenter. O número da instância DO HANA deve ser definido de acordo com a porta de comunicação. Em nossa instância de configuração, o número "00" é usado.

Uma descrição mais detalhada pode ser encontrada em ["Configuração específica de recursos do SnapCenter para backups de bancos de dados SAP HANA"](#)

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbuserstore set SMAKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

A conectividade pode ser verificada com o comando abaixo.

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbsql -U SMAKEY
Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit
smaadm@hana-1:/usr/sap/SMA/HDB00
```

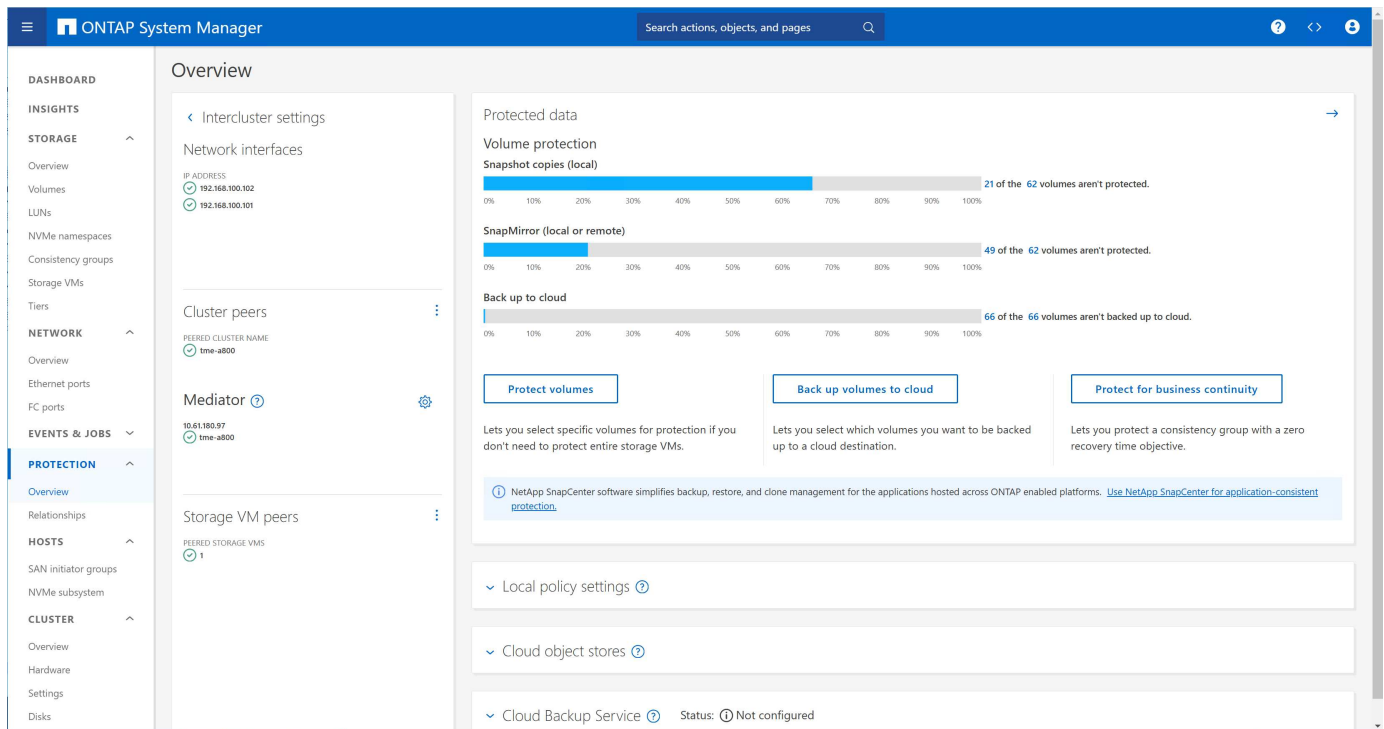
Configuração de sincronização ativa do SnapMirror

este artigo aborda as etapas de configuração necessárias para esta solução.

Pré-requisitos

Os clusters de storage e as SVMs relevantes devem ser colocados em Contato.

O ONTAP Mediator precisa estar disponível e configurado em ambos os clusters de storage.



Storage VM peers				
Protection overview				
+ Peer storage VMs				
Storage VM	Peered cluster	Peered storage VM	Status	Applications using this peer
svm200_blueexpdr_a700s	tme-a800	svm200_blueexpdr_a800	Peered	SnapMirror

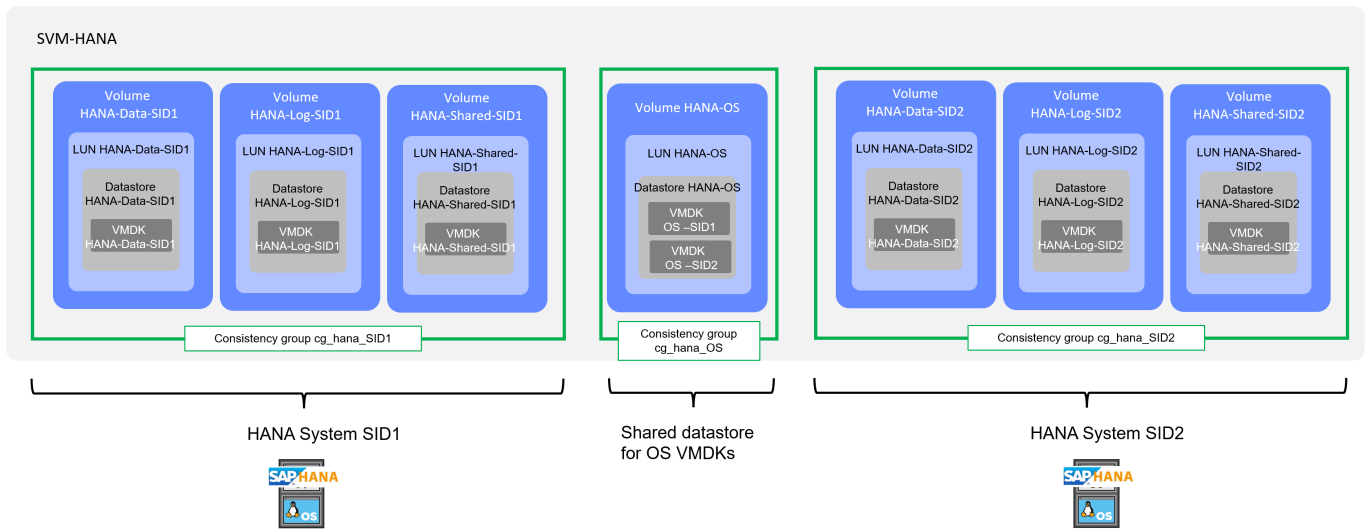
Layout de armazenamento e configuração de grupo de consistência

Na documentação do ONTAP "[Descrição geral da sincronização ativa do SnapMirror no ONTAP](#)", o conceito de grupos de consistência com a sincronização ativa do SnapMirror é descrito da seguinte forma:

Um grupo de consistência é uma coleção de volumes do FlexVol que oferece uma garantia de consistência para o workload da aplicação que precisa ser protegido para manter a continuidade dos negócios.

O objetivo de um grupo de consistência é tirar imagens instantâneas simultâneas de vários volumes, garantindo assim cópias consistentes com falhas de uma coleção de volumes em um momento. Um grupo de consistência garante que todos os volumes de um conjunto de dados sejam silenciados e, em seguida, encaixados exatamente no mesmo ponto no tempo. Isso fornece um ponto de restauração consistente com dados nos volumes que dão suporte ao conjunto de dados. Um grupo de consistência mantém, assim, consistência dependente da ordem de gravação. Se você decidir proteger aplicativos para a continuidade dos negócios, o grupo de volumes correspondentes a esse aplicativo deve ser adicionado a um grupo de consistência para que um relacionamento de proteção de dados seja estabelecido entre uma origem e um grupo de consistência de destino. A consistência de origem e destino deve conter o mesmo número e tipo de volumes.

Para a replicação de SISTEMAS HANA, o grupo de consistência precisa incluir todos os volumes usados pelo sistema HANA individual (dados, log e compartilhado). Os volumes que devem fazer parte de um grupo de consistência devem ser armazenados no mesmo SVM. As imagens do sistema operativo podem ser armazenadas num volume separado com o seu próprio grupo de consistência. A figura abaixo ilustra um exemplo de configuração com dois SISTEMAS HANA.



Configuração do grupo de iniciadores

Em nossa configuração de laboratório, criamos um grupo de iniciadores, incluindo as SVMs de storage, que são usadas para a replicação de sincronização ativa do SnapMirror. Na configuração de sincronização ativa do SnapMirror descrita posteriormente, definiremos que o grupo de iniciadores fará parte da replicação.

Usando as configurações de proximidade, definimos qual host do ESX está próximo a qual cluster de armazenamento. No nosso caso, o A700 está próximo do ESX-1 e o A800 está próximo do ESX-2.

ONTAP System Manager

Search actions, objects, and pages

SAN initiator groups

+ Add + Add to initiator group

cluster_87_1 All SAN initiator groups

Overview Hierarchy Mapped LUNs

STORAGE VM: svm200_bluexpdr_a700s

TYPE: VMware

PROTOCOL: Mixed (SCSI & FC)

COMMENT: -

CONNECTION STATUS: OK

Replication: OK

INITIATORS

Name	Description	Connection status	In proximity to
10:00:00:10:9b:17:04:69	-	OK	svm200_bluexpdr_a700s
10:00:00:10:9b:17:04:6a	-	OK	svm200_bluexpdr_a700s
10:00:00:10:9b:40:b9:7f	-	OK	svm200_bluexpdr_a800
10:00:00:10:9b:40:b9:80	-	OK	svm200_bluexpdr_a800

ESX-1

ESX-2

ONTAP System Manager

Search actions, objects, and pages

?

<>

!

DASHBOARD

INSIGHTS

STORAGE

Overview

Volumes

LUNs

NVMe namespaces

Consistency groups

Storage VMs

Tiers

NETWORK

Overview

Ethernet ports

FC ports

EVENTS & JOBS

PROTECTION

HOSTS

SAN initiator groups

NVMe subsystem

CLUSTER

SAN initiator groups

+ Add

+ Add to initiator group

Search

Filter

cluster_87_1

All SAN initiator groups

Edit

Delete

Overview

Hierarchy

Mapped LUNs

Name

cluster_87_1

esxi_118

esxi_120

INITIATOR GROUP TYPE

Nested initiator group

Replication

REPLICATED TO CLUSTER

time-a800

REPLICATION STATUS

OK

Initiators

Name	Description	Connection status	In proximity to
10.00.00:10:9b:17...	-	OK	svm200_bluexpdr...
10.00.00:10:9b:17...	-	OK	svm200_bluexpdr...
10.00.00:10:9b:40...	-	OK	svm200_bluexpdr...
10.00.00:10:9b:40...	-	OK	svm200_bluexpdr...

Mapped LUNs

Name	ID
hana_data_SMA	1
hana_log_SMA	2
hana_shared_SMA	3
hana_test_lun	4

Em uma configuração de acesso não uniforme, o grupo de iniciadores no cluster de armazenamento primário (A700) deve incluir somente os iniciadores do host ESX-1, já que não há conexão SAN ao ESX-2. Além disso, você precisa configurar outro grupo de iniciadores no segundo cluster de armazenamento (A800), que inclui apenas os iniciadores do host ESX-2. A configuração de proximidade e a replicação do grupo de iniciadores não são necessárias.

Configure a proteção com o gerenciador de sistema ONTAP

ONTAP System Manager

Search actions, objects, and pages

?

<>

!

DASHBOARD

INSIGHTS

STORAGE

Overview

Volumes

LUNs

NVMe namespaces

Consistency groups

Storage VMs

Tiers

NETWORK

EVENTS & JOBS

PROTECTION

HOSTS

SAN initiator groups

NVMe subsystem

CLUSTER

Overview

Intercluster settings

Network interfaces

Cluster peers

Mediator

Storage VM peers

Protected data

Volume protection

Snapshot copies (local)

Back up to cloud

Protect volumes

Back up volumes to cloud

Protect for business continuity

Local policy settings

Cloud object stores

Cloud Backup Service

Replicação do grupo de consistência e do grupo de iniciadores

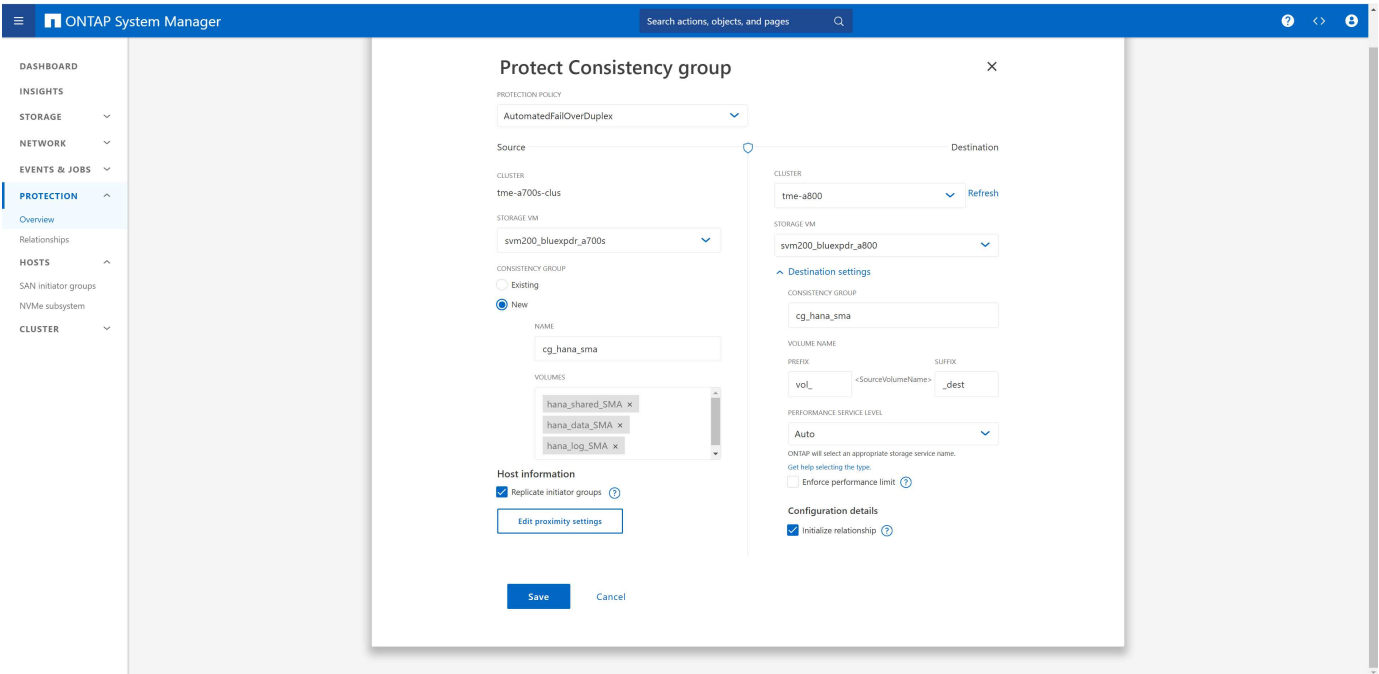
É necessário criar um novo grupo de consistência e adicionar todos os três LUNs do sistema HANA ao grupo de consistência.

148

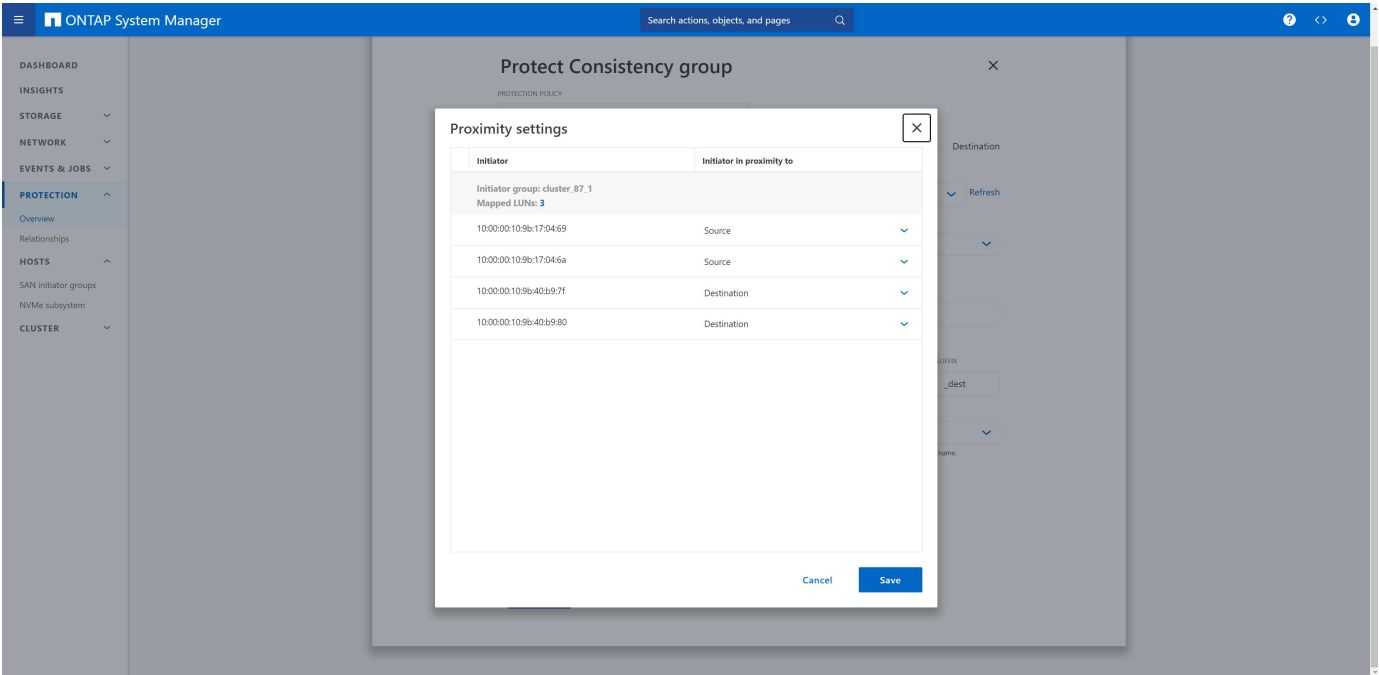
"Replicar grupo de iniciadores" foi ativado. O grupo imitator permanecerá em sincronia independente onde as alterações são feitas.



Em uma configuração de acesso não uniforme, o grupo de iniciadores não deve ser replicado, uma vez que um grupo de iniciadores separado deve ser configurado no segundo cluster de armazenamento.



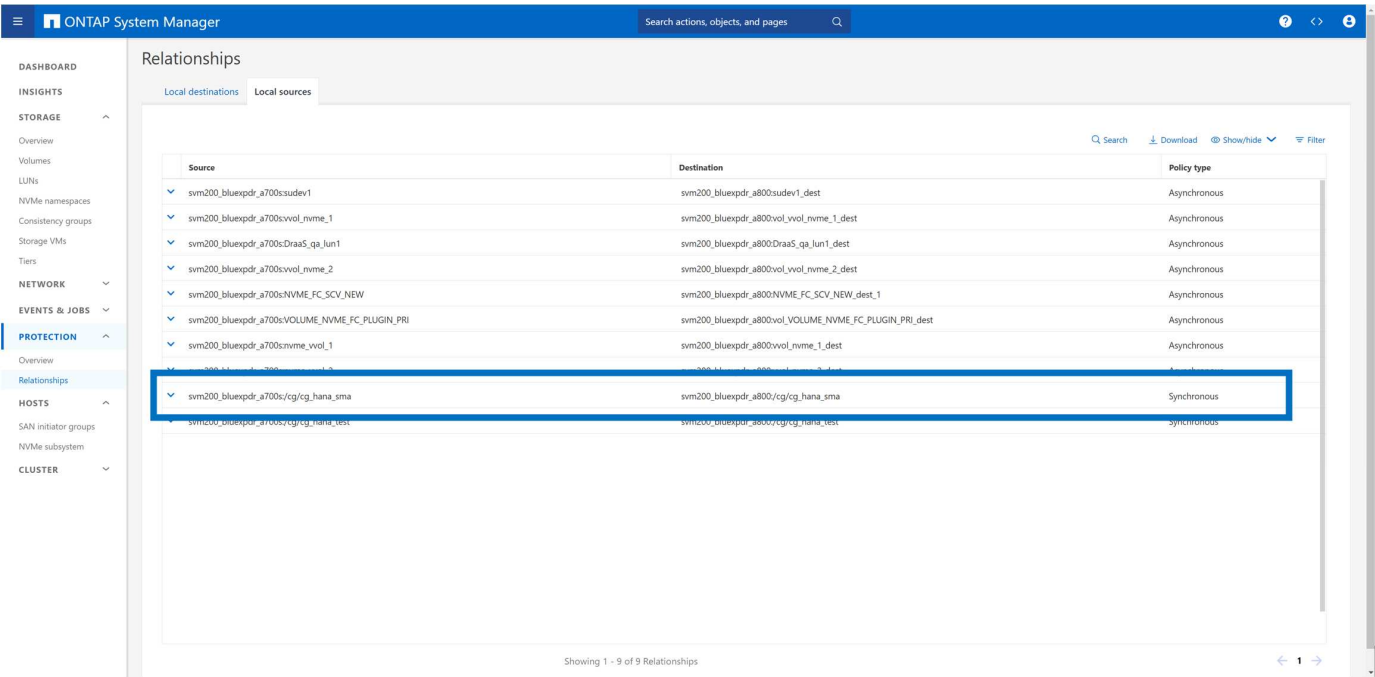
Ao clicar nas definições de proximidade, pode rever a configuração efetuada antes na configuração do grupo de iniciadores.



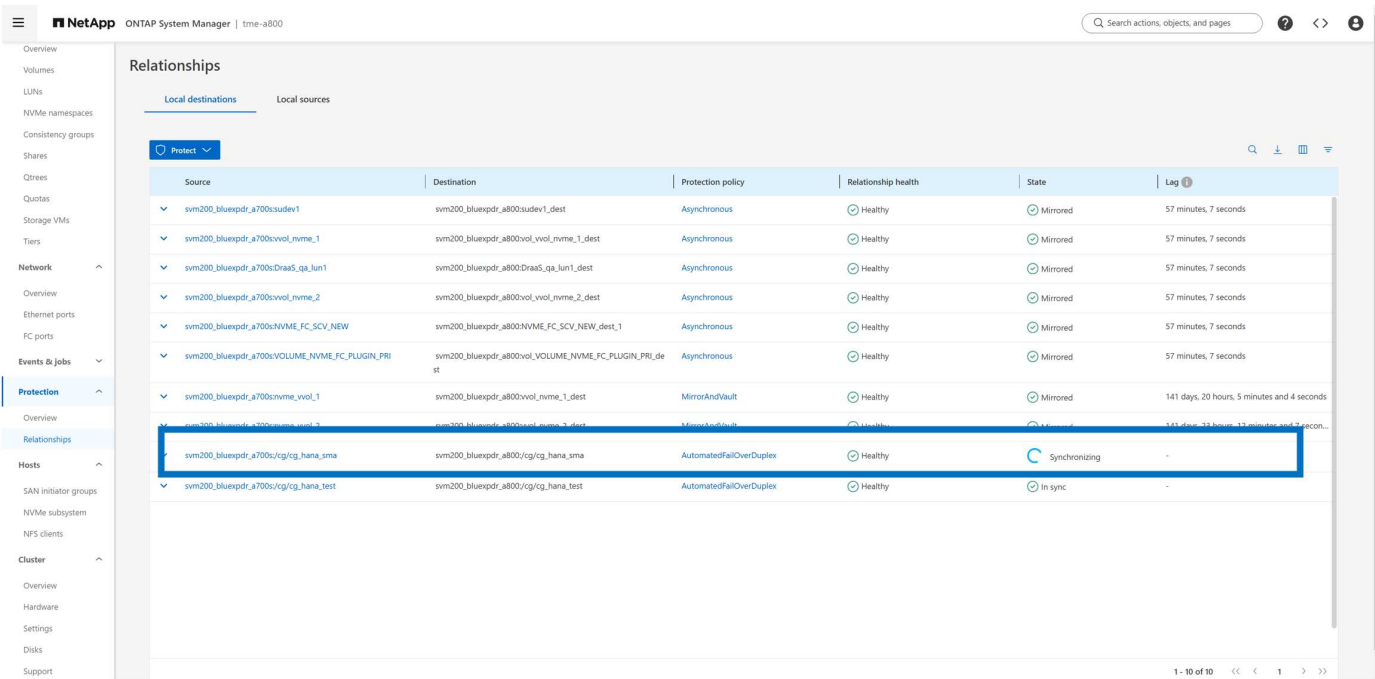
O cluster de armazenamento de destino deve ser configurado e "inicializar relacionamento" deve ser ativado.

Sincronização

No cluster de armazenamento A700 (fonte), a nova relação está agora listada.



No cluster de armazenamento A800 (destino), a nova relação e o status da replicação são listados.



Armazenamento de dados da infraestrutura

O armazenamento de dados, onde as imagens do SISTEMA OPERACIONAL do HANA, do SnapCenter e do plug-in vSphere são armazenadas, é replicado da mesma forma que descrito para os datastores do banco de dados HANA.

Local principal

O comportamento de sincronização ativa do SnapMirror é simétrico, com uma exceção importante - a configuração do site principal.

A sincronização ativa do SnapMirror considerará um site a "fonte" e o outro o "destino". Isso implica uma relação de replicação unidirecional, mas isso não se aplica ao comportamento de IO. A replicação é bidirecional e simétrica, e os tempos de resposta de e/S são os mesmos em ambos os lados do espelho.

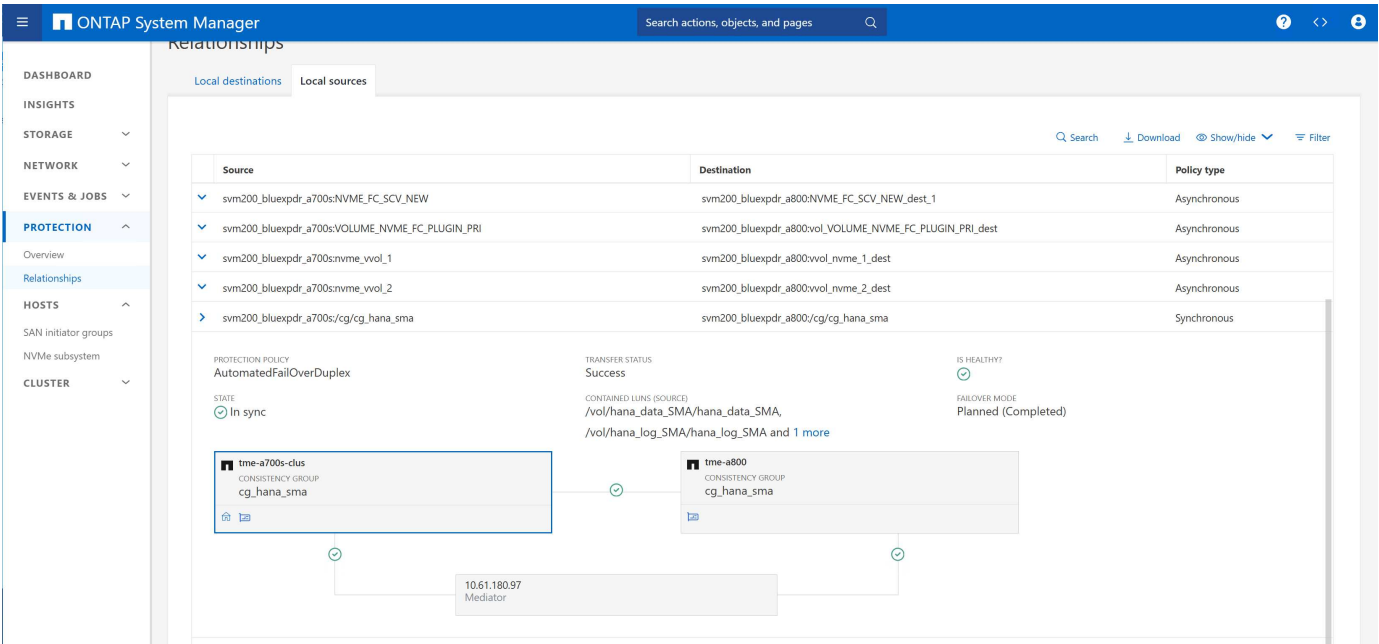
Se o link de replicação for perdido, os caminhos de LUN na cópia de origem continuarão a servir dados enquanto os caminhos de LUN na cópia de destino ficarão indisponíveis até que a replicação seja restabelecida e o SnapMirror entre novamente em um estado síncrono. Os caminhos irão então retomar a veiculação de dados.

O efeito de designar um cluster como uma fonte simplesmente controla qual cluster sobrevive como um sistema de armazenamento de leitura e gravação se o link de replicação for perdido.

O local principal é detetado pelo SnapCenter e usado para executar operações de backup, restauração e clonagem.



Lembre-se de que a origem e o destino não estão vinculados ao SVM ou ao cluster de storage, mas podem ser diferentes para cada relacionamento de replicação.



Configuração do SnapCenter

Conforme declarado no início do documento, o objetivo do documento é fornecer as melhores práticas para um AMBIENTE HANA usando o VMware com VMFS e a sincronização ativa do SnapMirror. Apenas abordaremos detalhes e etapas importantes relevantes para esta solução específica e não explicaremos os conceitos gerais do SnapCenter. Estes conceitos e outras informações adicionais sobre o SnapCenter podem ser encontrados em:

["Backup e recuperação do SAP HANA com o SnapCenter"](#)

"Replicação do sistema SAP HANA: Backup e recuperação com o SnapCenter"

"Automatizando as operações de clonagem e cópia do sistema SAP HANA com o SnapCenter"

Pré-requisitos

Em geral, a sincronização ativa do SnapMirror deve ser configurada antes que os recursos protegidos sejam adicionados ao SnapCenter. Se os backups tiverem sido criados antes da configuração da sincronização ativa do SnapMirror, eles só existirão no armazenamento primário original e não serão replicados posteriormente.

O recurso do SnapCenter HANA deve ser descoberto automaticamente

Os recursos configurados com o VMware VMFS ou os recursos protegidos com a sincronização ativa do SnapMirror devem ser automaticamente descobertos pelo SnapCenter para permitir operações específicas necessárias para essas configurações.

Como os volumes que não são de dados HANA sempre são recursos configurados manualmente no SnapCenter, eles não são compatíveis com o SnapCenter pronto para uso. Discutiremos opções e soluções alternativas para volumes que não sejam de dados posteriormente neste documento.

Vários sistemas host do SAP HANA devem ser configurados usando um plug-in HANA central e, portanto, são recursos configurados manualmente por padrão. Esses SISTEMAS HANA não são compatíveis com o SnapCenter ao usar o VMware VMFS ou a sincronização ativa do SnapMirror.

SnapCenter para VMware vSphere

O plug-in do SnapCenter para VMware vSphere deve ser implantado no ambiente VMware.

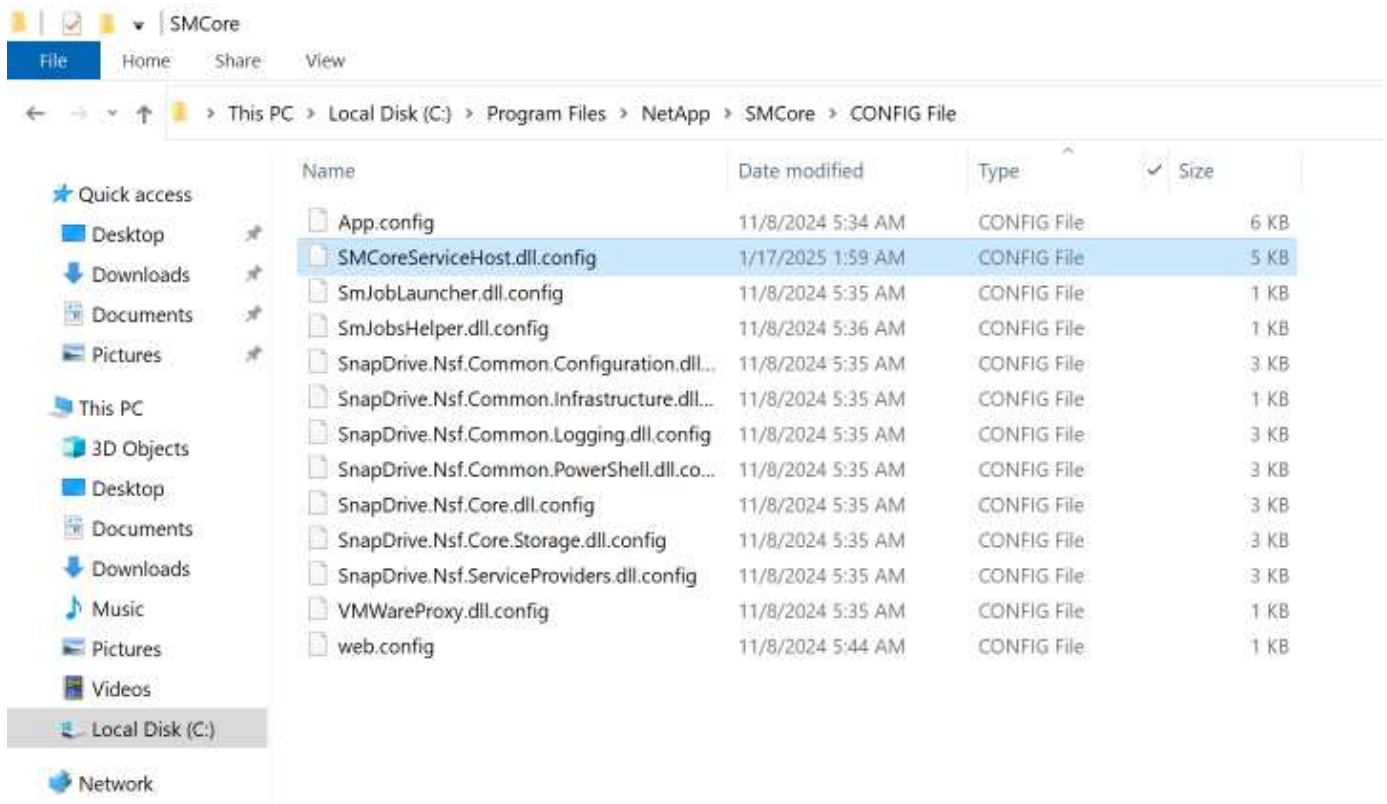
Endereço IP de gerenciamento no SVM que hospeda os volumes

Mesmo que os clusters sejam adicionados ao SnapCenter, os SVMs que hospedam os volumes de origem e destino devem ter um endereço IP de gerenciamento configurado.

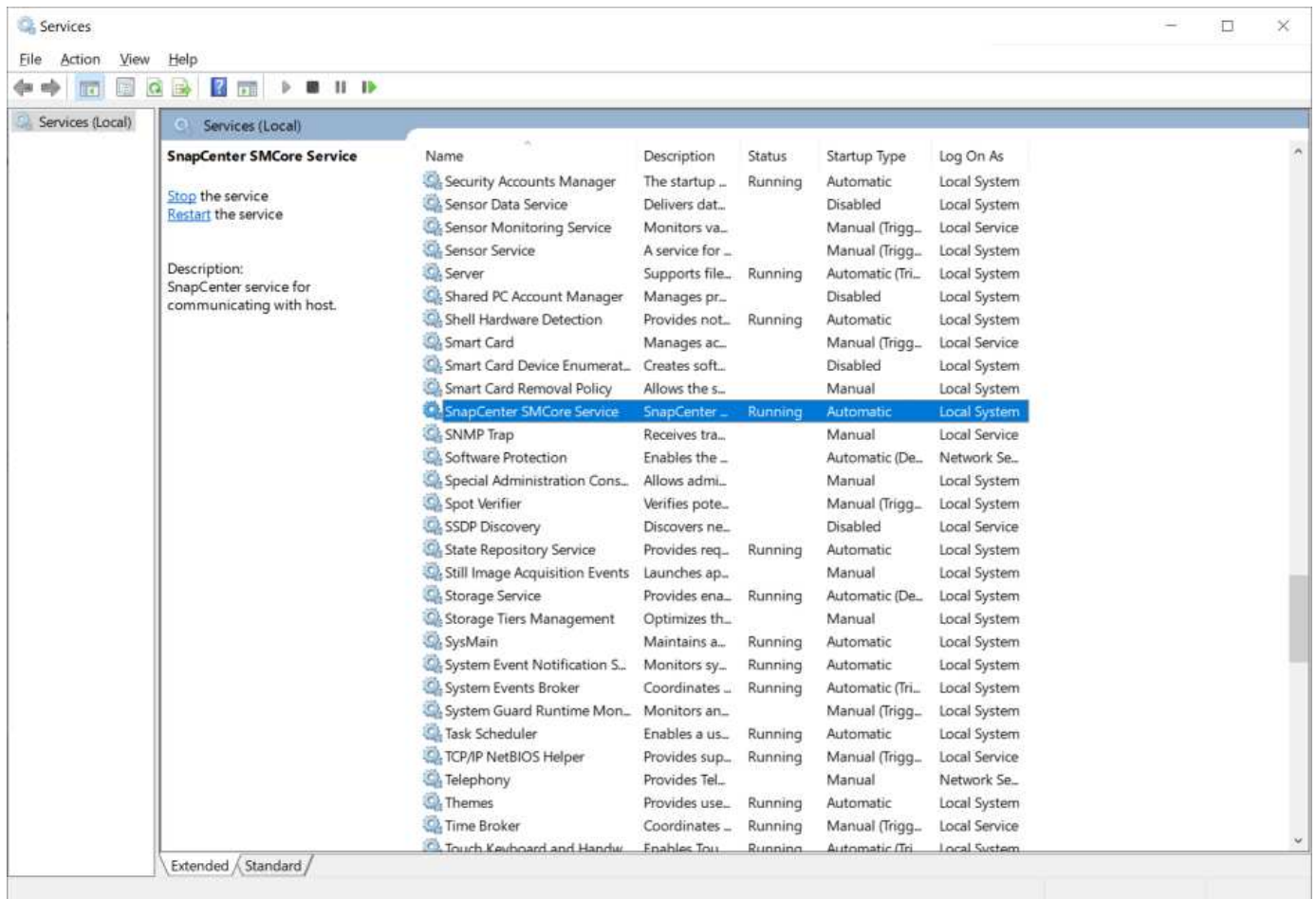
APIs REST para comunicação de storage

O gerenciamento e o monitoramento da sincronização ativa do SnapMirror exigem acesso à API REST. Portanto, o SnapCenter deve ser configurado para usar APIs REST para comunicações de storage. O parâmetro "IsRestEnabledForStorageConnection" no arquivo de configuração C: NetApp.dll.config deve ser definido como true.

```
<add key="IsRestEnabledForStorageConnection" value="true">
```

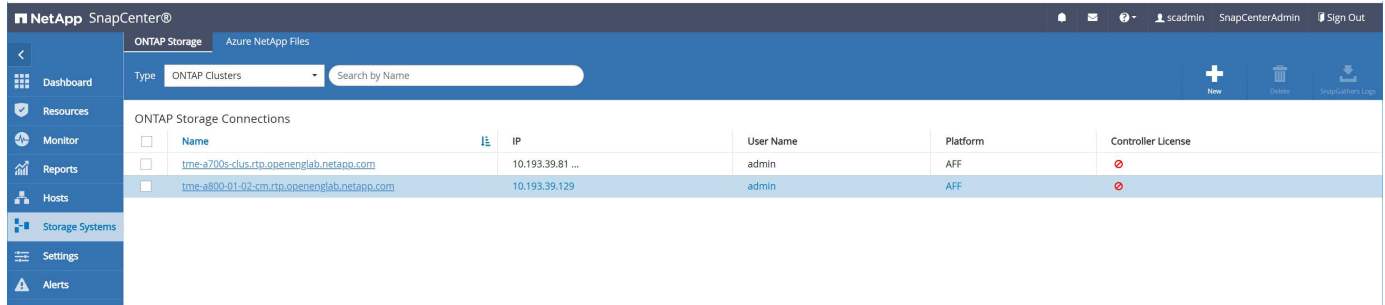



Após a alteração do parâmetro, o serviço SnapCenter SMCore deve ser reiniciado.



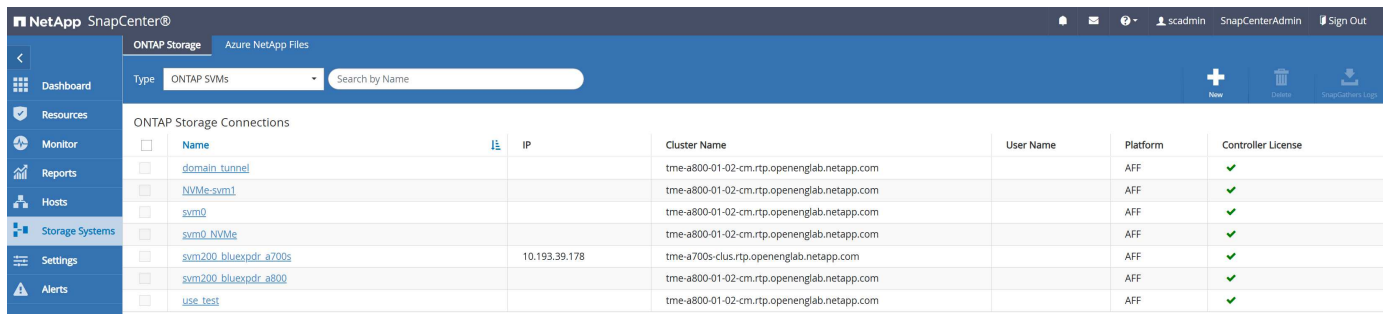
Adicione sistemas de storage

Os sistemas de storage podem ser adicionados depois que a API REST estiver habilitada para SnapCenter. É necessário adicionar os dois clusters de storage, e não o SVM individual.



The screenshot shows the NetApp SnapCenter interface with the 'ONTAP Storage' tab selected. The 'Type' is set to 'ONTAP Clusters'. The table below lists the storage connections.

Name	IP	User Name	Platform	Controller License
tme-a700s-clus.rtp.openenglab.netapp.com	10.193.39.81 ...	admin	AFF	⊘
tme-a800-01-02-cm.rtp.openenglab.netapp.com	10.193.39.129	admin	AFF	⊘



The screenshot shows the NetApp SnapCenter interface with the 'ONTAP Storage' tab selected. The 'Type' is set to 'ONTAP SVMs'. The table below lists the storage connections.

Name	IP	Cluster Name	User Name	Platform	Controller License
domain_tunnel		tme-a800-01-02-cm.rtp.openenglab.netapp.com		AFF	✓
NVMe-svm1		tme-a800-01-02-cm.rtp.openenglab.netapp.com		AFF	✓
svm0		tme-a800-01-02-cm.rtp.openenglab.netapp.com		AFF	✓
svm0_NVMe		tme-a800-01-02-cm.rtp.openenglab.netapp.com		AFF	✓
svm200_bluexpdr_a700s	10.193.39.178	tme-a700s-clus.rtp.openenglab.netapp.com		AFF	✓
svm200_bluexpdr_a800		tme-a800-01-02-cm.rtp.openenglab.netapp.com		AFF	✓
use_test		tme-a800-01-02-cm.rtp.openenglab.netapp.com		AFF	✓

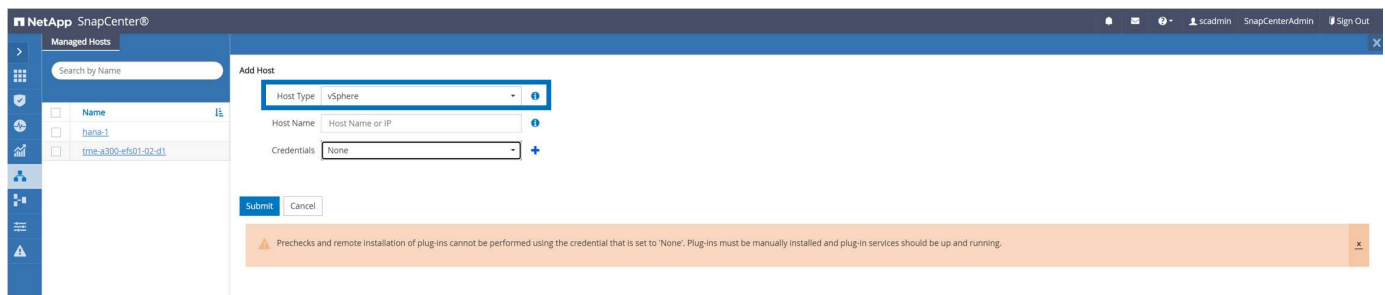
Adicionar host – plugin SnapCenter para VMware vSphere

Se um recurso no SnapCenter estiver sendo executado em um ambiente VMware virtualizado, o SnapCenter aproveita o plug-in do SnapCenter para VMware vSphere para estender os fluxos de trabalho de backup, restauração e clonagem do SnapCenter com as etapas necessárias na camada VMware.

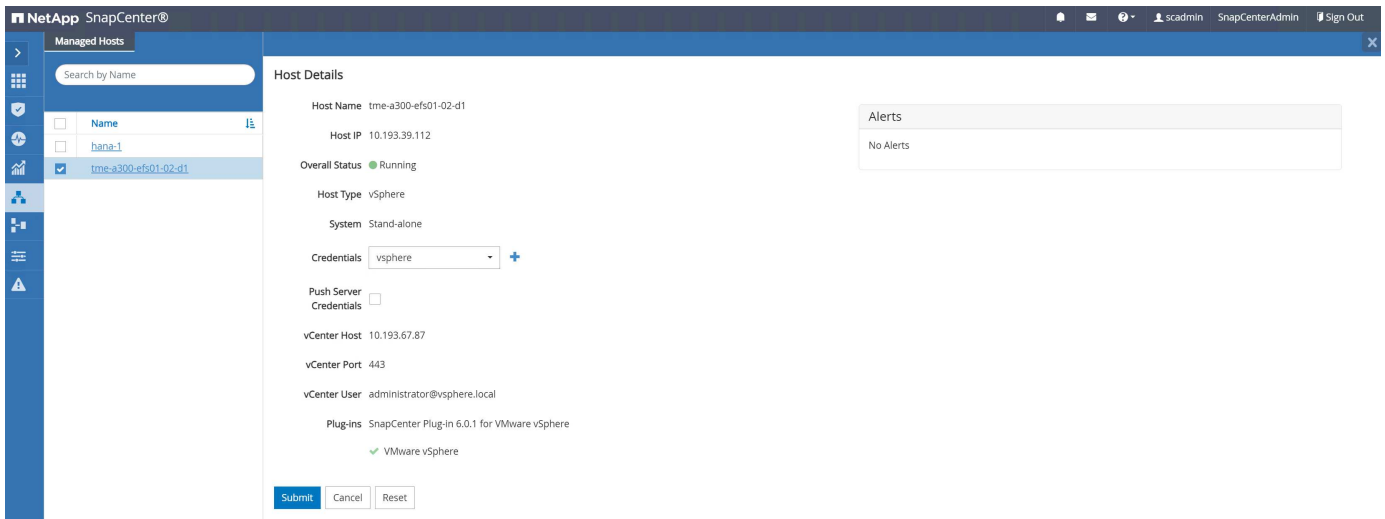
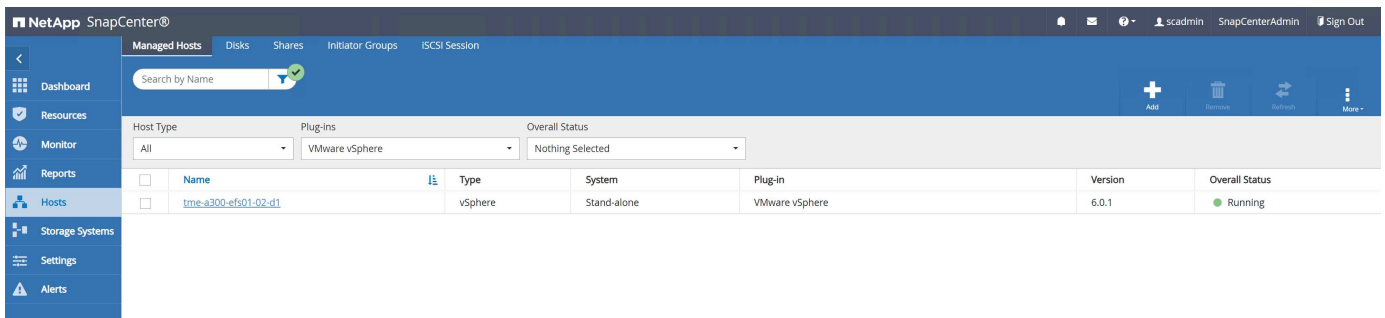
Antes que o host possa ser adicionado ao SnapCenter, o plug-in do SnapCenter para VMware vSphere deve ser implantado no ambiente VMware.



As credenciais devem ser definidas durante o fluxo de trabalho de adição do host, em que o vSphere pode ser selecionado como um tipo de host.



The screenshot shows the NetApp SnapCenter interface with the 'Managed Hosts' tab selected. The 'Add Host' dialog is open, showing the 'Host Type' set to 'vSphere'. The 'Host Name' field is empty, and the 'Credentials' field is set to 'None'. A warning message at the bottom states: 'Prechecks and remote installation of plug-ins cannot be performed using the credential that is set to 'None'. Plug-ins must be manually installed and plug-in services should be up and running.'



Nenhuma configuração adicional necessária no próprio plugin SnapCenter for vSphere.

Adicionar host – sistema HANA



Sem requisitos específicos. A implantação do plugin e a descoberta automática são feitas como de costume.

Com o processo de detecção automática, o SnapCenter deteta que o recurso HANA está sendo executado virtualizado com VMFS/VMDKs. O SnapCenter também deteta a configuração de sincronização ativa do SnapMirror e identifica o site principal atual.

Após a detecção automática de recursos, o local principal atual é mostrado na seção espaço físico do armazenamento da exibição de recursos. A detecção de qual sistema de armazenamento é mestre é baseada na saída do comando ONTAP, que é usado pelo SnapCenter.

```
volume show -vserver <vs> -volume <vol> -fields smbc-consensus,is-smbc-master
```

NetApp SnapCenter®

SAP HANA

Search databases

System

SMA

Resource - Details

Details for selected resource

Type	Multitenant Database Container
HANA System Name	SMA
SID	SMA
Tenant Databases	SMA
Plug-In Host	hana-1
HDB Secure User Store Key	SMAKEY
HDBSQL OS User	smaadm
Log backup location	/usr/sap/SMA/HDB00/backup/log
Backup catalog location	/usr/sap/SMA/HDB00/backup/log
System Replication	None
Plug-in name	SAP HANA
Last backup	01/29/2025 3:14:18 AM (Completed)
Resource Groups	hana-1_hana_MDC_SMA
Policy	SM-AS-Policy
Discovery Type	Auto

Storage Footprint

SVM	Volume	Junction Path	LUN/Qtree
10.193.39.178	hana_data_SMA		hana_data_SMA

Configuração da política

A política usada para o recurso protegido com a sincronização ativa do SnapMirror deve ser configurada usando a replicação do SnapMirror, mesmo que o SnapCenter não acione nenhuma operação de atualização do SnapMirror.

Modify SAP HANA Backup Policy

1 Name

2 Policy type

3 Snapshot

4 Replication and backup

5 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label: Hourly

Error retry count: 3

NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

SAP HANA

Search by Name

Name	Scope	Schedule Type	Snapshot	Backup	Replication
SM-AS-Policy	Data Backup	Hourly	Copies to keep : 7 copies		SnapMirror

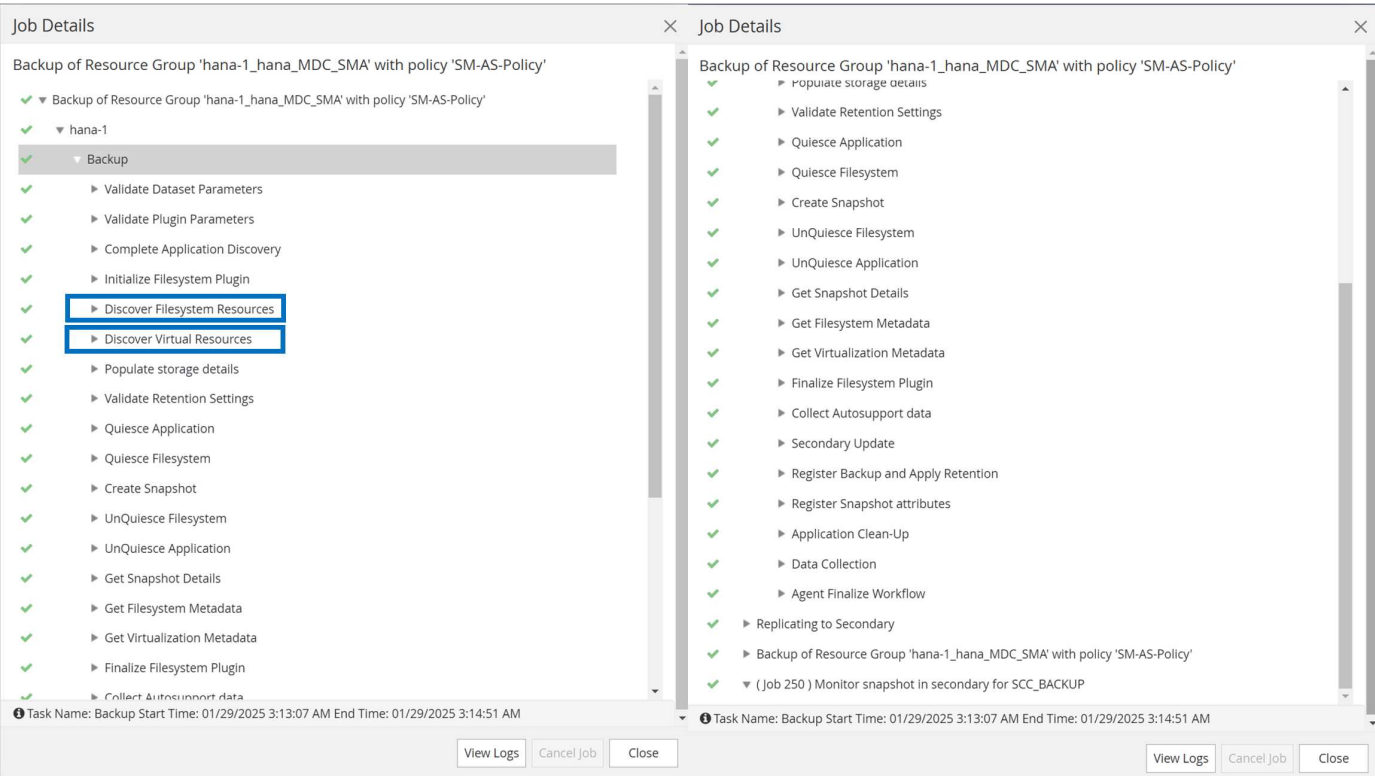
Configuração de proteção de recursos DO HANA

Sem requisitos específicos. A configuração de proteção de recursos é feita como de costume.

Operações de backup do SnapCenter

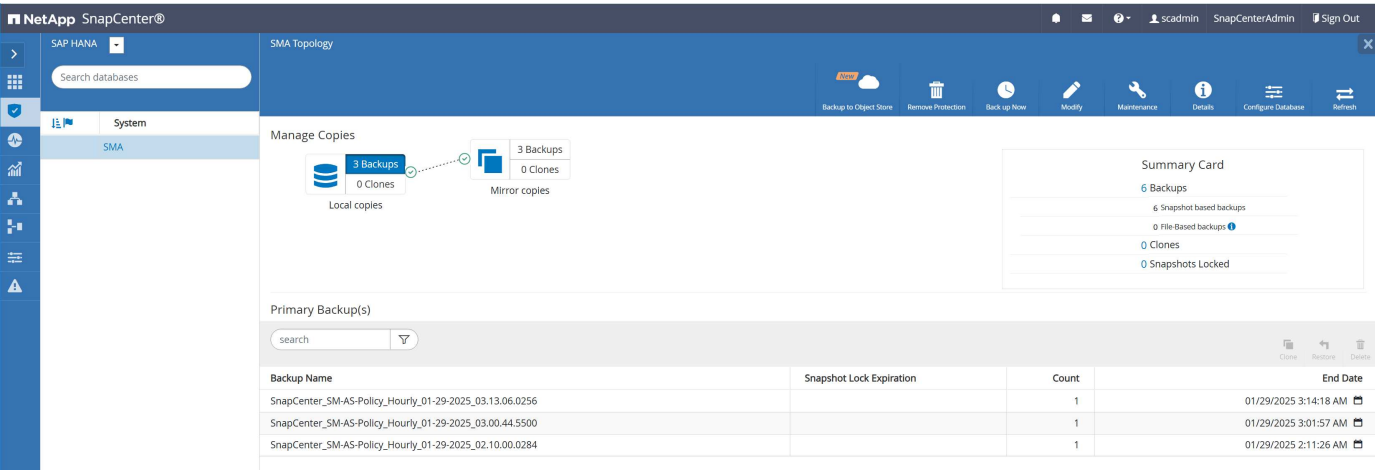
Com cada operação de backup, o SnapCenter executa a descoberta no lado da VMware,

bem como a detecção do local principal. Se houver um failover de storage, o SnapCenter detetará o novo local primário assim que um backup for executado para o recurso.



Visualização da topologia

Na visualização de topologia, o SnapCenter mostra os backups dos clusters de storage de origem e destino.



The screenshot displays the NetApp SnapCenter web interface. The top navigation bar includes the NetApp logo, user profile, and various system icons. The left sidebar contains navigation options like Home, System, and SMA. The main content area is titled "SMA Topology" and shows a diagram of the storage management architecture. Below the diagram, there's a "Manage Copies" section with a summary card indicating 6 Backups, 6 Snapshot based backups, 0 File-Based backups, 0 Clones, and 0 Snapshots Locked. A table at the bottom lists backup details.

Backup Name	Snapshot Lock Expiration	Count	End Date
SnapCenter_SM-AS-Policy_Hourly_01-29-2025_03.13.06.0256		1	01/29/2025 3:14:18 AM
SnapCenter_SM-AS-Policy_Hourly_01-29-2025_03.00.44.5500		1	01/29/2025 3:01:57 AM
SnapCenter_SM-AS-Policy_Hourly_01-29-2025_02.10.00.0284		1	01/29/2025 2:11:26 AM

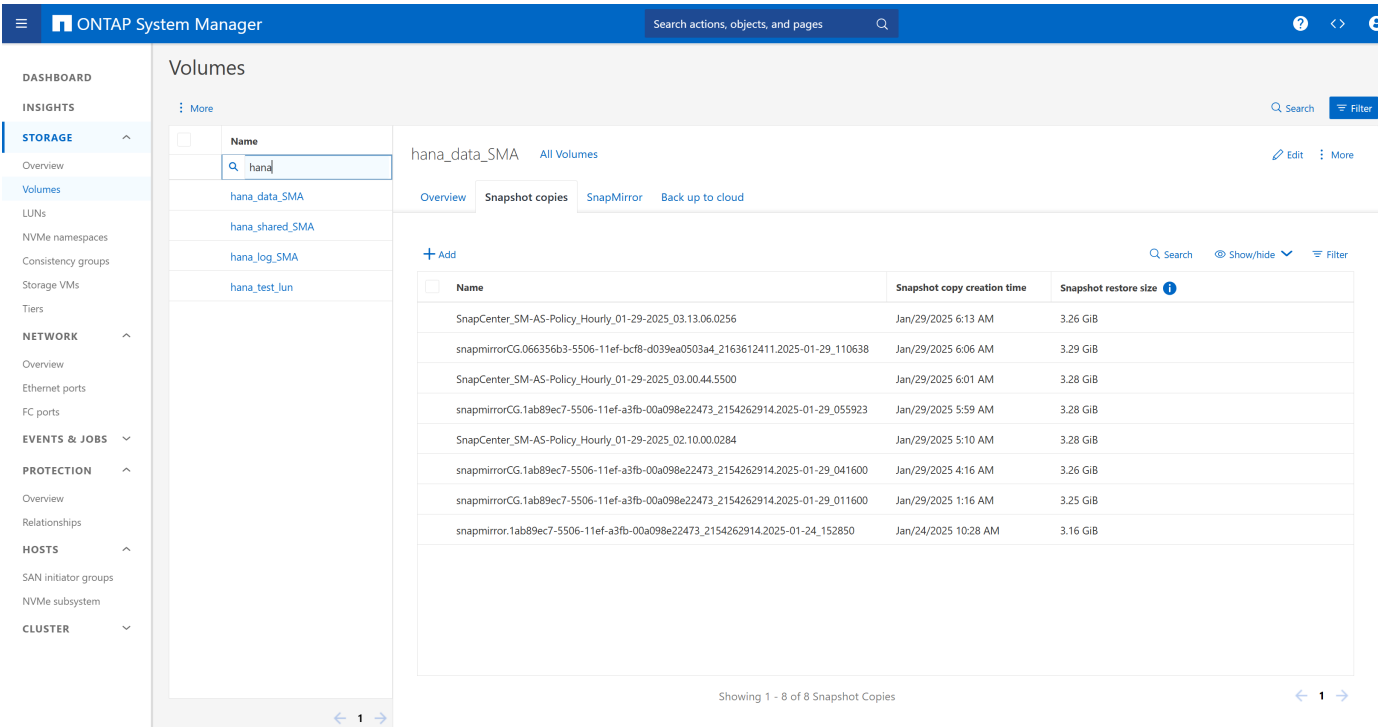
Ao clicar no número de contagem no armazenamento secundário, a relação atual e a direção de replicação são mostradas. A fonte é sempre o site principal atual. Após um failover de armazenamento, o local principal será alterado e o visor será adaptado em conformidade. Todos os backups têm sempre a mesma relação, dependendo do sistema de storage que atualmente é o local principal.

Details ✕			
Source	Relation	Destination	BackupCount
svm200_bluexpdr_a700s:hana_data_SMA	Mirror	svm200_bluexpdr_a800:vol_hana_data_SMA_dest	1
Total 1			

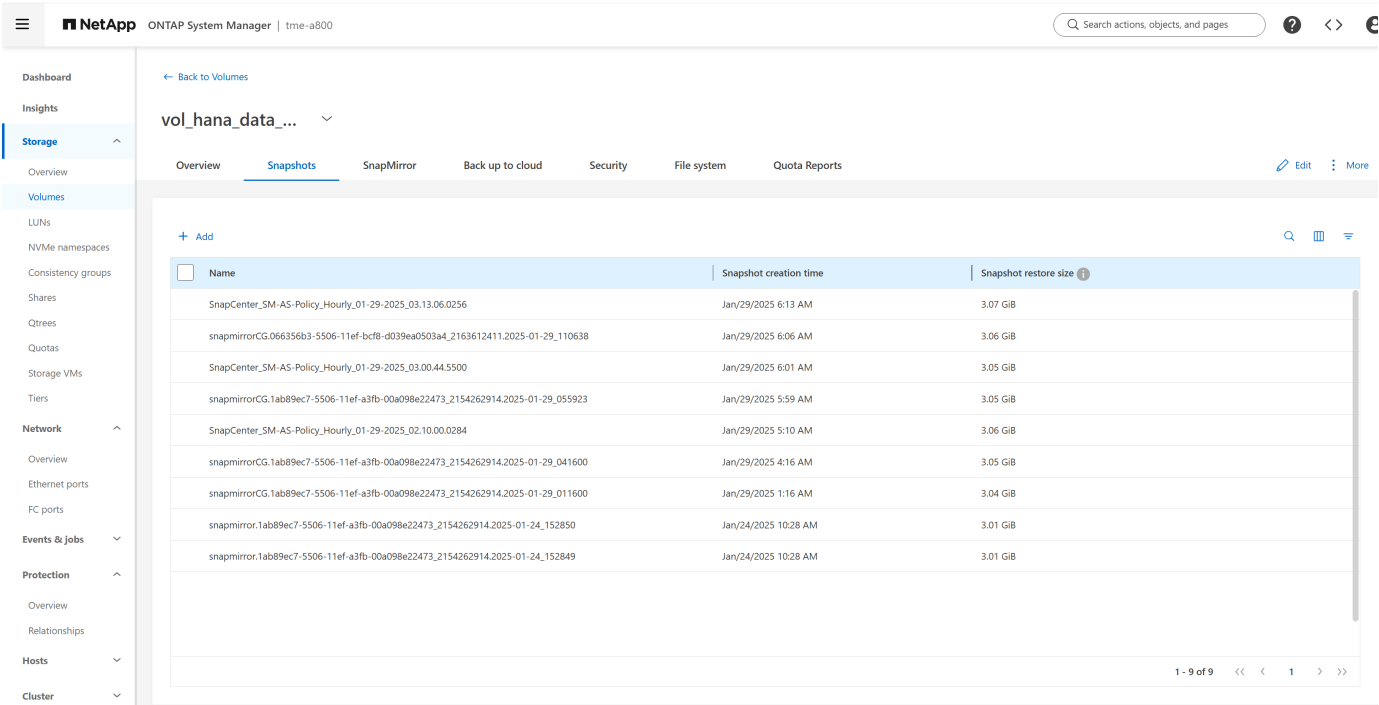
Snapshots em sistemas de storage

Os backups Snapshot criados pelo SnapCenter estão disponíveis em ambos os volumes de dados HANA em ambos os sistemas de storage. O ONTAP cria snapshots adicionais no nível do grupo de consistência, que também estão disponíveis em todos os outros volumes HANA.

A figura abaixo mostra os snapshots do volume de DADOS HANA no cluster A700.



A figura abaixo mostra os snapshots do volume de DADOS HANA no cluster A800.



Restauração e recuperação do SnapCenter

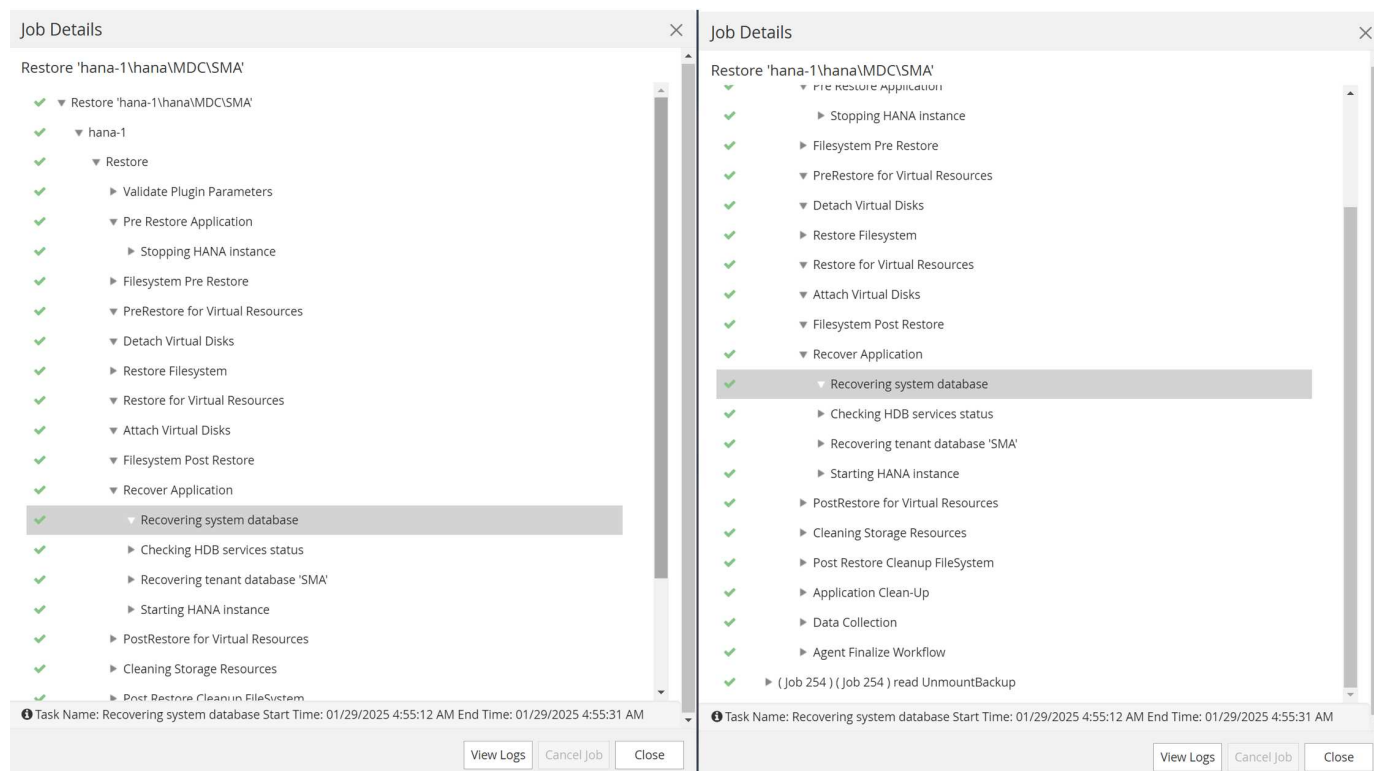
Com os recursos virtuais armazenados na operação de restauração do SnapCenter do VMFS/VMDK, a operação de restauração é sempre feita por uma operação de clone, montagem e cópia.

1. O SnapCenter cria um clone de volume com base no Snapshot selecionado

2. O SnapCenter monta o LUN no volume clonado como um novo datastore no host ESX
3. O SnapCenter adiciona o VMDK no datastore como um novo disco à VM HANA
4. O SnapCenter monta o novo disco para o sistema operacional Linux
5. O SnapCenter copia os dados do novo disco de volta para o local original
6. Quando a operação de cópia estiver concluída, todos os recursos acima são removidos novamente
7. A RECUPERAÇÃO DO HANA é feita como de costume

O tempo de execução geral da operação de restauração depende, portanto, do tamanho do banco de dados e da taxa de transferência da conexão FC entre os clusters de armazenamento e os hosts ESX.

Além disso, quando um recurso é configurado com a sincronização ativa do SnapMirror, a operação de restauração do SnapCenter só pode ser selecionada no local principal atual.



Enquanto a operação de restauração e recuperação está em execução, você pode ver um novo volume clonado, que foi criado no local principal atual.

ONTAP System Manager									
Search actions, objects, and pages									
Volumes									
More									
Search Download Show/Hide Filter									
	Name	Storage VM	Status	Capacity	IOPS	Latency (ms)	Throughput (MB/s)	Protection	
	hana	blue	(...)					(All)	
	hana_data_SMA	svm200_blueexpdr_a700s	Online	5.84 GiB used 298 GiB available 320 GiB	10	0.13	0.51		
	hana_data_SMA_Clone_0129250507433563	svm200_blueexpdr_a700s	Online	3.26 GiB used 301 GiB available 320 GiB	75	0.11	3.67		
	hana_shared_SMA	svm200_blueexpdr_a700s	Online	16 GiB used 188 GiB available 215 GiB	10	0.12	0.41		
	hana_log_SMA	svm200_blueexpdr_a700s	Online	4.1 GiB used 150 GiB available 163 GiB	10	0.10	0.35		
	hana_test_lun	svm200_blueexpdr_a700s	Online	58.9 MiB used 1.03 TiB available 1.03 TiB	12	0.27	1.31		

No host HANA Linux, você pode ver um novo disco, que foi montado no host. Quando a operação de restauração for concluída, o disco, o datastore e os volumes serão removidos novamente pelo SnapCenter.

```
hana-1:~ # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 58M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 36G 24G 60% /
/dev/mapper/system-root 60G 36G 24G 60% /.snapshots
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 36G 24G 60% /home
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 36G 24G 60% /opt
/dev/mapper/system-root 60G 36G 24G 60% /srv
/dev/mapper/system-root 60G 36G 24G 60% /usr/local
/dev/mapper/system-root 60G 36G 24G 60% /tmp
/dev/mapper/system-root 60G 36G 24G 60% /root
/dev/mapper/system-root 60G 36G 24G 60% /var
/dev/sdb 200G 8.0G 192G 4% /hana/data/SMA/mnt00001
/dev/sdc 120G 7.0G 113G 6% /hana/log/SMA/mnt00001
/dev/sda1 253M 5.1M 247M 3% /boot/efi
/dev/sdd 150G 28G 123G 19% /hana/shared
tmpfs 6.3G 48K 6.3G 1% /run/user/467
tmpfs 6.3G 28K 6.3G 1% /run/user/0
/dev/sde 200G 8.0G 192G 4%
/var/opt/snapcenter/scu/clones/hana_data_SMAmnt00001_255_scu_clone_1
hana-1:~ #
```

Operação de atualização do sistema SAP

As operações de clonagem podem ser executadas no local primário ou no storage

secundário.

O volume clonado não fará parte do grupo de CONSISTÊNCIA HANA e não será replicado com a sincronização ativa do SnapMirror.

Informações detalhadas sobre os fluxos de trabalho de atualização do sistema podem ser encontradas em: ["Automatizando as operações de clonagem e cópia do sistema SAP HANA com o SnapCenter"](#)

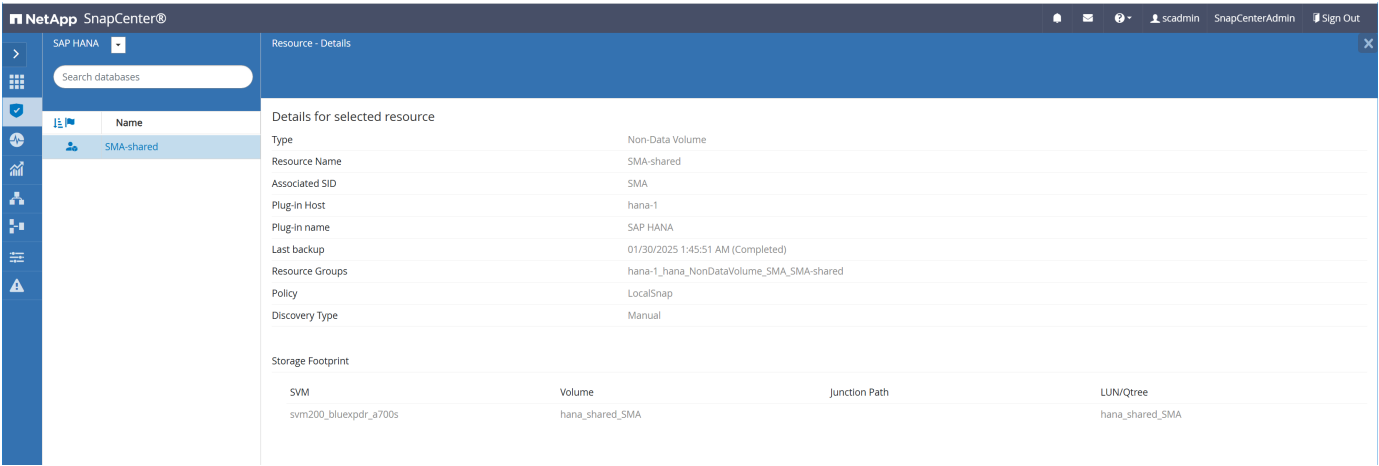
Volumes SnapCenter que não são de dados

Quando os recursos são configurados manualmente no SnapCenter e não são detetados automaticamente, o SnapCenter não tem conhecimento da sincronização ativa do VMware e do SnapMirror. Portanto, eles não são suportados nativamente pelo SnapCenter.

Para volumes que não são de dados, como HANA compartilhado, as operações de backup e restauração ainda poderiam ser feitas usando o SnapCenter ao considerar etapas manuais adicionais.

Falha do sistema de storage configurado no SnapCenter

Se ocorrer uma falha do sistema de storage configurado no SnapCenter, o SnapCenter não mudará automaticamente para o outro sistema de storage. O recurso de volume não-dados deve ser adaptado manualmente para que a cópia espelhada do volume seja usada para operações de backup e restauração.



Operações de backup

Embora o SnapCenter não esteja ciente da configuração de sincronização ativa do SnapMirror para o volume compartilhado HANA, os snapshots são replicados para ambos os locais.

ONTAP System Manager

Search actions, objects, and pages

DASHBOARD

INSIGHTS

STORAGE

Overview

Volumes

LUNs

NVMe namespaces

Consistency groups

Storage VMs

Tiers

NETWORK

EVENTS & JOBS

PROTECTION

Overview

Relationships

HOSTS

CLUSTER

Overview

Hardware

Settings

Volumes

Delete Protect More

hana_shared_SMA

hana_data_SMA

hana_shared_SMA

hana_log_SMA

hana_test_lun

Overview Snapshot copies SnapMirror Back up to cloud

+ Add

Search Show/hide Filter

Name	Snapshot copy creation time	Snapshot restore size
SnapCenter_LocalSnap_Hourly_01-30-2025_01.45.31.3354	Jan/30/2025 4:45 AM	15.6 GiB
SnapCenter_LocalSnap_Hourly_01-30-2025_01.45.22.2981	Jan/30/2025 4:45 AM	15.6 GiB
snapmirrorCG.1ab89ec7-5506-11ef-a3fb-00a098e22473_2154262914.2025-01-30_041615	Jan/30/2025 4:16 AM	15.6 GiB
snapmirrorCG.1ab89ec7-5506-11ef-a3fb-00a098e22473_2154262914.2025-01-30_011600	Jan/30/2025 1:16 AM	15.4 GiB
snapmirrorCG.066356b3-5506-11ef-bcf8-d039ea0503a4_2163612411.2025-01-29_163439	Jan/29/2025 11:34 AM	16 GiB
snapmirrorCG.066356b3-5506-11ef-bcf8-d039ea0503a4_2163612411.2025-01-29_110638	Jan/29/2025 6:06 AM	15.9 GiB
snapmirror.1ab89ec7-5506-11ef-a3fb-00a098e22473_2154262915.2025-01-24_152850	Jan/24/2025 10:28 AM	14.2 GiB

NetApp

ONTAP System Manager

tme-a800

Search actions, objects, and pages

Dashboard

Insights

Storage

Overview

Volumes

LUNs

NVMe namespaces

Consistency groups

Shares

Qtrees

Quotas

Storage VMs

Tiers

Network

Events & Jobs

Protection

Hosts

Cluster

vol_hana_share...

Overview Snapshots SnapMirror Back up to cloud Security File system Quota Reports

+ Add

Search Filter

Name	Snapshot creation time	Snapshot restore size
SnapCenter_LocalSnap_Hourly_01-30-2025_01.45.31.3354	Jan/30/2025 4:45 AM	16.2 GiB
SnapCenter_LocalSnap_Hourly_01-30-2025_01.45.22.2981	Jan/30/2025 4:45 AM	16.2 GiB
snapmirrorCG.1ab89ec7-5506-11ef-a3fb-00a098e22473_2154262914.2025-01-30_041615	Jan/30/2025 4:16 AM	16.1 GiB
snapmirrorCG.1ab89ec7-5506-11ef-a3fb-00a098e22473_2154262914.2025-01-30_011600	Jan/30/2025 1:16 AM	16 GiB
snapmirrorCG.066356b3-5506-11ef-bcf8-d039ea0503a4_2163612411.2025-01-29_163439	Jan/29/2025 11:34 AM	15.7 GiB
snapmirrorCG.066356b3-5506-11ef-bcf8-d039ea0503a4_2163612411.2025-01-29_110638	Jan/29/2025 6:06 AM	15.8 GiB
snapmirror.1ab89ec7-5506-11ef-a3fb-00a098e22473_2154262915.2025-01-24_152850	Jan/24/2025 10:28 AM	14.1 GiB
snapmirror.1ab89ec7-5506-11ef-a3fb-00a098e22473_2154262915.2025-01-24_152849	Jan/24/2025 10:28 AM	14.1 GiB

Operação de restauro

No caso de uma restauração, o SnapCenter apenas executaria uma restauração de volume sem quaisquer etapas específicas do VMware. Normalmente, você precisaria desmontar o volume compartilhado HANA no host Linux, desconectar o datastore e, em seguida, fazer a restauração de volume, conectar o datastore novamente e montar o sistema de arquivos no host Linux. Como uma operação manual, você pode parar a VM HANA, restaurar o volume compartilhado HANA com o SnapCenter e reiniciar a VM novamente.

Cenários de failover

este artigo destacará os cenários de failover para essa solução.

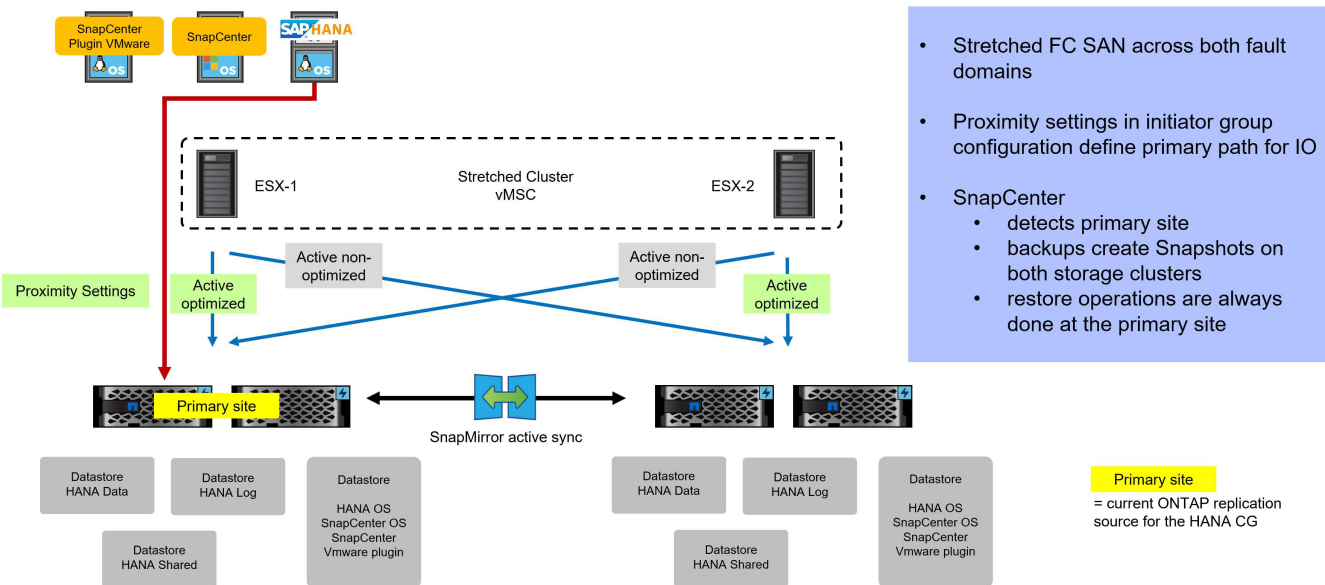
Configuração de acesso uniforme

Em uma configuração de acesso uniforme, a SAN Fibre Channel é estendida em ambos os locais. Os hosts ESX em ambos os locais poderiam acessar ambas as cópias dos conjuntos de dados. Durante a operação normal, o host ESX que executa o sistema HANA está acessando a cópia local dos dados com base nas configurações de proximidade na configuração do grupo de iniciadores. Cada host ESX tem um caminho

otimizado ativo para a cópia local e um caminho não otimizado ativo para a cópia espelhada.

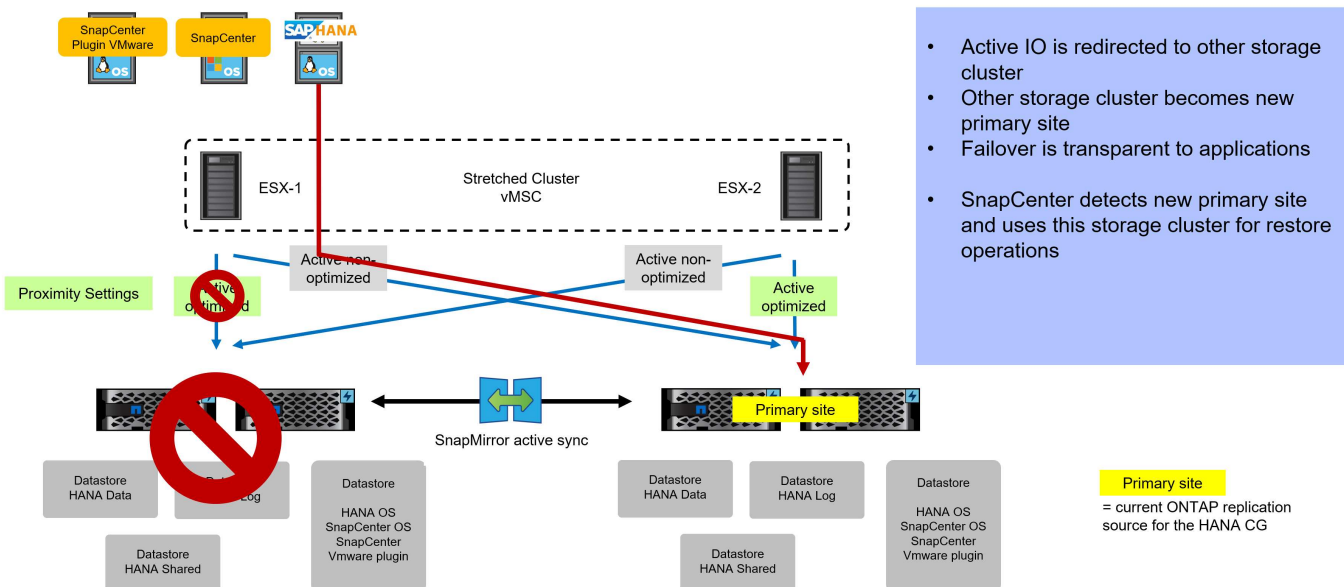
Funcionamento normal

Durante a operação normal, o sistema HANA lê e grava de/para a cópia local com base no caminho otimizado ativo do ESX-1 host. Em cada operação de backup, o SnapCenter detecta o local principal atual da relação de replicação e executa as operações de backup no local principal. Os instantâneos são replicados para a cópia espelhada e estão disponíveis em ambos os sites. Uma operação de restauração do SnapCenter seria executada no local principal.



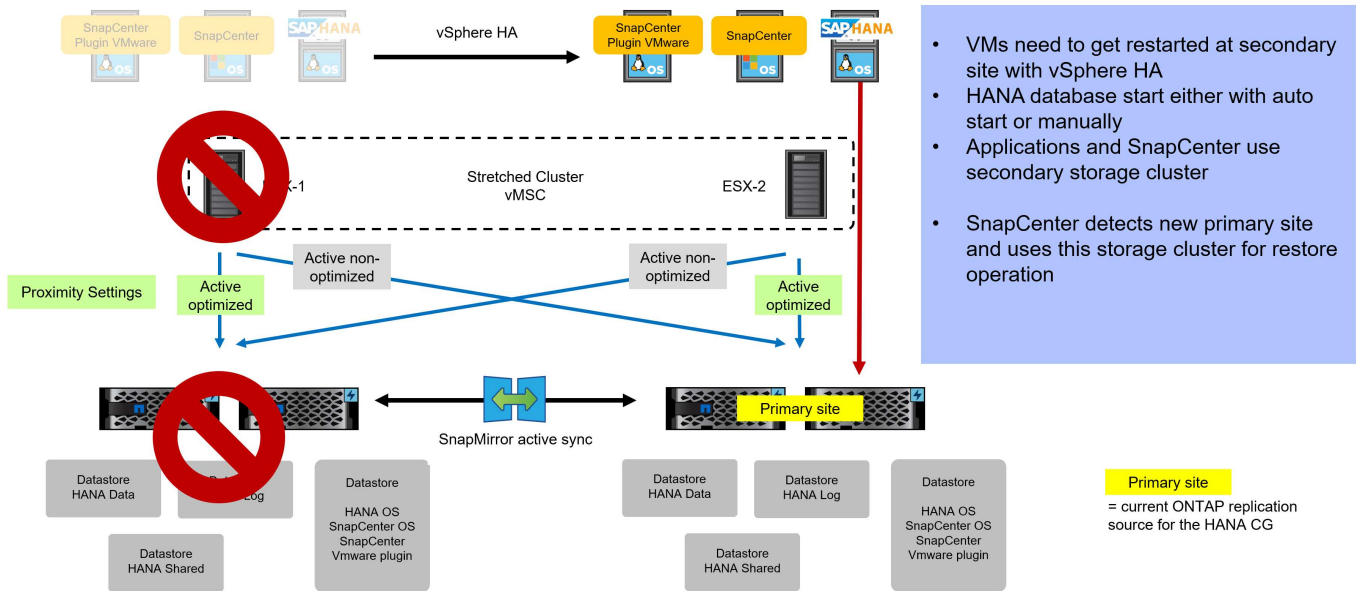
Falha de storage

Se o sistema de storage no local 1 falhar, os SISTEMAS HANA acessarão a cópia espelhada no local 2 e continuarão a operação. O local primário muda para o local secundário e o SnapCenter agora executa operações de backup e restauração no novo local primário.



Falha do local

Em caso de falha do site, a VM HANA, bem como a VM do plug-in SnapCenter e SnapCenter for VMware, farão failover para o host ESX no site secundário usando o vSphere HA. O banco de DADOS HANA precisa começar e, em seguida, acessar a cópia espelhada no segundo local. O local primário muda para o local secundário e o SnapCenter agora executa operações de backup e restauração no novo local primário.

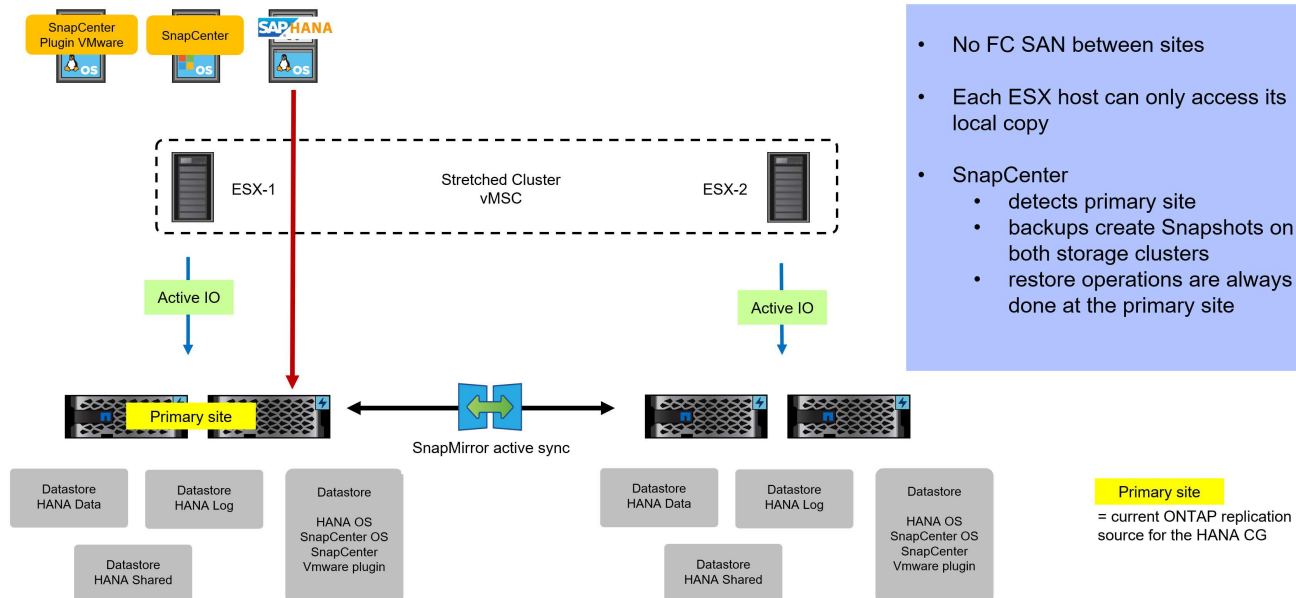


Configuração de acesso não uniforme

Em uma configuração de acesso não uniforme, a SAN Fibre Channel não é estendida em ambos os locais. Cada host ESX em cada local pode acessar apenas a cópia local dos conjuntos de dados.

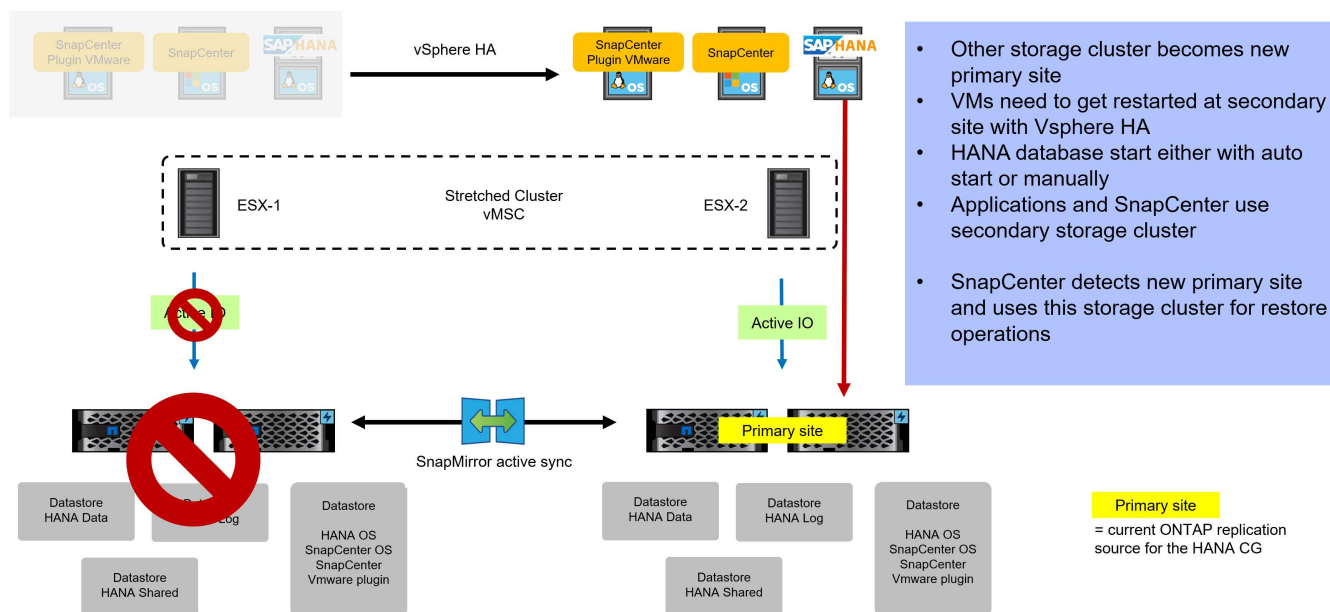
Funcionamento normal

Durante a operação normal, o SISTEMA HANA lê e grava de/para a cópia local. Em cada operação de backup, o SnapCenter detecta o local principal atual da relação de replicação e executa as operações de backup no local principal. Os instantâneos são replicados para a cópia espelhada e estão disponíveis em ambos os sites. Uma operação de restauração do SnapCenter seria executada no local principal.



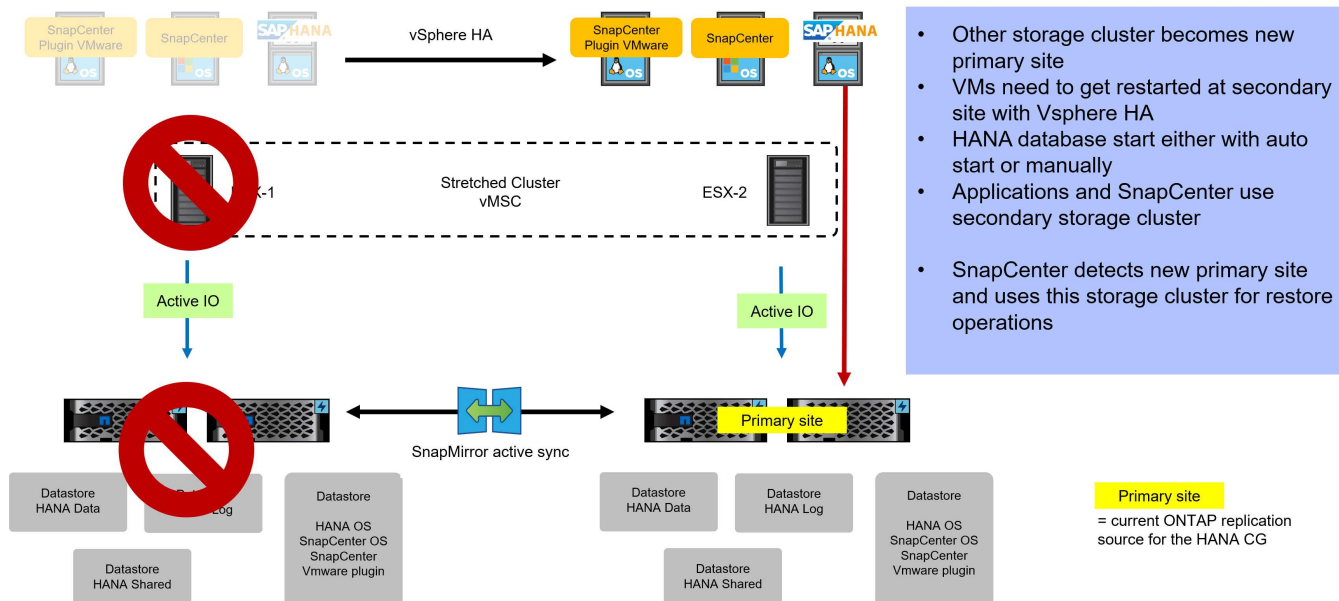
Falha de storage

Em caso de falha de storage, a VM HANA, bem como a VM do plug-in SnapCenter e SnapCenter para VMware farão failover para o host ESX no local secundário usando o vSphere HA. O banco de DADOS HANA precisa começar e, em seguida, acessar a cópia espelhada no segundo local. O local primário muda para o local secundário e o SnapCenter agora executa operações de backup e restauração no novo local primário.



Falha do local

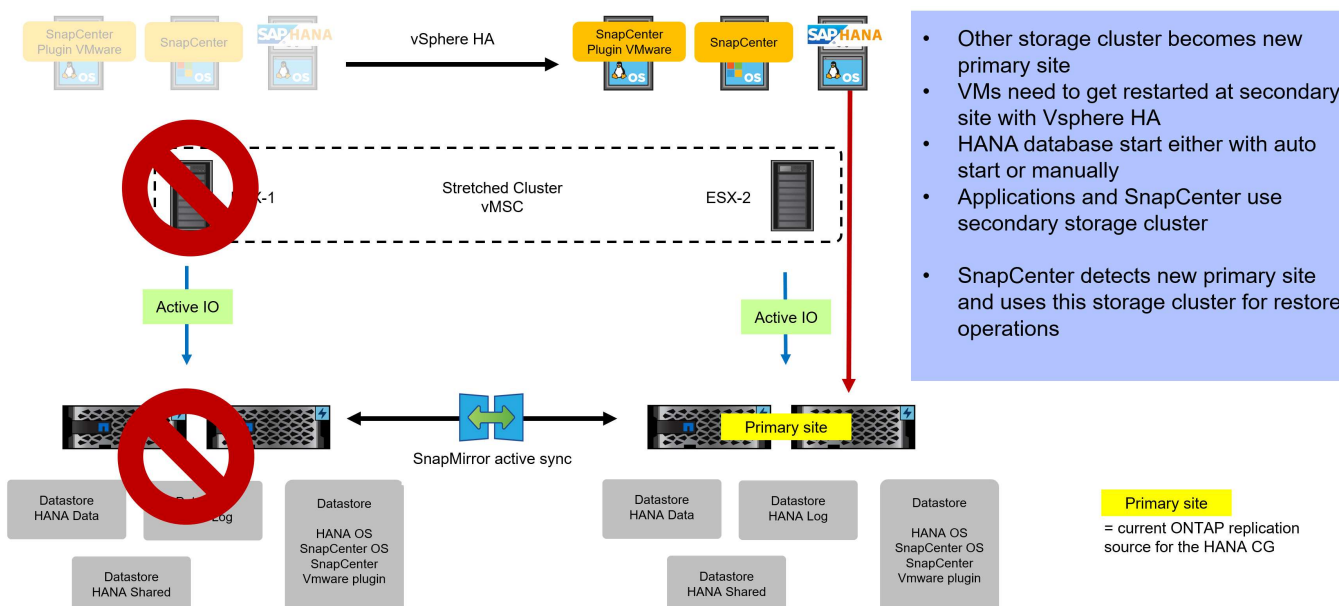
O mesmo que falha de storage.



Realocação da VM HANA ou do local principal

Se a VM HANA for realocada para o outro host ESX e o local principal do storage permanecer o mesmo, uma operação de restauração com o SnapCenter falhará. Como o SnapCenter usa o local principal para executar operações de restauração, o clone será criado no lado esquerdo, enquanto a VM HANA é executada no lado direito. Como não há caminho de dados entre os sites, o SnapCenter não será copiado os dados.

Como solução alternativa, você precisa garantir que a realocação da VM e do lado primário seja feita em conjunto ou que você precise fazer o failover do local principal antes da operação de restauração com o SnapCenter.



Informações adicionais e histórico de versões

este artigo fornece links para recursos adicionais relevantes para esta solução.

SnapCenter -

"Backup e recuperação do SAP HANA com o SnapCenter"

"Replicação do sistema SAP HANA: Backup e recuperação com o SnapCenter"

"Automatizando as operações de clonagem e cópia do sistema SAP HANA com o SnapCenter"

"Documentação do software SnapCenter"

Sincronização ativa do SnapMirror:

"Descrição geral da sincronização ativa do SnapMirror no ONTAP"

"NetApp ONTAP com NetApp SnapMirror ativo Sync com VMware vSphere Metro Storage Cluster (vmc)."

"Cluster de armazenamento Metro do VMware vSphere com sincronização ativa do SnapMirror"

"VMware vSphere Metro Storage Cluster (vMSC)"

Histórico de versões:

Versão	Data	Comentário
Versão 1,0	Março de 2025	Versão inicial

Proteção de dados SAP HANA com SnapCenter com sistemas VMware VMFS e NetApp ASA

Proteção de dados SAP HANA com SnapCenter com sistemas VMware VMFS e NetApp ASA

Este documento descreve as práticas recomendadas para proteção de dados usando o SnapCenter para sistemas HANA em execução no VMware com armazenamentos de dados usando VMFS e LUNs armazenados em sistemas NetApp ASA .

Autor: Nils Bauer, NetApp

Âmbito deste documento

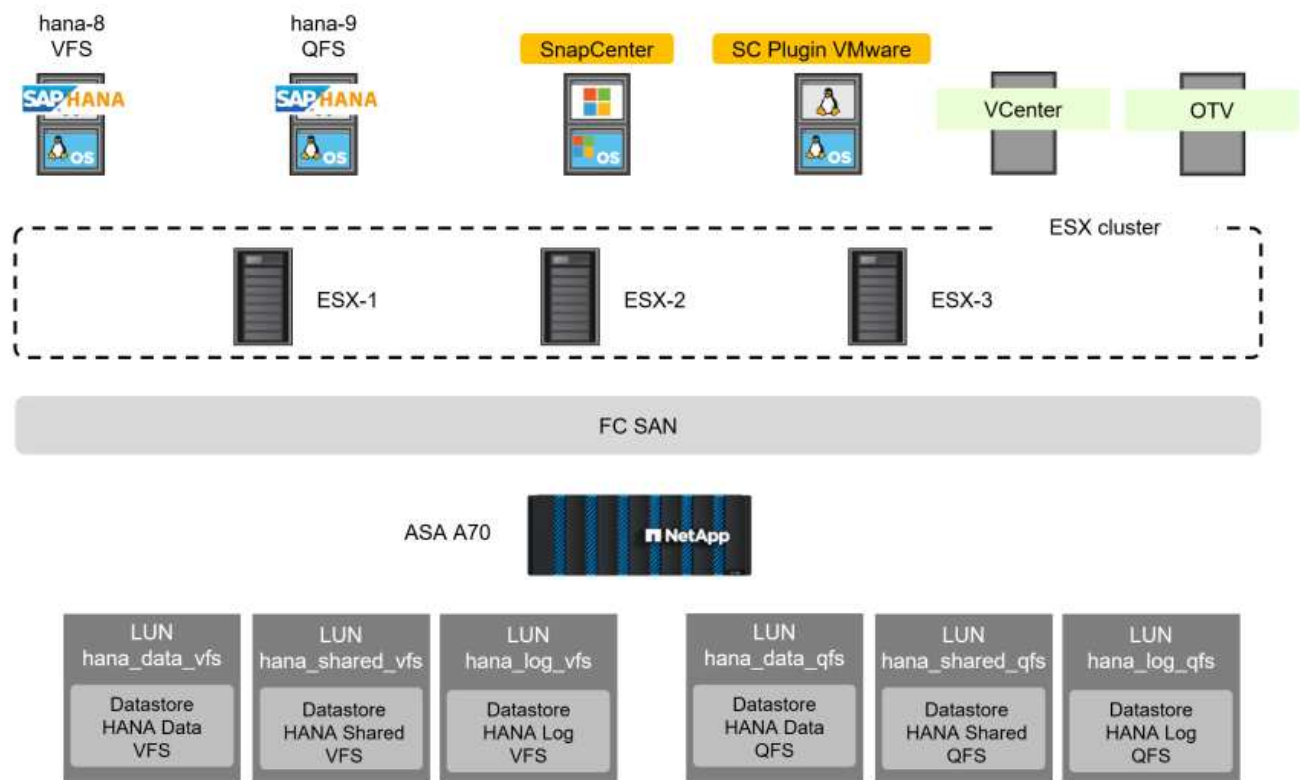
Ele não serve como um guia passo a passo para configurar todo o ambiente, mas se concentra em detalhes específicos do SnapCenter e do HANA no VMFS, incluindo:

- Configurando sistemas SAP HANA com VMware VMFS
- Configurações específicas do SnapCenter para HANA no VMware com VMFS
- Operações de backup, restauração e recuperação do SnapCenter para HANA no VMware com VMFS
- Operações de atualização do sistema SnapCenter SAP para HANA no VMware com VMFS

Para obter mais informações e instruções detalhadas de configuração, consulte os documentos listados no ["Informações adicionais"](#) capítulo.

Configuração de laboratório usada para este documento

A figura abaixo apresenta uma visão geral de alto nível da configuração de laboratório utilizada. Dois sistemas HANA MDC de host único são usados para demonstrar as diversas operações. O VFS do sistema HANA é designado para executar operações de backup, restauração e recuperação, enquanto o QFS do sistema HANA serve como sistema de destino para operações de atualização do sistema SAP. O plug-in SnapCenter para VMware é essencial para permitir que o SnapCenter gerencie recursos HANA configurados com VMware VMFS. Embora ferramentas ONTAP para VMware tenham sido usadas para provisionar as unidades de armazenamento para os sistemas HANA, elas não são um componente obrigatório.



Versões de software

Software	Versão
ONTAP	ASA A70 ONTAP 9.16.1
Cliente vSphere	8.0.3
ESXi	8.0.3
Plug-in do SnapCenter para vSphere	6.1.0
Ferramentas do ONTAP para VMware vSphere	10,4
OS do Linux	SLES PARA SAP 15 SP6
SAP HANA	2,0 SPS8
SnapCenter	6.1P1

Provisionamento e instalação do SISTEMA HANA

Este capítulo descreve a instalação e configuração do sistema SAP HANA específico para uma configuração VMware usando VMFS. As melhores práticas genéricas adicionais podem ser encontradas em ["SAP HANA em sistemas NetApp ASA com protocolo Fibre Channel"](#).

Configuração de armazenamento

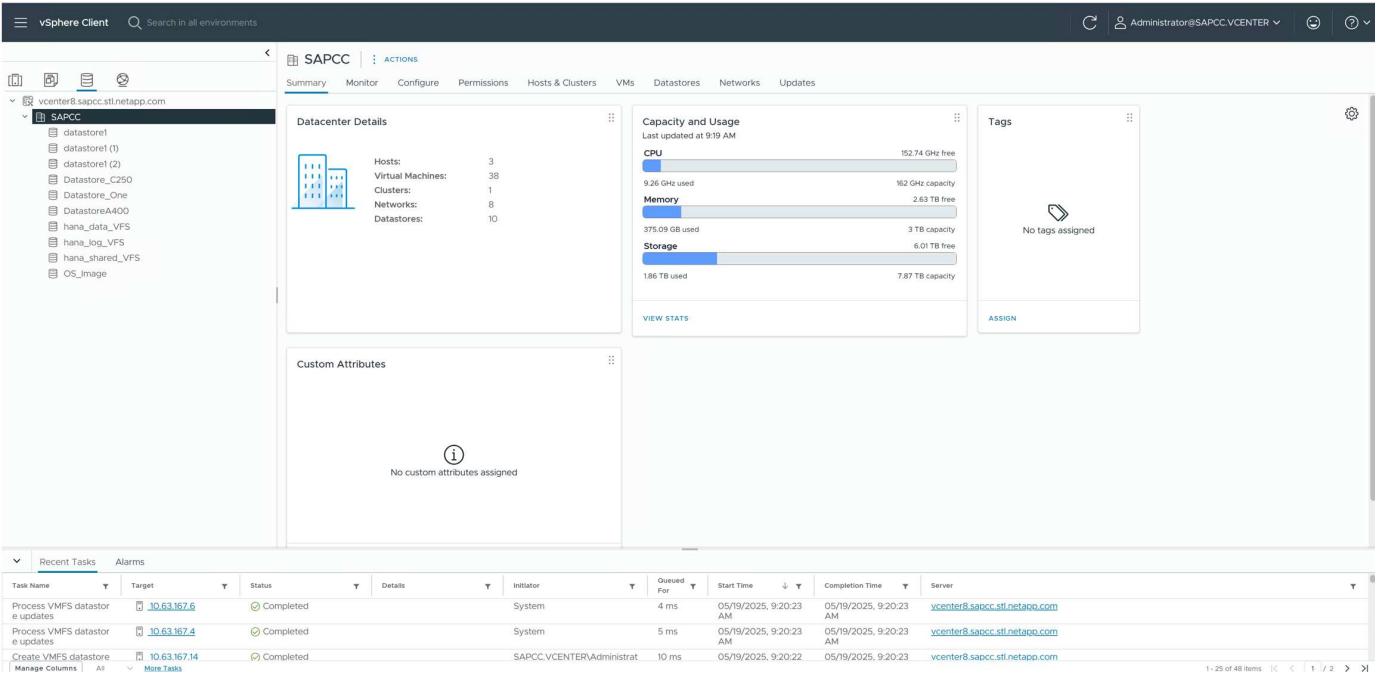
Para atender aos KPIs de desempenho de armazenamento definidos pela SAP para sistemas HANA de produção, LUNs e datastores dedicados devem ser configurados para os sistemas de arquivos de dados e log do sistema HANA. Os datastores não devem ser compartilhados entre vários sistemas HANA ou outras cargas de trabalho.

As ferramentas ONTAP para VMware (OTV) foram usadas para provisionar os três armazenamentos de dados para o VFS do sistema HANA.

- hana_dados_VFS
- hana_log_VFS
- hana_compartilhado_VFS



O armazenamento de dados do sistema de arquivos compartilhado HANA também pode ser compartilhado entre vários sistemas HANA.



No sistema de armazenamento, três LUNs foram criados pelo OTV.

ONTAP System Manager | A70-SAPCC

Search actions, objects, and pages

Dashboard

Insights

Storage

Hosts

Network

Overview

Ethernet ports

FC ports

Events & jobs

Protection

Cluster

Storage

The basic unit of storage is a LUN (for SCSI hosts) or NVMe namespace (for NVMe). You can add LUN or NVMe namespace storage units based on your data center configuration. [More](#)

19

Storage units

68.6 TiB

Available

19

Online

0

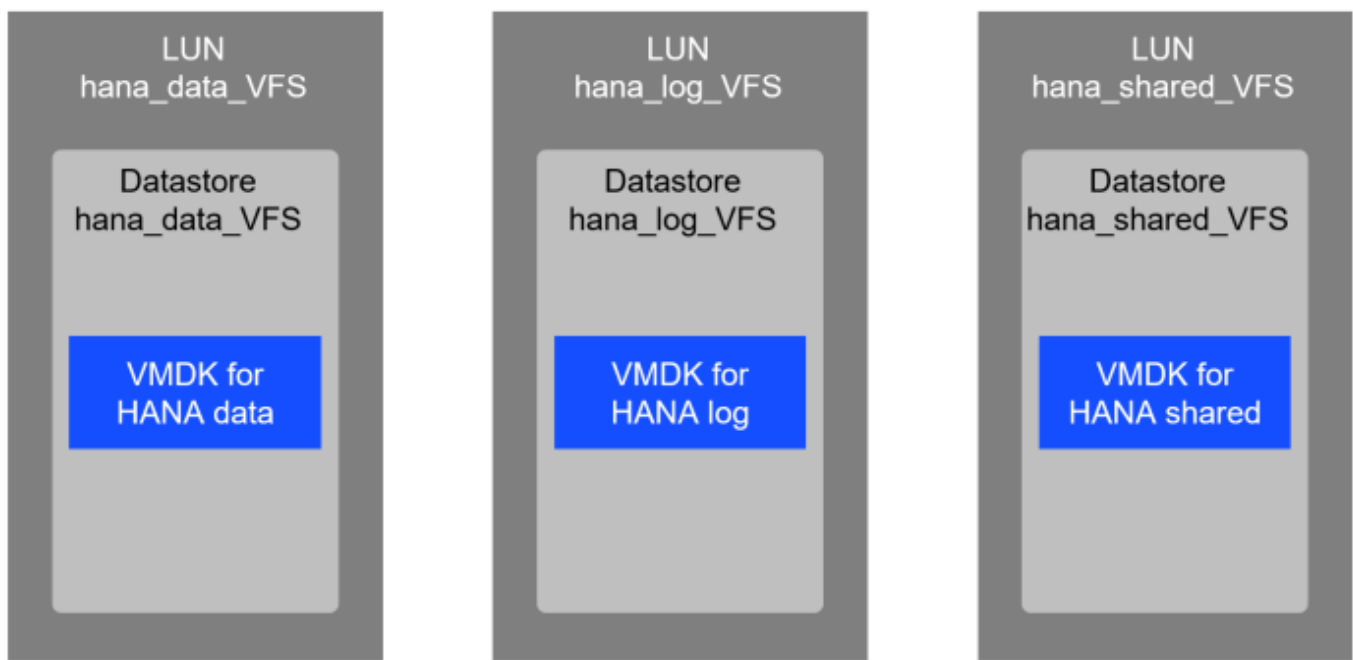
Offline

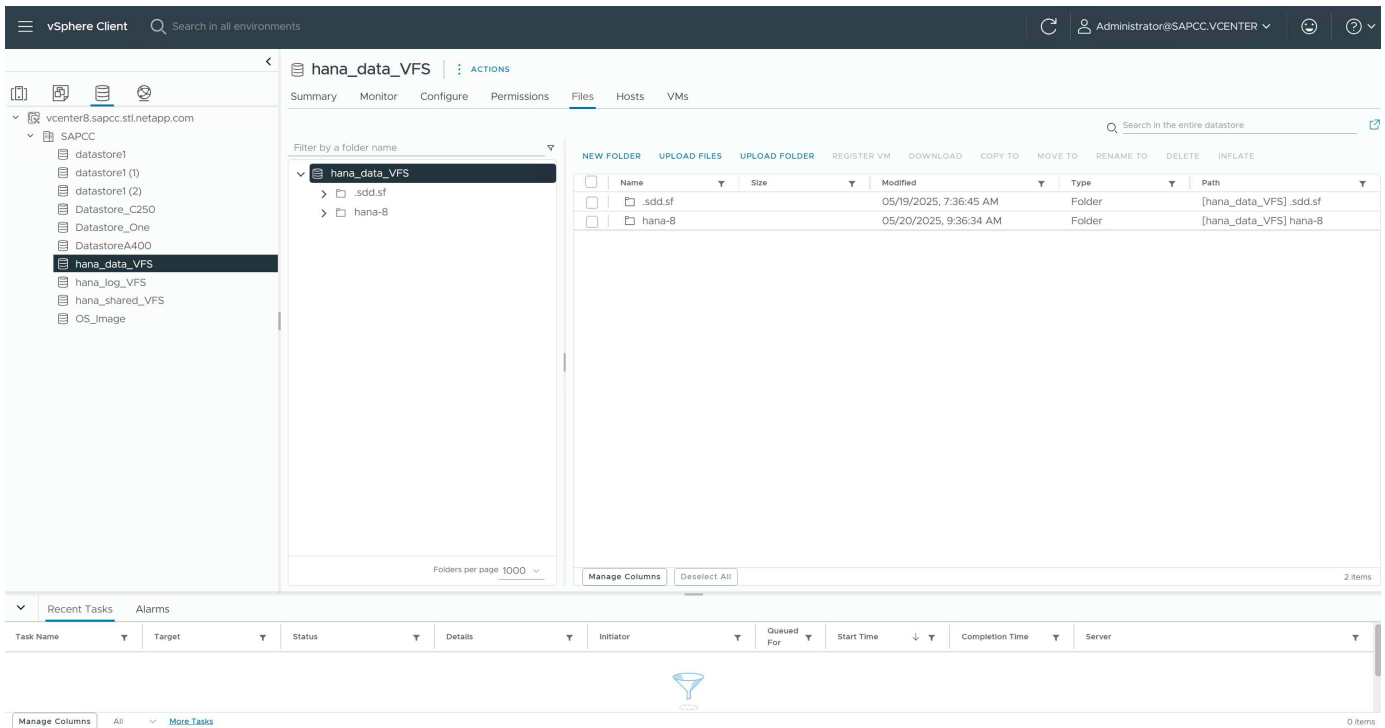
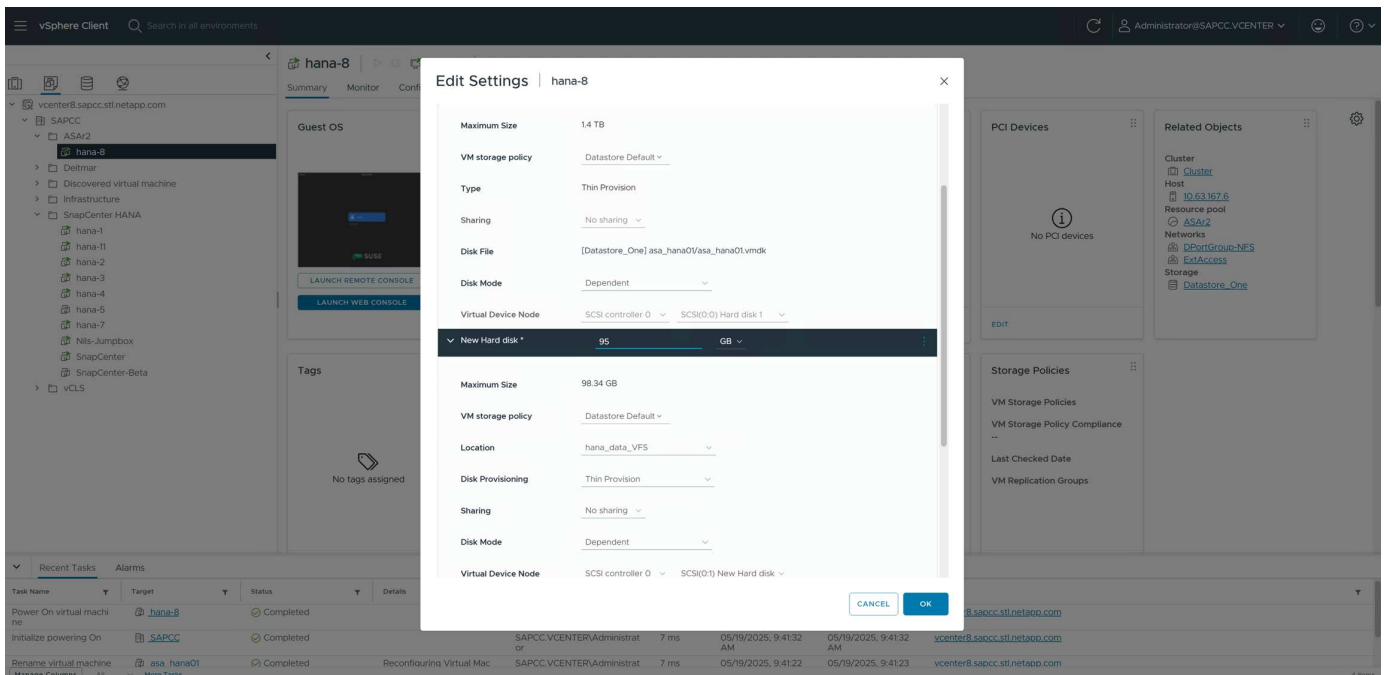
+ Add

	Name	Consistency group	Capacity	Data reduction	Host mapping	IOPS	Latency (ms)	Throughput (MB/s)
☐	hana_data_VFS	-	100 GiB	8.75 to 1	otv_host-44_e3d7e9d4-46f3-4f5c	0	0	0
☒	hana_log_VFS	-	100 GiB	8.69 to 1	otv_host-44_e3d7e9d4-46f3-4f5c	0	0	0
☒	hana_shared_VFS	-	100 GiB	3.13 to 1	otv_host-44_e3d7e9d4-46f3-4f5c	0	0	0

Configuração de disco de VM

Três novos discos (VMDK) devem ser adicionados à VM HANA. Cada disco deve estar em um dos datastores criados anteriormente, conforme ilustrado na imagem abaixo.





Quando os três discos forem adicionados à VM, eles poderão ser listados no nível do sistema operacional.

```

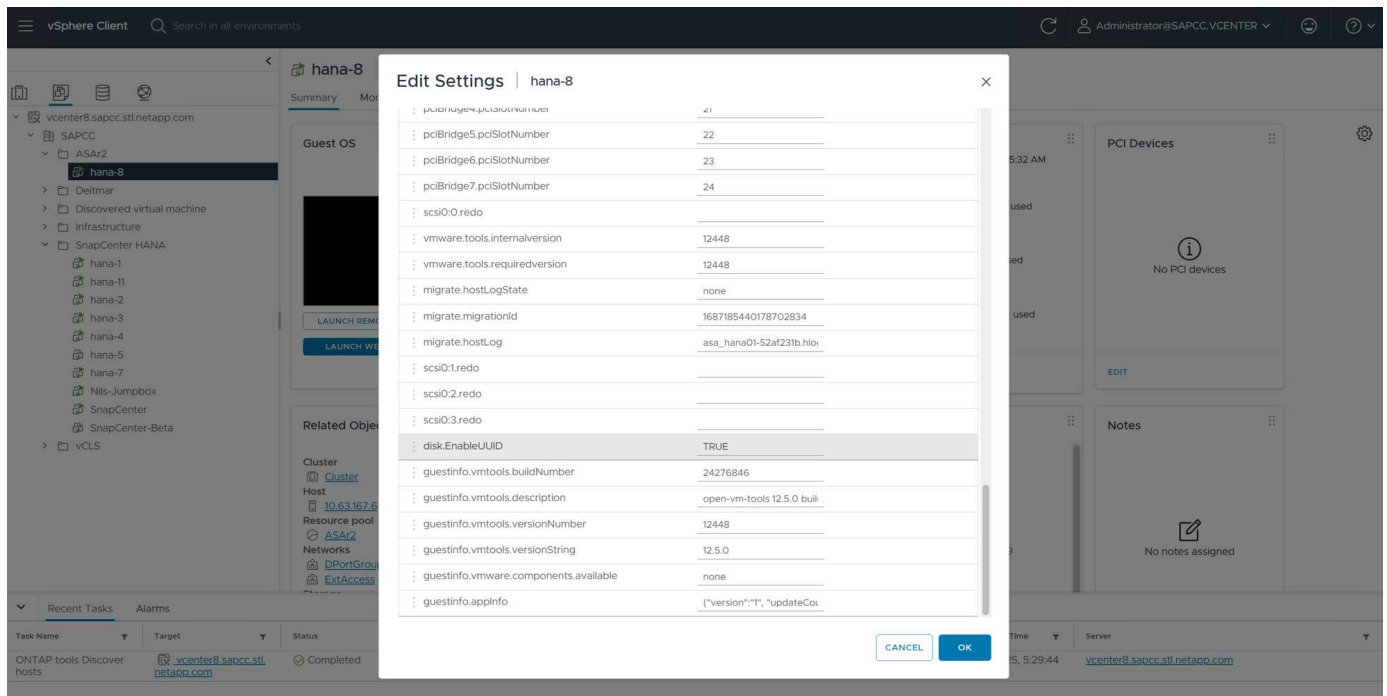
hana-8:~ # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 100G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
   ├─system-root 254:0 0 60G 0 lvm /root
   │ /var
   │ /usr/local
   │ /tmp
   │ /srv
   │ /opt
   │ /home
   │ /boot/grub2/x86++_++64-efi
   │ /boot/grub2/i386-pc
   │ /.snapshots
   │ /
   └─system-swap 254:1 0 2G 0 lvm [SWAP]
sdb 8:16 0 95G 0 disk
sdc 8:32 0 95G 0 disk
sdd 8:48 0 95G 0 disk
sr0 11:0 1 17.1G 0 rom

```

Parâmetro da VM `disk.EnableUUID`

Este parâmetro deve ser definido adequadamente, caso contrário, a descoberta automática do banco de dados SnapCenter falhará.

1. Desligar VM
2. Adicione o novo parâmetro “`disk.EnableUUID`” e defina como “`TRUE`”
3. Iniciar VM



Preparação do sistema de arquivos no host Linux

Criação do sistema de arquivos xfs em novos discos

Um sistema de arquivos xfs foi criado em cada um dos três novos discos.

```
hana-8:~ # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nnext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.
```

```
hana-8:~ # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nnext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.
```

```
hana-8:~ # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nnext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.
```

```
hana-8:~ #
```

```

hana-8:/ # mkdir -p /hana/data/VFS/mnt00001
hana-8:/ # mkdir -p /hana/log/VFS/mnt00001
hana-8:/ # mkdir -p /hana/shared
hana-8:/ # chmod -R 777 /hana/log/SMA
hana-8:/ # chmod -R 777 /hana/data/SMA
hana-8:/ # chmod -R 777 /hana/shared

```

Configuração do /etc/fstab

```

hana-8:/ # cat /etc/fstab

/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=@/var 0 0
/dev/system/root /usr/local btrfs subvol=@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=@/tmp 0 0
/dev/system/root /srv btrfs subvol=@/srv 0 0
/dev/system/root /root btrfs subvol=@/root 0 0
/dev/system/root /opt btrfs subvol=@/opt 0 0
/dev/system/root /home btrfs subvol=@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2
### SAPCC_share
192.168.175.86:/sapcc_share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsiz=1048576,intr,noatime,nolock 0
0
/dev/sdb /hana/data/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-8:/ #

hana-8:/ # df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 4.4G 54G 8% /
devtmpfs 4.0M 0 4.0M 0% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 18M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service

```



```

tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/mapper/system-root 60G 4.4G 54G 8% /.snapshots
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 4.4G 54G 8% /home
/dev/mapper/system-root 60G 4.4G 54G 8% /opt
/dev/mapper/system-root 60G 4.4G 54G 8% /srv
/dev/mapper/system-root 60G 4.4G 54G 8% /tmp
/dev/mapper/system-root 60G 4.4G 54G 8% /usr/local
/dev/mapper/system-root 60G 4.4G 54G 8% /var
/dev/sda1 253M 5.9M 247M 3% /boot/efi
/dev/mapper/system-root 60G 4.4G 54G 8% /root
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
192.168.175.86:/sapcc_share 1.4T 840G 586G 59% /mnt/sapcc-share
/dev/sdb 95G 1.9G 94G 2% /hana/data/VFS/mnt00001
/dev/sdc 95G 1.9G 94G 2% /hana/log/VFS/mnt00001
/dev/sdd 95G 1.9G 94G 2% /hana/shared

hana-8:/ #

```

INSTALAÇÃO HANA

A instalação HANA agora pode ser executada.

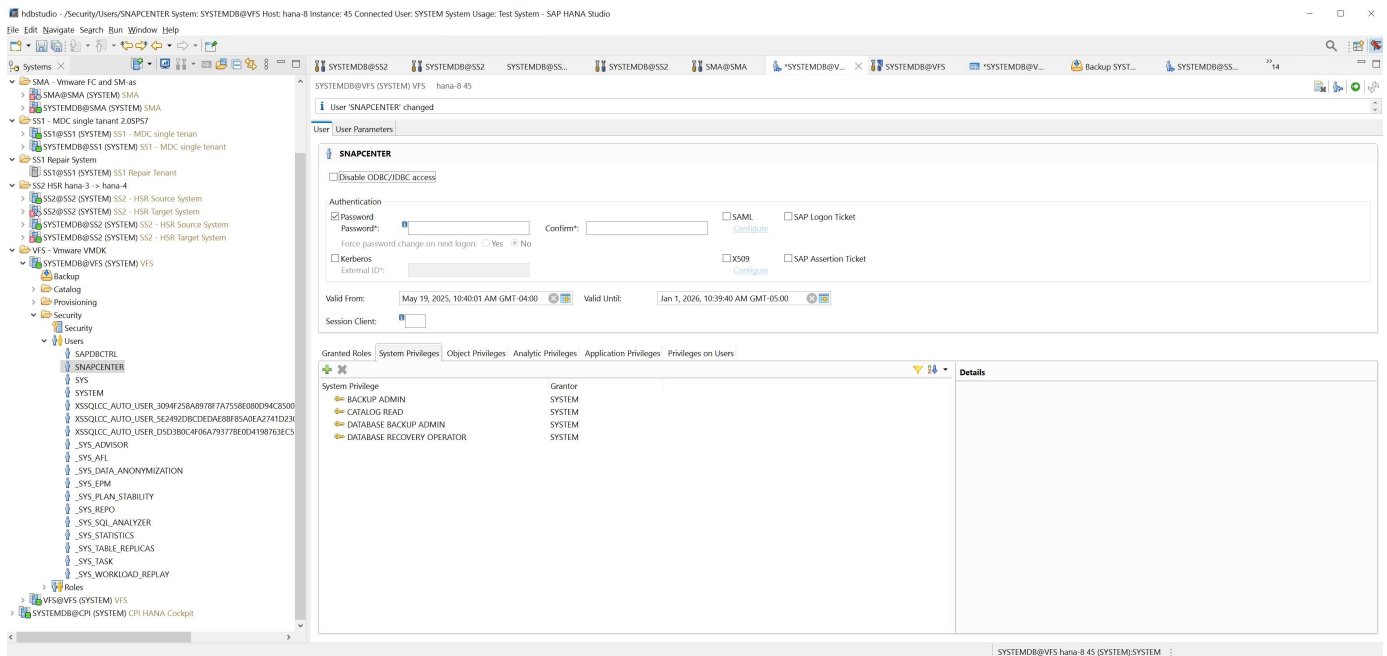


Com a configuração descrita, o diretório `/usr/sap/VFS` estará no VMDK do os. Se `/usr/sap/VFS` deve ser armazenado no VMDK compartilhado, o disco compartilhado HANA pode ser particionado para fornecer outro sistema de arquivos para `/usr/sap/VFS`.

Configuração HANA

Configurar usuário do banco de dados SnapCenter

É necessário criar um arquivo de usuário para um usuário de banco de dados do sistema, que deve ser usado pelo SnapCenter.



Configurar chave hdb userstore

Uma chave de armazenamento de usuário deve ser criada para o usuário vfsadm. O número da instância HANA deve ser definido adequadamente para a comunicação da porta. Em nossa instância de configuração, o número "45" é usado.

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbuserstore SET VFSKEY hana-8:34513
SNAPCENTER <password>
```

Retroactive report: Operation succeed.

Verifique o acesso com:

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbsql -U VFSKEY

Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit

vfsadm@hana-8:/usr/sap/VFS/HDB45>
```

Configuração do SnapCenter

Pré-requisitos

O recurso do SnapCenter HANA deve ser descoberto automaticamente

Os recursos configurados com o VMware VMFS devem ser descobertos automaticamente pelo SnapCenter para habilitar operações específicas necessárias para essas configurações.

Como os volumes não relacionados a dados do HANA são sempre recursos configurados manualmente no SnapCenter, eles não são suportados pelo SnapCenter com VMFS.

Sistemas SAP HANA com múltiplos hosts devem ser configurados usando um plugin HANA central e, portanto, são configurados manualmente por padrão. Esses sistemas também não são suportados pelo SnapCenter ao usar o VMware VMFS.

Plug-in do SnapCenter para VMware vSphere

O plug-in do SnapCenter para VMware vSphere deve ser implantado no ambiente VMware.

IP de gerenciamento de SVM de armazenamento

Os SVMs de armazenamento que hospedam os LUNs devem ter uma interface de gerenciamento configurada, caso contrário, os SVMs não serão listados no SnapCenter ao adicionar armazenamento com a opção “adicionar cluster” e a operação de descoberta automática falhará.

Job Details



Discover resources for host 'hana-8.sapcc.stl.netapp.com'

✖ ▼ Discover resources for host 'hana-8.sapcc.stl.netapp.com'

✖ ▼ hana-8.sapcc.stl.netapp.com

✖ ▼ Discover

✔ ▶ Complete Application Discovery

✔ ▶ Discover Filesystem Resources

✖ ▶ Discover Virtual Resources

✔ ▶ Discover_OnFailure

✖ Failure in virtual resources discovery: [Failed to resolve the storage associated with the VMware virtual disks 6000c2964ec4375910dc9953d9f870ca]

View Logs

Cancel Job

Close

NetApp SnapCenter®

ONTAP Storage Azure NetApp Files

Type: ONTAP SVMs Search by Name

ONTAP Storage Connections

Name	IP	Cluster Name	User Name	Platform	Controller License
svm1	10.63.167.55	10.63.167.54		ASA	✓
hana		10.63.150.245		AFF	✓
hana-backup	10.63.150.246	10.63.150.245		AFF	✓
hana-cloud-dr		10.1.2.175		FSx	Not applicable
hana-dr	10.63.150.247	10.63.150.245		AFF	✓
hana-primary	10.63.150.248 ...	10.63.150.245		AFF	✓

Parâmetro de disco da VM

O parâmetro deve ser definido conforme descrito no capítulo ["Parâmetros da VM disk.EnableUUID"](#), caso contrário, a descoberta automática do banco de dados SnapCenter falhará.

Configure Database

Plug-in host: hana-8.sapcc.stl.netapp.com

HDBSQL OS User: vfsadm

HDB Secure User Store Key: VFSKEY

Failure in getting storage details: [Failed to retrieve the unit serial number for the device '/dev/sdb', Reason: 'SCSI inquiry failed. Check if the disk.EnableUUID parameter is set to TRUE in the VM configuration file.']

Cancel OK

Configurar o SnapCenter para usar APIs REST para comunicação de armazenamento

O SnapCenter deve ser configurado para usar APIs REST para comunicações de armazenamento. Caso contrário, a operação de criação de Snapshot falhará, exibindo a mensagem de erro mostrada abaixo.

Job Details

×

Backup of Resource Group 'hana-8_sapcc_stl_netapp_com_hana_MDC_VFS' with policy 'LocalSnap'

✖

▼ Backup of Resource Group 'hana-8_sapcc_stl_netapp_com_hana_MDC_VFS' with policy 'LocalSnap'

✖

▼ hana-8.sapcc.stl.netapp.com

✖

▼ Backup

✔

▶ Validate Dataset Parameters

✔

▶ Validate Plugin Parameters

✔

▶ Complete Application Discovery

✔

▶ Initialize Filesystem Plugin

✔

▶ Discover Filesystem Resources

✔

▶ Discover Virtual Resources

✔

▶ Populate storage details

✔

▶ Validate Retention Settings

✔

▶ Quiesce Application

✔

▶ Quiesce Filesystem

✖

▼ Create Snapshot

⚠

▶ Backup_OnFailure

✖

SCC-STORAGE-02002: Creating Snapshot copy [SnapCenter_hana-8_LocalSnap_Hourly_05-20-2025_10.33.58.2195] on storage resource [svm1:hana_data_VFS] failed with error [Snapshot operation failed. [400]: POST, DELETE, and PATCH requests on the snapshot session endpoint are not supported on this platform.]

View Logs

Cancel Job

Close

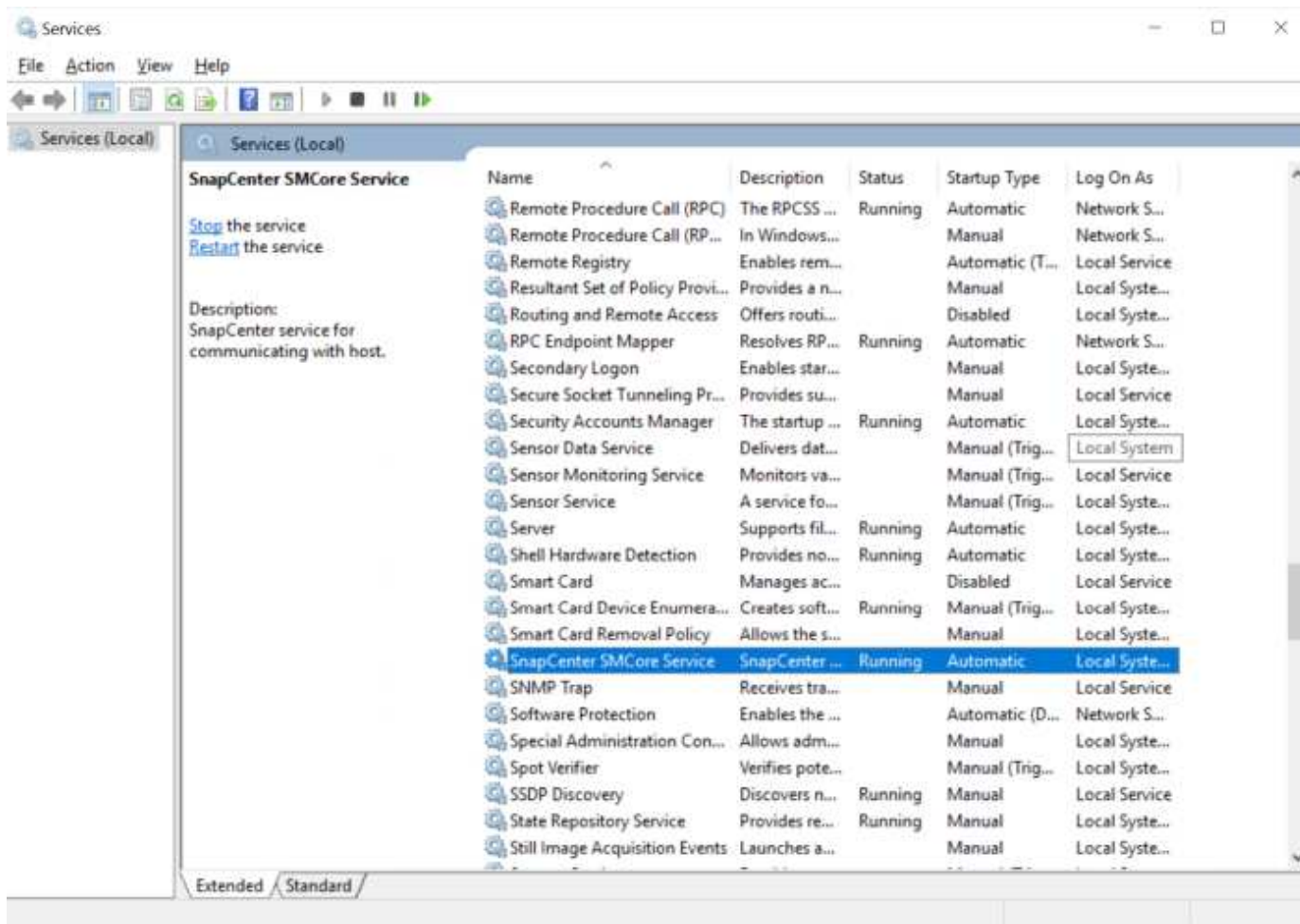
O parâmetro "IsRestEnabledForStorageConnection" no arquivo de configuração + C:\Program Files\NetApp\SMCore\SMCoreServiceHost.dll.config deve ser definido como "true".

<adicionar chave="IsRestEnabledForStorageConnection" valor="true" />

```
SMCoreServiceHost.dll.config - Notepad
File Edit Format View Help

<add keys="EnableCancelJob" value="true" />
<add keys="PSErrorString" value="Internal network error,API invoke failed,No such file or directory" />
<add keys="CommandErrorDuringMccFailure" value="timed out,Unknown internal error,API invoke failed,metrocluster" />
<add keys="VolumeEnumerationOptimized" value="true" />
<add keys="CloneSplitStatusCheckPollTime" value="300000" />
<add keys="ConfigCheckerJobStatusTimeout" value="20" />
<add keys="ConfigCheckerJobStatusRetry" value="30" />
<add keys="AzureEnvironment" value="AzureGlobalCloud" />
<add keys="AzureLongRunningOperationRetryTimeoutInSec" value="20" />
<add keys="AzureClientType" value="sdk" />
<add keys="AzureThreadSleepTime" value="10000" />
<add keys="AzureRestVersion" value="2019-11-01" />
<add keys="GetStorageIDBeforeCacheInitialize" value="true" />
<add keys="SccCloneSuffix" value="Clone" />
<add keys="SourceComponent" value="smcore" />
<add keys="WmiTimeoutIntervalMinutes" value="30" />
<add keys="IsWmiTimeoutSet" value="true" />
<add keys="OracleAlmActivityParallelExecution" value="true" />
<add keys="OracleAlmActivityParallelMountInterval" value="20" />
<add keys="OracleAlmActivityParallelUnmountInterval" value="10" />
<add keys="SkipOracleAlmBackupsCatalogAndUncatalog" value="false" />
<add keys="UseVolumeFilterInGetSnapshot" value="true" />
<add keys="EnablePredefinedWindowsScriptsDirectory" value="true" />
<add keys="PredefinedWindowsScriptsDirectory" value="C:\Program Files\NetApp\SMCore\Scripts" />
<add keys="IsRestEnabledForStorageConnection" value="true" />
<add keys="ExcludeForDetectionOfDetectionOfSmeCommands" value="AddNclunMap" />
<add keys="MinOntapVersionToUseREST" value="9.13.1" />
<add keys="IS_COLO_SNAPCENTER_AGENT" value="true" />
<add keys="IS_SCM_PLUGIN_SERVICE_PRESENT" value="false" />
<add keys="SMCORE_IMAGE_PATH" value="C:\Program Files\NetApp\SMCore\" />
<add keys="REPOSITORY_PATH" value="C:\ProgramData\NetApp\SnapCenter\" />
<add keys="SNAPGATHERS_PATH" value="C:\Program Files\NetApp\SnapGathers\" />
<add keys="SNAPGATHERS_PATH_WINDOWS" value="C:\Program Files\NetApp\SnapCenter\SnapGathers\" />
<add keys="smcoreprotocol" value="https" />
<add keys="SERVICE_CERTIFICATE_PATH" value="/var/opt/snapcenter/certs/snapcenter.pfx" />
<add keys="SERVICE_CERTIFICATE_PASSWORD" value="" />
<add keys="ForceSHA256EncryptionKey" value="false" />
<add keys="WINRM_PROTOCOL" value="http" />
<add keys="WINRM_PORT" value="5985" />
<add keys="WINRM_AUTH_TYPE" value="ntlm" />
<add keys="DoNotSaveOracleBlob" value="false" />
<add keys="IsRestEnabledForLowerONTAP" value="false" />
</appSettings>
</configuration>
```

Após a alteração ser feita, o SnapCenter SMCore Service deve ser interrompido e iniciado.

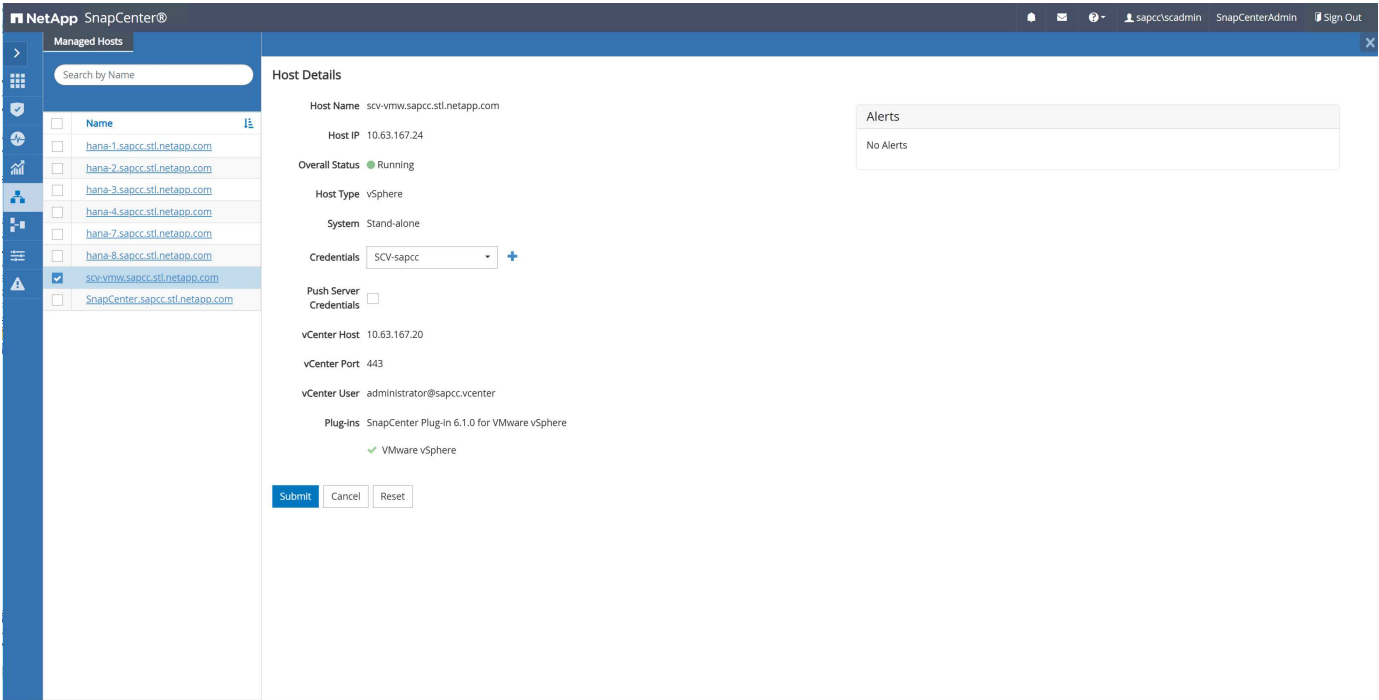


Adicionar o plugin VMware ao SnapCenter

Antes que o host possa ser adicionado ao SnapCenter, o plug-in do SnapCenter para VMware vSphere deve ser implantado no ambiente VMware. Consulte também ["Implante o plug-in do SnapCenter para VMware vSphere"](#).



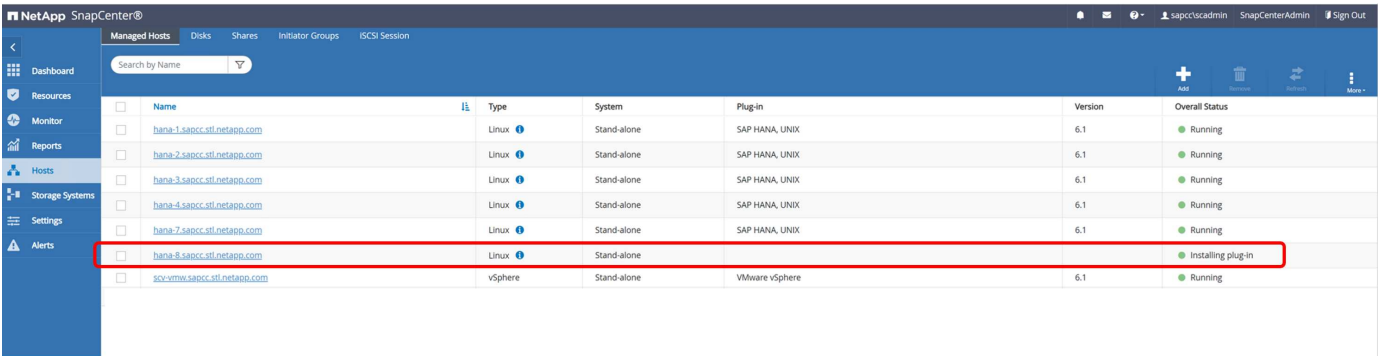
As credenciais devem ser definidas durante o fluxo de trabalho de adição do host, em que o vSphere pode ser selecionado como um tipo de host.



Adicionar host HANA



Sem requisitos específicos. A implantação do plugin e a descoberta automática são feitas como de costume.



Com o processo de descoberta automática, o SnapCenter detecta que o recurso HANA está sendo executado virtualizado com VMFS.

NetApp SnapCenter®

SAP HANA

Search databases

System
Q51
SM1
SS1
SS2
SS2
VFS

Total 6

Resource - Details

Details for selected resource

Type	Multitenant Database Container
HANA System Name	VFS
SID	VFS
Tenant Databases	VFS
Plug-in Host	hana-8.sapcc.stl.netapp.com
HDB Secure User Store Key	VFSKEY
HDBSQL OS User	vfsadm
Log backup location	/usr/sap/VFS/HDB45/backup/log
Backup catalog location	/usr/sap/VFS/HDB45/backup/log
System Replication	None
Plug-in name	SAP HANA
Last backup	None
Resource Groups	None
Policy	None
Discovery Type	Auto

Storage Footprint

SVM	Volume	Junction Path	LUN/Qtree
svm1			hana_data_VFS

Activity The 5 most recent jobs are displayed

5 Completed
0 Warnings
0 Failed
0 Canceled
0 Running
0 Queued

Configuração de política e proteção de recursos

Nada específico para VMware com VMFS.

Operações de backup

Nada específico para VMware com VMFS.

Job Details



Backup of Resource Group 'hana-8_sapcc_stl_ne.....na_MDC_VFS' with policy 'LocalSnap'

✓ ▾ Backup of Resource Group 'hana-8_sapcc_stl_netapp_com_hana_MDC_VFS' with policy 'LocalSnap'

✓ ▾ hana-8.sapcc.stl.netapp.com

✓ ▾ Backup

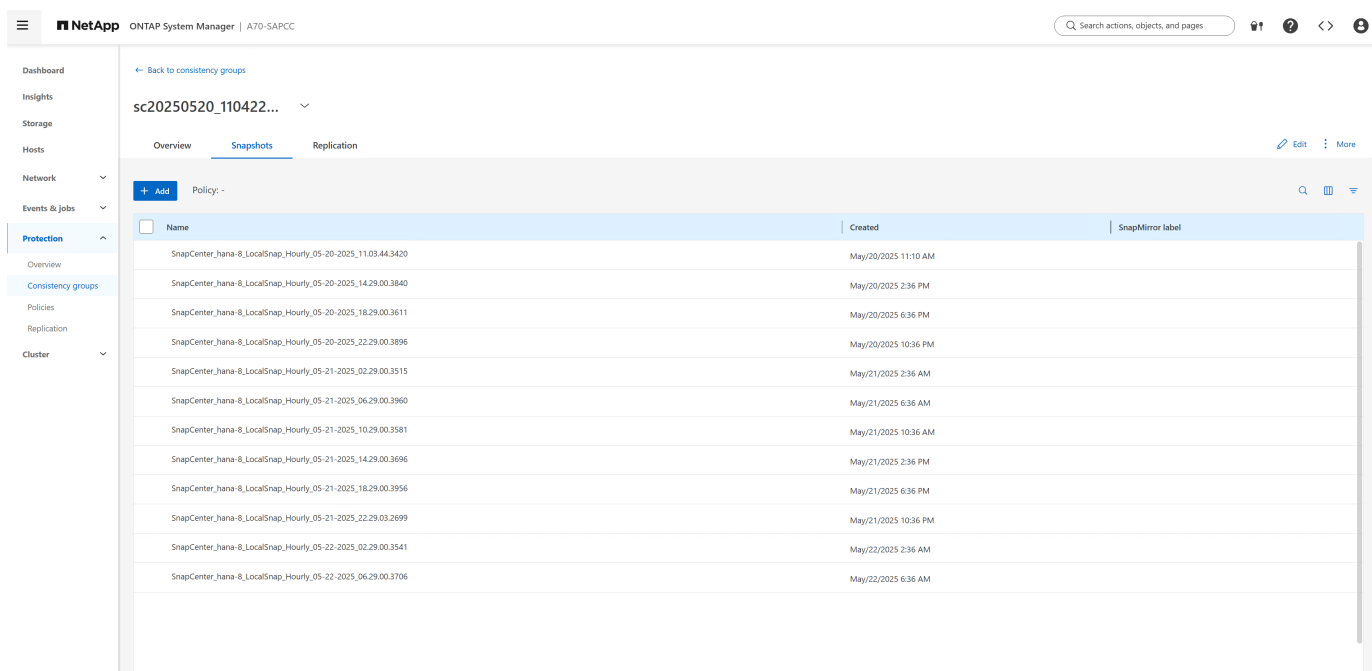
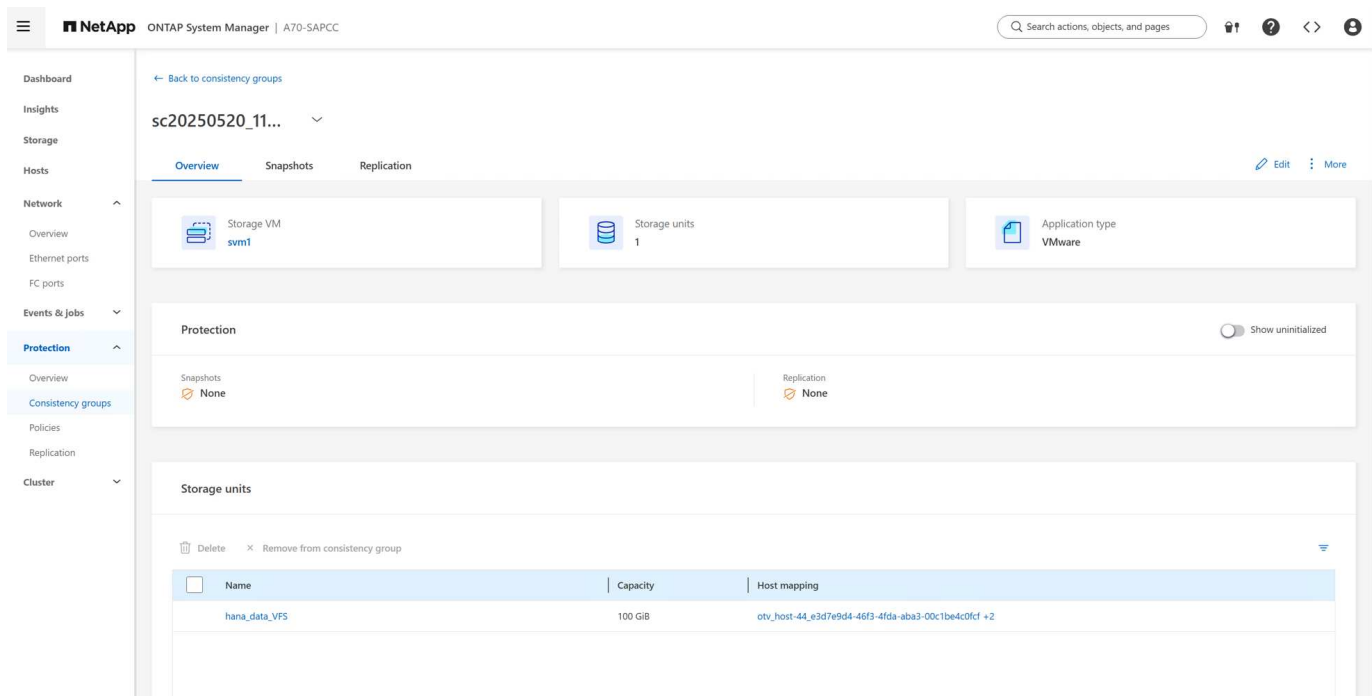
- ✓ ▶ Validate Dataset Parameters
- ✓ ▶ Validate Plugin Parameters
- ✓ ▶ Complete Application Discovery
- ✓ ▶ Initialize Filesystem Plugin
- ✓ ▶ Discover Filesystem Resources
- ✓ ▶ Discover Virtual Resources
- ✓ ▶ Populate storage details
- ✓ ▶ Validate Retention Settings
- ✓ ▶ Quiesce Application
- ✓ ▶ Quiesce Filesystem
- ✓ ▶ Create Snapshot
- ✓ ▶ UnQuiesce Filesystem
- ✓ ▶ UnQuiesce Application
- ✓ ▶ Get Snapshot Details
- ✓ ▶ Get Filesystem Metadata
- ✓ ▶ Get Virtualization Metadata
- ✓ ▶ Finalize Filesystem Plugin
- ✓ ▶ Collect Autosupport data
- ✓ ▶ Register Backup and Apply Retention
- ✓ ▶ Register Snapshot attributes
- ✓ ▶ Application Clean-Up
- ✓ ▶ Data Collection
- ✓ ▶ Agent Finalize Workflow

i Task Name: Backup Start Time: 05/21/2025 10:29:05 PM End Time: 05/21/2025 10:30:38 PM

View Logs

Cancel Job

Close



Operações de restauração e recuperação

Com recursos virtuais armazenados no SnapCenter do VMFS/VMDK, as operações de restauração são sempre feitas por meio de uma operação de clonagem, montagem e cópia.

1. O SnapCenter cria um clone de armazenamento com base no Snapshot selecionado
2. O SnapCenter monta o LUN como um novo armazenamento de dados no host ESX
3. O SnapCenter adiciona o VMDK no datastore como um novo disco à VM HANA
4. O SnapCenter monta o novo disco para o sistema operacional Linux
5. O SnapCenter copia os dados do novo disco de volta para o local original

6. Quando a operação de cópia estiver concluída, todos os recursos acima são removidos novamente
7. O SnapCenter executa a recuperação do banco de dados do sistema HANA
8. O SnapCenter executa a recuperação do banco de dados do locatário HANA

O tempo de execução geral da operação de restauração depende do tamanho do banco de dados e da taxa de transferência da conexão FC entre os clusters de armazenamento e os hosts ESX. Em nossa configuração de laboratório com uma instalação inicial do HANA, o tempo de execução foi de cerca de 12 minutos.

Restore from SnapCenter_hana-8_LocalSnap_Hourly_05-22-2025_06.29.00.3706

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource

☐ Tenant Database

Restore from SnapCenter_hana-8_LocalSnap_Hourly_05-22-2025_06.29.00.3706

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Recover database files using

☒ Recover to most recent state

☐ Recover to point in time

☐ Recover to specified data backup

☐ No recovery

Specify log backup locations

Add

/usr/sap/VFS/HDB45/backup/log

Specify backup catalog location

/usr/sap/VFS/HDB45/backup/log

Enquanto a operação de restauração e recuperação estiver em execução, você poderá ver uma nova unidade de armazenamento clonada.

NetApp

ONTAP System Manager | A70-SAPCC

Search actions, objects, and pages

Dashboard

Insights

Storage

Hosts

Network

Events & Jobs

Protection

Cluster

Storage

The basic unit of storage is a LUN (for SCSI hosts) or NVMe namespace (for NVMe). You can add LUN or NVMe namespace storage units based on your data center configuration. [More](#)

20

Storage units

68.6

TiB Available

20

Online

0

Offline

+ Add

	Name	Consistency group	Capacity	Data reduction	Host mapping	IOPS	Latency (ms)	Throughput (MB/s)
☒	hana_data_VFS	sc20250520_110422_589	100 GiB	1.01 to 1	otv_host-44_e3d7e9d4-46f3-4fd5	0	0	0
☒	hana_data_VFS_Clone_0522250947396031	-	100 GiB	1 to 1	otv_host-57_e3d7e9d4-46f3-4fd5	-	-	-
☒	hana_log_VFS	-	100 GiB	1.19 to 1	otv_host-44_e3d7e9d4-46f3-4fd5	0	0	0
☒	hana_shared_VFS	-	100 GiB	2.33 to 1	otv_host-44_e3d7e9d4-46f3-4fd5	0	0	0

O novo LUN (datastore) baseado na unidade de armazenamento clonada é anexado ao cluster ESX.

vSphere Client

Search in all environments

hana_data_VFS(sc-20250522094807386)

ACTIONS

Summary

Monitor

Configure

Permissions

Files

Hosts

VMs

Filter by a folder name

hana_data_VFS(sc-20250522094807386)

datastore1

datastore1 (1)

datastore1 (2)

Datastore_C250

Datastore_One

DatastoreA400

hana_data_VFS

hana_data_VFS(sc-20250522094807386)

hana_log_VFS

hana_shared_VFS

OS_Image

NEW FOLDER

UPLOAD FILES

UPLOAD FOLDER

REGISTER VM

DOWNLOAD

COPY TO

MOVE TO

RENAME TO

DELETE

INFLATE

☐	Name	Size	Modified	Type	Path
☐	.sdd.sf		05/19/2025, 7:36:45 AM	Folder	[hana_data_VFS(sc-20250522094807386)] .sdd.sf
☐	hana-8		05/22/2025, 9:48:25 AM	Folder	[hana_data_VFS(sc-20250522094807386)] hana-8

Manage Columns

Select All

Folders per page: 1000

2 Items

Recent Tasks

Alarms

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Reconfigure virtual machine	hana-8	Completed		SAPCC.VCENTER\Administrat	7 ms	05/22/2025, 9:48:25 AM	05/22/2025, 9:48:26 AM	ycenter8.sapcc.stl.netapp.com
Rename datastore	scap-5781cdf2-hana_data_VFS	Completed		SAPCC.VCENTER\Administrat	5 ms	05/22/2025, 9:48:15 AM	05/22/2025, 9:48:21 AM	ycenter8.sapcc.stl.netapp.com
Disassociate unprovisioned Managed Columns	Non Task	Completed		SAPCC.VCENTER\Administrat	4 ms	05/22/2025, 9:48:05 AM	05/22/2025, 9:48:05 AM	ycenter8.sapcc.stl.netapp.com

O VMDK dentro do armazenamento de dados é mapeado para a VM HANA de destino e montado no sistema HANA.

```
hana-8:~ # df -h
```

```
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.3G 54G 9% /
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.3G 54G 9% /.snapshots
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.3G 54G 9% /home
/dev/mapper/system-root 60G 5.3G 54G 9% /opt
/dev/mapper/system-root 60G 5.3G 54G 9% /root
/dev/mapper/system-root 60G 5.3G 54G 9% /srv
/dev/mapper/system-root 60G 5.3G 54G 9% /usr/local
/dev/mapper/system-root 60G 5.3G 54G 9% /tmp
/dev/mapper/system-root 60G 5.3G 54G 9% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/VFS/mnt00001
/dev/sdb 95G 7.6G 88G 8% /hana/data/VFS/mnt00001
/dev/sdd 95G 15G 81G 16% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc_share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10%
/var/opt/snapcenter/scu/clones/hana_data_VFS_mnt00001_142592_scu_clone_1

hana-8:~ #
```

Job Details

×

Restore 'hana-8.sapcc.stl.netapp.com\hana\MDC\VFS'

✓

▼

Restore 'hana-8.sapcc.stl.netapp.com\hana\MDC\VFS'

✓

▼

hana-8.sapcc.stl.netapp.com

✓

▼

Restore

✓

▶

Validate Plugin Parameters

✓

▼

Pre Restore Application

✓

▼

Stopping HANA Instance

✓

▼

Filesystem Pre Restore

✓

▼

PreRestore for Virtual Resources

✓

▼

Detach Virtual Disks

✓

▶

Restore Filesystem

✓

▶

Restore for Virtual Resources

✓

▶

Attach Virtual Disks

✓

▶

Filesystem Post Restore

✓

▶

Recover Application

✓

▶

PostRestore for Virtual Resources

✓

▶

Cleaning Storage Resources

✓

▶

Post Restore Cleanup FileSystem

✓

▶

Application Clean-Up

✓

▶

Data Collection

✓

▶

Agent Finalize Workflow

✓

▶

(Job 142596) (Job 142596) read UnmountBackup

📘

Task Name: Recover Application Start Time: 05/22/2025 9:56:13 AM End Time: 05/22/2025 9:58:15 AM

View Logs

Cancel Job

Close

Atualização do sistema SAP

Informações detalhadas sobre as operações de atualização do sistema SAP usando SnapCenter podem ser encontradas em ["Automatizando as operações de clonagem e cópia do sistema SAP HANA com o](#)

SnapCenter".

O segundo sistema HANA QFS foi provisionado da mesma forma descrita no capítulo ["Provisionamento e instalação do sistema HANA"](#).

Pré-requisitos

Para versões do SnapCenter < 6.2, existem limitações que precisam ser consideradas.

1. É necessário reiniciar o processo spl após cada fluxo de trabalho "clone create" e "clone delete" usando o comando "systemctl restart spl" no host HANA de destino.
2. As VMs HANA usadas como origem e destino da operação de atualização do sistema SAP devem ser executadas no mesmo host ESX.

Resumo do fluxo de trabalho

Antes que a primeira operação de atualização do sistema SAP possa ser executada, o sistema HANA de destino deve ser instalado e o host deve ser adicionado ao SnapCenter. Em seguida, o sistema HANA deve ser desligado e o disco de dados HANA deve ser desmontado do host.

Fluxo de trabalho de criação de clone do SnapCenter

1. Criar clone de armazenamento
2. Configurar mapeamento de host para clone de armazenamento
3. Anexar clone de armazenamento (datastore) ao host ESX
4. Adicionar novo disco do armazenamento de dados à VM HANA de destino
5. Montar disco no sistema operacional HANA VM
6. Recuperar sistema HANA usando post-script

Duração: 12 minutos



Em comparação com a operação de restauração, o tempo de execução da operação de clonagem é independente do tamanho do banco de dados HANA. O tempo de execução das etapas 1 a 5 também será semelhante para bancos de dados muito grandes. A recuperação, é claro, levará mais tempo para sistemas HANA maiores.

Fluxo de trabalho de exclusão de clone do SnapCenter

1. Desligue o sistema HANA usando pré-script
2. Desmontar disco do sistema operacional HANA VM
3. Remover disco da VM HANA
4. Remover armazenamento de dados do host ESX
5. Excluir clone do storage

Duração: 11 minutos

Fluxo de trabalho de criação de clone do SnapCenter

O fluxo de trabalho de criação de clones é iniciado selecionando o Snapshot desejado e clicando no botão clonar.

NetApp SnapCenter®

SAP HANA

Search databases

VF5 Topology

Manage Copies

12 Backups
0 Clones
Local copies

Summary Card

13 Backups
12 Snapshot based backups
1 File Based backup ✓
0 Clones
0 Snapshots Locked

Primary Backup(s)

search

Backup Name	Snapshot Lock Expiration	Count	End Date
SnapCenter_hana-8_LocalSnap_Hourly_06-16-2025_06.29.00.4157		1	06/16/2025 6:30:29 AM
SnapCenter_hana-8_LocalSnap_Hourly_06-16-2025_02.29.00.4072		1	06/16/2025 2:30:28 AM
SnapCenter_hana-8_LocalSnap_Hourly_06-15-2025_22.29.00.4010		1	06/15/2025 10:30:30 PM
SnapCenter_hana-8_LocalSnap_Hourly_06-15-2025_18.29.00.3828		1	06/15/2025 6:30:28 PM
SnapCenter_hana-8_LocalSnap_Hourly_06-15-2025_14.29.00.3772		1	06/15/2025 2:30:28 PM
SnapCenter_hana-8_LocalSnap_Hourly_06-15-2025_10.29.00.4143		1	06/15/2025 10:30:28 AM
SnapCenter_hana-8_LocalSnap_Hourly_06-15-2025_06.29.00.3640		1	06/15/2025 6:30:28 AM
SnapCenter_hana-8_LocalSnap_Hourly_06-15-2025_02.29.03.3879		1	06/15/2025 2:30:34 AM
SnapCenter_hana-8_LocalSnap_Hourly_06-14-2025_22.29.00.3826		1	06/14/2025 10:30:28 PM
SnapCenter_hana-8_LocalSnap_Hourly_06-14-2025_18.29.00.3832		1	06/14/2025 6:30:28 PM
SnapCenter_hana-8_LocalSnap_Hourly_06-14-2025_14.29.00.3741		1	06/14/2025 2:30:28 PM
SnapCenter_hana-8_LocalSnap_Hourly_06-14-2025_10.29.00.3930		1	06/14/2025 10:30:29 AM

Total 7

Total 12

Activity The 5 most recent jobs are displayed

3 Completed 0 Warnings 0 Failed 0 Canceled 2 Running 0 Queued

<https://snapcenter.sapcc.at.netapp.com:8146/Datacenter/Database/CloneFromBackup?view>

O host de destino e o SID devem ser fornecidos.

Clone From Backup

- Location
- Settings
- Scripts
- Notification
- Summary

Select the host to create the clone

Plug-in host: hana-9.sapcc.stl.netapp.com

Target Clone SID: QFS

Clone From Backup

- Location
- Settings
- Scripts
- Notification
- Summary

LUN Map Settings

Igroup protocol: FCP

Select
Mixed
FCP
iSCSI

Em nosso exemplo, estamos usando um pós-script para executar a recuperação no host de destino.

Clone From Backup

1 Location

2 Settings

3 Scripts

4 Notification

5 Summary

The following commands will run on the Plug-in Host: **hana-9.sapcc.stl.netapp.com**

Enter optional commands to run before performing a clone operation ⓘ

Pre clone command

Enter optional commands to run after performing a clone operation ⓘ

Post clone command

Quando o fluxo de trabalho é iniciado, o SnapCenter cria uma unidade de armazenamento clonada com base no Snapshot selecionado.

NetApp

ONTAP System Manager | A70-SAPCC

Search actions, objects, and pages

Dashboard

Insights

Storage

Hosts

Network

Events & Jobs

Protection

Cluster

Storage

The basic unit of storage is a LUN (for SCSI hosts) or NVMe namespace (for NVMe). You can add LUN or NVMe namespace storage units based on your data center configuration. [More](#)

22 Storage units

68.5 TiB Available

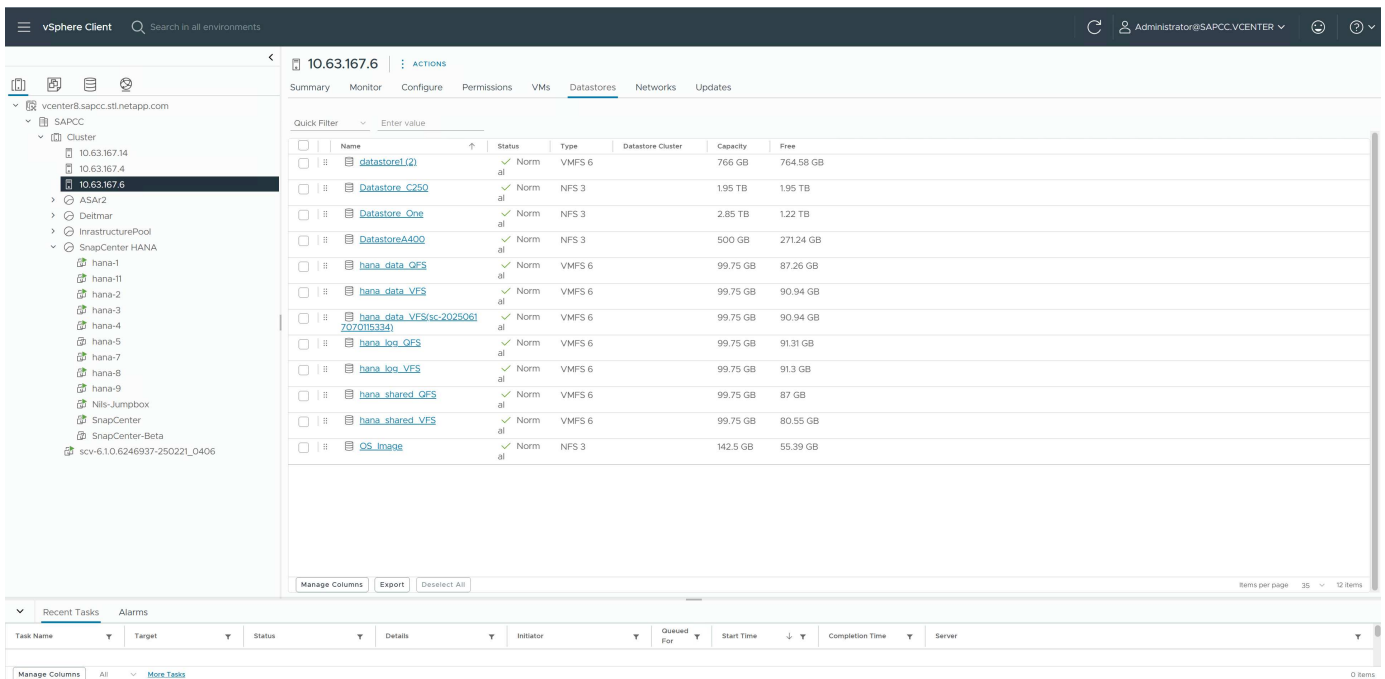
22 Online

0 Offline

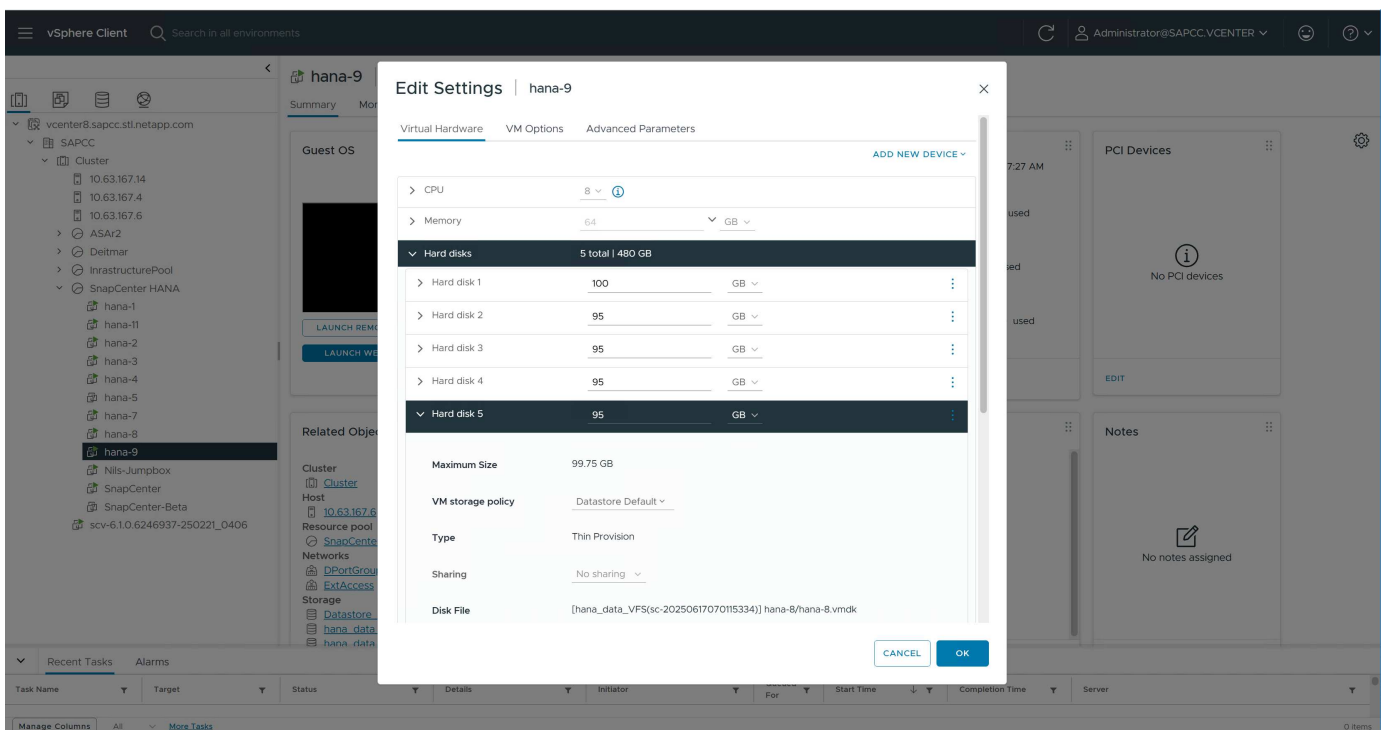
+ Add

Name	Consistency group	Capacity	Data reduction	Host mapping	IOPS	Latency (ms)	Throughput (MB/s)
hana_data_QFS	-	100 GiB	5.46 to 1	otv_host-44_e3d7e9d4-46f3-4f5d	4	0.11	0.39
hana_data_VFS	sc20250520_110422_689	100 GiB	1 to 1	otv_host-44_e3d7e9d4-46f3-4f5d	5	0.12	0.39
hana_data_VFS_Clone_06172507005037511	-	100 GiB	1 to 1	otv_host-57_e3d7e9d4-46f3-4f5d	23	0.11	1.24
hana_log_QFS	-	100 GiB	4.1 to 1	otv_host-44_e3d7e9d4-46f3-4f5d	5	0.10	0.39
hana_log_VFS	-	100 GiB	1.22 to 1	otv_host-44_e3d7e9d4-46f3-4f5d	8	0.12	0.40
hana_shared_QFS	-	100 GiB	2.81 to 1	otv_host-44_e3d7e9d4-46f3-4f5d	5	0.11	0.39
hana_shared_VFS	-	100 GiB	1.69 to 1	otv_host-44_e3d7e9d4-46f3-4f5d	5	0.13	0.39

O SnapCenter então anexa o LUN (datastore) ao host ESX, no qual a VM HANA de destino está sendo executada.



O VMDK dentro do novo armazenamento de dados é então adicionado à VM HANA.



O SnapCenter então configura e monta o novo disco no sistema HANA Linux.

```
hana-9:/mnt/sapcc-share/SAP-System-Fresh # df -h
```

```
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.2G 52G 10% /
devtmpfs 4.0M 4.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
```

```

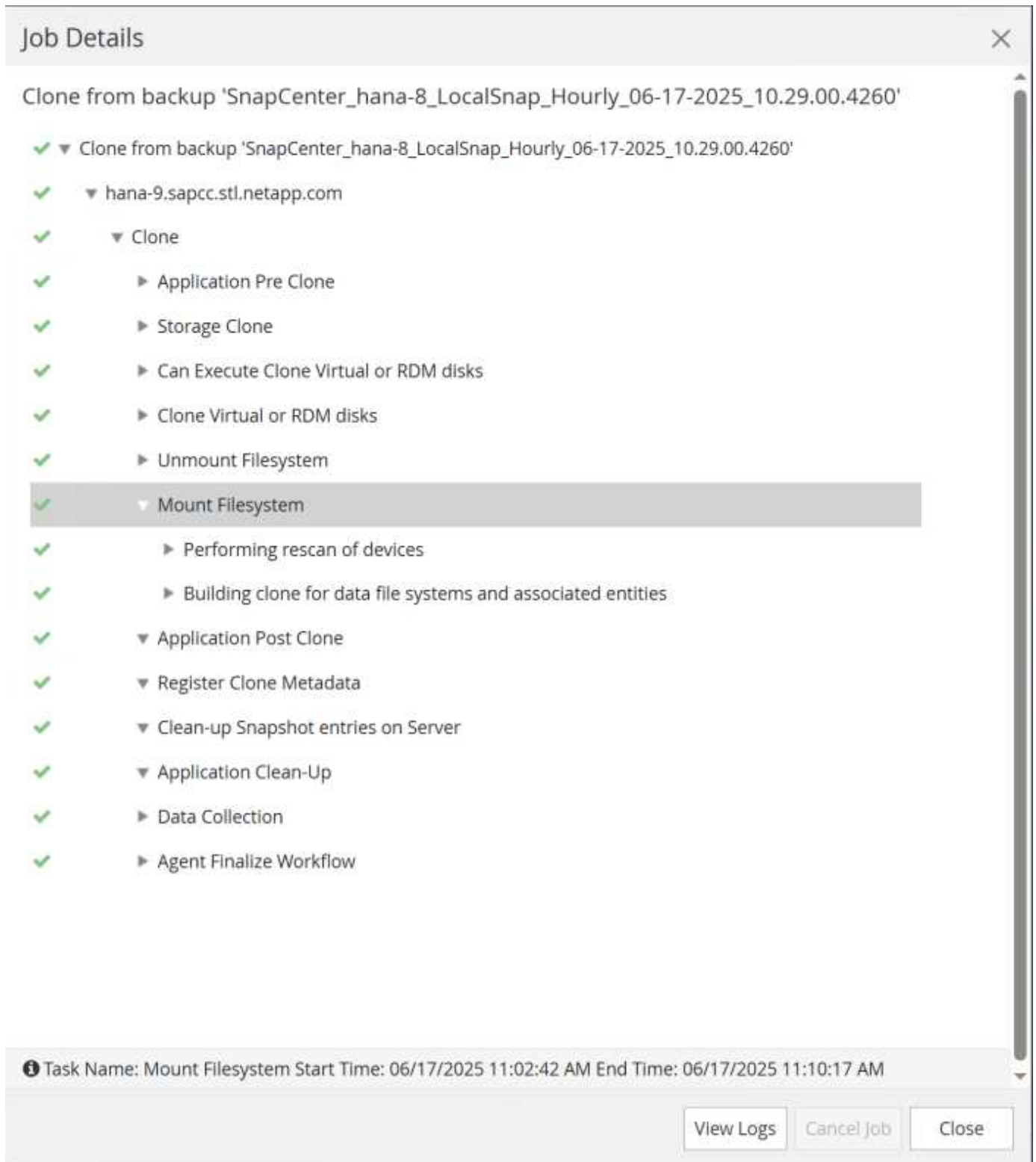
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.2G 52G 10% /.snapshots
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.2G 52G 10% /home
/dev/mapper/system-root 60G 5.2G 52G 10% /opt
/dev/mapper/system-root 60G 5.2G 52G 10% /srv
/dev/mapper/system-root 60G 5.2G 52G 10% /root
/dev/mapper/system-root 60G 5.2G 52G 10% /tmp
/dev/mapper/system-root 60G 5.2G 52G 10% /usr/local
/dev/mapper/system-root 60G 5.2G 52G 10% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/QFS/mnt00001
/dev/sdd 95G 14G 82G 14% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc++_++share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10% /hana/data/QFS/mnt00001
tmpfs 6.3G 56K 6.3G 1% /run/user/1001
hana-9:/mnt/sapcc-share/SAP-System-Refresh #

hana-9:/mnt/sapcc-share/SAP-System-Refresh # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=/@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2

```

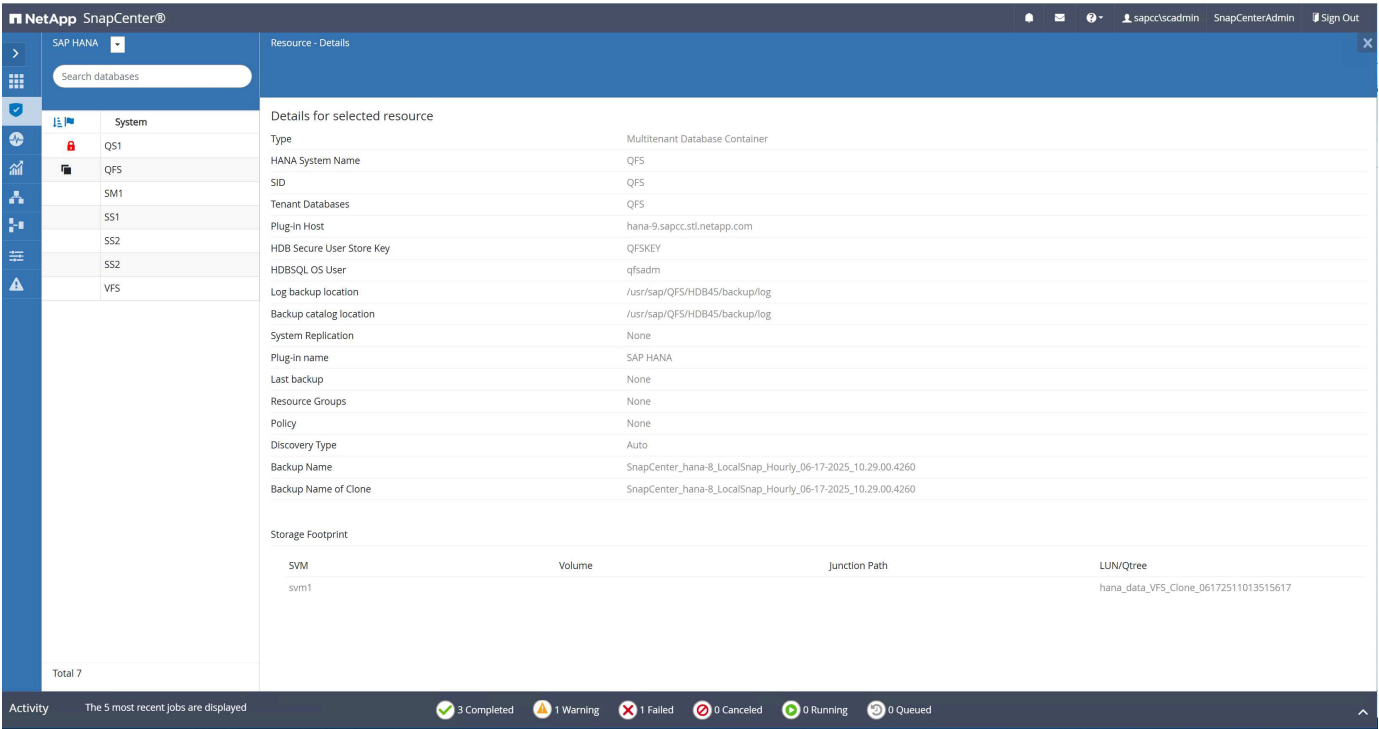
```
192.168.175.86:/sapcc+_+_share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsiz=1048576,wsiz=1048576,intr,noatime,nolock 0
0
#/dev/sdb /hana/data/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
# The following entry has been added by NetApp (SnapCenter Plug-in for
UNIX)
/dev/sde /hana/data/QFS/mnt00001 xfs
rw,relatime,attr2,inode64,logbufs=8,logbsize=32k,noquota 0 0
hana-9:/mnt/sapcc-share/SAP-System-Refresh #
```

A captura de tela a seguir mostra as etapas do trabalho executadas pelo SnapCenter.



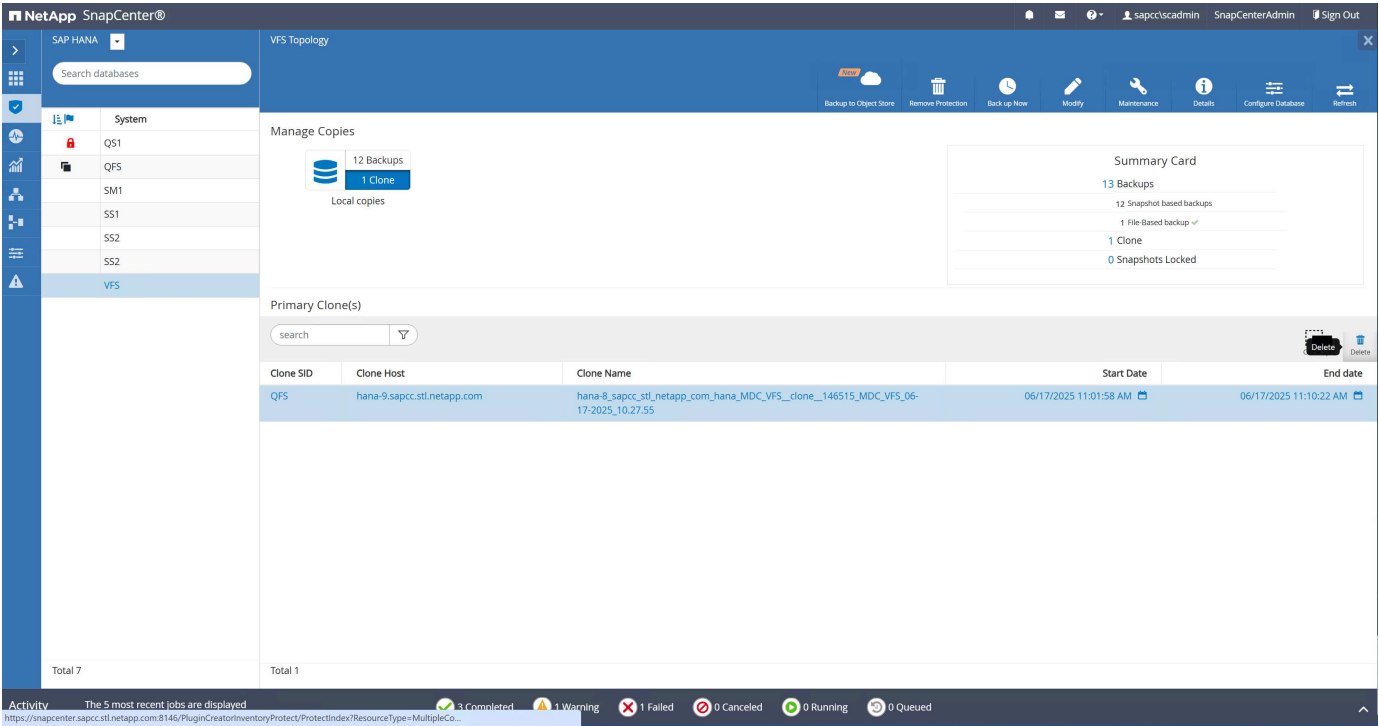
Conforme mencionado na seção "Pré-requisitos", o serviço SnapCenter SPL no host HANA deve ser reiniciado usando o comando "systemctl restart spl" para iniciar a limpeza adequada. Isso deve ser feito após a conclusão do trabalho.

Após a conclusão do fluxo de trabalho de clonagem, a descoberta automática pode ser iniciada clicando no recurso QFS. Após a conclusão do processo de descoberta automática, o novo espaço de armazenamento é listado na visualização de detalhes do recurso.



Fluxo de trabalho de exclusão de clone do SnapCenter

O fluxo de trabalho de exclusão de clones é iniciado selecionando o clone no recurso HANA de origem e clicando no botão excluir.



Em nosso exemplo, estamos usando um pré-script para desligar o banco de dados HANA de destino.

Delete Clone



i Cloned volume will be deleted. SnapCenter backups and HANA backup catalog must be deleted manually.

Enter commands to execute before clone deletion

Pre clone delete :

```
/mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh  
shutdown
```

The selected clone(s) will be permanently deleted. If the selected clone contains other resource(s) it will also be deleted.

If the cloned databases are protected then the protection needs to be removed to delete the clone.

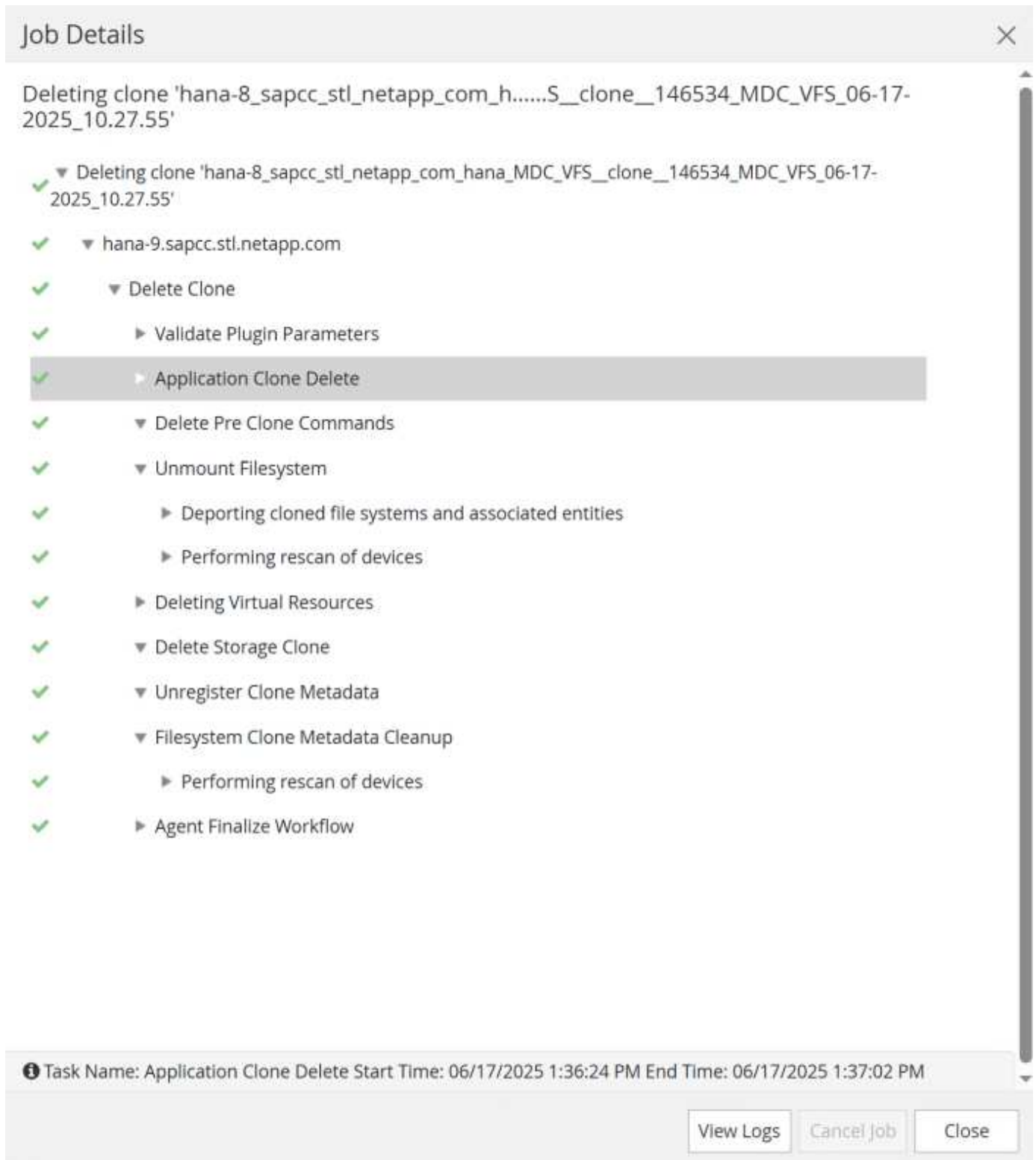
Do you want to proceed?

☐ Force Delete

Cancel

OK

A captura de tela a seguir mostra as etapas do trabalho executadas pelo SnapCenter.



Conforme mencionado na seção “Pré-requisitos”, para SnapCenter releases < 6.2, o serviço SnapCenter spl no host HANA deve ser reiniciado usando o comando “systemctl restart spl” para iniciar a limpeza adequada.

Informações adicionais e histórico de versões

Melhores práticas do HANA:

- "SAP HANA em sistemas NetApp ASA com protocolo Fibre Channel".

- ["Backup e recuperação do SAP HANA com o SnapCenter"](#)
- ["Replicação do sistema SAP HANA: Backup e recuperação com o SnapCenter"](#)
- ["Automatizando as operações de clonagem e cópia do sistema SAP HANA com o SnapCenter"](#)
- ["Proteção de dados SAP HANA e alta disponibilidade com sincronização ativa SnapCenter, SnapMirror e VMware Metro Storage Cluster"](#)
- ["Documentação do software SnapCenter"](#)

Histórico de versões:

Versão	Data	Comentário
Versão 1,0	07/2025	Versão inicial

Backup e recuperação de replicação do sistema SAP HANA com o SnapCenter

Replicação do sistema SAP HANA: Backup e recuperação com o SnapCenter

O SAP HANA System Replication é comumente usado como uma solução de alta disponibilidade ou recuperação de desastres para bancos de dados SAP HANA. O SAP HANA System Replication oferece diferentes modos de operação que você pode usar, dependendo do caso de uso ou dos requisitos de disponibilidade.

Autor: Nils Bauer, NetApp

Existem dois casos de uso primários que podem ser combinados:

- Alta disponibilidade com objetivo de ponto de restauração (RPO) zero e objetivo de tempo de recuperação (rto) mínimo usando um host SAP HANA secundário dedicado.
- Recuperação de desastres em uma grande distância. O host secundário do SAP HANA também pode ser usado para desenvolvimento ou teste durante a operação normal.

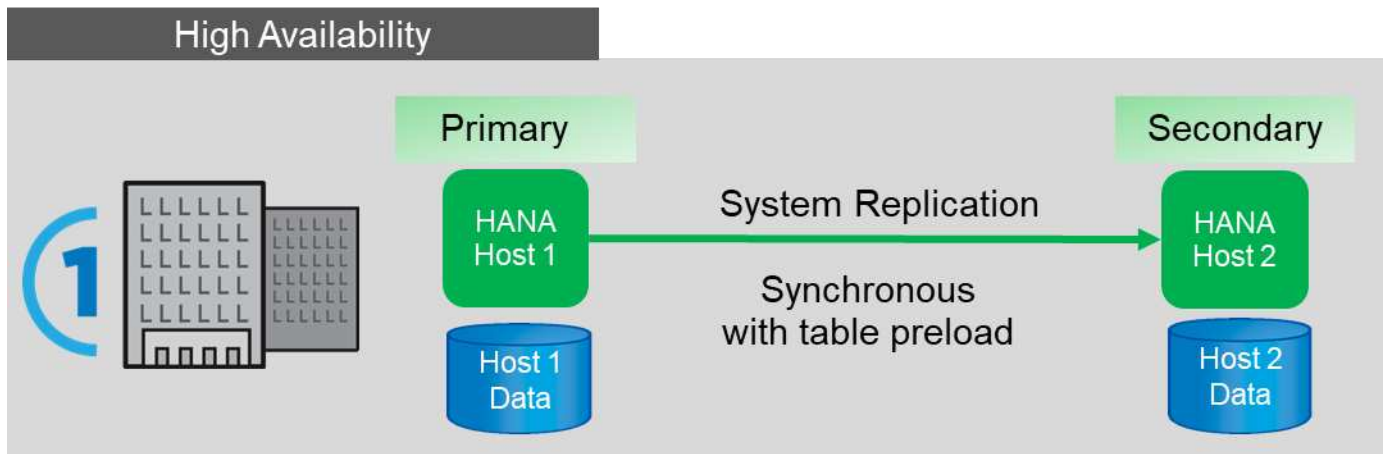
Alta disponibilidade com RPO de zero e rto mínimo

A replicação do sistema é configurada com replicação síncrona usando tabelas pré-carregadas na memória no host secundário do SAP HANA. Essa solução de alta disponibilidade pode ser usada para solucionar falhas de hardware ou software e também para reduzir o tempo de inatividade planejado durante as atualizações de software do SAP HANA (operações de inatividade quase zero).

As operações de failover geralmente são automatizadas com o uso de software de cluster de terceiros ou com um fluxo de trabalho de um clique com o software SAP Landscape Management.

Do ponto de vista dos requisitos de backup, você precisa ser capaz de criar backups independentemente do qual host SAP HANA é primário ou secundário. Uma infraestrutura de backup compartilhada é usada para restaurar qualquer backup, independentemente de qual host o backup foi criado.

O restante deste documento se concentra nas operações de backup com o SAP System Replication configurado como uma solução de alta disponibilidade.



Recuperação de desastres em uma grande distância

A replicação do sistema pode ser configurada com replicação assíncrona sem tabela pré-carregada na memória no host secundário. Essa solução é usada para solucionar falhas do data center, e as operações de failover geralmente são executadas manualmente.

Em relação aos requisitos de backup, você precisa ser capaz de criar backups durante a operação normal no data center 1 e durante a recuperação de desastres no data center 2. Uma infraestrutura de backup separada está disponível nos data centers 1 e 2, e as operações de backup são ativadas como parte do failover de desastres. A infraestrutura de backup normalmente não é compartilhada e não é possível executar uma operação de restauração de um backup criado no outro data center.



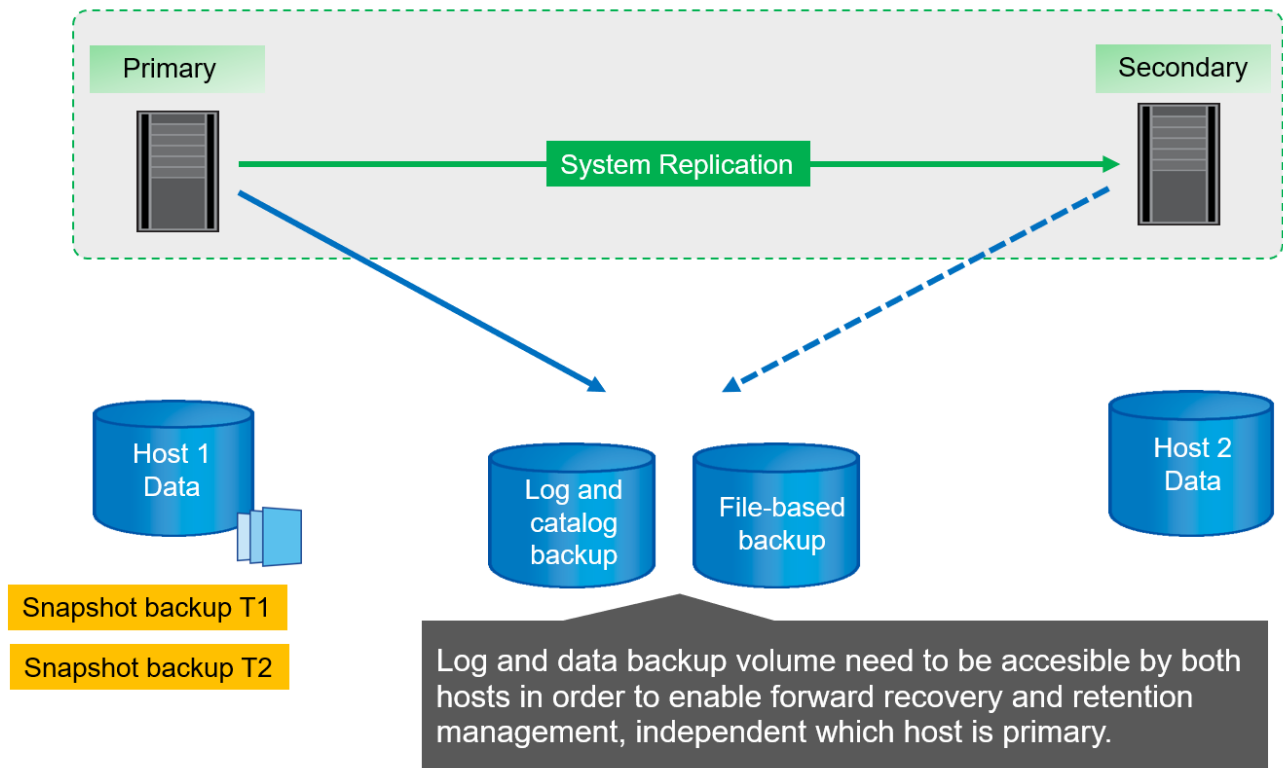
Backups de Snapshot de storage e replicação do sistema SAP

Operações de backup sempre são executadas no host principal do SAP HANA. Os comandos SQL necessários para a operação de backup não podem ser executados no host secundário do SAP HANA.

Para operações de backup do SAP HANA, os hosts SAP HANA primário e secundário são uma única entidade. Eles compartilham o mesmo catálogo de backup do SAP HANA e usam backups para restauração e recuperação, independentemente de o backup ter sido criado no host SAP HANA primário ou secundário.

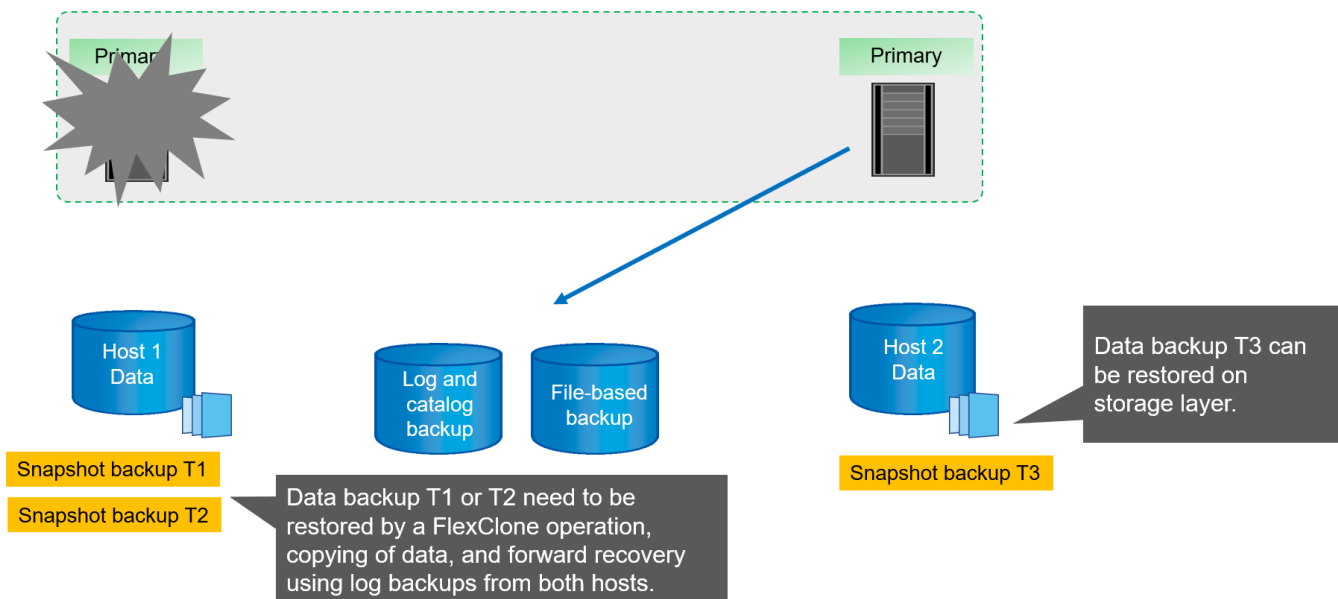
A capacidade de usar qualquer backup para restauração e encaminhar a recuperação usando backups de log de ambos os hosts requer um local de backup de log compartilhado acessível a partir de ambos os hosts. A NetApp recomenda que você use um volume de storage compartilhado. No entanto, você também deve separar o destino de backup de log em subdiretórios dentro do volume compartilhado.

Cada host do SAP HANA tem seu próprio volume de storage. Quando você usa um Snapshot baseado em storage para executar um backup, um Snapshot consistente com banco de dados é criado no volume de storage do host SAP HANA primário.



Quando um failover para o host 2 é executado, o host 2 se torna o host principal, os backups são executados no host 2 e os backups Snapshot são criados no volume de storage do host 2.

O backup criado no host 2 pode ser restaurado diretamente na camada de storage. Se você precisar usar um backup criado no host 1, o backup deve ser copiado do volume de storage do host 1 para o volume de storage do host 2. A recuperação avançada usa os backups de log de ambos os hosts.

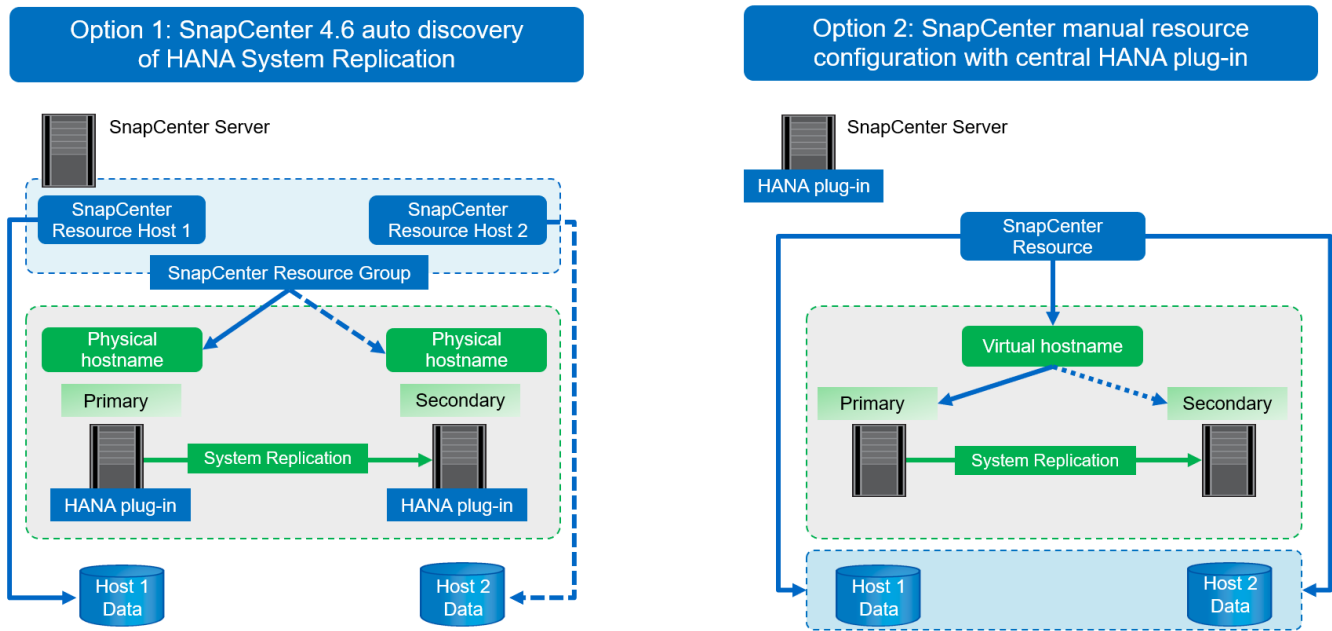


Opções de configuração do SnapCenter para replicação do sistema SAP

Há duas opções para configurar a proteção de dados com o software NetApp

SnapCenter em um ambiente de replicação do sistema SAP HANA:

- Um grupo de recursos do SnapCenter, incluindo hosts SAP HANA e descoberta automática com o SnapCenter versão 4,6 ou posterior.
- Um único recurso do SnapCenter para ambos os hosts SAP HANA que usam um endereço IP virtual.



A partir do SnapCenter 4,6, o SnapCenter oferece suporte à descoberta automática de SISTEMAS HANA configurados em uma relação de replicação do SISTEMA HANA. Cada host é configurado usando seu endereço IP físico (nome do host) e seu volume de dados individual na camada de armazenamento. Os dois recursos do SnapCenter são combinados em um grupo de recursos, e o SnapCenter identifica automaticamente qual host é primário ou secundário e executa as operações de backup necessárias de acordo. O gerenciamento de retenção para cópias Snapshot e backups baseados em arquivos criados pelo SnapCenter é realizado em ambos os hosts para garantir que os backups antigos também sejam excluídos no host secundário atual.

Com uma configuração de recurso único para ambos os hosts SAP HANA, o único recurso do SnapCenter é configurado usando o endereço IP virtual dos hosts de replicação do sistema SAP HANA. Os dois volumes de dados dos hosts do SAP HANA estão incluídos no recurso SnapCenter. Por se tratar de um único recurso SnapCenter, o gerenciamento de retenção para snapshots e backups baseados em arquivos criados pelo SnapCenter funciona independentemente do host que atualmente é primário ou secundário. Essas opções são possíveis com todas as versões do SnapCenter.

A tabela a seguir resume as principais diferenças das duas opções de configuração.

	Grupo de recursos com SnapCenter 4,6	Único recurso SnapCenter e endereço IP virtual
Operação de backup (Snapshot e baseada em arquivo)	Identificação automática do host primário no grupo de recursos	Use automaticamente o endereço IP virtual
Gerenciamento de retenção (Snapshot e baseado em arquivo)	Executado automaticamente em ambos os hosts	Usar automaticamente um único recurso

	Grupo de recursos com SnapCenter 4,6	Único recurso SnapCenter e endereço IP virtual
Requisitos de capacidade de backup	Os backups são criados apenas no volume de host primário	Os backups sempre são criados em ambos os volumes de hosts. O backup do segundo host é apenas consistente com falhas e não pode ser usado para fazer um roll forward.
Operação de restauro	Backups do host ativo atual estão disponíveis para operação de restauração	Script de pré-backup necessário para identificar quais backups são válidos e podem ser usados para restauração
Operação de recuperação	Todas as opções de recuperação disponíveis, assim como para qualquer recurso descoberto automaticamente	Recuperação manual necessária



Em geral, a NetApp recomenda o uso da opção de configuração de grupo de recursos com o SnapCenter 4,6 para proteger sistemas HANA com replicação de sistema HANA habilitada. O uso de uma única configuração de recurso SnapCenter só é necessário se a abordagem de operação do SnapCenter for baseada em um host de plug-in central e o plug-in HANA não for implantado nos hosts de banco de dados HANA.

As duas opções são discutidas em detalhes nas seções a seguir.

Configuração do SnapCenter 4,6 usando um grupo de recursos

O SnapCenter 4,6 é compatível com detecção automática de SISTEMAS HANA configurados com replicação do sistema HANA. O SnapCenter 4,6 inclui a lógica para identificar hosts HANA primário e secundário durante operações de backup e também gerenciar o gerenciamento da retenção em ambos os hosts HANA. Além disso, restauração e recuperação automatizadas agora também estão disponíveis para ambientes HANA System Replication.

Configuração do SnapCenter 4,6 de ambientes de replicação do SISTEMA HANA

A figura a seguir mostra a configuração do laboratório usada para este capítulo. Dois hosts HANA, HANA-3 e HANA-4, foram configurados com HANA System Replication.

Foi criado um usuário de banco de dados "SnapCenter" para o banco de dados do sistema HANA com os privilégios necessários para executar operações de backup e recuperação (consulte "[Backup e recuperação do SAP HANA com o SnapCenter](#)"). Uma chave de armazenamento de usuário HANA deve ser configurada em ambos os hosts usando o usuário de banco de dados acima.

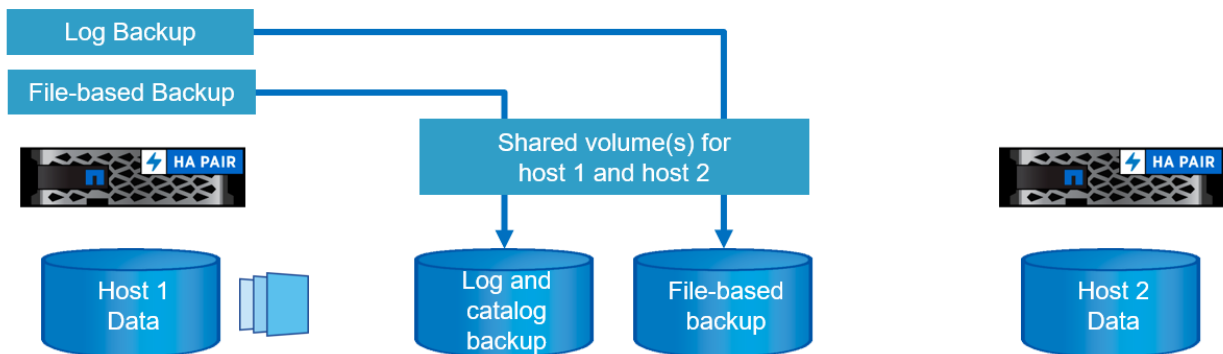
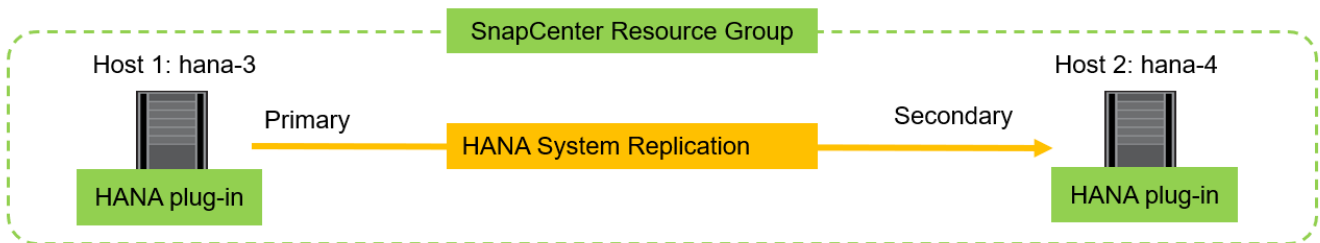
```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```



```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

De um ponto de vista de alto nível, você deve executar as etapas a seguir para configurar a replicação do SISTEMA HANA no SnapCenter.

1. Instale o plug-in HANA no host primário e secundário. A detecção automática é executada e o status de replicação do sistema HANA é detetado para cada host primário ou secundário.
2. Execute o SnapCenter configure database e forneça a hdbuserstore chave. Outras operações de autodescoberta são executadas.
3. Crie um grupo de recursos, incluindo hosts e configure a proteção.



Depois de instalar o plug-in do SnapCenter HANA em ambos os hosts HANA, os SISTEMAS HANA são exibidos na visualização de recursos do SnapCenter da mesma maneira que outros recursos descobertos automaticamente. A partir do SnapCenter 4,6, é exibida uma coluna adicional que mostra o status da replicação do SISTEMA HANA (habilitado/desabilitado, primário/secundário).

NetApp SnapCenter®									
SAP HANA									
View: Multitenant Database Container Search databases									
Resources	System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
	SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com				Not protected
	SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com				Not protected

Ao clicar no recurso, o SnapCenter solicita a chave de armazenamento do USUÁRIO HANA para o sistema HANA.

Configure Database

Plug-in host

hana-3.sapcc.stl.netapp.com

HDBSQL OS User

ss2adm

HDB Secure User Store Key

SS2KEY

Cancel

OK

Etapas adicionais de autodescoberta são executadas e o SnapCenter mostra os detalhes do recurso. Com o SnapCenter 4,6, o status da replicação do sistema e o servidor secundário são listados nesta exibição.

NetApp SnapCenter

SAP HANA

Search databases

System

SS2

SS2

Details for selected resource

Type

Multitenant Database Container

HANA System Name

SS2

SID

SS2

Tenant Databases

SS2

Plug-in Host

hana-3.sapcc.stl.netapp.com

HDB Secure User Store Key

SS2KEY

HDBSQL OS User

ss2adm

Log backup location

/mnt/backup/SS2

Backup catalog location

/mnt/backup/SS2

System Replication

Enabled (Primary)

Secondary Servers

hana-4

plug-in name

SAP HANA

Last backup

None

Resource Groups

None

Policy

None

Discovery Type

Auto

Storage Footprint

SVM	Volume	Junction Path	LUN/Qtree
hana-primary.sapcc.stl.netapp.com	SS2_data_mnt00001	/SS2_data_mnt00001	

Total 2

Activity

The 5 most recent jobs are displayed

0 Completed

0 Warnings

0 Failed

0 Canceled

0 Running

0 Queued

Depois de executar as mesmas etapas para o segundo recurso HANA, o processo de descoberta automática é concluído e os dois recursos HANA são configurados no SnapCenter.

NetApp SnapCenter

SAP HANA

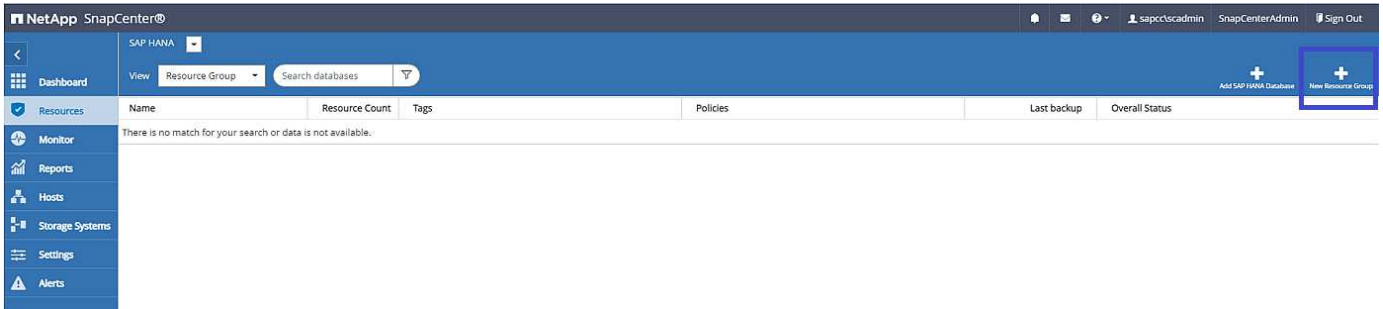
View Multitenant Database Container

Search databases

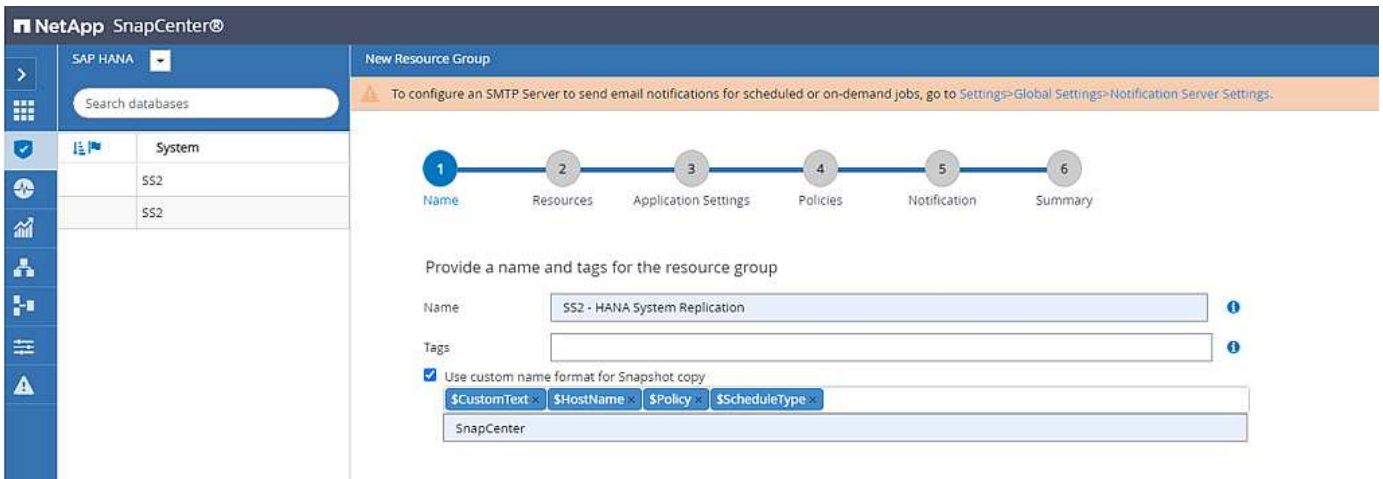
Resources

System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com				Not protected
SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com				Not protected

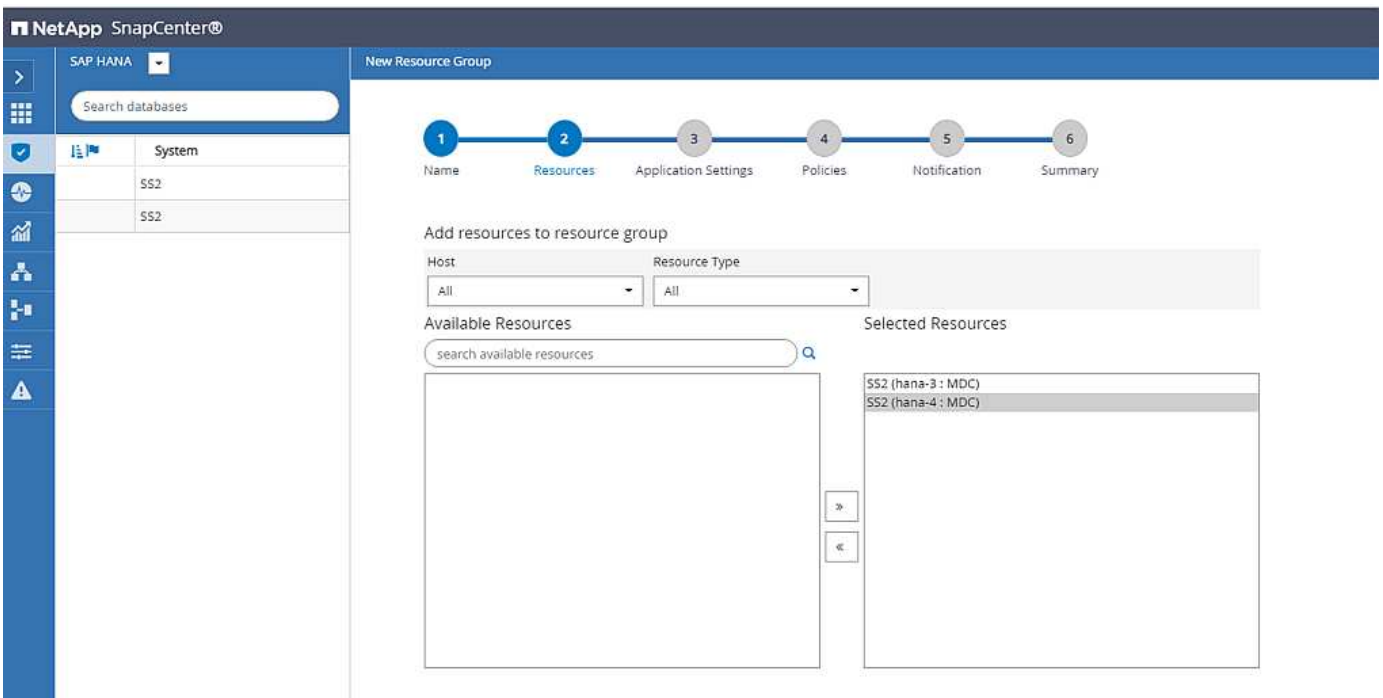
Para sistemas habilitados para replicação do sistema HANA, você deve configurar um grupo de recursos do SnapCenter, incluindo ambos os recursos HANA.



O NetApp recomenda o uso de um formato de nome personalizado para o nome da captura instantânea, que deve incluir o nome do host, a política e a programação.



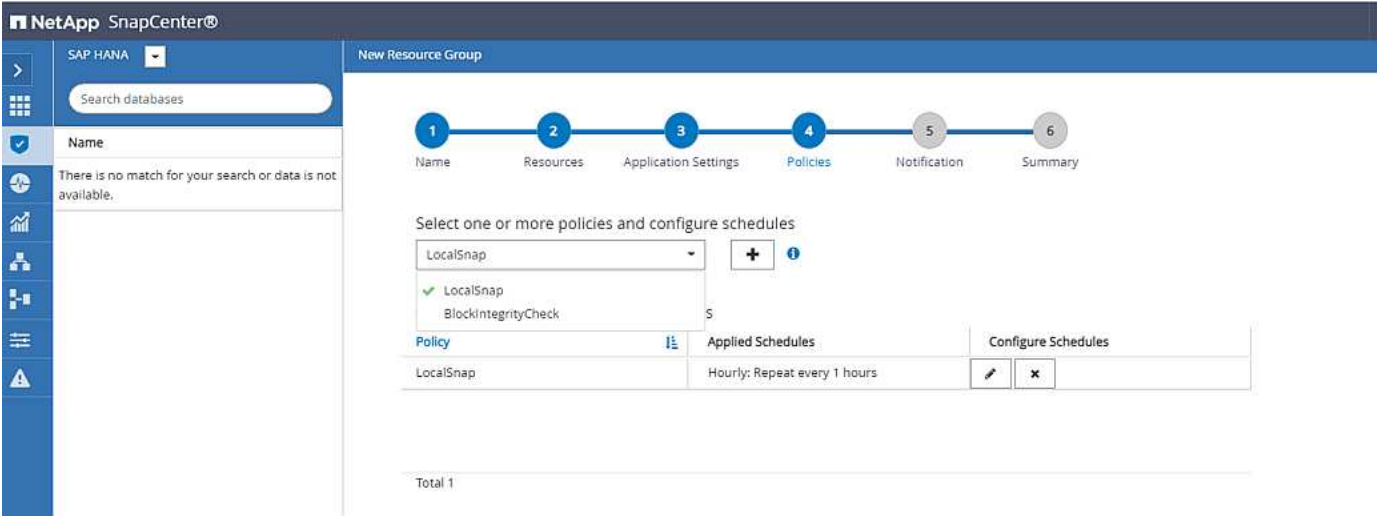
Você deve adicionar ambos os HOSTS HANA ao grupo de recursos.



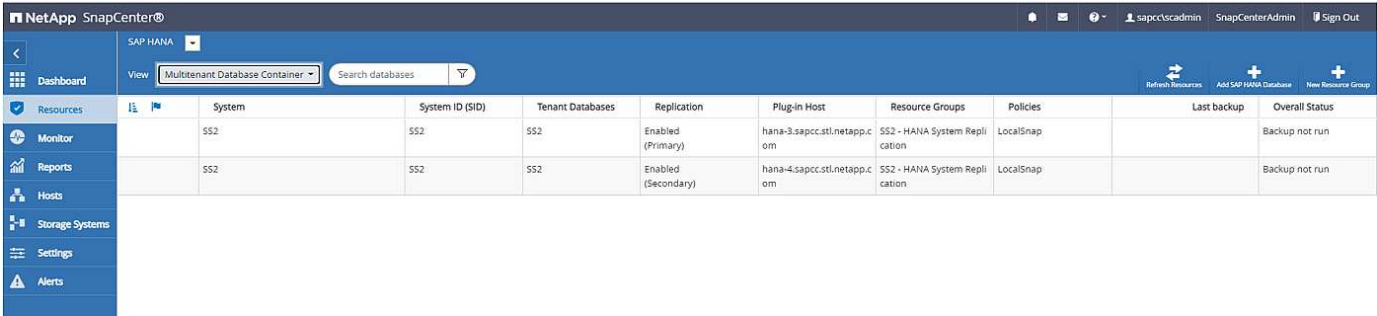
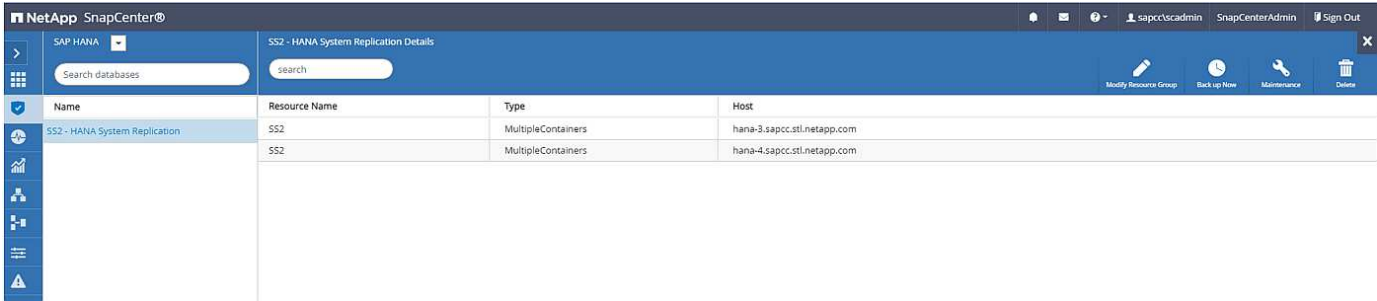
As políticas e programações são configuradas para o grupo de recursos.



A retenção definida na política é usada em ambos os hosts HANA. Se, por exemplo, uma retenção de 10 for definida na política, a soma de backups de ambos os hosts será usada como um critério para exclusão de backup. O SnapCenter exclui o backup mais antigo independentemente se ele tiver sido criado no host primário ou secundário atual.

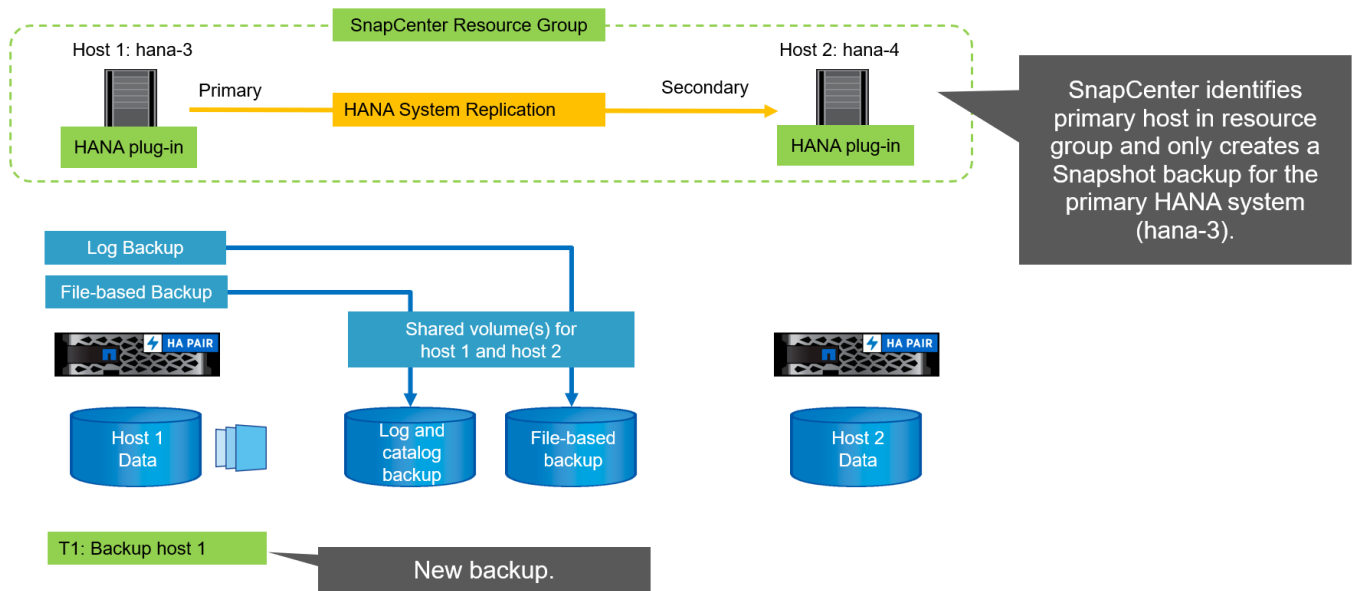


A configuração do grupo de recursos agora está concluída e backups podem ser executados.

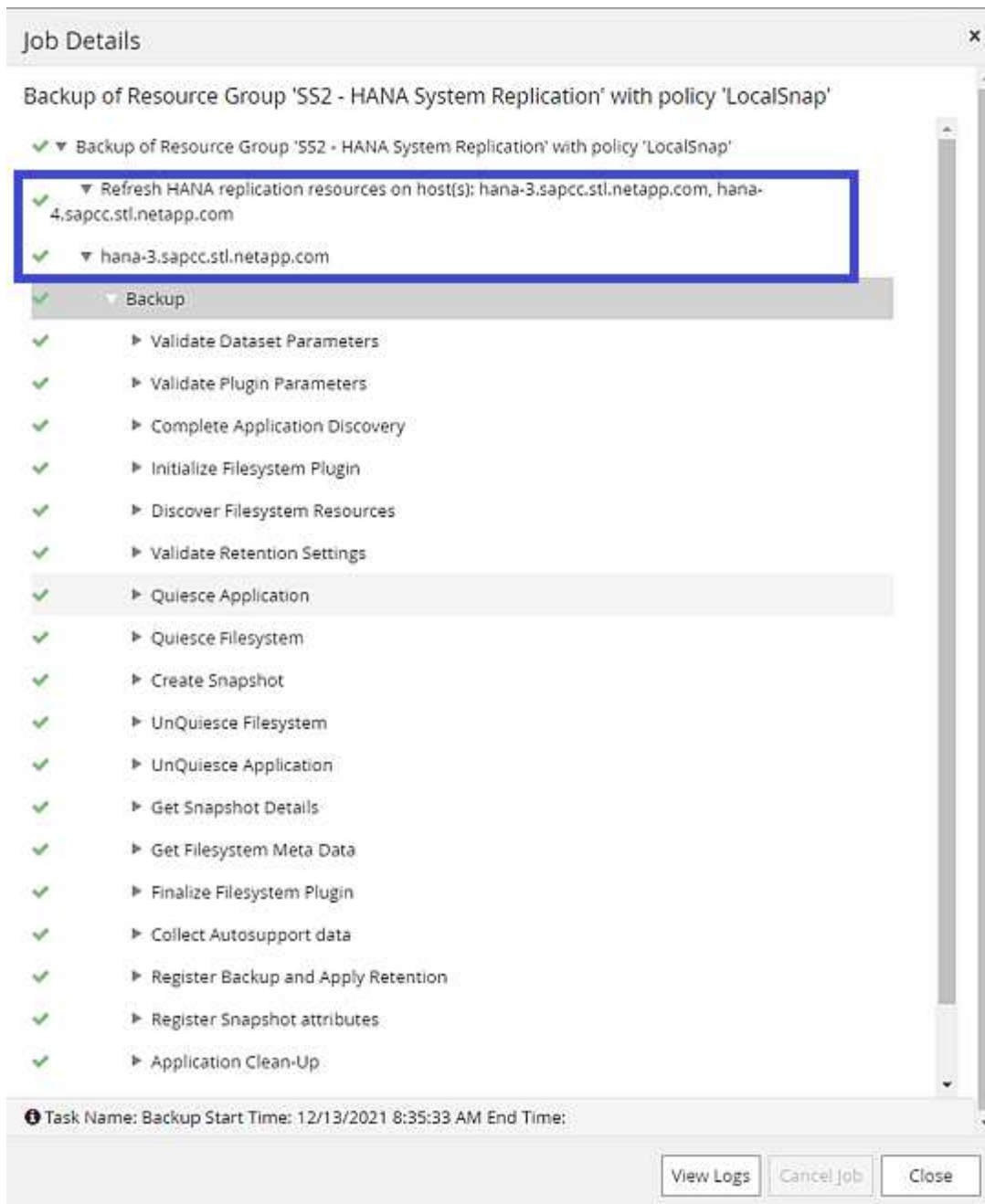


Operações de backup do Snapshot

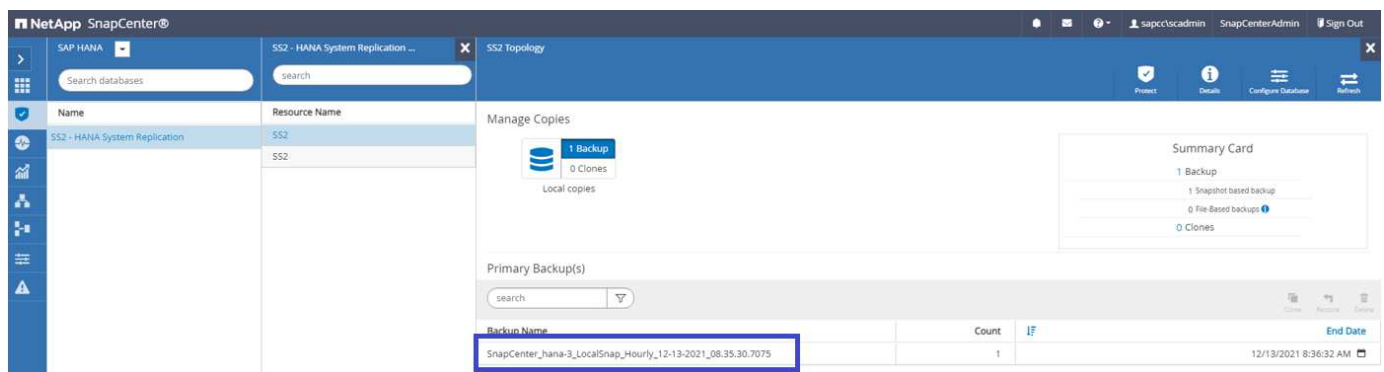
Quando uma operação de backup do grupo de recursos é executada, o SnapCenter identifica qual host é primário e aciona apenas um backup no host primário. Isso significa que apenas o volume de dados do host primário será ajustado. Em nosso exemplo, o HANA-3 é o host principal atual e um backup é executado nesse host.



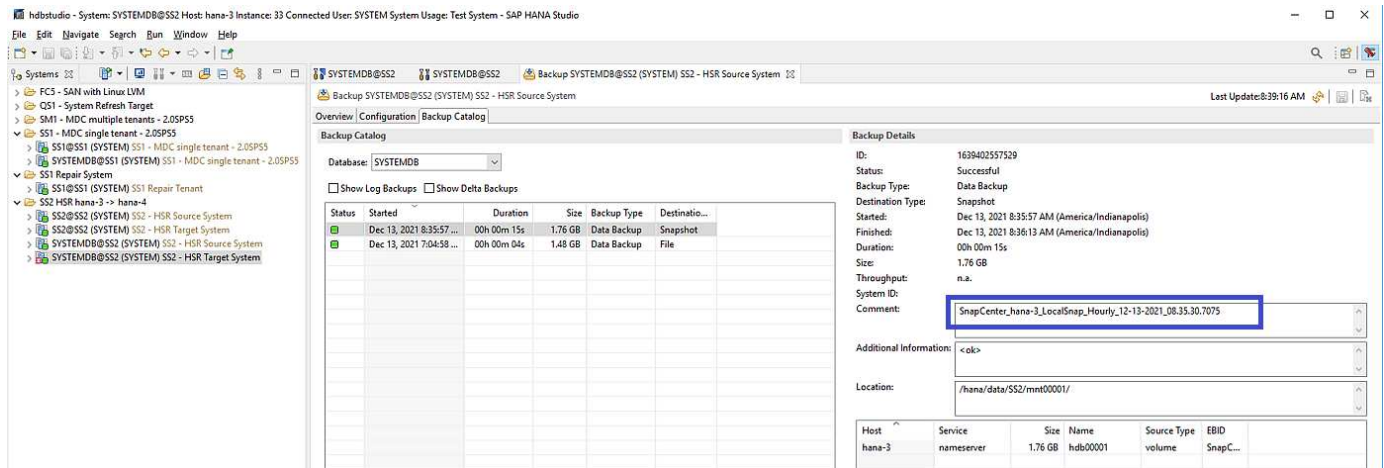
O log de tarefas do SnapCenter mostra a operação de identificação e a execução do backup no host principal atual HANA-3.



Um backup Snapshot agora foi criado no recurso HANA principal. O nome do host incluído no nome do backup mostra HANA-3.



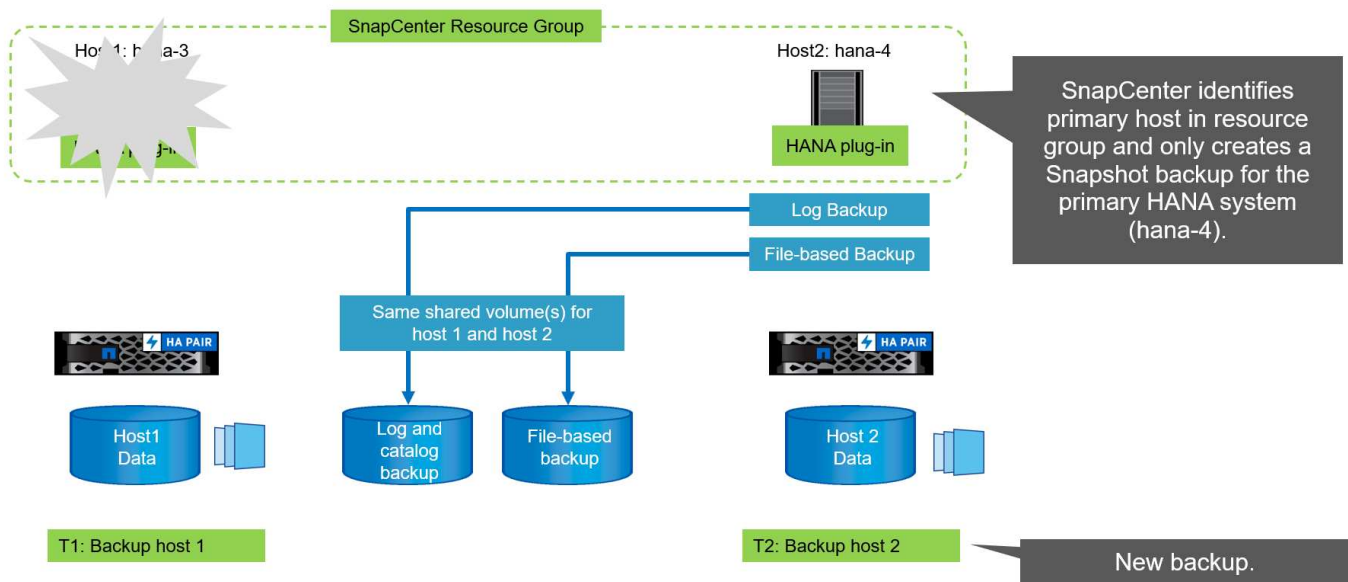
O mesmo backup Snapshot também está visível no catálogo de backup DO HANA.



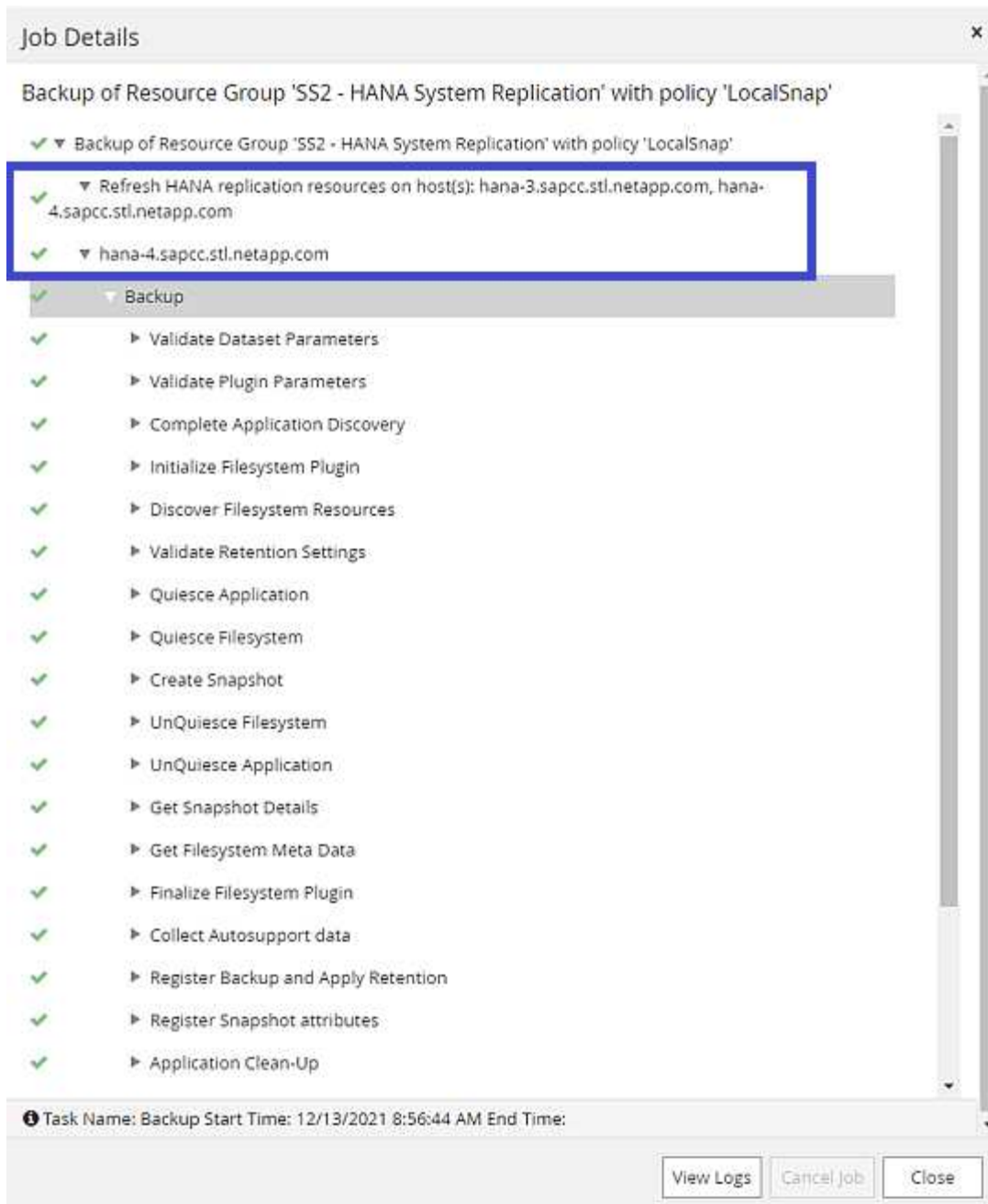
Se uma operação de takeover for executada, backups adicionais do SnapCenter agora identificam o antigo host secundário (HANA-4) como primário e a operação de backup será executada em HANA-4. Novamente, apenas o volume de dados do novo host primário (HANA-4) é ajustado.



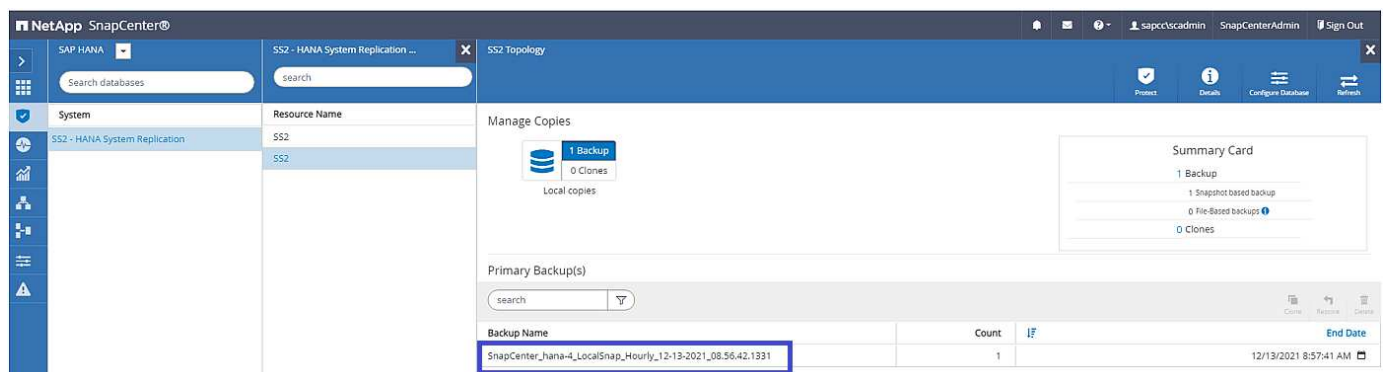
A lógica de identificação do SnapCenter abrange apenas cenários em que os hosts HANA estão em uma relação primária-secundária ou quando um dos HOSTS HANA está offline.



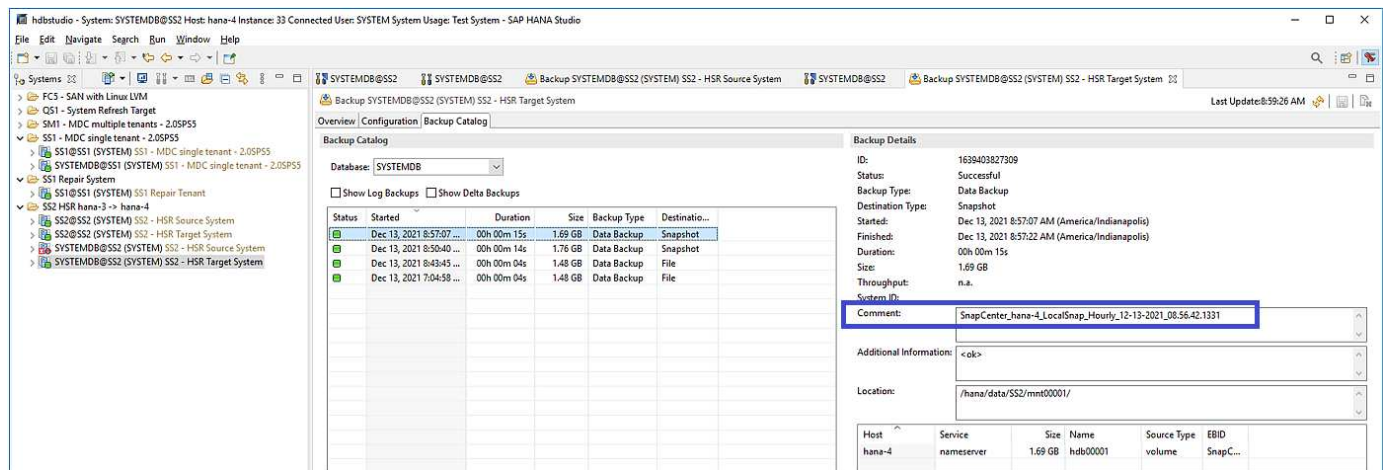
O log de tarefas do SnapCenter mostra a operação de identificação e a execução do backup no host principal atual HANA-4.



Um backup Snapshot agora foi criado no recurso HANA principal. O nome do host incluído no nome do backup mostra HANA-4.



O mesmo backup Snapshot também está visível no catálogo de backup DO HANA.



Operações de verificação de integridade de bloco com backups baseados em arquivo

O SnapCenter 4,6 usa a mesma lógica descrita para operações de backup do Snapshot para operações de verificação de integridade de bloco com backups baseados em arquivo. O SnapCenter identifica o host HANA primário atual e executa o backup baseado em arquivo para esse host. O gerenciamento de retenção também é executado em ambos os hosts, portanto, o backup mais antigo é excluído independentemente de qual host é atualmente o principal.

Replicação SnapVault

Para permitir operações de backup transparentes sem interação manual no caso de um takeover e independente de qual host HANA é atualmente o host principal, você precisa configurar uma relação do SnapVault para os volumes de dados de ambos os hosts. O SnapCenter executa uma operação de atualização do SnapVault para o host principal atual em cada execução de backup.

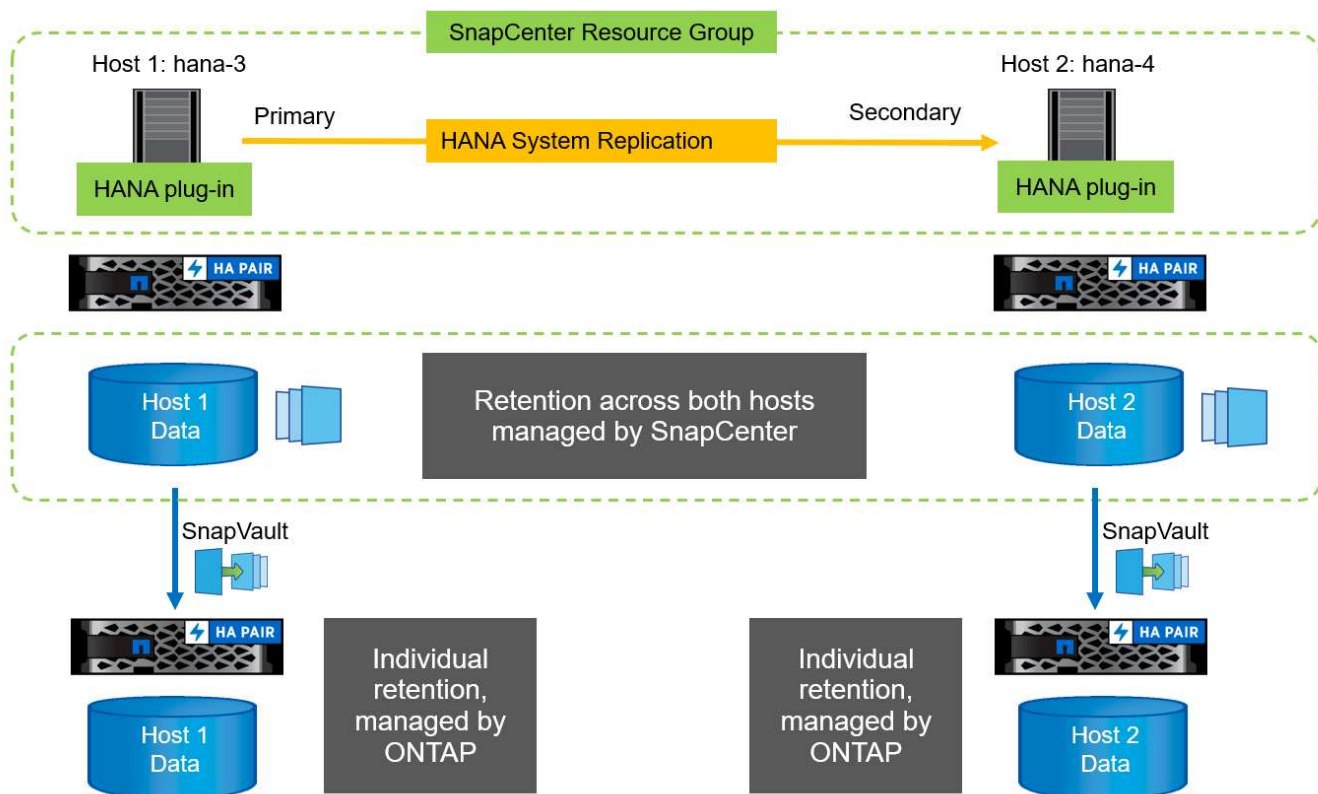


Se uma tomada de controle para o host secundário não for executada por um longo tempo, o número de blocos alterados para a primeira atualização do SnapVault no host secundário será alto.

Como o gerenciamento da retenção no destino SnapVault é gerenciado fora do SnapCenter pela ONTAP, a retenção não pode ser tratada em ambos os hosts HANA. Portanto, os backups que foram criados antes de um takeover não são excluídos com operações de backup no secundário anterior. Esses backups permanecem até que o primeiro primário se torne primário novamente. Para que esses backups não bloqueiem o gerenciamento de retenção de backups de log, eles precisam ser excluídos manualmente no destino do SnapVault ou no catálogo de backup DO HANA.



Uma limpeza de todas as cópias Snapshot do SnapVault não é possível, porque uma cópia Snapshot é bloqueada como ponto de sincronização. Se a cópia Snapshot mais recente também precisar ser excluída, a relação de replicação do SnapVault deve ser excluída. Nesse caso, a NetApp recomenda excluir os backups no catálogo de backup HANA para desbloquear o gerenciamento de retenção de backup de log.



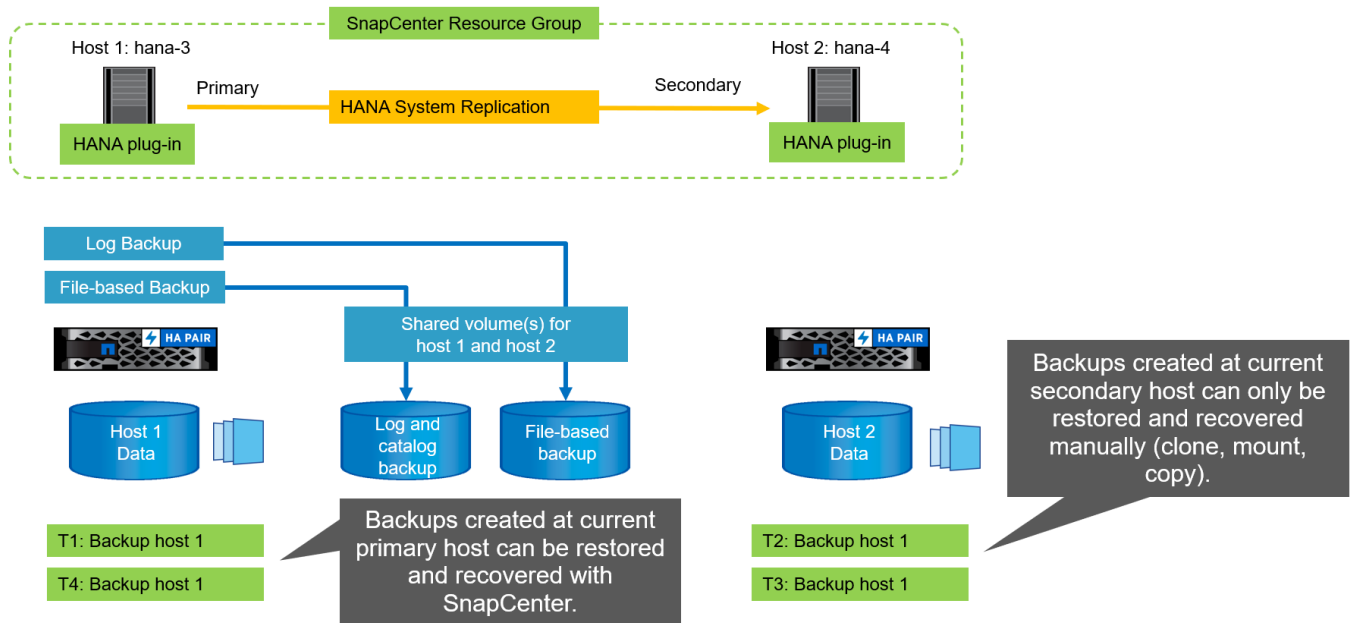
Gerenciamento de retenção

O SnapCenter 4,6 gerencia a retenção para backups Snapshot, operações de verificação de integridade de bloco, entradas de catálogo de backup HANA e backups de log (se não estiver desativado) em ambos os HOSTS HANA, não importa qual host é primário ou secundário atualmente. Os backups (dados e log) e as entradas no CATÁLOGO HANA são excluídos com base na retenção definida, independentemente de uma operação de exclusão ser necessária no host primário ou secundário atual. Em outras palavras, nenhuma interação manual é necessária se uma operação de aquisição for executada e/ou a replicação for configurada na outra direção.

Se a replicação do SnapVault fizer parte da estratégia de proteção de dados, a interação manual é necessária para cenários específicos, conforme descrito na seção ["Replicação do SnapVault"](#)

Restauração e recuperação

A figura a seguir mostra um cenário em que várias aquisições foram executadas e os backups Snapshot foram criados em ambos os locais. Com o status atual, o host HANA-3 é o host principal e o backup mais recente é o T4, que foi criado no host HANA-3. Se você precisar executar uma operação de restauração e recuperação, os backups T1 e T4 estão disponíveis para restauração e recuperação no SnapCenter. Os backups, criados no host HANA-4 (T2, T3), não podem ser restaurados usando o SnapCenter. Esses backups devem ser copiados manualmente para o volume de dados do HANA-3 para recuperação.



As operações de restauração e recuperação para uma configuração de grupo de recursos do SnapCenter 4.6 são idênticas a uma configuração de replicação não-sistema descoberta automaticamente. Todas as opções de restauração e recuperação automática estão disponíveis. Para obter mais detalhes, consulte o relatório técnico. "[Backup e recuperação do SAP HANA com o SnapCenter](#)".

Uma operação de restauração de um backup criado no outro host é descrita na "[Restaurar e recuperar a partir de um backup criado no outro host](#)" seção .

Configuração do SnapCenter com um único recurso

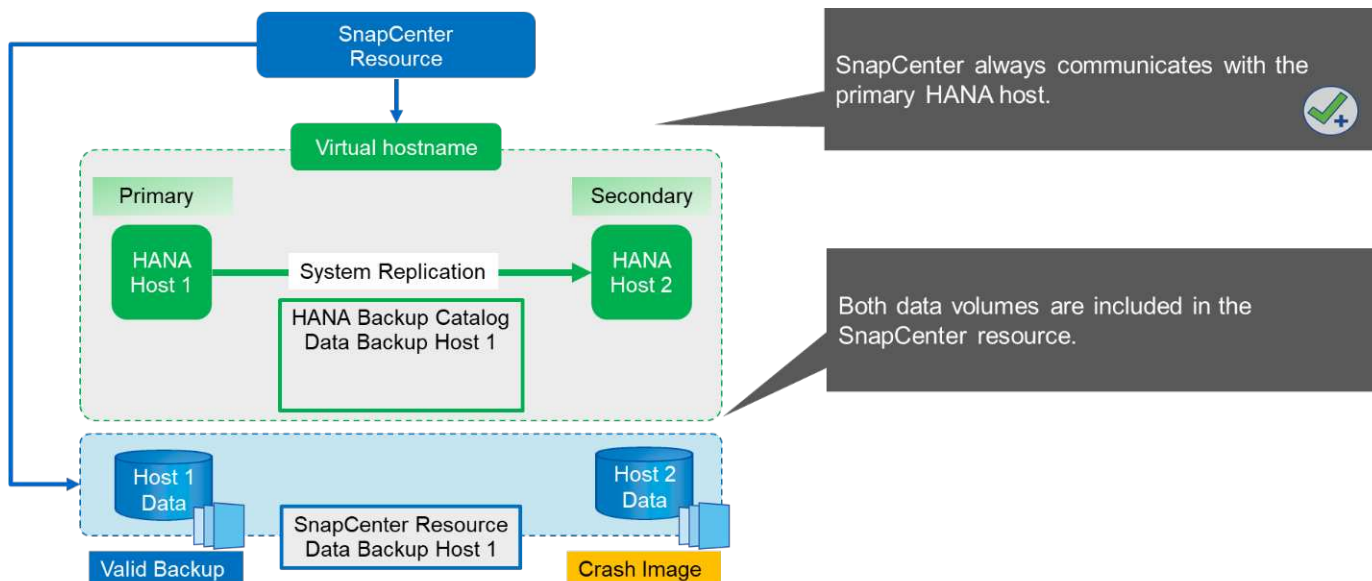
Um recurso SnapCenter é configurado com o endereço IP virtual (nome do host) do ambiente de replicação do SISTEMA HANA. Com essa abordagem, o SnapCenter sempre se comunica com o host principal, independentemente de o host 1 ou o host 2 ser primário. Os volumes de dados de ambos os hosts do SAP HANA estão incluídos no recurso SnapCenter.



Assumimos que o endereço IP virtual está sempre vinculado ao host SAP HANA primário. O failover do endereço IP virtual é realizado fora do SnapCenter como parte do fluxo de trabalho de failover de replicação do SISTEMA HANA.

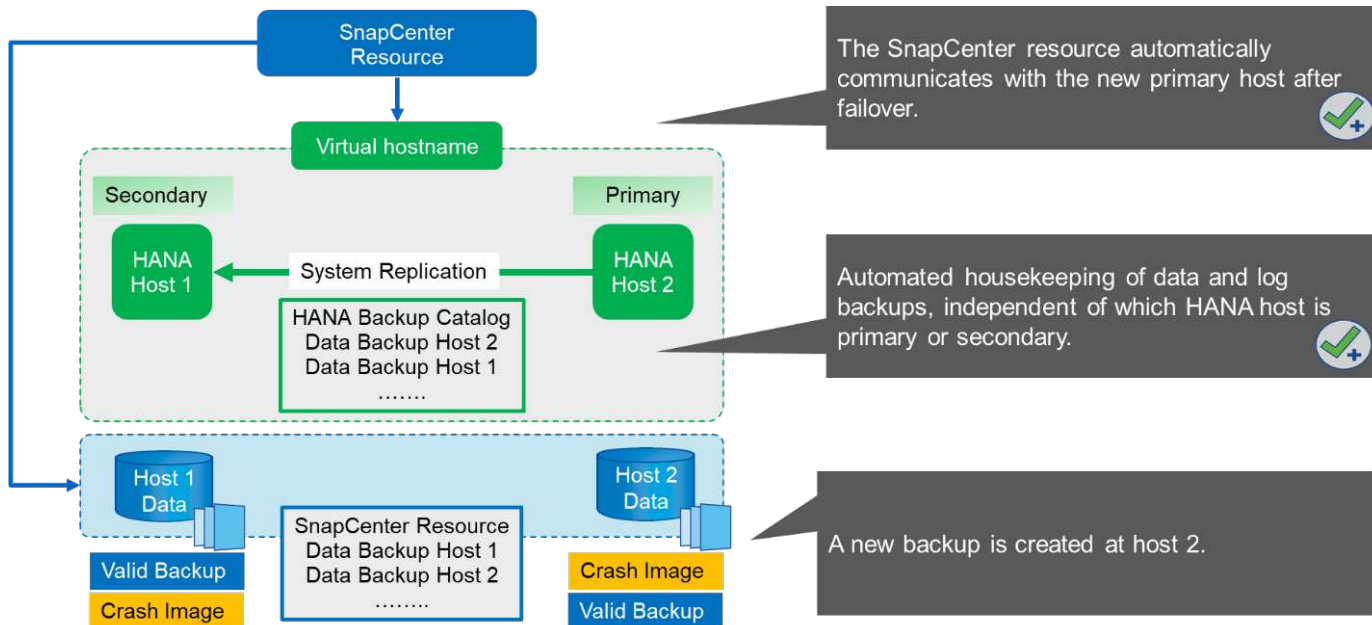
Quando um backup é executado com o host 1 como o host principal, um backup Snapshot consistente com banco de dados é criado no volume de dados do host 1. Como o volume de dados do host 2 faz parte do recurso SnapCenter, outra cópia Snapshot é criada para esse volume. Essa cópia Snapshot não é consistente com o banco de dados; em vez disso, é apenas uma imagem de falha do host secundário.

O catálogo de backup do SAP HANA e o recurso SnapCenter incluem o backup criado no host 1.



A figura a seguir mostra a operação de backup após o failover para o host 2 e a replicação do host 2 para o host 1. O SnapCenter se comunica automaticamente com o host 2 usando o endereço IP virtual configurado no recurso SnapCenter. Os backups agora são criados no host 2. Duas cópias snapshot são criadas pelo SnapCenter: Um backup consistente com banco de dados no volume de dados no host 2 e uma imagem com falha cópia Snapshot no volume de dados no host 1. O catálogo de backup do SAP HANA e o recurso SnapCenter agora incluem o backup criado no host 1 e o backup criado no host 2.

O serviço de limpeza dos backups de dados e de log é baseado na política de retenção definida do SnapCenter, e os backups são excluídos independentemente de qual host é primário ou secundário.

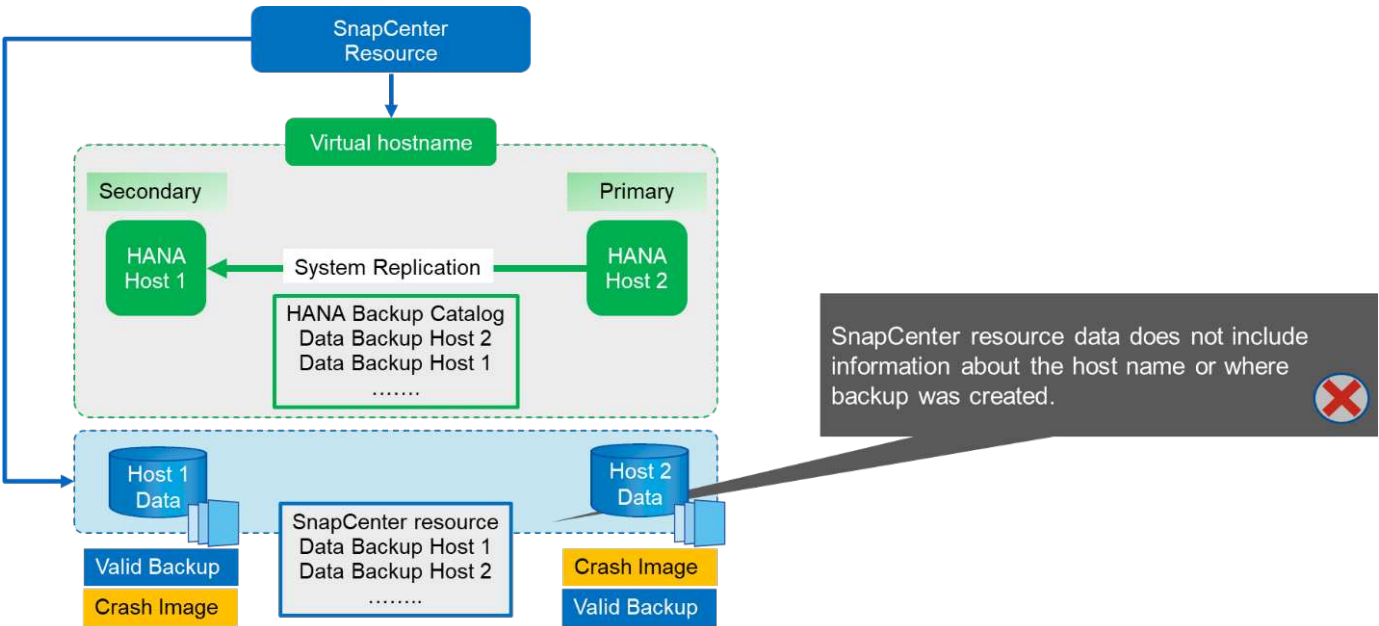


Conforme discutido na "[Backups de Snapshot de storage e replicação do sistema SAP](#)" seção , uma operação de restauração com backups Snapshot baseados em storage é diferente, dependendo de qual backup deve ser restaurado. É importante identificar em qual host o backup foi criado para determinar se a restauração pode ser executada no volume de armazenamento local ou se a restauração deve ser realizada no volume de armazenamento do outro host.

Com a configuração SnapCenter de recurso único, o SnapCenter não sabe onde o backup foi criado.

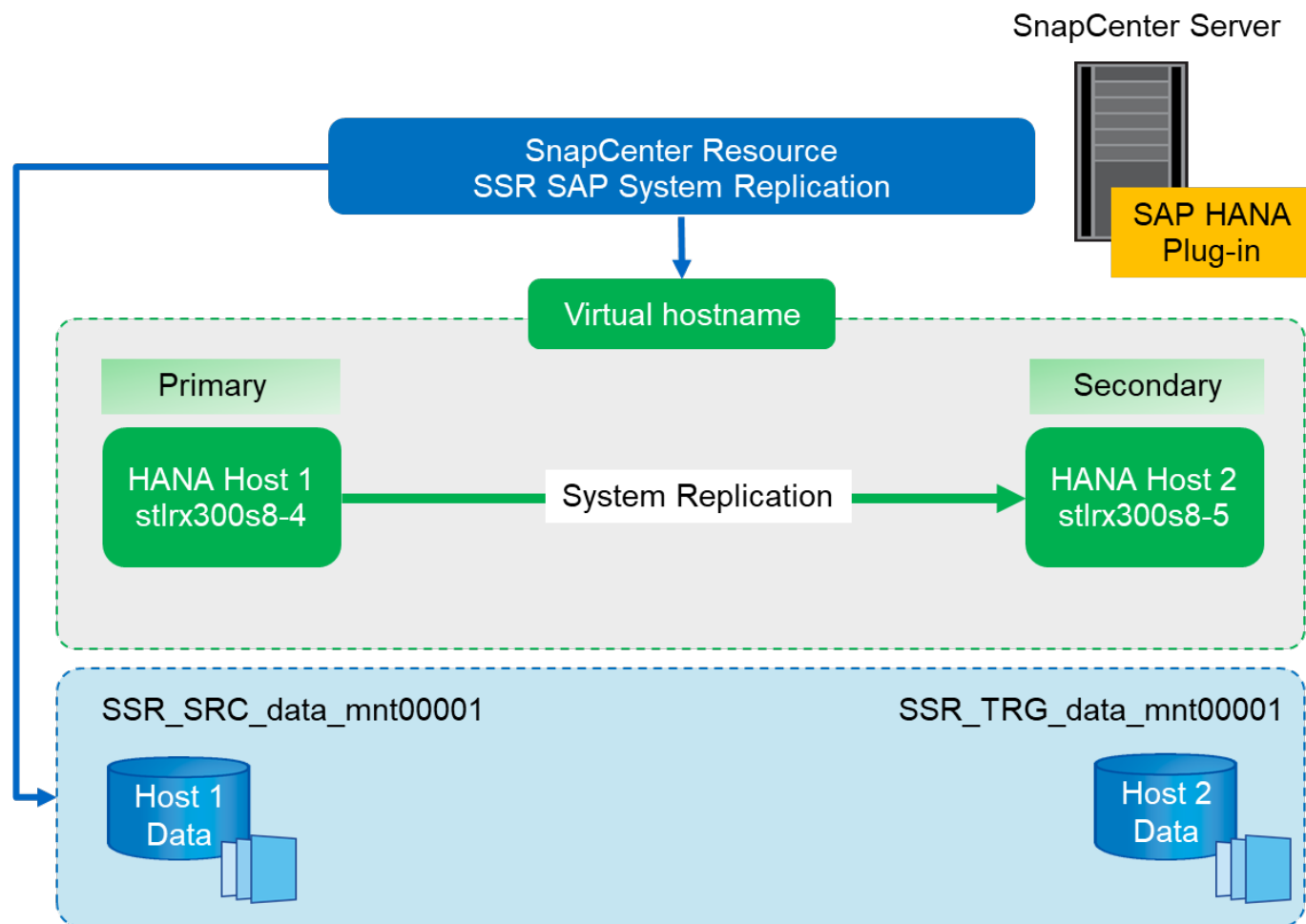
Portanto, a NetApp recomenda que você adicione um script de pré-backup ao fluxo de trabalho de backup do SnapCenter para identificar qual host é atualmente o principal host do SAP HANA.

A figura a seguir mostra a identificação do host de backup.



Configuração do SnapCenter

A figura a seguir mostra a configuração do laboratório e uma visão geral da configuração SnapCenter necessária.



Para executar operações de backup, independentemente de qual host SAP HANA é primário e mesmo quando um host está inativo, o plug-in SAP HANA do SnapCenter deve ser implantado em um host de plug-in central. Em nossa configuração de laboratório, usamos o servidor SnapCenter como um host de plug-in central e implantamos o plug-in SAP HANA no servidor SnapCenter.

Um usuário foi criado no banco de DADOS HANA para executar operações de backup. Uma chave de armazenamento de usuário foi configurada no servidor SnapCenter no qual o plug-in SAP HANA foi instalado. A chave de armazenamento de usuários inclui o endereço IP virtual dos hosts SAP HANA System Replication (ssr-vip).

```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

Você pode encontrar mais informações sobre as opções de implantação do plug-in SAP HANA e a configuração do armazenamento de usuários em "[Backup e recuperação do SAP HANA com o SnapCenter](#)".

No SnapCenter, o recurso é configurado como mostrado na figura a seguir usando a chave de armazenamento de usuário, configurada antes, e o servidor SnapCenter como o hdbsql host de comunicação.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Resource Details

☐ Single Container

☒ Multitenant Database Container (MDC) - Single Tenant

☐ Non-data Volumes

Resource Type

HANA System Name

SSR - SAP System Replication

SID

SSR

Tenant Database

SSR

HDBSQL Client Host

SC30-V2.sapcc.stl.netapp.com

HDB Secure User Store Keys

SSRKEY

HDBSQL OS User

SYSTEM

Previous

Next

Os volumes de dados de ambos os hosts do SAP HANA estão incluídos na configuração de espaço físico do storage, como mostra a figura a seguir.

222

Add SAP HANA Database

1 Name
2 **Storage Footprint**
3 Resource Settings
4 Summary

Provide Storage Footprint Details

Storage Systems for storage footprint

hana

Modify hana

Select one or more volumes and if required their associated Qtrees and LUNs

Volume Name

SSR_TRG_data_mnt00001

SSR_SRC_data_mnt00001

LUNs or Qtrees

Default is 'None' or type to find

Default is 'None' or type to find

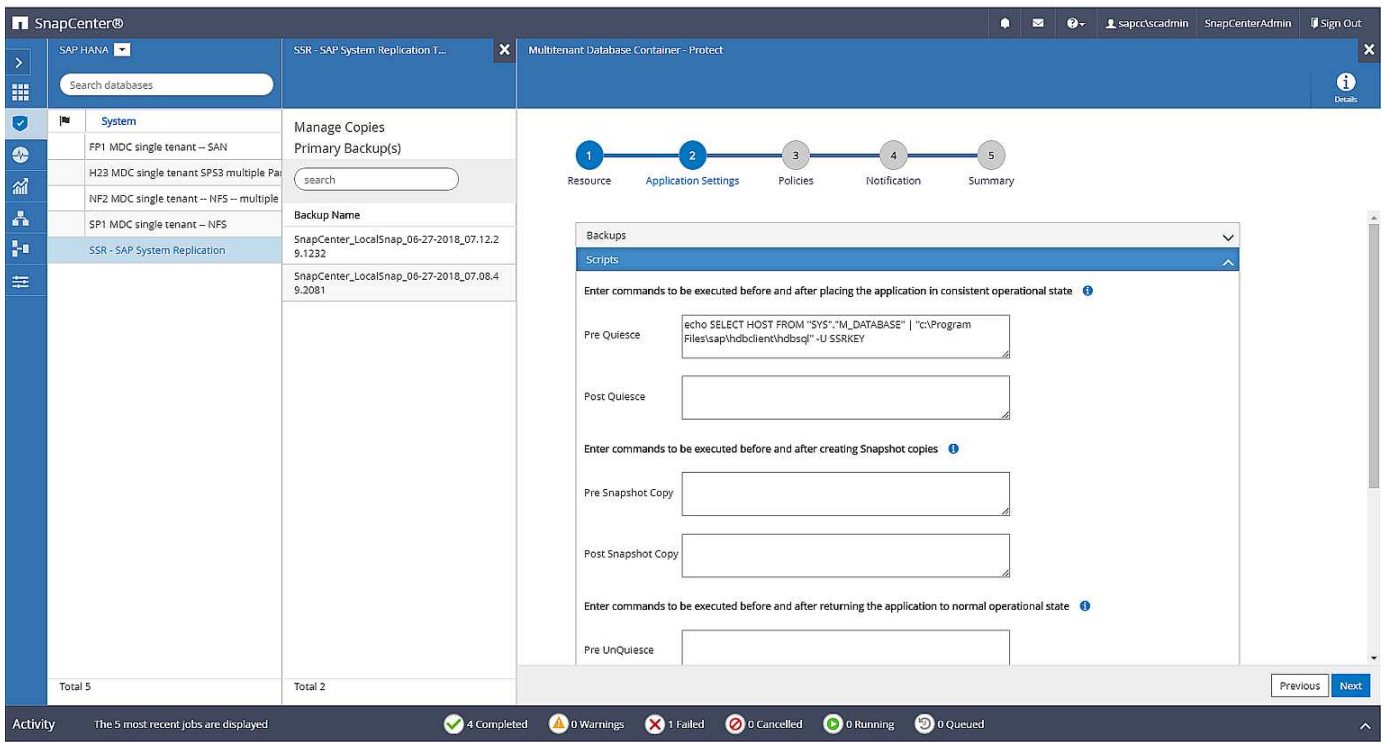
Save

Previous

Next

Como discutido anteriormente, o SnapCenter não sabe onde o backup foi criado. Portanto, a NetApp recomenda que você adicione um script de pré-backup no fluxo de trabalho de backup do SnapCenter para identificar qual host é atualmente o principal host do SAP HANA. Você pode executar essa identificação usando uma instrução SQL que é adicionada ao fluxo de trabalho de backup, como mostra a figura a seguir.

```
Select host from "SYS".M_DATABASE
```

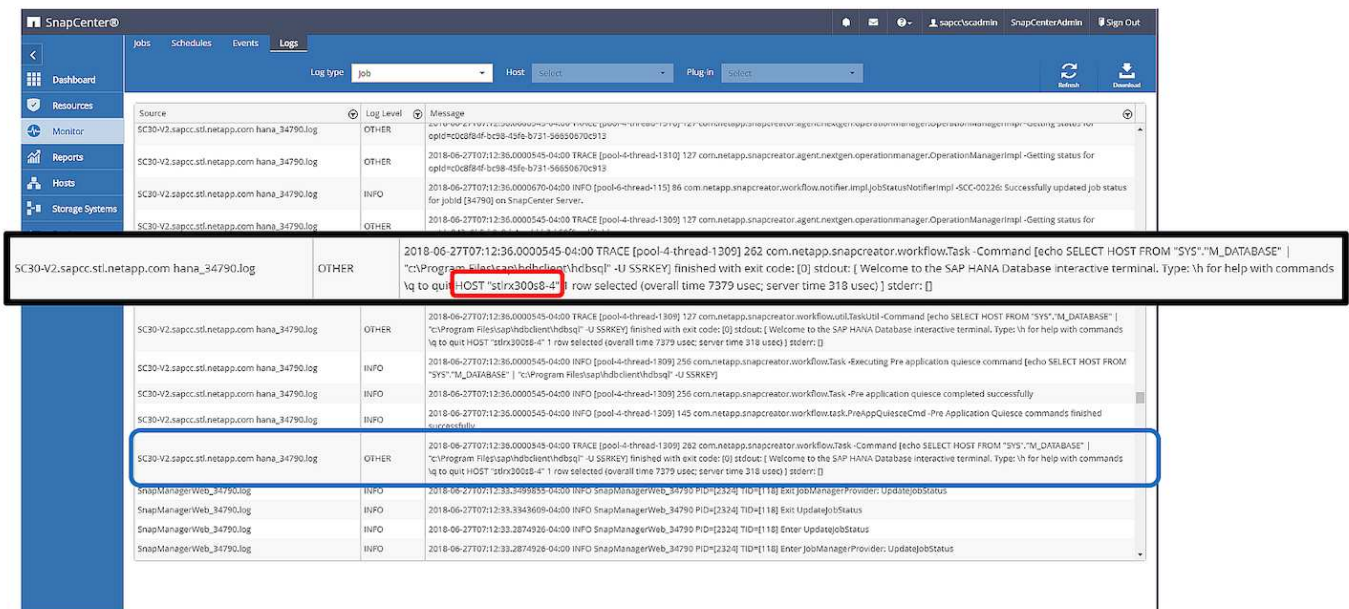



Operação de backup do SnapCenter

As operações de backup agora são executadas como de costume. O serviço de limpeza de dados e backups de log é realizado independentemente de qual host SAP HANA é primário ou secundário.

Os logs de tarefas de backup incluem a saída da instrução SQL, que permite identificar o host SAP HANA onde o backup foi criado.

A figura a seguir mostra o log de tarefas de backup com o host 1 como o host principal.



Esta figura mostra o log de tarefas de backup com o host 2 como o host principal.

The screenshot shows the SAP HANA Studio Logs window. The log entry for 'SC30-V2.sapcc.stl.netapp.com hana_34799.log' is highlighted, showing a successful backup of the SYSTEMDB database. The log entry is as follows:

Source	Log Level	Message
SC30-V2.sapcc.stl.netapp.com hana_34799.log	OTHER	2018-06-27T07:45:53.0000174-04:00 TRACE [pool-4-thread-1347] 262 com.netapp.snapcreator.workflow.Task-Command [echo SELECT HOST FROM "SYS"."M_DATABASE" "c:\Program Files\hdb\bin\hdbsql" -U SSRKEY] finished with exit code: [0] stdout: [Welcome to the SAP HANA Database interactive terminal. Type: \h for help with commands \q to quit] HOST "stlx300s8-5" 1 row selected (overall time 5613 usec; server time 202 usec) ; stderr: []

A figura a seguir mostra o catálogo de backup do SAP HANA no SAP HANA Studio. Quando o banco de dados do SAP HANA está online, o host do SAP HANA onde o backup foi criado fica visível no SAP HANA Studio.



O catálogo de backup do SAP HANA no sistema de arquivos, que é usado durante uma operação de restauração e recuperação, não inclui o nome do host no qual o backup foi criado. A única maneira de identificar o host quando o banco de dados está inativo é combinar as entradas do catálogo de backup com o backup.log arquivo de ambos os hosts SAP HANA.

The screenshot shows the SAP HANA Studio Backup Catalog window. The backup details are visible, including the host name 'stlx300s8-4'. The backup details are as follows:

Host	Service	Size	Name	Source Type	EBID
stlx300s8-4	nameserver	1.47 GB	hdb0001	volume	SnapC...

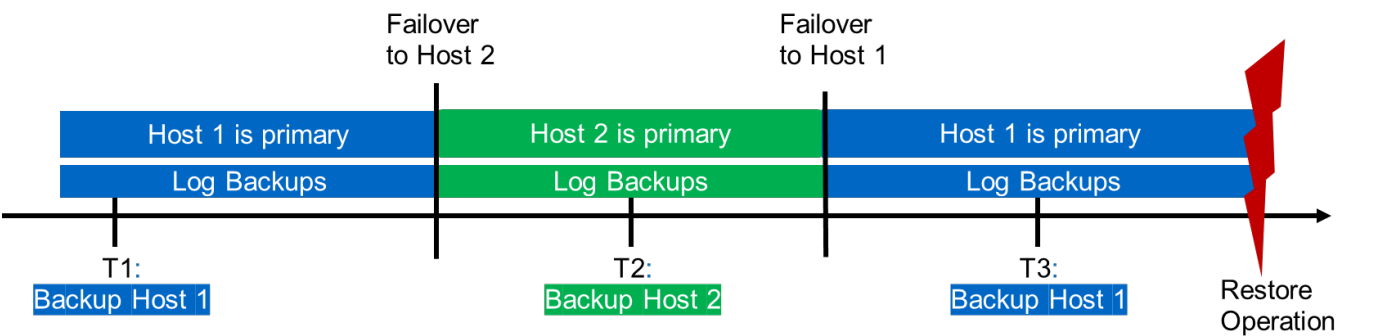
Restauração e recuperação

Como discutido anteriormente, você deve ser capaz de identificar onde o backup selecionado foi criado para definir a operação de restauração necessária. Se o banco de dados do SAP HANA ainda estiver online, você poderá usar o SAP HANA Studio para identificar o host no qual o backup foi criado. Se a base de dados estiver offline, as informações só estarão disponíveis no registo de trabalhos de cópia de segurança do SnapCenter.

A figura a seguir ilustra as diferentes operações de restauração, dependendo do backup selecionado.

Se uma operação de restauração tiver de ser executada após o carimbo de data/hora T3 e o host 1 for o principal, você poderá restaurar o backup criado em T1 ou T3 usando o SnapCenter. Esses backups Snapshot estão disponíveis no volume de storage conectado ao host 1.

Se você precisar restaurar usando o backup criado no host 2 (T2), que é uma cópia Snapshot no volume de storage do host 2, o backup precisa estar disponível para o host 1. Você pode disponibilizar esse backup criando uma cópia NetApp FlexClone a partir do backup, montando a cópia FlexClone no host 1 e copiando os dados para o local original.



Restore Operation With	
Backup T1	SnapCenter
Backup T2	Create FlexClone from „Backup host 2“, mount and copy
Backup T3	SnapCenter

Com uma única configuração de recurso do SnapCenter, as cópias Snapshot são criadas em ambos os volumes de storage de ambos os hosts do SAP HANA System Replication. Somente o backup Snapshot criado no volume de storage do host principal SAP HANA é válido para uso para recuperação futura. A cópia Snapshot criada no volume de storage do host secundário SAP HANA é uma imagem de falha que não pode ser usada para recuperação futura.

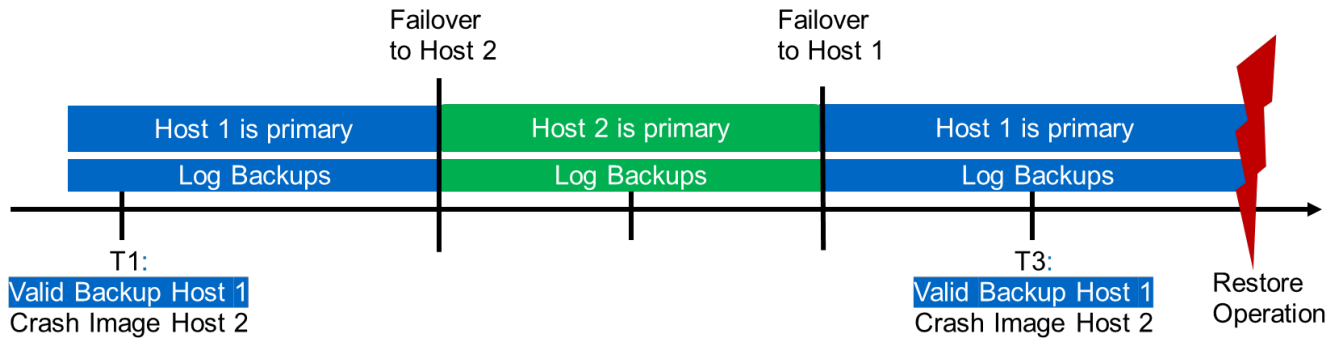
Uma operação de restauração com SnapCenter pode ser executada de duas maneiras diferentes:

- Restaure apenas a cópia de segurança válida
- Restaure o recurso completo, incluindo a cópia de segurança válida e a imagem de falha. As secções seguintes discutem mais detalhadamente as duas operações de restauro diferentes.

Uma operação de restauração de um backup criado no outro host é descrita na ["Restaurar e recuperar a partir de um backup criado no outro host"](#) seção .

A figura a seguir mostra as operações de restauração com uma única configuração de recursos do

SnapCenter.

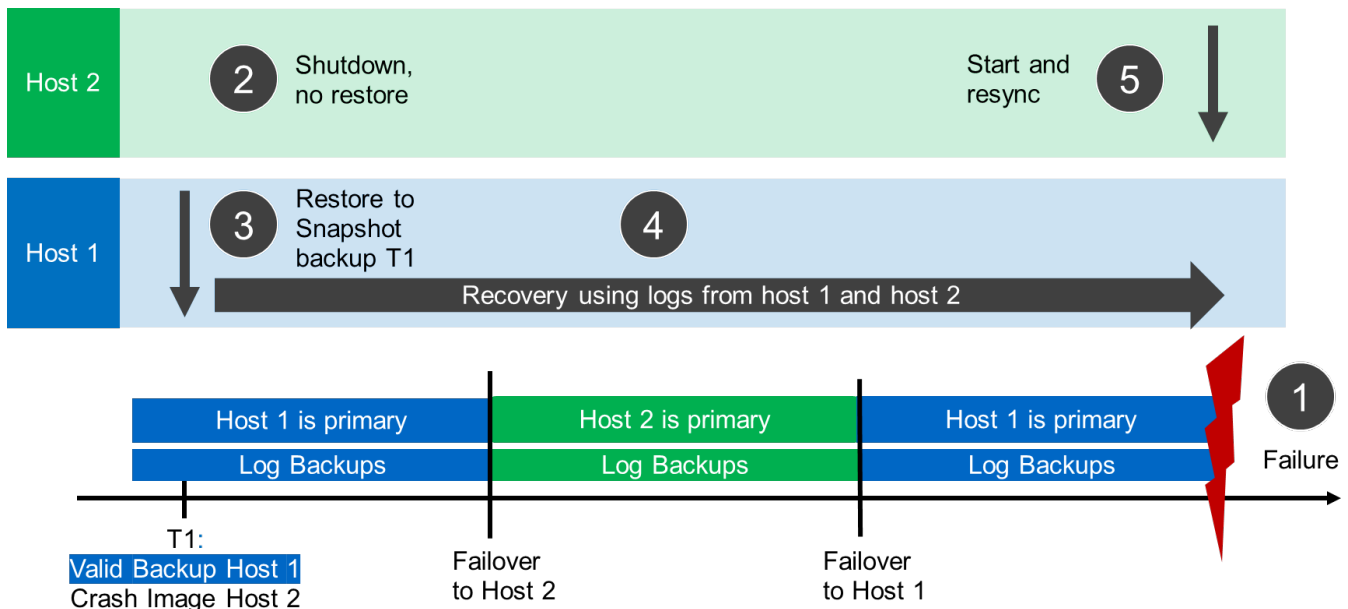


Restauração do SnapCenter somente do backup válido

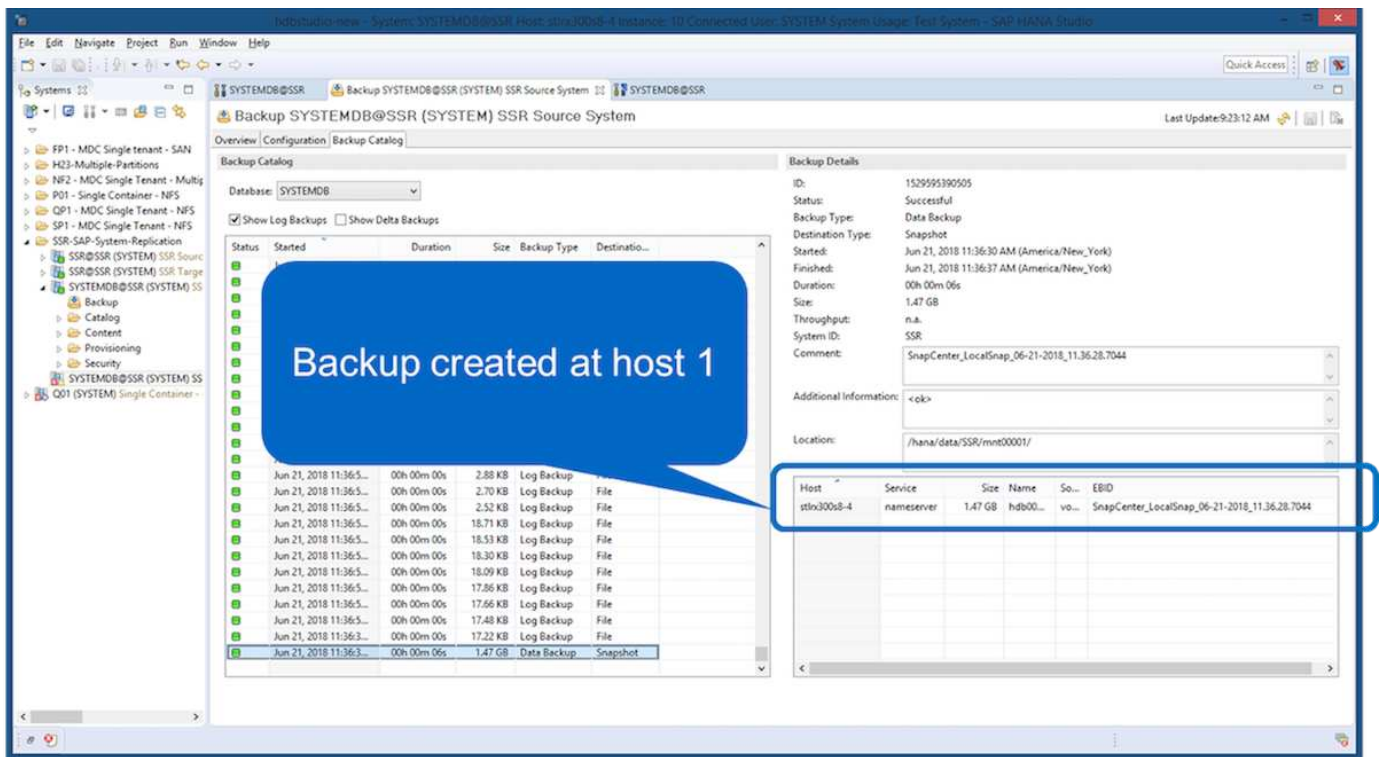
A figura a seguir mostra uma visão geral do cenário de restauração e recuperação descrito nesta seção.

Um backup foi criado em T1 no host 1. Um failover foi executado no host 2. Após um certo ponto no tempo, outro failover de volta ao host 1 foi executado. No momento atual, o host 1 é o host principal.

1. Ocorreu uma falha e você deve restaurar o backup criado em T1 no host 1.
2. O host secundário (host 2) é desligado, mas nenhuma operação de restauração é executada.
3. O volume de armazenamento do host 1 é restaurado para o backup criado em T1.
4. Uma recuperação avançada é realizada com logs do host 1 e host 2.
5. O host 2 é iniciado e uma ressincronização de replicação do sistema do host 2 é iniciada automaticamente.



A figura a seguir mostra o catálogo de backup do SAP HANA no SAP HANA Studio. O backup realçado mostra o backup criado em T1 no host 1.

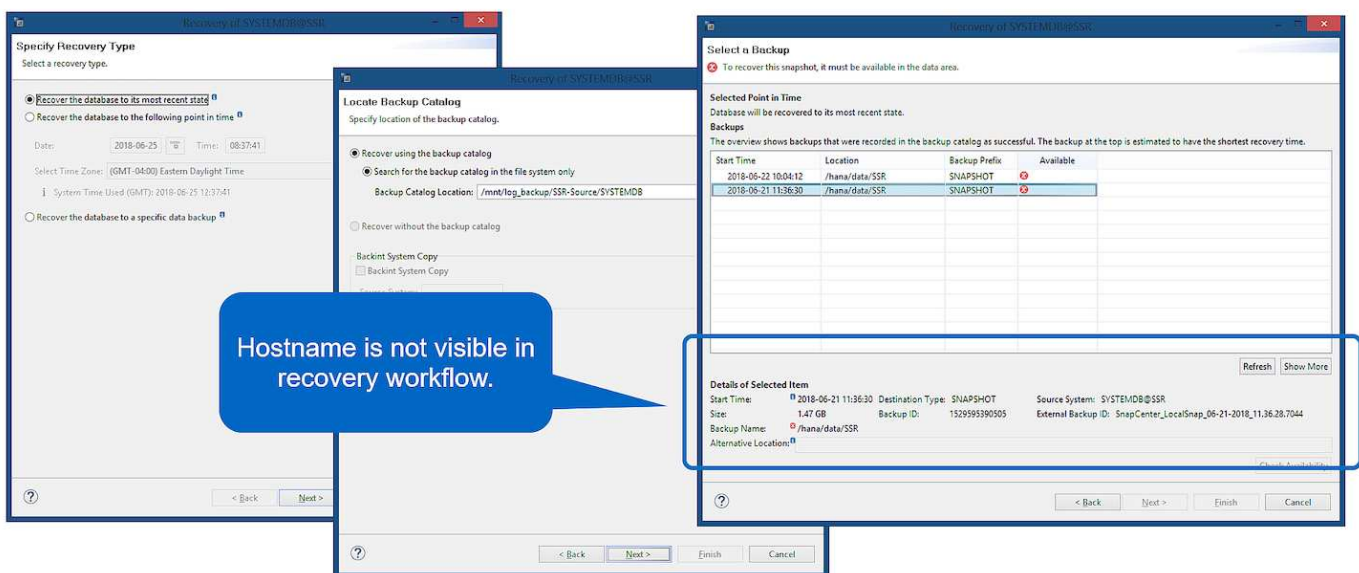


25

Uma operação de restauração e recuperação é iniciada no SAP HANA Studio. Como mostra a figura a seguir, o nome do host onde o backup foi criado não é visível no fluxo de trabalho de restauração e recuperação.

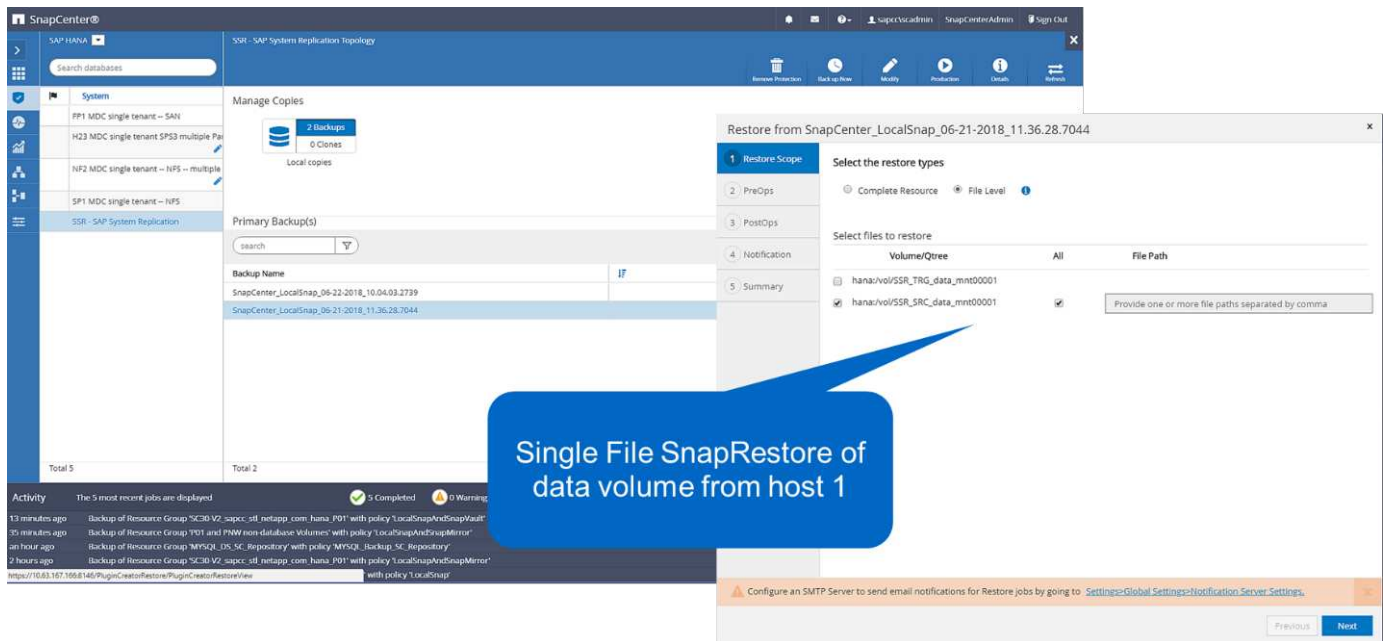


Em nosso cenário de teste, conseguimos identificar o backup correto (o backup criado no host 1) no SAP HANA Studio quando o banco de dados ainda estava online. Se a base de dados não estiver disponível, tem de verificar o registo de trabalhos de cópia de segurança do SnapCenter para identificar a cópia de segurança correta.

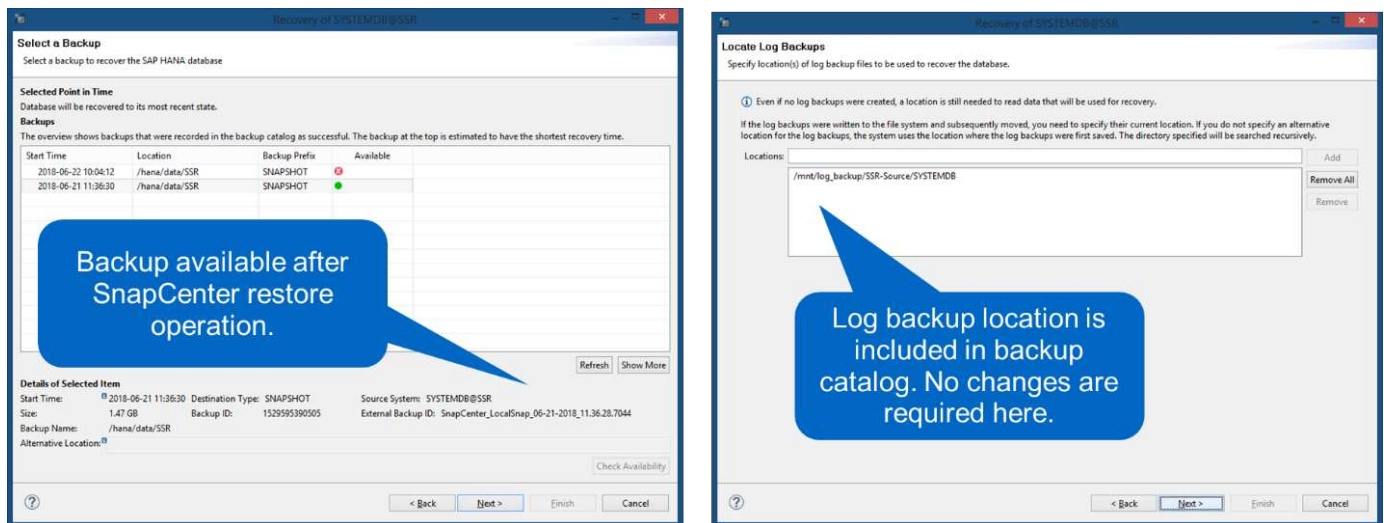


No SnapCenter, o backup é selecionado e uma operação de restauração no nível do arquivo é executada. Na tela de restauração no nível do arquivo, apenas o volume do host 1 é selecionado para que somente o backup

válido seja restaurado.



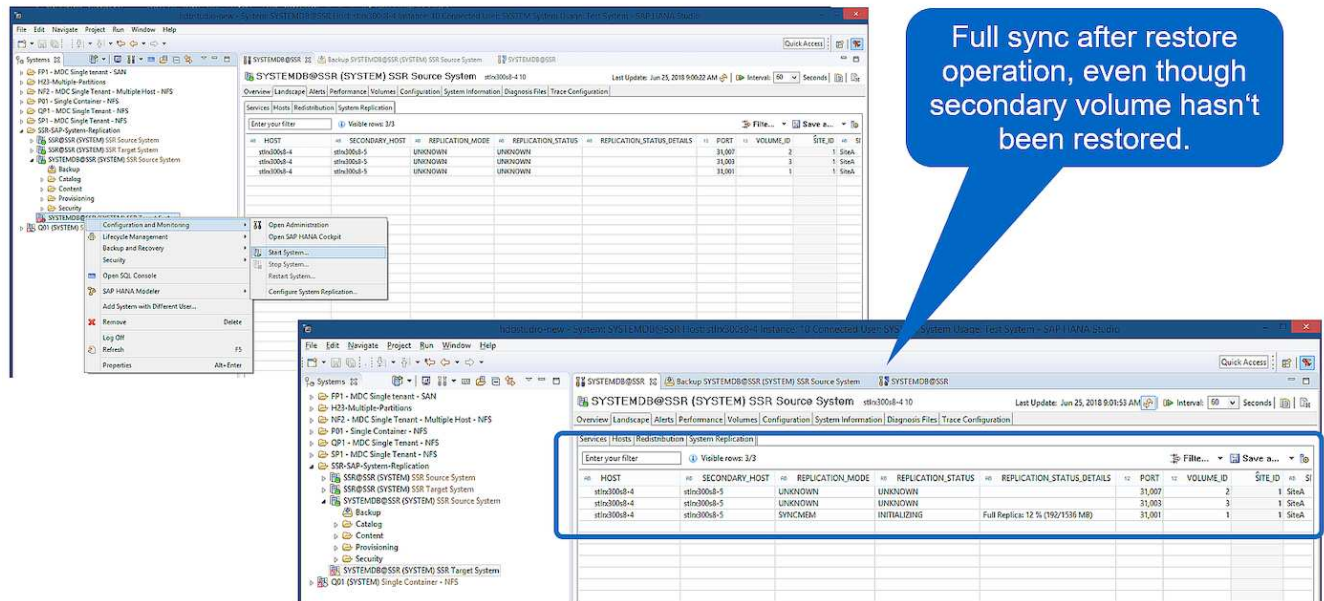
Após a operação de restauração, o backup é destacado em verde no SAP HANA Studio. Você não precisa inserir um local de backup de log adicional, porque o caminho do arquivo dos backups de log do host 1 e do host 2 estão incluídos no catálogo de backup.



Após a conclusão da recuperação avançada, o host secundário (host 2) é iniciado e a resincronização do SAP HANA System Replication é iniciada.



Embora o host secundário esteja atualizado (nenhuma operação de restauração foi realizada para o host 2), o SAP HANA executa uma replicação completa de todos os dados. Esse comportamento é padrão após uma operação de restauração e recuperação com o SAP HANA System Replication.

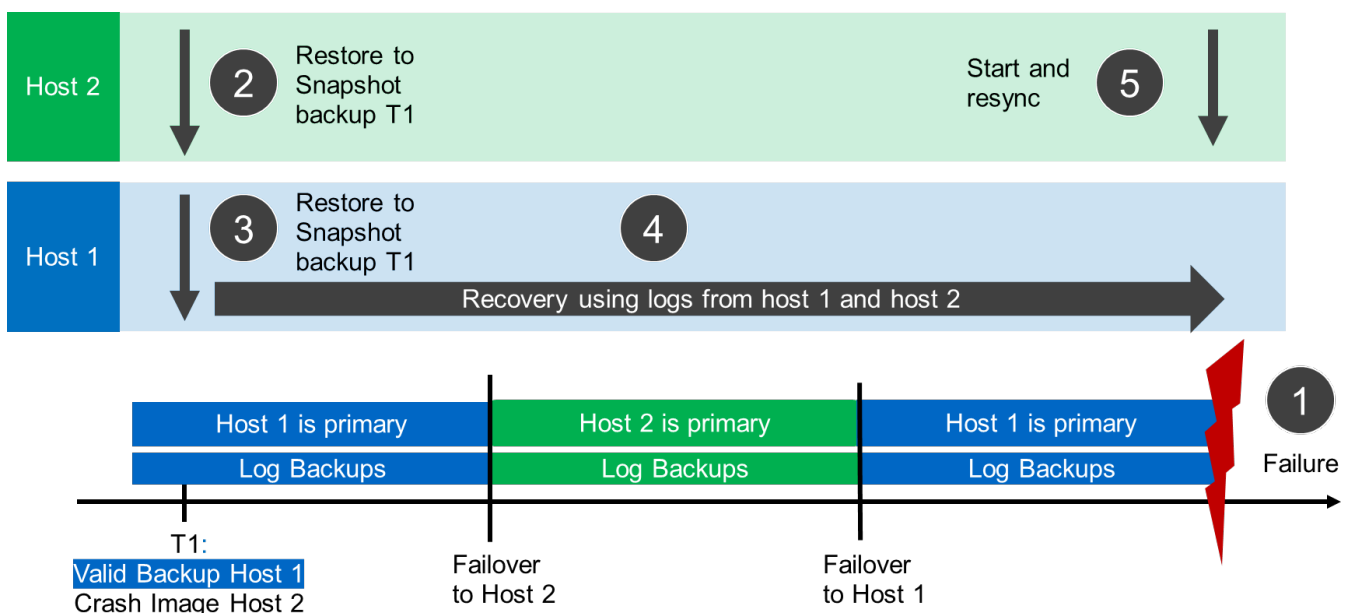


Restauração de SnapCenter de backup válido e imagem de falha

A figura a seguir mostra uma visão geral do cenário de restauração e recuperação descrito nesta seção.

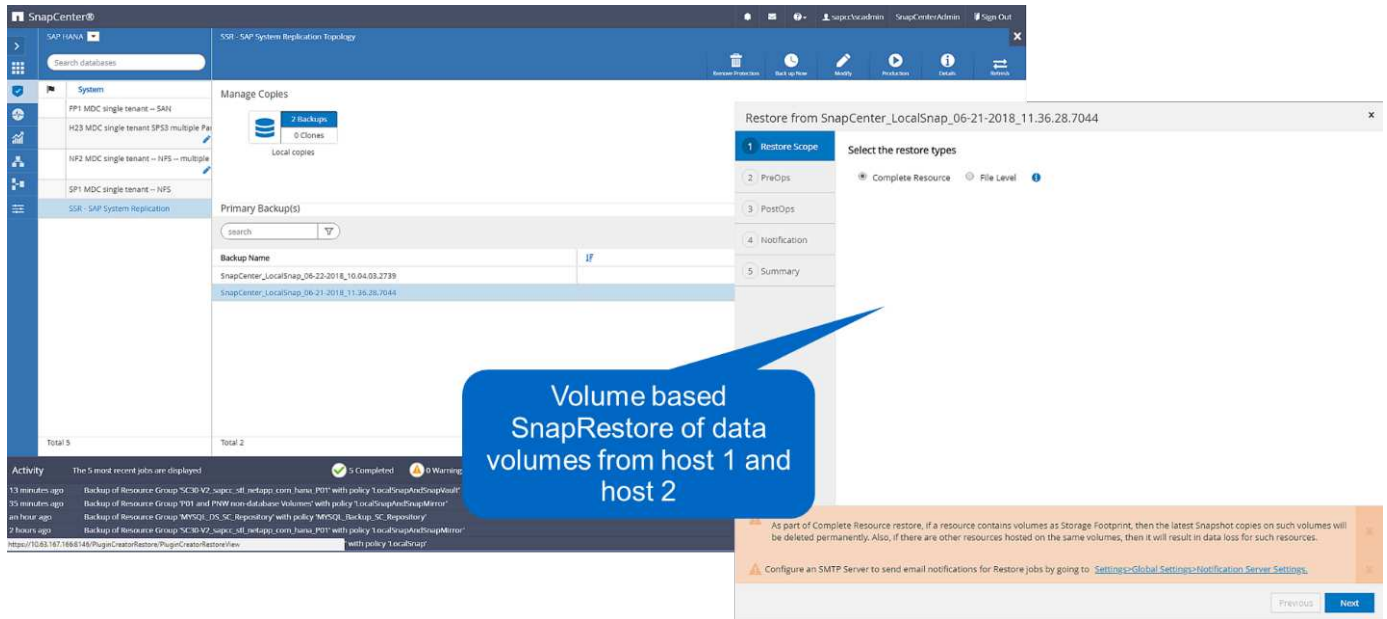
Um backup foi criado em T1 no host 1. Um failover foi executado no host 2. Após um certo ponto no tempo, outro failover de volta ao host 1 foi executado. No momento atual, o host 1 é o host principal.

1. Ocorreu uma falha e você deve restaurar o backup criado em T1 no host 1.
2. O host secundário (host 2) é encerrado e a imagem de falha T1 é restaurada.
3. O volume de armazenamento do host 1 é restaurado para o backup criado em T1.
4. Uma recuperação avançada é realizada com logs do host 1 e host 2.
5. O host 2 é iniciado e uma resincronização de replicação do sistema do host 2 é iniciada automaticamente.

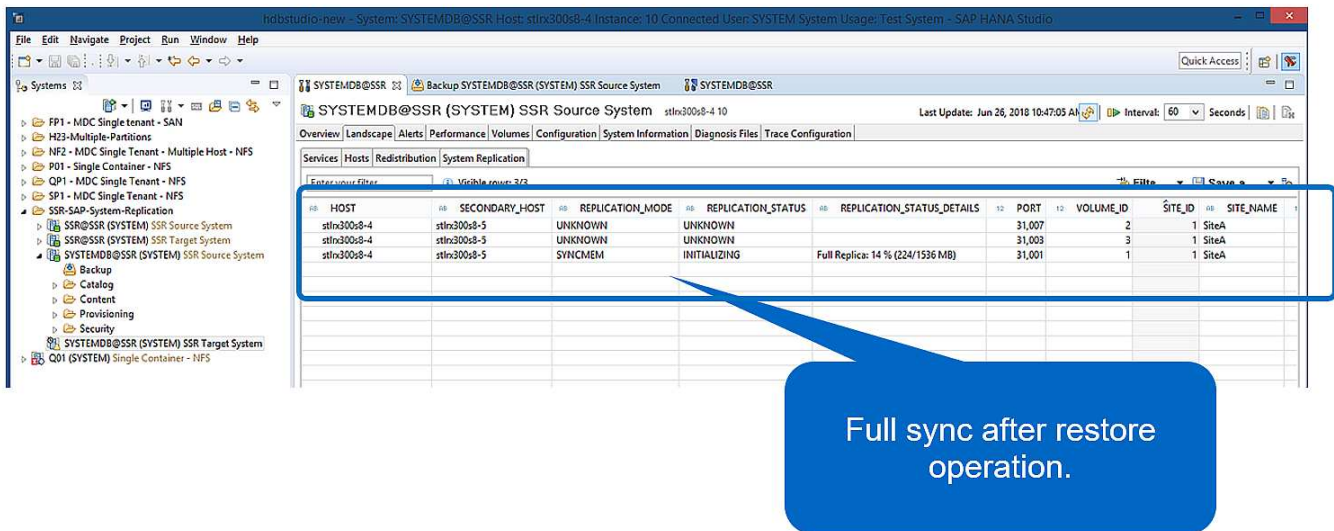


A operação de restauração e recuperação com o SAP HANA Studio é idêntica às etapas descritas na "Restauração do SnapCenter somente do backup válido" seção .

Para executar a operação de restauração, selecione concluir recurso no SnapCenter. Os volumes de ambos os hosts são restaurados.



Após a conclusão da recuperação avançada, o host secundário (host 2) é iniciado e a ressyncronização do SAP HANA System Replication é iniciada. A replicação completa de todos os dados é executada.



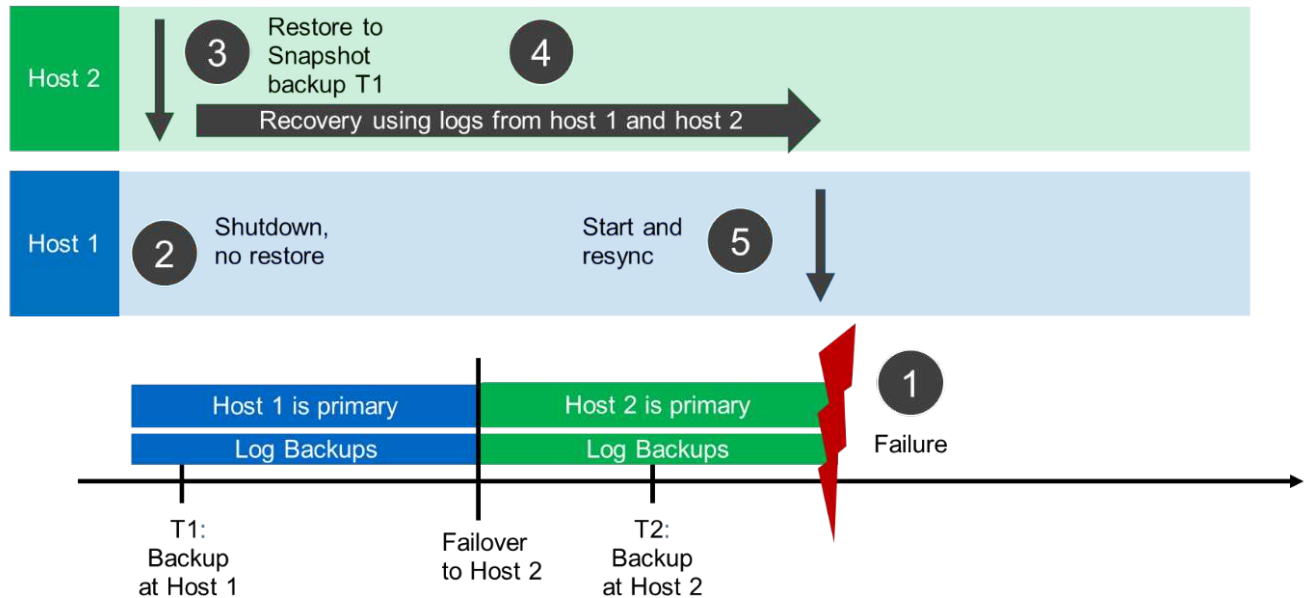
Restauração e recuperação a partir de um backup criado no outro host

Uma operação de restauração a partir de um backup criado no outro host SAP HANA é um cenário válido para ambas as opções de configuração do SnapCenter.

A figura a seguir mostra uma visão geral do cenário de restauração e recuperação descrito nesta seção.

Um backup foi criado em T1 no host 1. Um failover foi executado no host 2. No momento atual, o host 2 é o host principal.

1. Ocorreu uma falha e você deve restaurar o backup criado em T1 no host 1.
2. O host principal (host 1) é desligado.
3. Os dados de backup T1 do host 1 são restaurados para o host 2.
4. Uma recuperação avançada é realizada usando logs do host 1 e do host 2.
5. O host 1 é iniciado e uma ressincronização de replicação do sistema do host 1 é iniciada automaticamente.



31

A figura a seguir mostra o catálogo de backup do SAP HANA e destaca o backup, criado no host 1, que foi usado para a operação de restauração e recuperação.

The screenshot shows the SAP HANA Studio Backup Catalog for the SYSTEMDB@SSR (SYSTEM) SSR Target System. The backup details are as follows:

Status	Started	Duration	Size	Backup Type	Destination...
Success	Jun 28, 2018 9:23:46 ...	00h 00m 07s	1.53 GB	Data Backup	File
Success	Jun 27, 2018 7:45:56 ...	00h 00m 03s	1.52 GB	Data Backup	Snapshot
Success	Jun 27, 2018 7:12:37 ...	00h 00m 05s	1.55 GB	Data Backup	Snapshot

Backup Details:

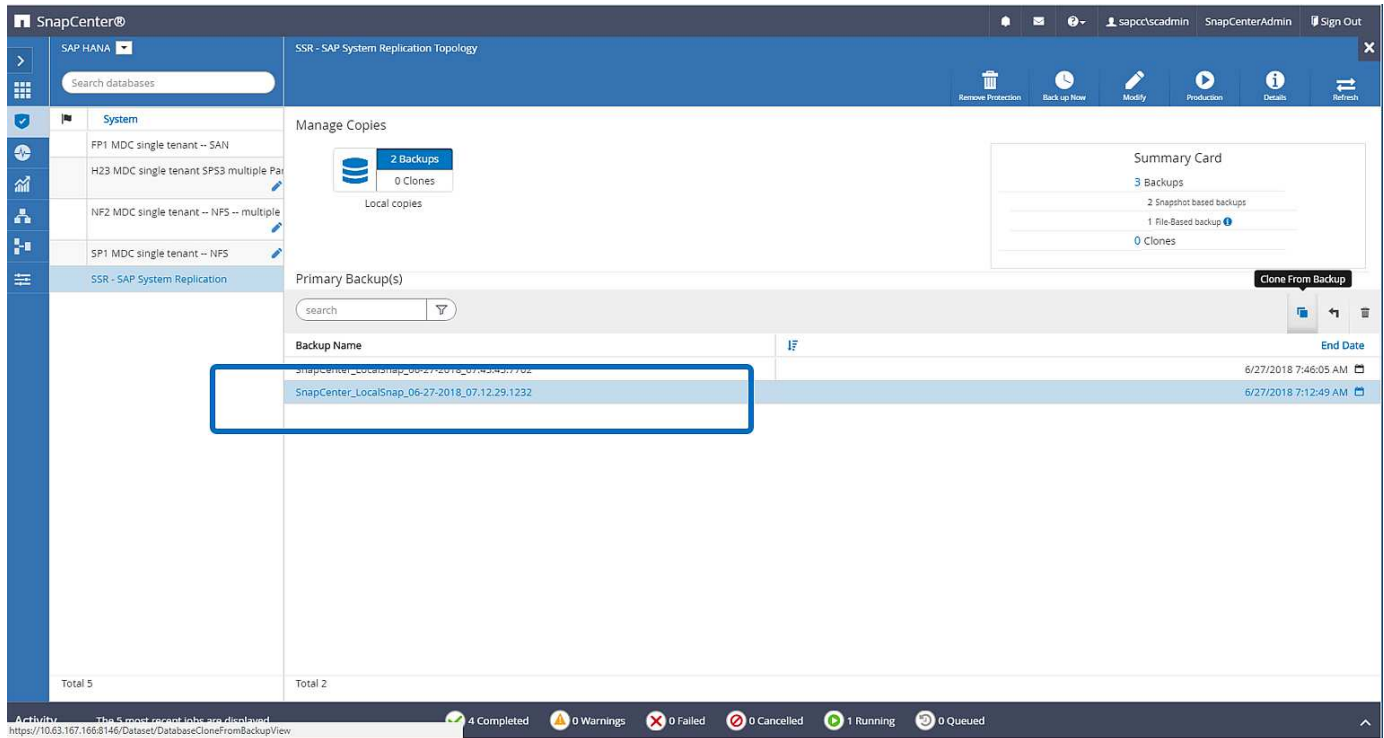
- ID: 1530097957115
- Status: Successful
- Backup Type: Data Backup
- Destination Type: Snapshot
- Started: Jun 27, 2018 7:12:37 AM (America/New_York)
- Finished: Jun 27, 2018 7:12:43 AM (America/New_York)
- Duration: 00h 00m 06s
- Size: 1.55 GB
- Throughput: n.a.
- System ID: SSR
- Comment: SnapCenter_LocalSnap_06-27-2018_07.12.29.1232
- Additional Information: <ok>
- Location: /hana/data/SSR/mnt00001/

Host	Service	Size	Name	Source Type	EBID
stln300x8-4	nameserver	1.55 GB	hdb00001	volume	SnapC...

A operação de restauração envolve as seguintes etapas:

1. Crie um clone a partir do backup criado no host 1.
2. Monte o volume clonado no host 2.
3. Copie os dados do volume clonado para o local original.

No SnapCenter, o backup é selecionado e a operação de clone é iniciada.



Você deve fornecer o servidor clone e o endereço IP de exportação NFS.



Em uma configuração de recurso único do SnapCenter, o plug-in do SAP HANA não é instalado no host do banco de dados. Para executar o fluxo de trabalho clone do SnapCenter, qualquer host com um plug-in HANA instalado pode ser usado como um servidor clone.

Em uma configuração do SnapCenter com recursos separados, o host do banco de dados HANA é selecionado como um servidor clone, e um script de montagem é usado para montar o clone no host de destino.


```
stlrx300s8-5:/mnt/tmp # mount 192.168.173.101:/Scc373da37-00ff-4694-b1e1-8153dbd46caf /mnt/tmp
```

O volume clonado contém os dados do banco de DADOS HANA.

```
stlrx300s8-5:/mnt/tmp/# ls -al
drwxr-x--x 2 ssradm sapsys 4096 Jun 27 11:12 hdb00001
drwx----- 2 ssradm sapsys 4096 Jun 21 09:38 hdb00002.00003
drwx----- 2 ssradm sapsys 4096 Jun 27 11:12 hdb00003.00003
-rw-r--r-- 1 ssradm sapsys  22 Jun 27 11:12 nameserver.lck
```

Os dados são copiados para a localização original.

```
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00001 /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00002.00003/ /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00003.00003/ /hana/data/SSR/mnt00001/
```

A recuperação com o SAP HANA Studio é realizada conforme descrito na "[Restauração do SnapCenter somente do backup válido](#)" seção .

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos:

- "[Backup e recuperação do SAP HANA com o SnapCenter](#)"
- "[Automatizando as operações de clonagem e cópia do sistema SAP HANA com o SnapCenter](#)"
- Recuperação de desastres do SAP HANA com replicação de storage

["https://www.netapp.com/us/media/tr-4646.pdf"](https://www.netapp.com/us/media/tr-4646.pdf)

Histórico de versões

Histórico de versões:

Versão	Data	Histórico de versões do documento
Versão 1,0	Outubro de 2018	Versão inicial
Versão 2,0	Janeiro de 2022	Atualização para abranger o suporte à replicação do sistema SnapCenter 4,6 HANA

Recuperação de desastres do SAP HANA com o Azure NetApp Files

Recuperação de desastres do SAP HANA com o Azure NetApp Files

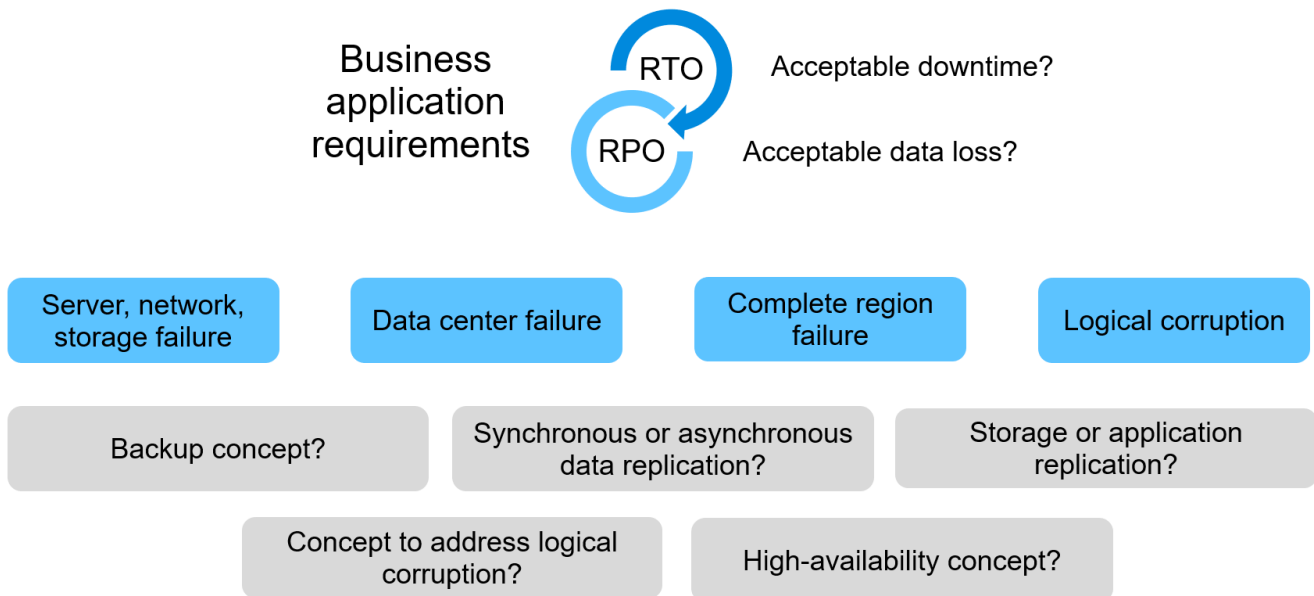
Estudos mostraram que o tempo de inatividade de aplicativos de negócios tem um impacto negativo significativo nos negócios das empresas.

Autores: Nils Bauer, NetApp Ralf Klahr, Microsoft

Além do impacto financeiro, o tempo de inatividade também pode prejudicar a reputação da empresa, o moral da equipe e a fidelidade do cliente. Surpreendentemente, nem todas as empresas têm uma política abrangente de recuperação de desastres.

Executar o SAP HANA no Azure NetApp Files (ANF) oferece aos clientes acesso a recursos adicionais que ampliam e aprimoram os recursos integrados de proteção de dados e recuperação de desastres do SAP HANA. Esta seção de visão geral explica essas opções para ajudar os clientes a selecionar opções que atendam às suas necessidades de negócios.

Para desenvolver uma política abrangente de recuperação de desastres, os clientes precisam entender os requisitos de aplicações empresariais e os recursos técnicos de que precisam para proteção de dados e recuperação de desastres. A figura a seguir fornece uma visão geral da proteção de dados.



Requisitos de aplicação empresarial

Existem dois indicadores-chave para aplicações empresariais:

- O objetivo do ponto de restauração (RPO) ou a perda de dados máxima tolerável
- O objetivo de tempo de recuperação (RTO) ou o tempo de inatividade máximo tolerável da aplicação empresarial

Esses requisitos são definidos pelo tipo de aplicativo usado e pela natureza dos seus dados de negócios. O RPO e o RTO podem ser diferentes se você estiver protegendo contra falhas em uma única região do Azure.

Eles também podem ser diferentes se você estiver se preparando para desastres catastróficos, como a perda de uma região completa do Azure. É importante avaliar os requisitos de negócios que definem o RPO e o RTO, porque esses requisitos têm um impacto significativo nas opções técnicas disponíveis.

Alta disponibilidade

A infraestrutura para SAP HANA, como máquinas virtuais, rede e storage, precisa ter componentes redundantes para garantir que não haja um único ponto de falha. O MS Azure fornece redundância para os diferentes componentes de infraestrutura.

Para fornecer alta disponibilidade no lado da computação e da aplicação, os hosts SAP HANA de reserva podem ser configurados para alta disponibilidade integrada com um sistema SAP HANA de vários hosts. Se um servidor ou um serviço SAP HANA falhar, o serviço SAP HANA fará failover para o host de reserva, o que causa inatividade do aplicativo.

Se o tempo de inatividade do aplicativo não for aceitável em caso de falha do servidor ou do aplicativo, você também poderá usar a replicação do sistema SAP HANA como uma solução de alta disponibilidade que habilita o failover em um período de tempo muito curto. Os clientes da SAP usam a replicação do SISTEMA HANA não apenas para solucionar a alta disponibilidade de falhas não planejadas, mas também para minimizar o tempo de inatividade para operações planejadas, como atualizações de SOFTWARE HANA.

Corrupção lógica

A corrupção lógica pode ser causada por erros de software, erros humanos ou sabotagem. Infelizmente, a corrupção lógica muitas vezes não pode ser tratada com soluções padrão de alta disponibilidade e recuperação de desastres. Como resultado, dependendo da camada, aplicativo, sistema de arquivos ou storage em que ocorreu a corrupção lógica, os requisitos de RTO e RPO às vezes não podem ser atendidos.

O pior caso é uma corrupção lógica em um aplicativo SAP. Os aplicativos SAP geralmente operam em um cenário em que diferentes aplicativos se comunicam entre si e trocam dados. Portanto, restaurar e recuperar um sistema SAP no qual ocorreu uma corrupção lógica não é a abordagem recomendada. Restaurar o sistema a um ponto no tempo antes que a corrupção ocorra resulta na perda de dados, de modo que o RPO se torne maior que zero. Além disso, o cenário SAP não estaria mais em sincronia e exigiria pós-processamento adicional.

Em vez de restaurar o sistema SAP, a melhor abordagem é tentar corrigir o erro lógico dentro do sistema, analisando o problema em um sistema de reparo separado. A análise de causa raiz requer o envolvimento do processo de negócios e do proprietário do aplicativo. Para esse cenário, você cria um sistema de reparo (um clone do sistema de produção) com base nos dados armazenados antes da corrupção lógica ocorrer. Dentro do sistema de reparo, os dados necessários podem ser exportados e importados para o sistema de produção. Com essa abordagem, o sistema produtivo não precisa ser interrompido e, no melhor cenário, nenhum dado ou apenas uma pequena fração de dados é perdido.



As etapas necessárias para configurar um sistema de reparo são idênticas a um cenário de teste de recuperação de desastres descrito neste documento. A solução de recuperação de desastres descrita pode, portanto, ser facilmente estendida para lidar com a corrupção lógica também.

Backups

Os backups são criados para permitir a restauração e a recuperação de diferentes conjuntos de dados pontuais. Normalmente, esses backups são mantidos por alguns dias a algumas semanas.

Dependendo do tipo de corrupção, a restauração e a recuperação podem ser realizadas com ou sem perda de

dados. Se o RPO precisar ser zero, mesmo quando o storage primário e de backup for perdido, o backup deve ser combinado com a replicação de dados síncrona.

O rto para restauração e recuperação é definido pelo tempo de restauração necessário, pelo tempo de recuperação (incluindo o início do banco de dados) e pelo carregamento de dados na memória. Para bancos de dados grandes e abordagens tradicionais de backup, o rto pode ser facilmente várias horas, o que pode não ser aceitável. Para alcançar valores de rto muito baixos, um backup deve ser combinado com uma solução de espera quente, que inclui pré-carregamento de dados na memória.

Em contraste, uma solução de backup deve resolver a corrupção lógica, porque as soluções de replicação de dados não podem cobrir todos os tipos de corrupção lógica.

Replicação de dados síncrona ou assíncrona

O RPO determina principalmente qual método de replicação de dados você deve usar. Se o RPO precisar ser zero, mesmo quando o storage primário e de backup forem perdidos, os dados precisam ser replicados de forma síncrona. No entanto, existem limitações técnicas para replicação síncrona, como a distância entre duas regiões do Azure. Na maioria dos casos, a replicação síncrona não é apropriada para distâncias maiores que 100km devido à latência e, portanto, essa não é uma opção para replicação de dados entre regiões do Azure.

Se um RPO maior for aceitável, a replicação assíncrona poderá ser usada em grandes distâncias. O RPO, neste caso, é definido pela frequência de replicação.

Replicação do SISTEMA HANA com ou sem pré-carga dos dados

O tempo de inicialização de um banco de dados SAP HANA é muito mais longo do que o dos bancos de dados tradicionais, porque uma grande quantidade de dados precisa ser carregada na memória antes que o banco de dados possa fornecer a performance esperada. Portanto, uma parte significativa do rto é o tempo necessário para iniciar o banco de dados. Com qualquer replicação baseada em storage e com O HANA System Replication sem pré-carga dos dados, o banco de dados SAP HANA precisa ser iniciado em caso de failover para o local de recuperação de desastre.

A replicação do sistema SAP HANA oferece um modo de operação no qual os dados são pré-carregados e atualizados continuamente no host secundário. Este modo permite valores de rto muito baixos, mas também requer um servidor dedicado que é usado apenas para receber os dados de replicação do sistema de origem.

Comparação da solução de recuperação de desastres

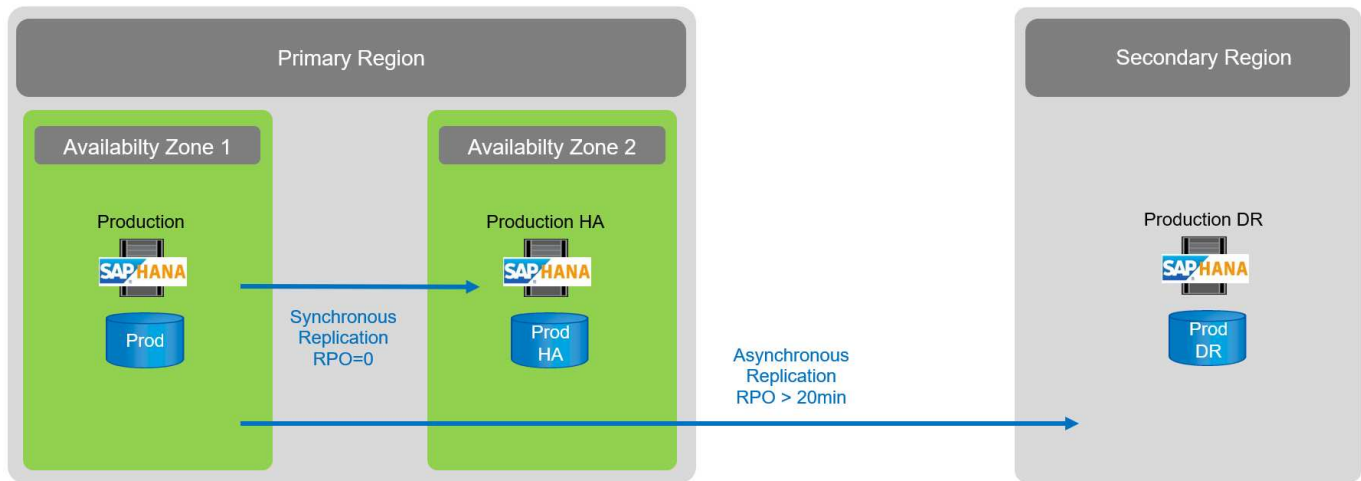
Uma solução abrangente de recuperação de desastres deve permitir que os clientes se recuperem de uma falha completa do local principal. Portanto, os dados precisam ser transferidos para um local secundário, e uma infraestrutura completa é necessária para executar os sistemas SAP HANA de produção necessários em caso de falha do local. Dependendo dos requisitos de disponibilidade do aplicativo e do tipo de desastre que você deseja proteger, uma solução de recuperação de desastres de dois ou três locais deve ser considerada.

A figura a seguir mostra uma configuração típica na qual os dados são replicados de forma síncrona dentro da mesma região do Azure em uma segunda zona de disponibilidade. A distância curta permite que você replique os dados de forma síncrona para alcançar um RPO de zero (normalmente usado para fornecer HA).

Além disso, os dados também são replicados de forma assíncrona para uma região secundária a ser protegida contra desastres, quando a região primária é afetada. O RPO mínimo alcançável depende da frequência de replicação de dados, que é limitada pela largura de banda disponível entre a região primária e a

região secundária. Um RPO mínimo típico está no intervalo de 20 minutos a várias horas.

Este documento discute diferentes opções de implementação de uma solução de recuperação de desastres de duas regiões.



Replicação do sistema SAP HANA

O SAP HANA System Replication funciona na camada de banco de dados. A solução é baseada em um sistema SAP HANA adicional no local de recuperação de desastres que recebe as alterações do sistema primário. Este sistema secundário deve ser idêntico ao sistema primário.

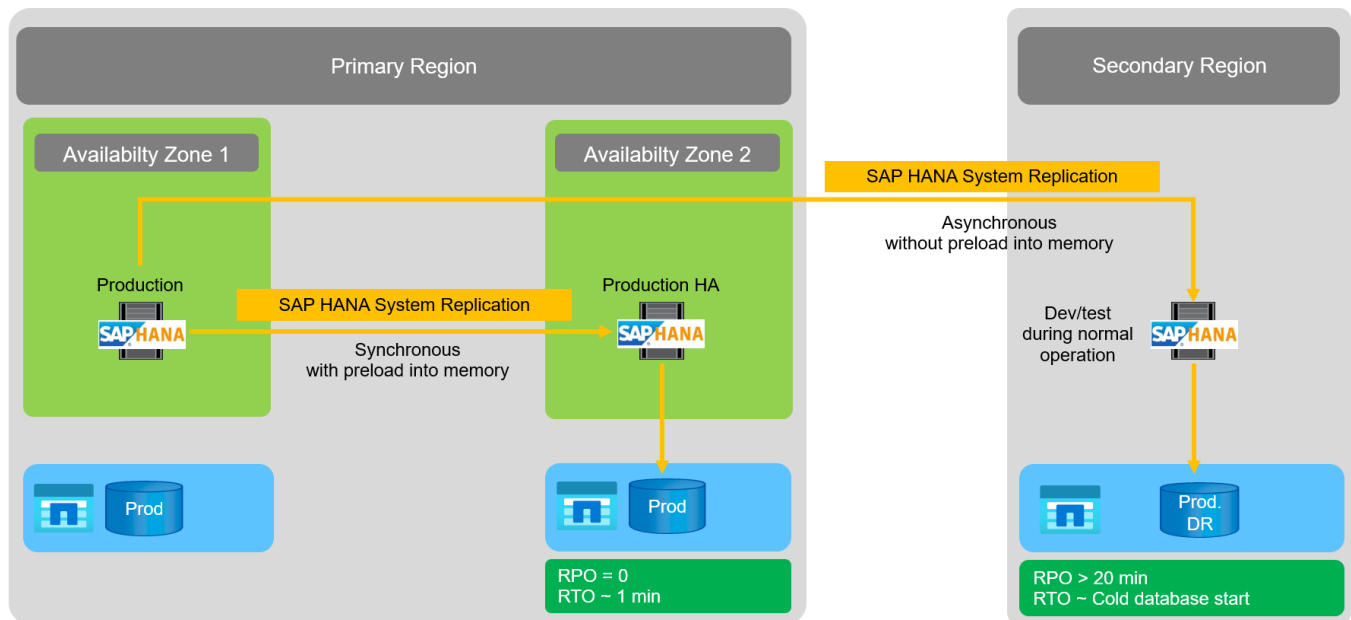
A replicação do sistema do SAP HANA pode ser operada em um de dois modos:

- Com dados pré-carregados na memória e um servidor dedicado no local de recuperação de desastres:
 - O servidor é usado exclusivamente como um host secundário SAP HANA System Replication.
 - Valores de rto muito baixos podem ser alcançados porque os dados já estão carregados na memória e não é necessário iniciar o banco de dados em caso de failover.
- Sem dados pré-carregados na memória e um servidor compartilhado no local de recuperação de desastres:
 - O servidor é compartilhado como um secundário SAP HANA System Replication e como um sistema de desenvolvimento/teste.
 - O rto depende principalmente do tempo necessário para iniciar o banco de dados e carregar os dados na memória.

Para obter uma descrição completa de todas as opções de configuração e cenários de replicação, consulte o ["Guia de administração do SAP HANA"](#).

A figura a seguir mostra a configuração de uma solução de recuperação de desastres em duas regiões com SAP HANA System Replication. A replicação síncrona com dados pré-carregados na memória é usada para HA local na mesma região do Azure, mas em diferentes zonas de disponibilidade. A replicação assíncrona sem dados pré-carregados está configurada para a região de recuperação de desastres remota.

A figura a seguir mostra a replicação do sistema SAP HANA.



Replicação do sistema SAP HANA com dados pré-carregados na memória

Valores de rto muito baixos com o SAP HANA só podem ser alcançados com a replicação do sistema SAP HANA com dados pré-carregados na memória. Operar o SAP HANA System Replication com um servidor secundário dedicado no local de recuperação de desastres permite um valor de rto de aproximadamente 1 minuto ou menos. Os dados replicados são recebidos e pré-carregados na memória no sistema secundário. Devido a esse baixo tempo de failover, a replicação do sistema do SAP HANA também costuma ser usada para operações de manutenção de inatividade quase zero, como atualizações de software HANA.

Normalmente, a replicação do sistema do SAP HANA é configurada para replicar de forma síncrona quando a pré-carga dos dados é escolhida. A distância máxima suportada para replicação síncrona está na faixa de 100km.

Replicação do sistema SAP sem dados pré-carregados na memória

Para requisitos de rto menos rigorosos, você pode usar a replicação do sistema SAP HANA sem dados pré-carregados. Neste modo operacional, os dados na região de recuperação de desastres não são carregados na memória. O servidor na região de DR ainda é usado para processar a replicação do sistema SAP HANA executando todos os processos necessários do SAP HANA. No entanto, a maior parte da memória do servidor está disponível para executar outros serviços, como sistemas de desenvolvimento/teste SAP HANA.

Em caso de desastre, o sistema de desenvolvimento/teste deve ser desligado, o failover deve ser iniciado e os dados devem ser carregados na memória. O rto desta abordagem de espera a frio depende do tamanho do banco de dados e da taxa de transferência de leitura durante a carga do armazenamento de linhas e colunas. Partindo do pressuposto de que os dados são lidos com uma taxa de transferência de 1000Mbps Gbps, o carregamento de 1TB TB de dados deve demorar aproximadamente 18 minutos.

Recuperação de desastres no SAP HANA com replicação entre regiões do ANF

A replicação entre regiões do ANF foi incorporada ao ANF como uma solução de recuperação de desastres usando replicação de dados assíncrona. A replicação entre regiões do ANF é configurada por meio de uma relação de proteção de dados entre dois volumes do ANF em uma região do Azure primário e secundário. A replicação entre regiões do ANF atualiza o volume secundário usando replicações eficientes de delta em blocos. As agendas de atualização podem ser definidas durante a configuração de replicação.

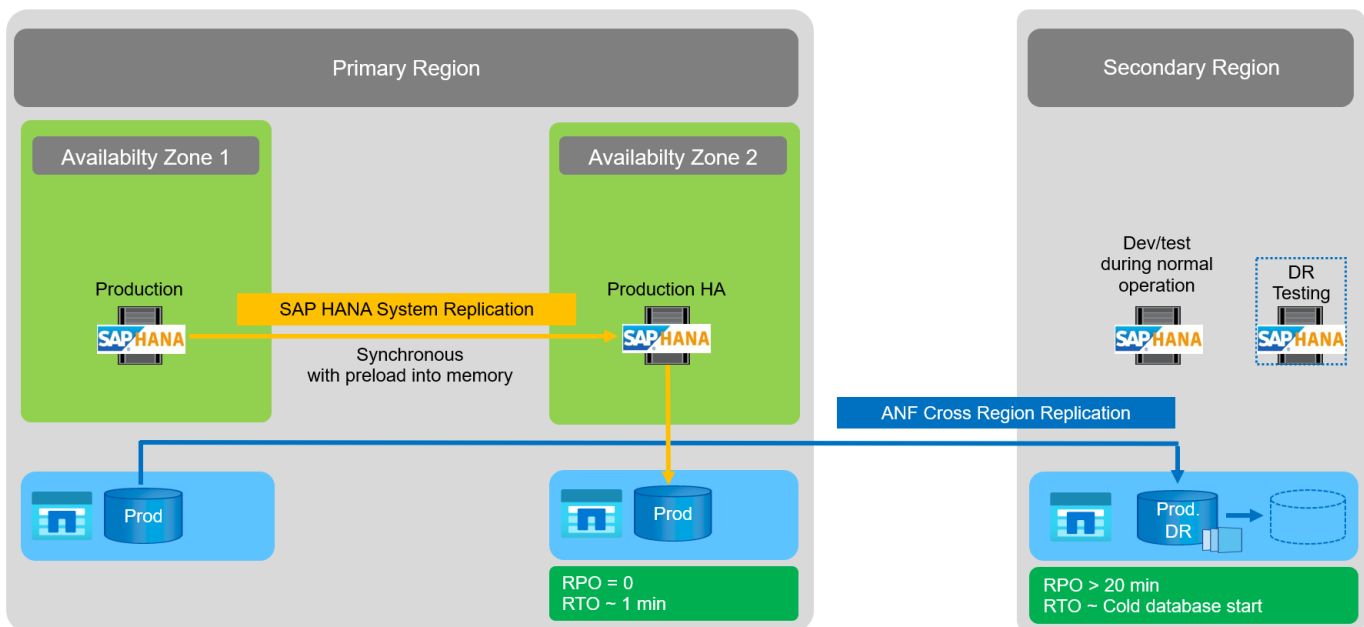
A figura a seguir mostra um exemplo de solução de recuperação de desastres em duas regiões, usando a replicação entre regiões do ANF. Neste exemplo, o sistema HANA é protegido com a replicação do sistema HANA na região principal, conforme discutido no capítulo anterior. A replicação para uma região secundária é feita usando a replicação entre regiões do ANF. O RPO é definido pelo cronograma de replicação e pelas opções de replicação.

O rto depende principalmente do tempo necessário para iniciar o banco de DADOS HANA no local de recuperação de desastres e para carregar os dados na memória. Partindo do pressuposto de que os dados são lidos com uma taxa de transferência DE 1000Mb MB/s, o carregamento de 1TB MB de dados levaria aproximadamente 18 minutos. Dependendo da configuração de replicação, a recuperação avançada também é necessária e aumentará o valor total de rto.

Mais detalhes sobre as diferentes opções de configuração são fornecidos no ["Opções de configuração para replicação entre regiões com SAP HANA"](#) capítulo .

Os servidores nos locais de recuperação de desastres podem ser usados como sistemas de desenvolvimento/teste durante a operação normal. Em caso de desastre, os sistemas de desenvolvimento/teste devem ser desligados e iniciados como servidores de produção de DR.

A replicação entre regiões do ANF permite testar o fluxo de trabalho de DR sem impactar o RPO e o rto. Isso é feito criando clones de volume e anexando-os ao servidor de teste de DR.



Resumo das soluções de recuperação de desastres

A tabela a seguir compara as soluções de recuperação de desastres discutidas nesta seção e destaca os indicadores mais importantes.

Os principais resultados são os seguintes:

- Se for necessário um rto muito baixo, a replicação do sistema SAP HANA com pré-carga na memória é a única opção.
 - Um servidor dedicado é necessário no local de DR para receber os dados replicados e carregar os dados na memória.
- Além disso, a replicação de storage é necessária para os dados que residem fora do banco de dados (por

exemplo, arquivos compartilhados, interfaces etc.).

- Se os requisitos de rto/RPO forem menos rigorosos, a replicação entre regiões do ANF também poderá ser usada para:
 - Combine replicação de dados de banco de dados e não banco de dados.
 - Cobrir casos de uso adicionais, como teste de recuperação de desastres e atualização de desenvolvimento/teste.
 - Com a replicação de armazenamento, o servidor no local de DR pode ser usado como um sistema de teste ou QA durante a operação normal.
- Uma combinação do SAP HANA System Replication como uma solução de HA com RPO igual a 0 e replicação de storage para uma longa distância faz sentido atender aos diferentes requisitos.

A tabela a seguir fornece uma comparação das soluções de recuperação de desastres.

	Replicação de storage	Replicação do sistema SAP HANA	
	Replicação entre regiões	Com pré-carga de dados	Sem pré-carga de dados
RTO	Baixo a médio, dependendo do tempo de inicialização do banco de dados e da recuperação avançada	Muito baixo	Baixo a médio, dependendo do tempo de inicialização do banco de dados
RPO	Replicação assíncrona RPO > 20min	Replicação síncrona RPO > 20min RPO/0	Replicação síncrona RPO > 20min RPO/0
Os servidores no local de DR podem ser usados para desenvolvimento/teste	Sim	Não	Sim
Replicação de dados que não são de banco de dados	Sim	Não	Não
Os dados de DR podem ser usados para atualizar os sistemas de desenvolvimento/teste	Sim	Não	Não
Testes de DR sem afetar o rto e o RPO	Sim	Não	Não

Replicação entre regiões do ANF com SAP HANA

Replicação entre regiões do ANF com SAP HANA

Informações agnósticas de aplicativos sobre replicação entre regiões podem ser encontradas no seguinte local.

["Documentação do Azure NetApp Files | Microsoft Docs"](#) nas seções conceitos e instruções.

Opções de configuração para replicação entre regiões com SAP HANA

A figura a seguir mostra as relações de replicação de volume para um sistema SAP HANA que usa a replicação entre regiões do ANF. Com a replicação entre regiões do ANF, os DADOS HANA e o volume compartilhado HANA precisam ser replicados. Se apenas o volume de DADOS HANA for replicado, os valores típicos de RPO estarão na faixa de um dia. Se forem necessários valores de RPO mais baixos, os backups de log DO HANA também devem ser replicados para recuperação futura.



O termo "backup de log" usado neste documento inclui o backup de log e o backup do catálogo de backup HANA. O catálogo de BACKUP DO HANA é necessário para executar operações de recuperação futuras.

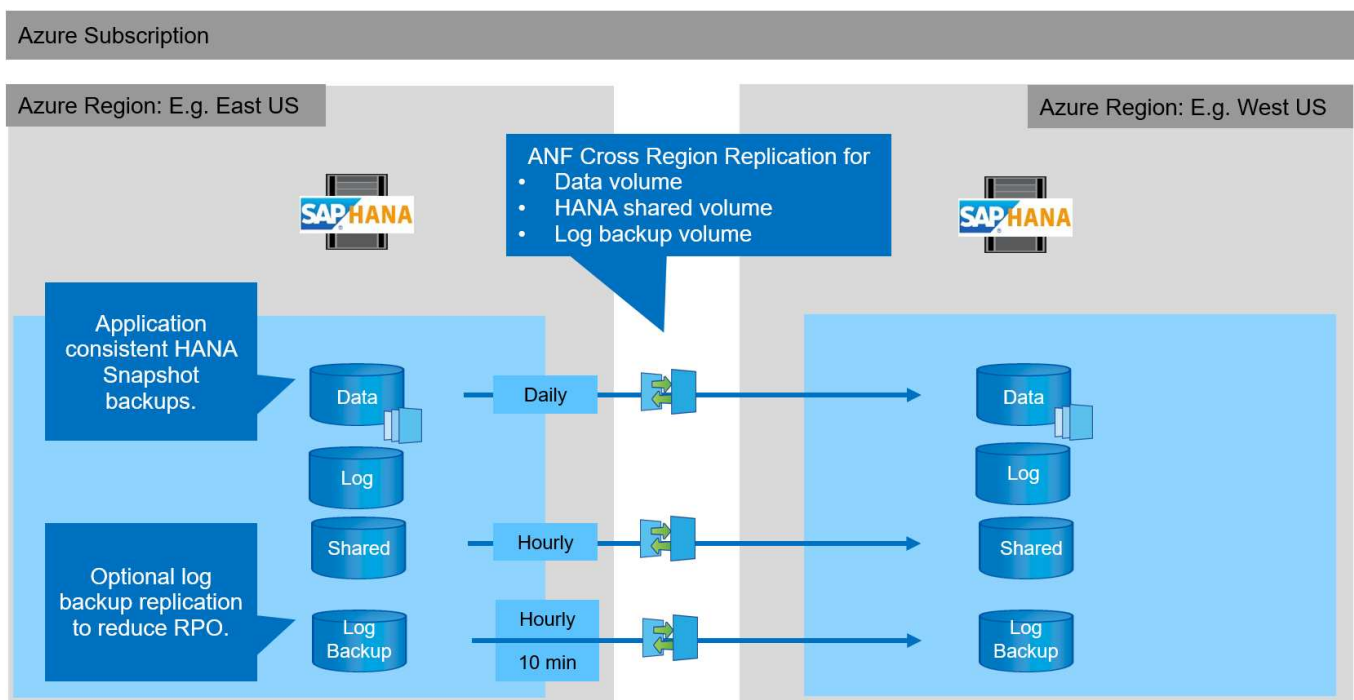


A descrição a seguir e a configuração do laboratório se concentram no banco de dados HANA. Outros arquivos compartilhados, por exemplo, o diretório de transporte SAP, seriam protegidos e replicados da mesma forma que o volume compartilhado HANA.

Para habilitar a recuperação do ponto de salvamento ou a recuperação avançada DO HANA usando os backups de log, os backups de Snapshot de dados consistentes com aplicações devem ser criados no local principal para o volume de dados HANA. Isso pode ser feito, por exemplo, com a ferramenta de backup do ANF AzAcSnap (consulte também "[O que é a ferramenta Snapshot consistente de aplicativos do Azure para o Azure NetApp Files | Microsoft Docs](#)"). Os backups Snapshot criados no local principal são replicados para o local de recuperação de desastres.

No caso de um failover de desastres, a relação de replicação deve ser quebrada, os volumes devem ser montados no servidor de produção de DR e o banco de DADOS HANA deve ser recuperado, seja no último ponto de salvamento DO HANA ou com recuperação avançada usando os backups de log replicados. O "[Failover de recuperação de desastres](#)" capítulo , descreve os passos necessários.

A figura a seguir mostra as opções de CONFIGURAÇÃO HANA para replicação entre regiões.



Com a versão atual da replicação entre regiões, apenas é possível selecionar agendas fixas e o tempo real de atualização da replicação não pode ser definido pelo usuário. Os horários disponíveis são diários, de hora em hora e a cada 10 minutos. Com essas opções de agendamento, duas configurações diferentes fazem sentido dependendo dos requisitos RPO: Replicação de volume de dados sem replicação de backup de log e replicação de backup de log com diferentes programações, por hora ou a cada 10 minutos. O RPO mais baixo alcançável é de cerca de 20 minutos. A tabela a seguir resume as opções de configuração e os valores RPO e rto resultantes.

	Replicação de volume de dados	Replicação de volume de backup de dados e log	Replicação de volume de backup de dados e log
Volume de dados de programação CRR	Diariamente	Diariamente	Diariamente
Volume de cópia de segurança do registo de agendamento CRR	n/a.	Por hora	10 min
RPO máximo	Mais de 6 horas e agendamento de instantâneos (por exemplo, mais de 24 horas)	1 hora	2 x 10 min
Rto máx	Definido principalmente pelo tempo de INICIALIZAÇÃO DO HANA	Tempo de inicialização DO HANA e tempo de recuperação mais	Tempo de inicialização DO HANA e tempo de recuperação mais
Recuperação avançada	NA	Registros para as últimas 24 horas e agendamento instantâneo (por exemplo, 6 horas)	Registros para as últimas 24 horas e agendamento instantâneo (por exemplo, 6 horas)

Requisitos e práticas recomendadas

O Microsoft Azure não garante a disponibilidade de um tipo de máquina virtual (VM) específico na criação ou ao iniciar uma VM desalocada. Especificamente, em caso de falha de região, muitos clientes podem exigir VMs adicionais na região de recuperação de desastres. Portanto, é recomendável usar ativamente uma VM com o tamanho necessário para o failover de desastres como um sistema de teste ou QA na região de recuperação de desastres para ter o tipo de VM necessário alocado.

Para otimização dos custos, faz sentido usar um pool de capacidade do ANF com uma categoria de performance mais baixa durante as operações normais. A replicação de dados não exige alta performance e, portanto, pode usar um pool de capacidade com uma categoria de performance padrão. Para testes de recuperação de desastre ou se for necessário um failover de desastre, os volumes precisam ser movidos para um pool de capacidade com uma categoria de alta performance.

Se um segundo pool de capacidade não for uma opção, os volumes de destino de replicação devem ser configurados com base nos requisitos de capacidade e não nos requisitos de desempenho durante as operações normais. A cota ou a taxa de transferência (para QoS manual) pode ser adaptada para testes de recuperação de desastres em caso de failover de desastres.

Mais informações podem ser encontradas em ["Requisitos e considerações para usar a replicação entre regiões de volume Azure NetApp Files | Microsoft Docs"](#).

Configuração do laboratório

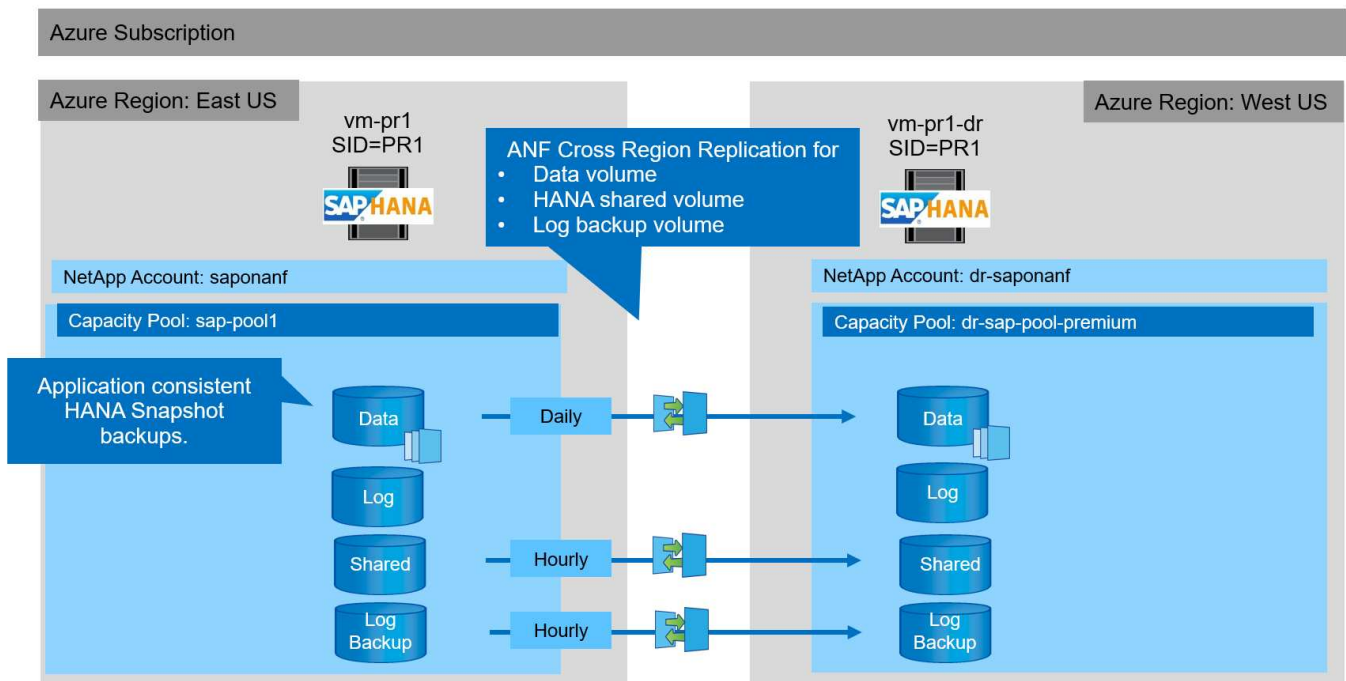
A validação da solução foi realizada com um sistema SAP HANA de um único host. A ferramenta de backup do Microsoft AzAcSnap Snapshot para ANF foi usada para configurar backups de Snapshot consistentes com APLICAÇÕES HANA. Um volume de dados diário, backup de log por hora e replicação de volume compartilhado foram todos configurados. O teste e o failover de recuperação de desastres foram validados com um ponto de economia e com operações de recuperação avançadas.

As seguintes versões de software foram usadas na configuração do laboratório:

- Um único sistema SAP HANA 2,0 SPS5 de host com um único locatário
- SUSE SLES PARA SAP 15 SP1
- AzAcSnap 5,0

Um único pool de capacidade com QoS manual foi configurado no local de DR.

A figura a seguir mostra a configuração do laboratório.



Configuração de backup do Snapshot com AzAcSnap

No local principal, o AzAcSnap foi configurado para criar backups Snapshot consistentes com aplicações do SISTEMA HANA PR1. Esses backups do Snapshot estão disponíveis no volume de dados do ANF do sistema PR1 HANA. Eles também estão registrados no catálogo de backup do SAP HANA, conforme mostrado nas duas figuras a seguir. Os backups de snapshot foram programados para cada 4 horas.

Com a replicação do volume de dados usando a replicação entre regiões do ANF, esses backups do Snapshot são replicados para o local de recuperação de desastre e podem ser usados para recuperar o banco de

A figura a seguir mostra os backups de Snapshot do volume de DADOS HANA.



Algumas etapas de preparação devem ser executadas no local de recuperação de desastres antes que a replicação de volume possa ser configurada.

- Uma conta do NetApp deve estar disponível e configurada com a mesma assinatura do Azure que a origem.

- Um pool de capacidade deve estar disponível e configurado usando a conta NetApp acima.
- Uma rede virtual deve estar disponível e configurada.
- Na rede virtual, uma sub-rede delegada deve estar disponível e configurada para uso com o ANF.

Agora é possível criar volumes de proteção para os DADOS HANA, o HANA compartilhado e o volume de backup de log DO HANA. A tabela a seguir mostra os volumes de destino configurados em nossa configuração de laboratório.



Para obter a melhor latência, os volumes precisam estar próximos das VMs que executam o SAP HANA em caso de failover. Portanto, o mesmo processo de fixação é necessário para os volumes de DR que para qualquer outro sistema de produção SAP HANA.

VOLUME HANA	Fonte	Destino	Agendamento de replicação
Volume de DADOS HANA	PR1-data-mnt00001	PR1-data-mnt00001-sm-dest	Diariamente
Volume compartilhado HANA	PR1-compartilhado	PR1-shared-sm-dest	Por hora
Volume de backup de catálogo/log DO HANA	hanabackup	mais fácil	Por hora

Para cada volume, os seguintes passos devem ser executados:

1. Crie um novo volume de proteção no local de recuperação de desastres:
 - a. Forneça o nome do volume, o pool de capacidade, a cota e as informações da rede.
 - b. Forneça as informações de acesso ao protocolo e ao volume.
 - c. Forneça a ID do volume de origem e uma programação de replicação.
 - d. Crie um volume de destino.
2. Autorizar replicação no volume de origem.
 - Forneça a ID do volume alvo.

As capturas de tela a seguir mostram os passos de configuração em detalhes.

No local de recuperação de desastres, um novo volume de proteção é criado selecionando volumes e clicando em Adicionar replicação de dados. Na guia Noções básicas, você deve fornecer o nome do volume, o pool de capacidade e as informações da rede.



A cota do volume pode ser definida com base nos requisitos de capacidade, porque o desempenho do volume não tem efeito no processo de replicação. No caso de um failover de recuperação de desastres, a cota deve ser ajustada para atender aos requisitos reais de desempenho.



Se o pool de capacidade tiver sido configurado com QoS manual, você poderá configurar a taxa de transferência além dos requisitos de capacidade. Da mesma forma que acima, você pode configurar a taxa de transferência com um valor baixo durante a operação normal e aumentá-la em caso de failover de recuperação de desastres.

Create a new protection volume

Basics Protocol Replication Tags Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. [Learn more about Azure NetApp Files](#)

Volume details

Volume name *	PR1-data-mnt00001-sm-dest	✓
Capacity pool * ⓘ	dr-sap-pool1	▼
Available quota (GiB) ⓘ	4096	4 TiB
Quota (GiB) * ⓘ	500	500 GiB ✓
Virtual network * ⓘ	dr-vnet (10.2.0.0/16,10.0.2.0/24)	▼
	Create new	
Delegated subnet * ⓘ	default (10.0.2.0/28)	▼
	Create new	
Show advanced section	☐	

Review + create

< Previous

Next : Protocol >

No separador Protocolo, tem de fornecer o protocolo de rede, o caminho de rede e a política de exportação.



O protocolo tem de ser o mesmo que o protocolo utilizado para o volume de origem.

Create a new protection volume

Basics **Protocol** Replication Tags Review + create

Configure access to your volume.

Access

Protocol type ☒ NFS ☐ SMB ☐ Dual-protocol (NFSv3 and SMB)

Configuration

File path * ⓘ

Versions * ▼

Kerberos ☐ Enabled ☒ Disabled

Export policy

Configure the volume's export policy. This can be edited later. [Learn more](#)

↑ Move up ↓ Move down ↑ Move to top ↓ Move to bottom 🗑 Delete

☒	Index	Allowed clients	Access	Root Access	
☒	1	0.0.0.0/0	Read & Write ▼	On ▼	...
			▼	▼	

Review + create

< Previous

Next : Replication >

Na guia replicação, você deve configurar o ID do volume de origem e o agendamento de replicação. Para replicação de volume de dados, configuramos um cronograma de replicação diário para nossa configuração de laboratório.



A ID do volume de origem pode ser copiada a partir do ecrã Propriedades do volume de origem.

Create a new protection volume

Basics

Protocol

Replication

Tags

Review + create

Source volume ID ⓘ

/subscriptions/28cfc403-f3f6-4b07-9847-4eb16109e870/resourceGroups/rg... ✓

Replication schedule ⓘ

Daily ^

Every 10 minutes

Hourly

Daily

Review + create

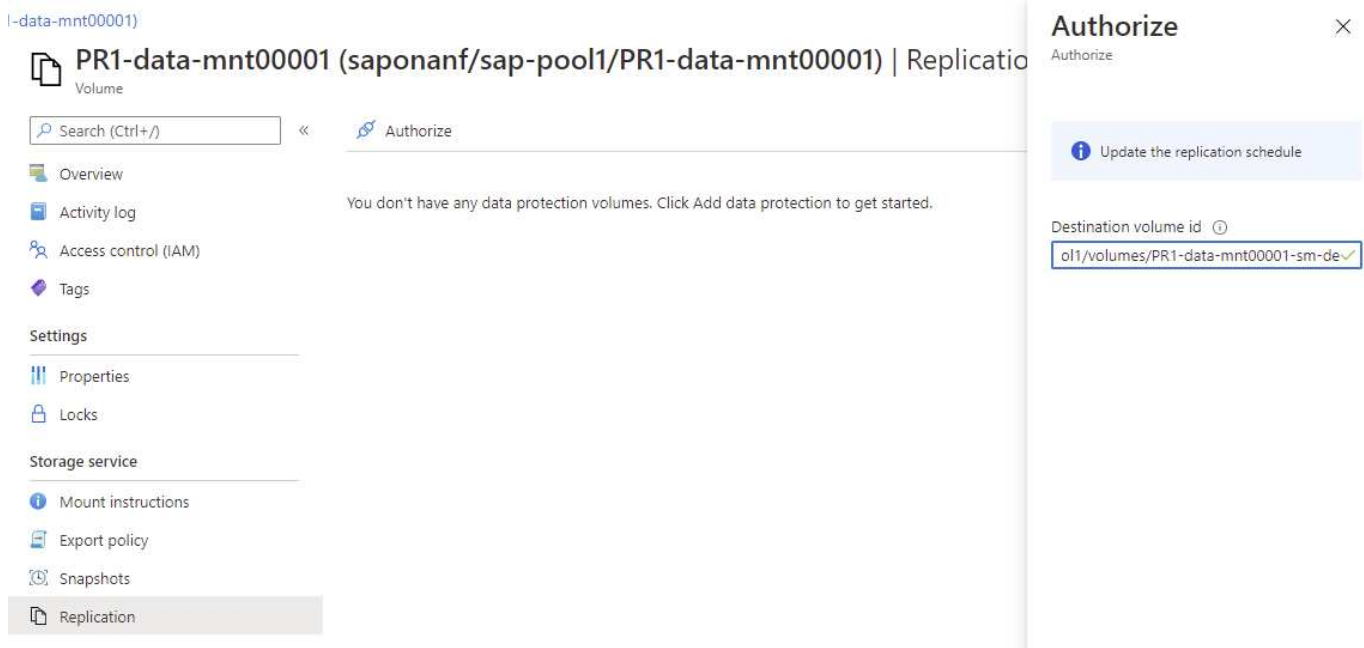
< Previous

Next : Tags >

Como etapa final, você deve autorizar a replicação no volume de origem fornecendo a ID do volume de destino.

ⓘ

Pode copiar a ID do volume de destino a partir do ecrã Propriedades do volume de destino.



As mesmas etapas devem ser executadas para o HANA compartilhado e o volume de backup de log.

Monitoramento da replicação entre regiões do ANF

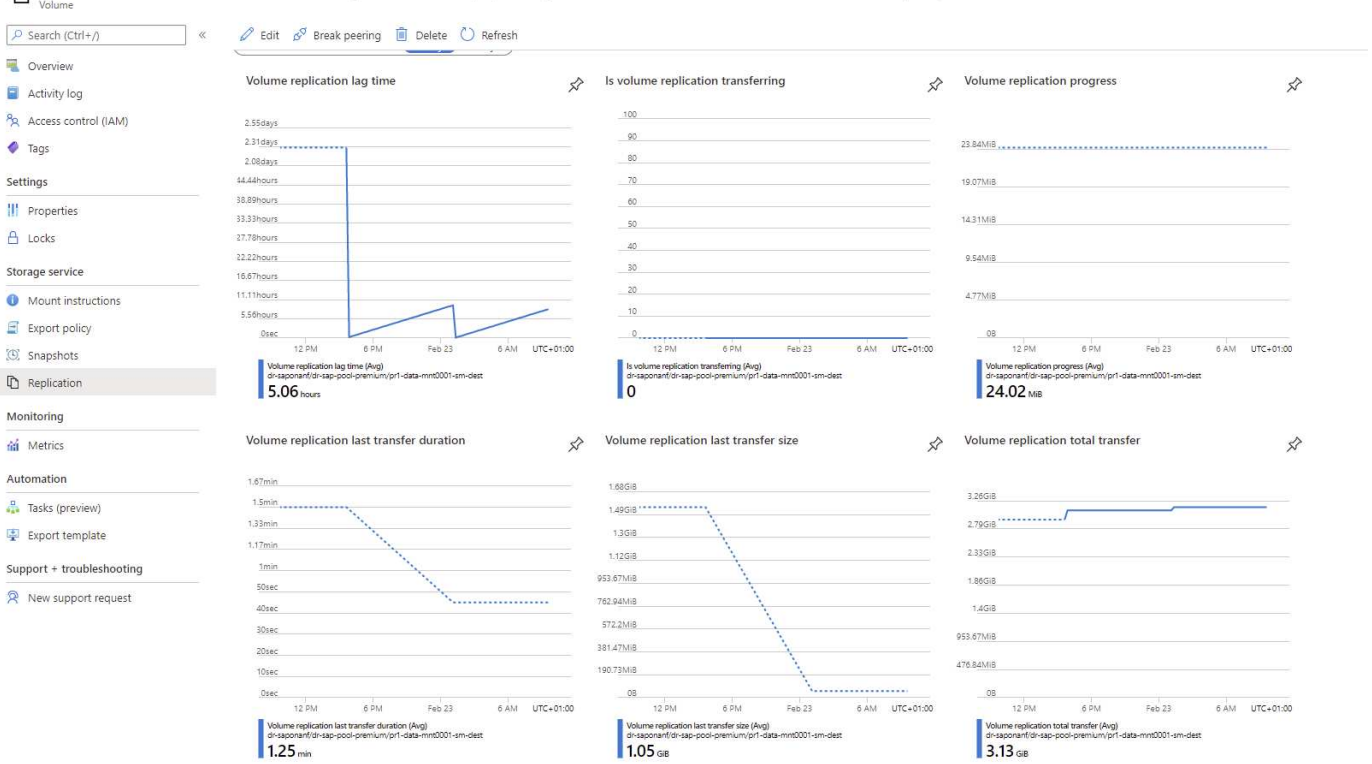
As três capturas de tela a seguir mostram o status da replicação para os dados, backup de log e volumes compartilhados.

O tempo de atraso de replicação de volume é um valor útil para entender as expectativas de RPO. Por exemplo, a replicação do volume de backup de log mostra um tempo de atraso máximo de 58 minutos, o que significa que o RPO máximo tem o mesmo valor.

A duração da transferência e o tamanho da transferência fornecem informações valiosas sobre os requisitos de largura de banda e alteram a taxa do volume replicado.

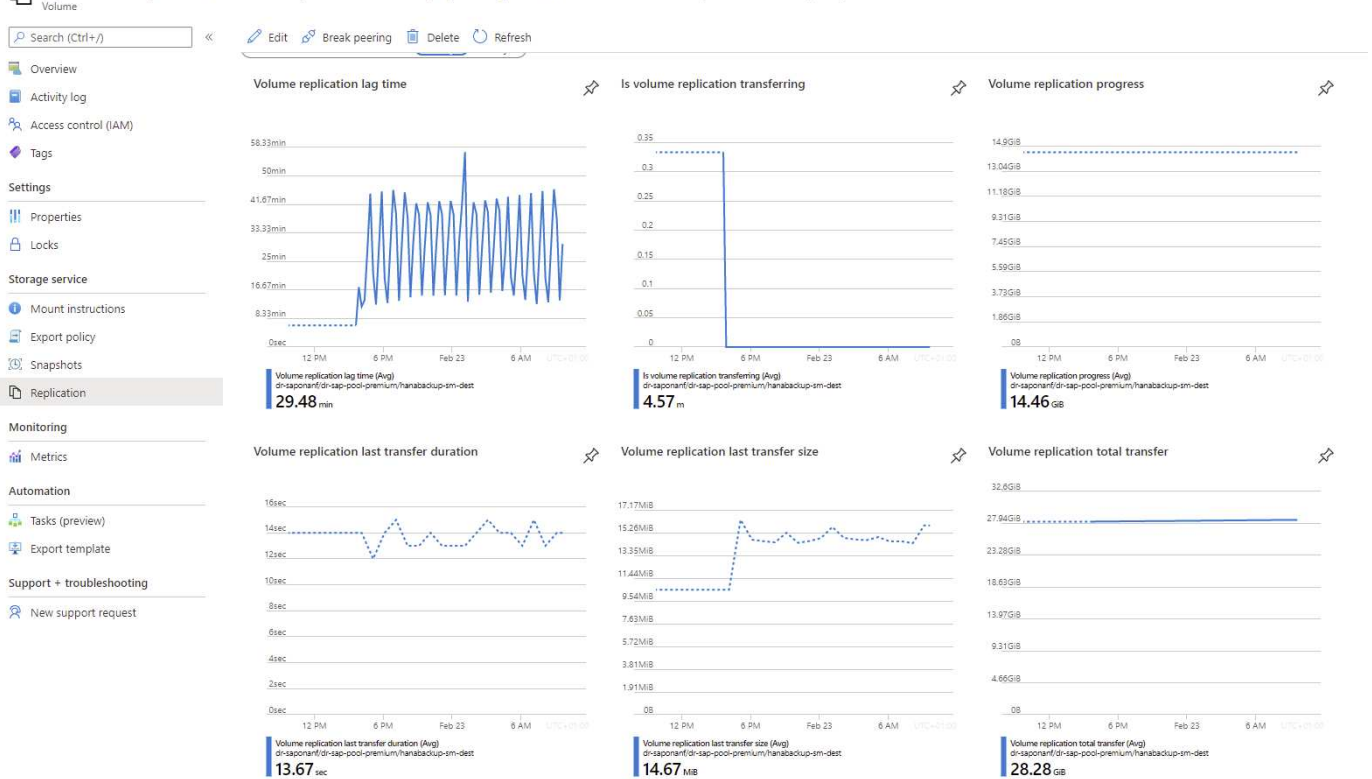
A captura de tela a seguir mostra o status da replicação do volume de DADOS HANA.

PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest) | Replication



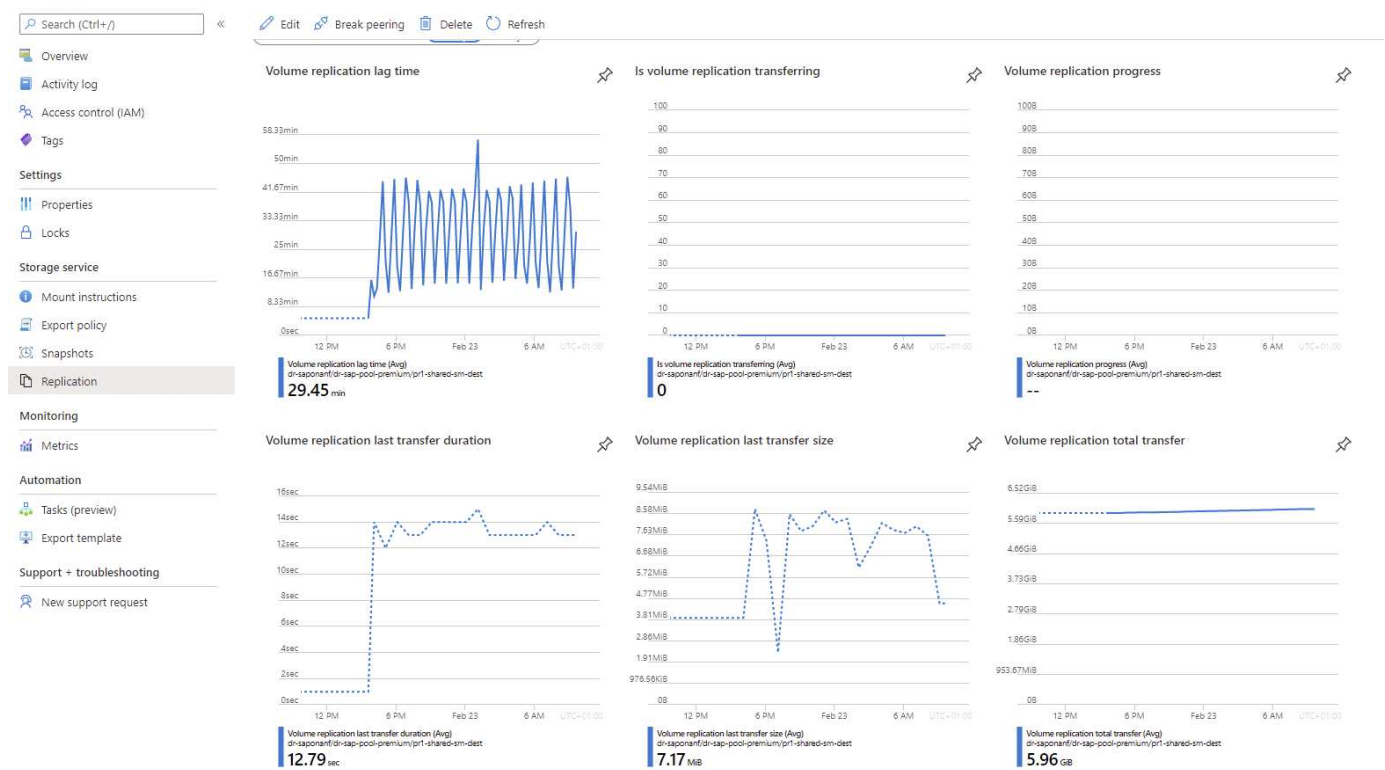
A captura de tela a seguir mostra o status da replicação do volume de backup DO log do HANA.

hanabackup-sm-dest (dr-saponanf/dr-sap-pool-premium/hanabackup-sm-dest) | Replication



A captura de tela a seguir mostra o status da replicação do volume compartilhado HANA.

PR1-shared-sm-dest (dr-sapnanf/dr-sap-pool-premium/PR1-shared-sm-dest) | Replication



Backups de snapshot replicados

Com cada atualização de replicação da origem para o volume de destino, todas as alterações de bloco ocorridas entre a última e a atualização atual são replicadas para o volume de destino. Isso também inclui os snapshots, que foram criados no volume de origem. A captura de tela a seguir mostra os instantâneos disponíveis no volume de destino. Como já discutido, cada um dos snapshots criados pela ferramenta AzAcSnap são imagens consistentes com aplicativos do banco de DADOS HANA que podem ser usadas para executar um ponto de salvamento ou uma recuperação avançada.



Dentro da origem e do volume de destino, as cópias Snapshot do SnapMirror também são criadas, que são usadas para operações de ressincronização e atualização de replicação. Essas cópias Snapshot não são consistentes com aplicações do ponto de vista do banco de DADOS HANA. Somente os snapshots consistentes com aplicações criados por meio do AzaCSnap podem ser usados para operações de RECUPERAÇÃO HANA.

PR1-data-mnt0001-sm-dest (dr-sapnanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest) | Snapshots

Volume

Search (Ctrl+/) << + Add snapshot Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Monitoring

Metrics

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Search snapshots

Name	Location	Created
azacsnap__2021-02-18T120002-2150721Z	West US	02/18/2021, 01:00:05 PM
azacsnap__2021-02-18T160002-1442691Z	West US	02/18/2021, 05:00:49 PM
azacsnap__2021-02-18T200002-0756687Z	West US	02/18/2021, 09:00:05 PM
azacsnap__2021-02-19T000002-0039686Z	West US	02/19/2021, 01:00:05 AM
azacsnap__2021-02-19T040001-8773746Z	West US	02/19/2021, 05:00:06 AM
azacsnap__2021-02-19T080001-5198653Z	West US	02/19/2021, 09:00:05 AM
azacsnap__2021-02-19T120002-1495322Z	West US	02/19/2021, 01:00:06 PM
azacsnap__2021-02-19T160002-3698678Z	West US	02/19/2021, 05:00:05 PM
azacsnap__2021-02-22T120002-3145398Z	West US	02/22/2021, 01:00:06 PM
snapmirrorb1e8e48d-7114-11eb-b147-d039ea1e211e_2155791247.2021-02-22_143159	West US	02/22/2021, 03:32:00 PM
azacsnap__2021-02-22T160002-0144647Z	West US	02/22/2021, 05:00:05 PM
azacsnap__2021-02-22T200002-0649581Z	West US	02/22/2021, 09:00:05 PM
azacsnap__2021-02-23T000002-0311379Z	West US	02/23/2021, 01:00:05 AM
snapmirrorb1e8e48d-7114-11eb-b147-d039ea1e211e_2155791247.2021-02-23_001000	West US	02/23/2021, 01:10:00 AM

Teste de recuperação de desastres

Teste de recuperação de desastres

Para implementar uma estratégia eficaz de recuperação de desastres, você deve testar o fluxo de trabalho necessário. O teste demonstra se a estratégia funciona e se a documentação interna é suficiente e também permite que os administradores treinem sobre os procedimentos necessários.

A replicação entre regiões do ANF permite testes de recuperação de desastres sem colocar o rto e o RPO em risco. Os testes de recuperação de desastres podem ser feitos sem interromper a replicação de dados.

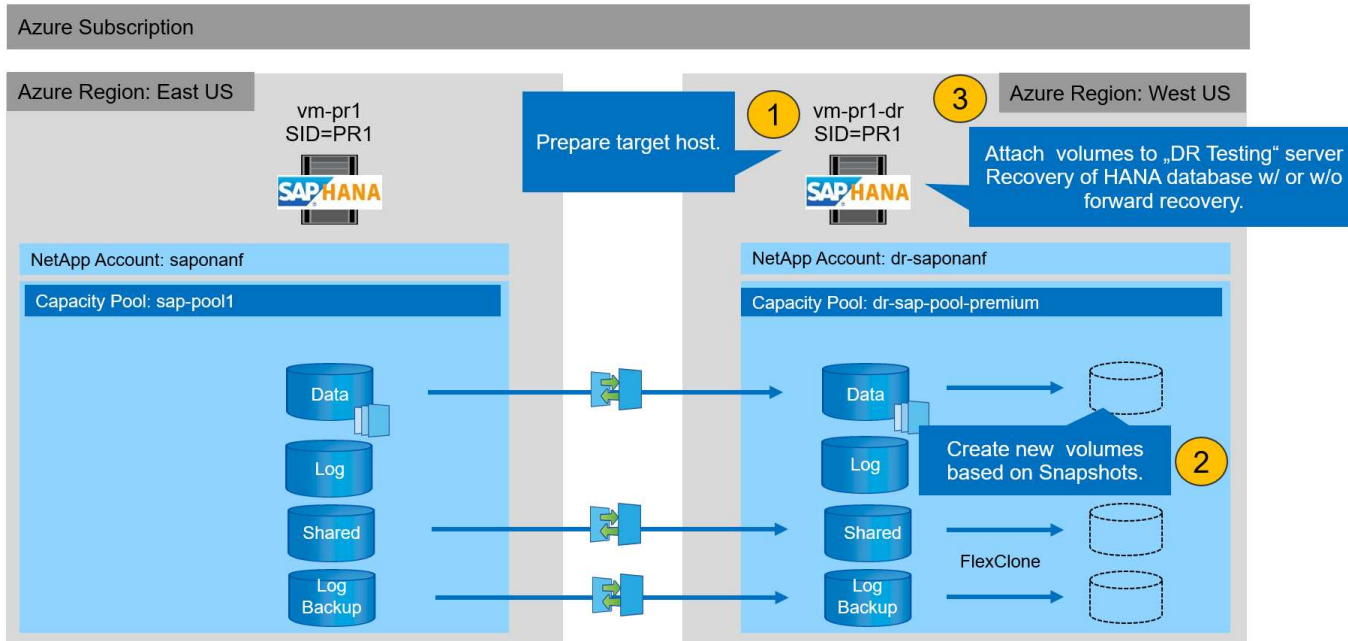
O workflow de teste de recuperação de desastres utiliza o recurso ANF para criar novos volumes com base nos backups atuais do Snapshot no destino de recuperação de desastres. ["Como funcionam os snapshots do Azure NetApp Files | Microsoft Docs"](#) Consulte .

Dependendo se a replicação de backup de log faz parte da configuração de recuperação de desastres ou não, as etapas para recuperação de desastres são ligeiramente diferentes. Esta seção descreve os testes de recuperação de desastres para replicação somente de backup de dados, bem como para replicação de volume de dados combinada com replicação de volume de backup de log.

Para executar o teste de recuperação de desastres, execute as seguintes etapas:

1. Prepare o host de destino.
2. Criar novos volumes com base nos backups Snapshot no local de recuperação de desastre.
3. Monte os novos volumes no host de destino.
4. Recuperar o banco de DADOS HANA.
 - Apenas recuperação de volume de dados.
 - Encaminhar a recuperação usando backups de log replicados.

As subseções a seguir descrevem esses passos em detalhes.



Prepare o host de destino

Esta seção descreve as etapas de preparação necessárias no servidor que é usado para o failover de recuperação de desastres.

Durante a operação normal, o host de destino geralmente é usado para outros fins, por exemplo, como um sistema de teste ou QA HANA. Portanto, a maioria das etapas descritas deve ser executada quando o teste de failover de desastres é executado. Por outro lado, os arquivos de configuração relevantes, como `/etc/fstab` e `/usr/sap/sapservices`, podem ser preparados e depois colocados em produção simplesmente copiando o arquivo de configuração. O procedimento de failover de recuperação de desastres garante que os arquivos de configuração preparados relevantes sejam configurados corretamente.

A preparação do host de destino também inclui o desligamento DO sistema de teste ou QA do HANA, bem como a interrupção de todos os serviços `systemctl stop sapinit` usando o `.`

Nome do host do servidor de destino e endereço IP

O nome do host do servidor de destino deve ser idêntico ao nome do host do sistema de origem. O endereço IP pode ser diferente.



A vedação adequada do servidor de destino deve ser estabelecida para que ele não possa se comunicar com outros sistemas. Se a vedação adequada não estiver no lugar, o sistema de produção clonado pode trocar dados com outros sistemas de produção, resultando em dados logicamente corrompidos.

Instale o software necessário

O software do agente host SAP deve ser instalado no servidor de destino. Para obter informações completas, consulte o "[Agente anfitrião SAP](#)" no portal de ajuda da SAP.



Se o host for usado como um sistema de teste ou QA HANA, o software do agente host SAP já estará instalado.

Configurar usuários, portas e serviços SAP

Os usuários e grupos necessários para o banco de dados SAP HANA precisam estar disponíveis no servidor de destino. Normalmente, o gerenciamento central de usuários é usado; portanto, nenhuma etapa de configuração é necessária no servidor de destino. As portas necessárias para o banco de DADOS HANA devem ser configuradas nos hosts de destino. A configuração pode ser copiada do sistema de origem copiando o `/etc/services` arquivo para o servidor de destino.

As entradas de serviços SAP necessárias devem estar disponíveis no host de destino. A configuração pode ser copiada do sistema de origem copiando o `/usr/sap/sapservices` arquivo para o servidor de destino. A saída a seguir mostra as entradas necessárias para o banco de dados SAP HANA usado na configuração do laboratório.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u prladm
limit.descriptors=1048576
```

Preparar o volume de log DO HANA

Como o volume de log HANA não faz parte da replicação, um volume de log vazio deve existir no host de destino. O volume de log deve incluir os mesmos subdiretórios que o sistema HANA de origem.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root  root  4096 Feb 19 16:20 .
drwxr-xr-x 3 root  root   22 Feb 18 13:38 ..
drwxr-xr-- 2 prladm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 prladm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 prladm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Preparar volume de cópia de segurança do registro

Como o sistema de origem está configurado com um volume separado para os backups de log DO HANA, um volume de backup de log também precisa estar disponível no host de destino. Um volume para os backups de log deve ser configurado e montado no host de destino.

Se a replicação do volume de backup de log fizer parte da configuração de recuperação de desastres, o volume de backup de log replicado será montado no host de destino e não será necessário preparar um volume de backup de log adicional.

Prepare montagens do sistema de arquivos

A tabela a seguir mostra as convenções de nomenclatura usadas na configuração do laboratório. Os nomes de volume no local de recuperação de desastre estão incluídos `/etc/fstab` no .

Volumes DO HANA para PR1	Volume e subdiretórios no local de recuperação de desastres	Ponto de montagem no host de destino
Volume de dados	PR1-data-mnt00001-sm-dest	/Hana/data/PR1/mnt00001
Volume compartilhado	PR1-shared-sm-dest/shared PR1-shared-sm-dest/usr-sap-PR1	/Hana/shared /usr/sap/PR1
Registrar o volume de cópia de segurança	mais fácil	/hanabackup



Os pontos de montagem desta tabela devem ser criados no host de destino.

Aqui estão as `/etc/fstab` entradas necessárias.

```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt00001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsz=262144,wsz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsz=262144,wsz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsz=262144,wsz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsz=262144,wsz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest /hanabackup nfs
rw,vers=3,hard,timeo=600,rsz=262144,wsz=262144,nconnect=8,bg,noatime,n
oalock 0 0
```

Criar novos volumes com base em backups de snapshot no local de recuperação de desastre

Dependendo da configuração de recuperação de desastres (com ou sem replicação de backup de log), dois ou três novos volumes com base em backups de snapshot devem ser criados. Em ambos os casos, é necessário criar um novo volume de dados e o volume compartilhado HANA.

Um novo volume do volume de backup de log deve ser criado se os dados de backup de log também forem replicados. No nosso exemplo, os dados e o volume de backup de log foram replicados para o local de recuperação de desastres. As etapas a seguir usam o Portal do Azure.

1. Um dos backups Snapshot consistentes com aplicações é selecionado como fonte para o novo volume do volume de DADOS HANA. Restore to New volume (Restaurar para novo volume) é selecionado para criar um novo volume com base no backup instantâneo.

PR1-data-mnt00001-sm-dest (dr-saponanf/dr-sap-pool1/PR1-data-mnt00001-sm-dest) | Snapshots

Volume

Search (Ctrl+/) « + Add snapshot Refresh

Overview
Activity log
Access control (IAM)
Tags
Settings
Properties
Locks
Storage service
Mount instructions
Export policy
Snapshots
Replication
Monitoring
Metrics
Automation
Tasks (preview)
Export template
Support + troubleshooting
New support request

Search snapshots

Name	Location	Created	
azacsnap__2021-02-16T134021-9431230Z	West US	02/16/2021, 02:40:27 PM	...
azacsnap__2021-02-16T134917-6284160Z	West US	02/16/2021, 02:49:20 PM	...
azacsnap__2021-02-16T135737-3778546Z	West US	02/16/2021, 02:57:41 PM	...
azacsnap__2021-02-16T160002-1354654Z	West US	02/16/2021, 05:00:05 PM	...
azacsnap__2021-02-16T200002-0790339Z	West US	02/16/2021, 09:00:08 PM	...
azacsnap__2021-02-17T000002-1753859Z	West US	02/17/2021, 01:00:06 AM	...
azacsnap__2021-02-17T040001-5454808Z	West US	02/17/2021, 05:00:05 AM	...
azacsnap__2021-02-17T080002-2933611Z	West US	02/17/2021, 09:00:18 AM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/17/2021, 12:46:22 PM	...
azacsnap__2021-02-17T120001-9196266Z	West US	02/17/2021, 01:00:08 PM	...
azacsnap__2021-02-17T160002-2801612Z	West US	02/17/2021, 05:00:06 PM	...
azacsnap__2021-02-17T200001-9149055Z	West US	02/17/2021, 09:00:05 PM	...
azacsnap__2021-02-18T000001-7955243Z	West US	02/18/2021, 01:00:07 PM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 01:10:00 PM	...

Restore to new volume
Revert volume
Delete

2. O novo nome do volume e a cota devem ser fornecidos na interface do usuário.

Home > Azure NetApp Files > dr-saponanf > dr-sap-pool1 (dr-saponanf/dr-sap-pool1) > PR1-data-mnt00001-sm-dest (d

Create a volume

Basics Protocol Tags Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. [Learn more about Azure NetApp Files](#)

Volume details

Volume name * PR1-data-mnt00001-sm-dest-clone ✓

Restoring from snapshot ⓘ azacsnap__2021-02-18T000001-7955243Z

Available quota (GiB) ⓘ 2096 2.05 TiB

Quota (GiB) * ⓘ 500 500 GiB ✓

Virtual network ⓘ dr-vnet (10.2.0.0/16,10.0.2.0/24) ▼

Delegated subnet ⓘ default (10.0.2.0/28) ▼

Show advanced section ☐

3. No separador Protocol (Protocolo), o caminho do ficheiro e a política de exportação são configurados.

[Home](#) > [Azure NetApp Files](#) > [dr-saponanf](#) > [dr-sap-pool1 \(dr-saponanf/dr-sap-pool1\)](#) > [PR1-data-mnt00001-sm-dest \(d](#)

Create a volume

Basics **Protocol** Tags Review + create

Configure access to your volume.

Access

Protocol type

☒ NFS ☐ SMB ☐ Dual-protocol (NFSv3 and SMB)

Configuration

File path * ⓘ

PR1-data-mnt00001-sm-dest-clone

Versions

NFSv4.1

Kerberos

☐ Enabled ☒ Disabled

Export policy

Configure the volume's export policy. This can be edited later. [Learn more](#)

↑ Move up ↓ Move down ↕ Move to top ⬇ Move to bottom 🗑 Delete

☒ Index	Allowed clients	Access	Root Access	
☒ 1	0.0.0.0/0	Read & Write	On	...

4. O ecrã criar e rever resume a configuração.

Create a volume

✓ Validation passed

Basics Protocol Tags **Review + create**

Basics

Subscription	Pay-As-You-Go
Resource group	dr-rg-sap
Region	West US
Volume name	PR1-data-mnt00001-sm-dest-clone
Capacity pool	dr-sap-pool1
Service level	Standard
Quota	500 GiB

Networking

Virtual network	dr-vnet (10.2.0.0/16,10.0.2.0/24)
Delegated subnet	default (10.0.2.0/28)

Protocol

Protocol	NFSv4.1
File path	PR1-data-mnt00001-sm-dest-clone

5. Um novo volume agora foi criado com base no backup instantâneo do HANA.

dr-saponanf | Volumes

NetApp account

Search (Ctrl+/)

«

+ Add volume

+ Add data replication

Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Azure NetApp Files

Active Directory connections

Storage service

Capacity pools

Volumes

Data protection

Snapshot policies

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Search volumes

Name	↑↓	Quota	↑↓	Protocol type	↑↓	Mount path	↑↓	Service level	↑↓	Capacity pool	↑↓
hanabackup-sm-dest		1000 GiB		NFSv3		10.0.2.4/hanabackup-sm-dest		Standard		dr-sap-pool1	...
PR1-data-mnt00001-sm-dest		500 GiB		NFSv4.1		10.0.2.4/PR1-data-mnt00001-s		Standard		dr-sap-pool1	...
PR1-data-mnt00001-sm-dest-clone		500 GiB		NFSv4.1		10.0.2.4/PR1-data-mnt00001-s		Standard		dr-sap-pool1	...
PR1-log-mnt00001-dr		250 GiB		NFSv4.1		10.0.2.4/PR1-log-mnt00001-dr		Standard		dr-sap-pool1	...
PR1-shared-sm-dest		250 GiB		NFSv4.1		10.0.2.4/PR1-shared-sm-dest		Standard		dr-sap-pool1	...

As mesmas etapas agora devem ser executadas para o HANA compartilhado e o volume de backup de log, como mostrado nas duas capturas de tela a seguir. Como não foram criados snapshots adicionais para o volume de backup compartilhado e de log do HANA, a cópia Snapshot mais recente do SnapMirror precisa ser selecionada como a origem do novo volume. Trata-se de dados não estruturados, e a cópia Snapshot do SnapMirror pode ser usada para esse caso de uso.

pool1/hanabackup-sm-dest

hanabackup-sm-dest (dr-saponanf/dr-sap-pool1/hanabackup-sm-dest) | Snapshots

Volume

Search (Ctrl+/) « + Add snapshot Refresh

Overview
Activity log
Access control (IAM)
Tags
Settings
Properties
Locks
Storage service
Mount instructions
Export policy
Snapshots
Replication

Search snapshots

Name	Location	Created	
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 02:05:00 PM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 03:05:00	...

- Restore to new volume
- Revert volume
- Delete

A captura de tela a seguir mostra o volume compartilhado DO HANA restaurado para o novo volume.

pool1/PR1-shared-sm-dest

PR1-shared-sm-dest (dr-saponanf/dr-sap-pool1/PR1-shared-sm-dest) | Snapshots

Volume

Search (Ctrl+/) « + Add snapshot Refresh

Overview
Activity log
Access control (IAM)
Tags
Settings
Properties
Locks
Storage service
Mount instructions
Export policy
Snapshots
Replication

Search snapshots

Name	Location	Created	
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 02:05:00 PM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 03:05:00	...

- Restore to new volume
- Revert volume
- Delete



Se um pool de capacidade com uma categoria de baixa performance tiver sido usado, os volumes precisam ser movidos para um pool de capacidade que forneça a performance necessária.

Todos os três novos volumes estão agora disponíveis e podem ser montados no host de destino.

Monte os novos volumes no host de destino

Os novos volumes agora podem ser montados no host de destino, com base no `/etc/fstab` arquivo criado anteriormente.

```
vm-pr1:~ # mount -a
```

A saída a seguir mostra os sistemas de arquivos necessários.

```
vm-pr1:/hana/data/PR1/mnt00001/hdb00001 # df
Filesystem                                1K-blocks      Used
Available Use% Mounted on
devtmpfs                                  8190344         8
8190336    1% /dev
tmpfs                                     12313116         0
12313116    0% /dev/shm
tmpfs                                     8208744      17292
8191452    1% /run
tmpfs                                     8208744         0
8208744    0% /sys/fs/cgroup
/dev/sda4                                29866736  2438052
27428684    9% /
/dev/sda3                                 1038336     101520
936816    10% /boot
/dev/sda2                                 524008       1072
522936    1% /boot/efi
/dev/sdb1                                 32894736     49176
31151560    1% /mnt
tmpfs                                     1641748         0
1641748    0% /run/user/0
10.0.2.4:/PR1-log-mnt00001-dr             107374182400      256
107374182144    1% /hana/log/PR1/mnt00001
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone 107377026560  6672640
107370353920    1% /hana/data/PR1/mnt00001
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared 107377048320 11204096
107365844224    1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 107377048320 11204096
107365844224    1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest-clone        107379429120 35293440
107344135680    1% /hanabackup
```

Recuperação de banco de DADOS HANA

A seguir mostra as etapas para a recuperação do banco de dados HANA

Inicie os serviços SAP necessários.

```
vm-pr1:~ # systemctl start sapinit
```

A saída a seguir mostra os processos necessários.

```
vm-pr1:/ # ps -ef | grep sap
root      23101      1  0 11:29 ?          00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm    23191      1  3 11:29 ?          00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm    23202      1  5 11:29 ?          00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root      23292      1  0 11:29 ?          00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root      23359    2597  0 11:29 pts/1      00:00:00 grep --color=auto sap
```

As subseções a seguir descrevem o processo de recuperação com e sem recuperação avançada usando os backups de log replicados. A recuperação é executada usando o script de recuperação HANA para o banco de dados do sistema e os comandos hdbsql para o banco de dados do locatário.

Recuperação para o ponto de salvamento mais recente DO backup de volume de DADOS HANA

A recuperação para o mais recente backup savepoint é executada com os seguintes comandos como usuário pr1adm:

- Base de dados do sistema

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG"
```

- Banco de dados do locatário

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

Você também pode usar O HANA Studio ou o Cockpit para executar a recuperação do sistema e do banco de dados do locatário.

A saída do comando a seguir mostra a execução da recuperação.

Recuperação de banco de dados do sistema

```

pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: =====2021-02-19 14:32:16 =====
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00 P0027646      177bab4d610 INFO      RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>

```

Recuperação de banco de dados do locatário

Se uma chave de armazenamento de usuário não tiver sido criada para o usuário pr1adm no sistema de origem, uma chave deve ser criada no sistema de destino. O usuário do banco de dados configurado na chave deve ter Privileges para executar operações de recuperação de locatário.

```

pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>

```

A recuperação do locatário é agora executada com hdbsql.


```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

O banco de DADOS HANA agora está ativo e o fluxo de trabalho de recuperação de desastres do banco de DADOS HANA foi testado.

Recuperação com recuperação avançada usando backups de log/catálogo

Os backups de log e o catálogo de BACKUP HANA estão sendo replicados a partir do sistema de origem.

A recuperação usando todos os backups de log disponíveis é executada com os seguintes comandos como usuário pr1adm:

- Base de dados do sistema

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Banco de dados do locatário

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```



Para recuperar usando todos os logs disponíveis, você pode usar a qualquer momento no futuro como o carimbo de data/hora na instrução de recuperação.

Você também pode usar O HANA Studio ou o Cockpit para executar a recuperação do sistema e do banco de dados do locatário.

A saída do comando a seguir mostra a execução da recuperação.

Recuperação de banco de dados do sistema

```

prladm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: =====2021-02-19 16:06:40 =====
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00 P0009897 177bb0b4416 INFO RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs

```

Recuperação de banco de dados do locatário

```

prladm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
      \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>

```

O banco de DADOS HANA agora está ativo e o fluxo de trabalho de recuperação de desastres do banco de DADOS HANA foi testado.

Verifique a consistência dos backups de log mais recentes

Como a replicação do volume de backup de log é realizada independentemente do processo de backup de log executado pelo banco de dados SAP HANA, pode haver arquivos de backup de log abertos e inconsistentes no local de recuperação de desastres. Somente os arquivos de backup de log mais recentes podem ser inconsistentes, e esses arquivos devem ser verificados antes que uma recuperação avançada seja executada no site de recuperação de desastres usando a `hdbbackupcheck` ferramenta.

Se a `hdbbackupcheck` ferramenta relatar um erro para os backups de log mais recentes, o conjunto mais recente de backups de log deve ser removido ou excluído.

```
prladm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivercache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

A verificação deve ser executada para os arquivos de backup de log mais recentes do sistema e do banco de dados do locatário.

Se a `hdbbackupcheck` ferramenta relatar um erro para os backups de log mais recentes, o conjunto mais recente de backups de log deve ser removido ou excluído.

Failover de recuperação de desastres

Failover de recuperação de desastres

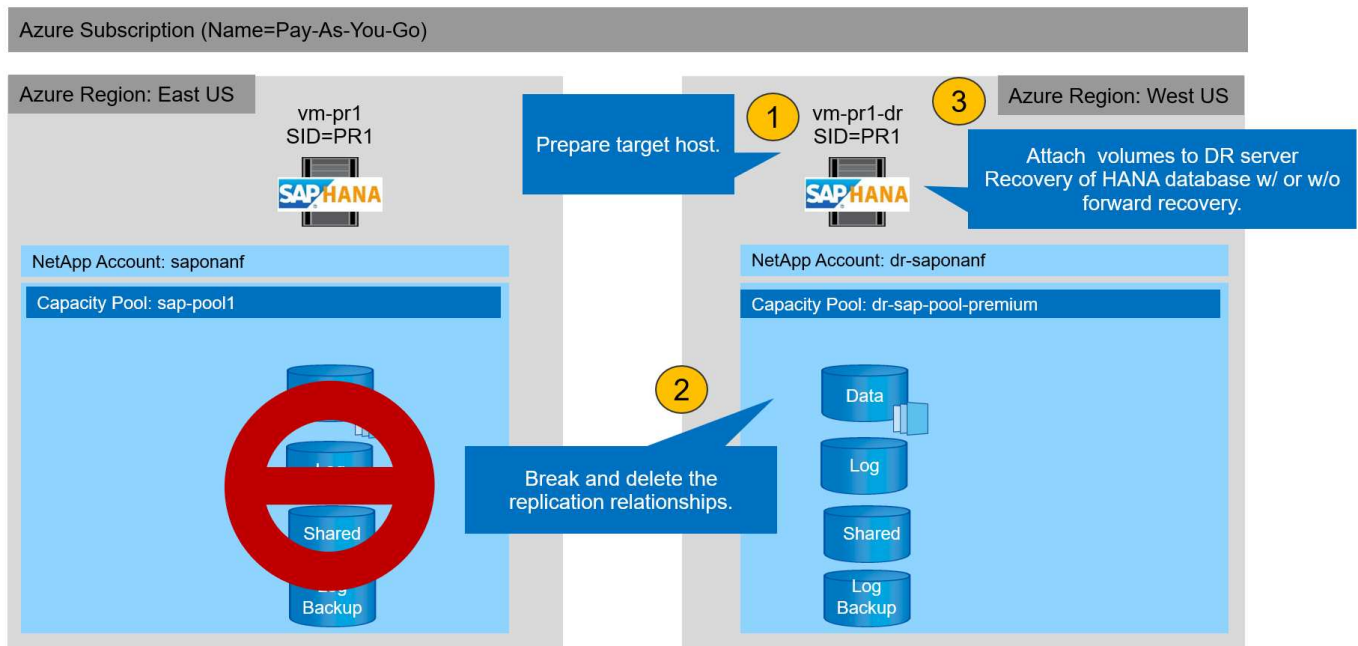
Dependendo se a replicação de backup de log faz parte da configuração de recuperação de desastres, as etapas para recuperação de desastres são ligeiramente diferentes. Esta seção descreve o failover de recuperação de desastres para replicação somente de backup de dados, bem como para replicação de volume de dados combinada com replicação de volume de backup de log.

Para executar o failover de recuperação de desastres, execute estas etapas:

1. Prepare o host de destino.
2. Quebre e exclua as relações de replicação.
3. Restaure o volume de dados para o backup instantâneo consistente com a aplicação mais recente.
4. Monte os volumes no host de destino.
5. Recuperar o banco de DADOS HANA.
 - Apenas recuperação de volume de dados.
 - Encaminhar a recuperação usando backups de log replicados.

As subseções a seguir descrevem essas etapas em detalhes, e a figura a seguir descreve os testes de

failover de desastres.



Prepare o host de destino

Esta seção descreve as etapas de preparação necessárias no servidor que é usado para o failover de recuperação de desastres.

Durante a operação normal, o host de destino geralmente é usado para outros fins, por exemplo, como um sistema de teste ou QA HANA. Portanto, a maioria das etapas descritas deve ser executada quando o teste de failover de desastres é executado. Por outro lado, os arquivos de configuração relevantes, como `/etc/fstab` e `/usr/sap/sapservices`, podem ser preparados e depois colocados em produção simplesmente copiando o arquivo de configuração. O procedimento de failover de recuperação de desastres garante que os arquivos de configuração preparados relevantes sejam configurados corretamente.

A preparação do host de destino também inclui o desligamento DO sistema de teste ou QA do HANA, bem como a interrupção de todos os serviços `systemctl stop sapinit` usando o .

Nome do host do servidor de destino e endereço IP

O nome do host do servidor de destino deve ser idêntico ao nome do host do sistema de origem. O endereço IP pode ser diferente.



A vedação adequada do servidor de destino deve ser estabelecida para que ele não possa se comunicar com outros sistemas. Se a vedação adequada não estiver no lugar, o sistema de produção clonado pode trocar dados com outros sistemas de produção, resultando em dados logicamente corrompidos.

Instale o software necessário

O software do agente host SAP deve ser instalado no servidor de destino. Para obter informações completas, consulte o "[Agente anfitrião SAP](#)" no portal de ajuda da SAP.



Se o host for usado como um sistema de teste ou QA HANA, o software do agente host SAP já estará instalado.

Configurar usuários, portas e serviços SAP

Os usuários e grupos necessários para o banco de dados SAP HANA precisam estar disponíveis no servidor de destino. Normalmente, o gerenciamento central de usuários é usado; portanto, nenhuma etapa de configuração é necessária no servidor de destino. As portas necessárias para o banco de DADOS HANA devem ser configuradas nos hosts de destino. A configuração pode ser copiada do sistema de origem copiando o `/etc/services` arquivo para o servidor de destino.

As entradas de serviços SAP necessárias devem estar disponíveis no host de destino. A configuração pode ser copiada do sistema de origem copiando o `/usr/sap/sapservices` arquivo para o servidor de destino. A saída a seguir mostra as entradas necessárias para o banco de dados SAP HANA usado na configuração do laboratório.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u prladm
limit.descriptors=1048576
```

Preparar o volume de log DO HANA

Como o volume de log HANA não faz parte da replicação, um volume de log vazio deve existir no host de destino. O volume de log deve incluir os mesmos subdiretórios que o sistema HANA de origem.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root    root    4096 Feb 19 16:20 .
drwxr-xr-x 3 root    root      22 Feb 18 13:38 ..
drwxr-xr-- 2 prladm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 prladm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 prladm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Preparar volume de cópia de segurança do registro

Como o sistema de origem está configurado com um volume separado para os backups de log DO HANA, um volume de backup de log também precisa estar disponível no host de destino. Um volume para os backups de log deve ser configurado e montado no host de destino.

Se a replicação do volume de backup de log fizer parte da configuração de recuperação de desastres, o volume de backup de log replicado será montado no host de destino e não será necessário preparar um volume de backup de log adicional.

Prepare montagens do sistema de arquivos

A tabela a seguir mostra as convenções de nomenclatura usadas na configuração do laboratório. Os nomes de volume no local de recuperação de desastre estão incluídos `/etc/fstab` no .

Volumes DO HANA para PR1	Volume e subdiretórios no local de recuperação de desastres	Ponto de montagem no host de destino
Volume de dados	PR1-data-mnt00001-sm-dest	/Hana/data/PR1/mnt00001
Volume compartilhado	PR1-shared-sm-dest/shared PR1-shared-sm-dest/usr-sap-PR1	/Hana/shared /usr/sap/PR1
Registrar o volume de cópia de segurança	mais fácil	/hanabackup



Os pontos de montagem desta tabela devem ser criados no host de destino.

Aqui estão as `/etc/fstab` entradas necessárias.

```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt00001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsiz=262144,wsiz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsiz=262144,wsiz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsiz=262144,wsiz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsiz=262144,wsiz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest /hanabackup nfs
rw,vers=3,hard,timeo=600,rsiz=262144,wsiz=262144,nconnect=8,bg,noatime,n
oalock 0 0
```

Quebrar e excluir peering de replicação

Em caso de failover de desastres, os volumes de destino devem ser desagregados para que o host de destino possa montar os volumes para operações de leitura e gravação.



Para o volume de DADOS HANA, você precisa restaurar o volume para o backup instantâneo HANA mais recente criado com o AzAcSnap. Esta operação de reversão de volume não é possível se o snapshot de replicação mais recente for marcado como ocupado devido ao peering de replicação. Portanto, você também deve excluir o peering de replicação.

As próximas duas capturas de tela mostram a operação de peering de quebra e exclusão do volume de dados HANA. As mesmas operações devem ser executadas também para o backup de log e o volume compartilhado HANA.

Ir-sap-pool-premium/PR1-data-mnt0001-sm-dest

PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest)

Volume

Search (Ctrl+/)

«

✎ Edit

✂ Break peering

🗑 Delete

🔄 Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Essentials

End point type : Destination

Healthy : Healthy

Mirror state : Mirrored

Source

Relationship status

Replication schedule

Total progress

Show data for last:

1 hour

6 hours

12 hours

1 day

7 days

Volume replication lag time

9.72hours

8.33hours

6.94hours

5.56hours

Is volume replication transfer

100

90

80

70

60

50

Break replication peering

Break replication peering

Warning! This action will stop data replication between the volumes and might result in loss of data.

Type 'yes' to proceed

yes

Ir-sap-pool-premium/PR1-data-mnt0001-sm-dest

PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest)

Volume

Search (Ctrl+/)

«

↺ Resync

🗑 Delete

🔄 Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Essentials

End point type : Destination

Healthy : Healthy

Mirror state : Broken

Source

Relationship status

Replication schedule

Total progress

Show data for last:

1 hour

6 hours

12 hours

1 day

7 days

Volume replication lag time

1.67min

1.5min

1.33min

1.17min

1min

50sec

Is volume replication transfer

100

90

80

70

60

50

Delete replication

Delete replication object

Warning this operation will delete the connection between PR1-data-mnt0001 and PR1-data-mnt0001-sm-dest

This will delete the replication object of PR1-data-mnt0001, type 'yes' to proceed

yes

Como o peering de replicação foi excluído, é possível reverter o volume para o backup de snapshot HANA mais recente. Se o peering não for excluído, a seleção do volume de reversão é cinza e não é selecionável. As duas capturas de tela a seguir mostram a operação de reversão de volume.



PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest) | Snapshots



Search (Ctrl+/)



+ Add snapshot Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Monitoring

Metrics

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Search snapshots

Name	↑↓	Location	↑↓	Created	↑↓
azacsnap__2021-02-18T120002-2150721Z		West US		02/18/2021, 01:00:05 PM	...
azacsnap__2021-02-18T160002-1442691Z		West US		02/18/2021, 05:00:49 PM	...
azacsnap__2021-02-18T200002-0758687Z		West US		02/18/2021, 09:00:05 PM	...
azacsnap__2021-02-19T000002-0039686Z		West US		02/19/2021, 01:00:05 AM	...
azacsnap__2021-02-19T040001-8773748Z		West US		02/19/2021, 05:00:06 AM	...
azacsnap__2021-02-19T080001-5198653Z		West US		02/19/2021, 09:00:05 AM	...
azacsnap__2021-02-19T120002-1495322Z		West US		02/19/2021, 01:00:06 PM	...
azacsnap__2021-02-19T160002-3698678Z		West US		02/19/2021, 05:00:05 PM	...
azacsnap__2021-02-22T120002-3145398Z		West US		02/22/2021, 01:00:06 PM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...		West US		02/22/2021, 03:32:00 PM	...
azacsnap__2021-02-22T160002-0144647Z		West US		02/22/2021, 05:00:05 PM	...
azacsnap__2021-02-22T200002-0649581Z		West US		02/22/2021, 09:00:05 PM	...
azacsnap__2021-02-23T000002-0311379Z		West US		02/23/2021, 01:00:05 PM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...		West US		02/23/2021, 01:10:00 PM	...

- Restore to new volume
- Revert volume
- Delete



PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest) | Snapshots

Search (Ctrl+/)



+ Add snapshot Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Monitoring

Metrics

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Search snapshots

Name	↑↓	Location
azacsnap__2021-02-18T120002-2150721Z		West US
azacsnap__2021-02-18T160002-1442691Z		West US
azacsnap__2021-02-18T200002-0758687Z		West US
azacsnap__2021-02-19T000002-0039686Z		West US
azacsnap__2021-02-19T040001-8773748Z		West US
azacsnap__2021-02-19T080001-5198653Z		West US
azacsnap__2021-02-19T120002-1495322Z		West US
azacsnap__2021-02-19T160002-3698678Z		West US
azacsnap__2021-02-22T120002-3145398Z		West US
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...		West US
azacsnap__2021-02-22T160002-0144647Z		West US
azacsnap__2021-02-22T200002-0649581Z		West US
azacsnap__2021-02-23T000002-0311379Z		West US
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...		West US

Revert volume to snapshot



Revert volume PR1-data-mnt0001-sm-dest to snapshot azacsnap__2021-...

⚠ This action is irreversible and it will delete all the volumes snapshots that are newer than azacsnap__2021-02-23T000002-0311379Z. Please type 'PR1-data-mnt0001-sm-dest' to confirm.

Are you sure you want to revert 'PR1-data-mnt0001-sm-dest' to state of 'azacsnap__2021-02-23T000002-0311379Z'?

PR1-data-mnt0001-sm-dest ✓

Após a operação de reversão de volume, o volume de dados é baseado no backup instantâneo HANA consistente e agora pode ser usado para executar operações de recuperação.



Se um pool de capacidade com uma categoria de baixa performance tiver sido usado, os volumes precisam ser movidos para um pool de capacidade que possa fornecer a performance necessária.

Monte os volumes no host de destino

Os volumes agora podem ser montados no host de destino, com base no `/etc/fstab` arquivo criado anteriormente.

```
vm-pr1:~ # mount -a
```

A saída a seguir mostra os sistemas de arquivos necessários.

```

vm-pr1:~ # df
Filesystem                                1K-blocks      Used
Available Use% Mounted on
devtmpfs                                  8201112         0
8201112   0% /dev
tmpfs                                     12313116         0
12313116   0% /dev/shm
tmpfs                                     8208744        9096
8199648   1% /run
tmpfs                                     8208744         0
8208744   0% /sys/fs/cgroup
/dev/sda4                                29866736    2543948
27322788   9% /
/dev/sda3                                1038336       79984
958352    8% /boot
/dev/sda2                                 524008        1072
522936    1% /boot/efi
/dev/sdb1                                32894736     49180
31151556   1% /mnt
10.0.2.4:/PR1-log-mnt00001-dr            107374182400    6400
107374176000   1% /hana/log/PR1/mnt00001
tmpfs                                     1641748         0
1641748   0% /run/user/0
10.0.2.4:/PR1-shared-sm-dest/hana-shared 107377178368 11317248
107365861120   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 107377178368 11317248
107365861120   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest             107379678976 35249408
107344429568   1% /hanabackup
10.0.2.4:/PR1-data-mnt0001-sm-dest       107376511232 6696960
107369814272   1% /hana/data/PR1/mnt00001
vm-pr1:~ #

```

Recuperação de banco de DADOS HANA

A seguir mostra as etapas para a recuperação do banco de dados HANA

Inicie os serviços SAP necessários.

```
vm-pr1:~ # systemctl start sapinit
```

A saída a seguir mostra os processos necessários.

```

vm-pr1:/ # ps -ef | grep sap
root      23101      1  0 11:29 ?          00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm    23191      1  3 11:29 ?          00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm    23202      1  5 11:29 ?          00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root      23292      1  0 11:29 ?          00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root      23359    2597  0 11:29 pts/1      00:00:00 grep --color=auto sap

```

As subseções a seguir descrevem o processo de recuperação com e sem recuperação avançada usando os backups de log replicados. A recuperação é executada usando o script de recuperação HANA para o banco de dados do sistema e os comandos hdbsql para o banco de dados do locatário.

Recuperação para o ponto de salvamento mais recente DO backup de volume de DADOS HANA

A recuperação para o mais recente backup savepoint é executada com os seguintes comandos como usuário pr1adm:

- Base de dados do sistema

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG"
```

- Banco de dados do locatário

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

Você também pode usar O HANA Studio ou o Cockpit para executar a recuperação do sistema e do banco de dados do locatário.

A saída do comando a seguir mostra a execução da recuperação.

Recuperação de banco de dados do sistema

```

pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: =====2021-02-19 14:32:16 =====
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00 P0027646      177bab4d610 INFO      RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>

```

Recuperação de banco de dados do locatário

Se uma chave de armazenamento de usuário não tiver sido criada para o usuário pr1adm no sistema de origem, uma chave deve ser criada no sistema de destino. O usuário do banco de dados configurado na chave deve ter Privileges para executar operações de recuperação de locatário.

```

pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>

```

A recuperação do locatário é agora executada com hdbsql.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

O banco de DADOS HANA agora está ativo e o fluxo de trabalho de recuperação de desastres do banco de DADOS HANA foi testado.

Recuperação com recuperação avançada usando backups de log/catálogo

Os backups de log e o catálogo de BACKUP HANA estão sendo replicados a partir do sistema de origem.

A recuperação usando todos os backups de log disponíveis é executada com os seguintes comandos como usuário pr1adm:

- Base de dados do sistema

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Banco de dados do locatário

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```



Para recuperar usando todos os logs disponíveis, você pode usar a qualquer momento no futuro como o carimbo de data/hora na instrução de recuperação.

Você também pode usar O HANA Studio ou o Cockpit para executar a recuperação do sistema e do banco de dados do locatário.

A saída do comando a seguir mostra a execução da recuperação.

Recuperação de banco de dados do sistema

```

prladm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: =====2021-02-19 16:06:40 =====
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00 P0009897 177bb0b4416 INFO RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs

```

Recuperação de banco de dados do locatário

```

prladm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
      \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>

```

O banco de DADOS HANA agora está ativo e o fluxo de trabalho de recuperação de desastres do banco de DADOS HANA foi testado.

Verifique a consistência dos backups de log mais recentes

Como a replicação do volume de backup de log é realizada independentemente do processo de backup de log executado pelo banco de dados SAP HANA, pode haver arquivos de backup de log abertos e inconsistentes no local de recuperação de desastres. Somente os arquivos de backup de log mais recentes podem ser inconsistentes, e esses arquivos devem ser verificados antes que uma recuperação avançada seja executada no site de recuperação de desastres usando a `hdbbackupcheck` ferramenta.

Se a `hdbbackupcheck` ferramenta relatar um erro para os backups de log mais recentes, o conjunto mais recente de backups de log deve ser removido ou excluído.

```
prladm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivercache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

A verificação deve ser executada para os arquivos de backup de log mais recentes do sistema e do banco de dados do locatário.

Se a `hdbbackupcheck` ferramenta relatar um erro para os backups de log mais recentes, o conjunto mais recente de backups de log deve ser removido ou excluído.

Histórico de atualizações

As seguintes alterações técnicas foram feitas a esta solução desde a sua publicação original.

Versão	Data	Atualizar resumo
Versão 1,0	Abril de 2021	Versão inicial

Recuperação de desastres do SAP HANA com replicação de storage

Este documento fornece uma visão geral das opções de proteção contra desastres para SAP HANA. Inclui informações detalhadas de configuração e uma descrição de caso de uso de uma solução de recuperação de desastres em três sites, baseada em replicação de armazenamento NetApp SnapMirror síncrona e assíncrona. A solução descrita utiliza NetApp SnapCenter com o plug-in SAP HANA para gerenciar a consistência do banco de dados.

Autor: Nils Bauer, NetApp

<https://www.netapp.com/pdf.html?item=/media/8584-tr4646pdf.pdf>

Backup e recuperação do SAP HANA usando NetApp Storage Systems e o software Commvault

Este documento descreve o projeto de uma solução da NetApp e Commvault para SAP HANA, que inclui a tecnologia de gerenciamento de snapshots Commvault IntelliSnap e a tecnologia Snapshot da NetApp. A solução é baseada no armazenamento NetApp e no pacote de proteção de dados Commvault.

Autores: Marco Schoen, NetApp; Dr. Tristan Daude, CommVault Systems

<https://www.netapp.com/pdf.html?item=/media/17050-tr4711pdf.pdf>

Integração SnapCenter para banco de dados SAP ASE

Este documento descreve as especificidades de integração do SnapCenter para o banco de dados SAP ASE usado em um ambiente SAP.

Introdução

O documento não se destina a ser uma descrição passo a passo de como configurar o ambiente completo, mas abrange conceitos e detalhes relevantes relacionados com:

- Exemplo de visão geral da configuração
- Esquema da amostra
- Proteger a instância do SAP ASE
- Restaurar e recuperar instância do SAP ASE

Autor: Michael Schlosser, NetApp

Exemplo de visão geral da configuração

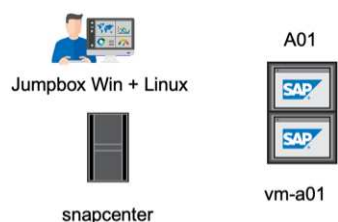
Exemplo de implementação para o plug-in SnapCenter ASE para um sistema SAP em execução na Plataforma Azure.



Esta implementação descreve a configuração mínima de volume necessária. Os backups de despejo de dados e os backups de despejo de Registro são configurados de acordo com a SAP Note 1588316.

Alternativamente, a estrutura de volume descrita neste "Blog da Comunidade Técnica MS" documento pode ser usada.

Ambiente de demonstração



Versões de software

Software	Versão
OS do Linux	SLES PARA SAP 15 SP5
SAP	SAP NetWeaver 7,5
SAP ASE	16,0 SP04 PL06 HF1
SnapCenter	6,1

Design de volume ASE

O layout do menor volume a seguir deve ser usado para habilitar casos de uso de backup/recuperação e clonar para o banco de dados SAP ASE. A configuração de exemplo usa <SID>: A01.

Nome do volume	Diretório (qtree) no volume	Ponto de montagem no servidor	Comentário
<SID>-sapase	sybase	/sybase	Diretório pai para arquivos relacionados ASE
		/Sybase/<SID>/backups	Backups de despejo de dados (podem ser colocados em um volume diferente)
		/Sybase/<SID>/log_archives	Backups de despejo de log (podem ser colocados em um volume diferente)
	<sid>.adm	/home/<sid>adm	Diretório base do usuário <sid>.adm
	usrsaptrans	/usr/sap/trans	Diretório de transporte
	Ursap<SID>	/Urs/sap/<SID>	Usr SAP
	Sapmnt<SID>	/Sapmnt/<SID>	SAP GlobalHost dir

Nome do volume	Diretório (qtree) no volume	Ponto de montagem no servidor	Comentário
<SID>-datalog	sapdata_1	/Sybase/<SID>/sapdata_1	Dados BD (SID)
	saplog_1	/Sybase/<SID>/saplog_1	Registo BD (SID)
	saptemp	/Sybase/<SID>/saptemp	PSAPTEMP
	sybsecurity	/Sybase/<SID>/sybsecurity	Banco de dados de segurança Sybase
	sistema sybssystem	/Sybase/<SID>/sybssystem	Sybase System DB
	sybtemp	/Sybase/<SID>/sybtemp	Sistema Sybase DB - Temp
	sapdiag	/Sybase/<SID>/sapdiag	base de dados 'saptools'

Passos para proteger banco de dados A01

- Verifique a distribuição do ficheiro, de acordo com o esquema da amostra
- Verificar pré-requisitos para o host (vm-A01)
- Verificar pré-requisitos para a base de dados (A01)
- Implantar / instalar o agente SnapCenter no host (vm-A01)
- Criar Configuração de recurso de instância do SnapCenter

Pré-requisitos no Host

Mais informações atuais podem estar disponíveis ["aqui"](#).

Antes de adicionar um host e instalar o pacote de plug-ins para Linux, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você pode usar a autenticação baseada em senha para o usuário root ou não root ou autenticação baseada em chave SSH.
- O plug-in do SnapCenter para sistemas de arquivos Unix pode ser instalado por um usuário não-root. No entanto, você deve configurar o sudo Privileges para que o usuário não-root instale e inicie o processo de plug-in. Depois de instalar o plug-in, os processos serão executados como um usuário não-root eficaz.
- Crie credenciais com o modo de autenticação como Linux para o usuário de instalação.
- Você deve ter instalado o Java 11 em seu host Linux.
- Certifique-se de ter instalado apenas a edição certificada DO Java 11 no host Linux
- Para obter informações sobre O download DO JAVA, consulte: Downloads Java para todos os sistemas operacionais
- Você deve ter bash como o shell padrão para instalação de plug-in.

Pré-requisitos para a base de dados – Ativar registo e cópias de segurança

- Criar diretórios para backups e log_archives (/sybase/A01/backups, /sybase/A01/log_archives)
- Conetar ao banco de dados A01 (como usuário do sistema operacional syba01)

- grant role sa_role,sso_role,oper_role,sybase_ts_role para backup
- vá

Implante o agente do SnapCenter no host vm-A01

Mais informações podem ser encontradas no ["Documentação do SnapCenter"](#).

Selecione Plug-ins SAP ASE e Unix File Systems.

Add Host

Host Type

Linux

Host Name

vm-a01

Credentials

snapcenter-linux

+

i

Select Plug-ins to Install

SnapCenter Plug-ins Package 6.1 for Linux

☐ IBM DB2	☐ MongoDB
☐ MySQL	☐ Oracle Applications <i>i</i>
☐ Oracle Database	☒ SAP ASE
☐ PostgreSQL	☐ SAP MaxDB
☐ SAP HANA	☐ Storage <i>i</i>
☒ Unix File Systems	

⚙ [More Options](#): Port, Install Path, Custom Plug-Ins...

Submit

Cancel

Criar configuração de recurso de instância do SnapCenter para banco de dados A01

Recursos → SAP ASE → Adicionar recursos

Add SAP ASE Resource

1 Name

2 Storage Footprint

3 Resource Settings

4 Summary

Provide Resource Details

Name

A01

Host Name

vm-a01.1h05kdpkcgaujd4qsseqldygg.bx.internal.cloudapp.net

Type

Instance

Credential Name

None

Add information for the credential

Credential Name

sapsa-A01

Username

sapsap

Password

Add

Previous

Next



Se a Senha contiver caracteres especiais, eles devem ser mascarados com uma barra invertida. Por exemplo, teste!123! → Teste!123!

Add SAP ASE Resource

1 Name

2 Storage Footprint

3 Resource Settings

4 Summary

Provide Resource Details

Name

A01

Host Name

vm-a01.1h05kdpkcgaujd4qsseqldygg.bx.internal.cloudapp.net

Type

Instance

Credential Name

sapsa-A01

Previous

Next

1 Name

2 Storage Footprint

3 Resource Settings

4 Summary

Provide Storage Footprint Details

Storage Type ☐ ONTAP ☐ Azure NetApp Files

Storage Systems for storage footprint

SAP-EastUS	A01-datalog		
------------	-------------	--	--

Modify SAP-EastUS

Select one or more Capacity pools and their associated Volumes

Capacity pool	Volume
sap-premium-mqos	A01-datalog

Save



Se estiver a utilizar o design do volume a partir do ["Blog da Comunidade Técnica MS"](#).

Volumes /vol<SID>_base, /vol<SID>_data, /vol<SID>_log deve ser configurado como espaço físico de storage

Os pares de chave-valor personalizados devem ser feitos (pelo menos).

Add SAP ASE Resource

1 Name
2 Storage Footprint
3 Resource Settings
4 Summary

Resource Settings

Custom key-value pairs for SAP ASE plug-in

Name	Value	
SYBASE_ISQL_CMD	isql -X	✕
SYBASE_USER	syba01	✕
SYBASE_SERVER	A01	✕
SYBASE_EXCLUDE_TEMPDB	Y	✕
SYBASE_DATABASES_EXCLUDE	saptempdb	+ ✕

Previous
Next

A tabela a seguir lista os parâmetros do plug-in Sybase, fornece suas configurações e os descreve:

Parâmetro	* Definição*	Descrição
SYBASE_ISQL_CMD	Exemplo: /Opt/sybase/OCS-15__0/bin/isql -X.	Define o caminho para o comando isql. Opções disponíveis: https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc34237.1500/html/mvsinst/CIHHFDGC.htm
SYBASE_USER	nome_utilizador	Especifica o usuário do sistema operacional que pode executar o comando isql. Este parâmetro é necessário para UNIX. Esse parâmetro é necessário se o usuário executando os comandos Snap Creator Agentstart e stop (geralmente o usuário raiz) e o usuário executando o comando isql forem diferentes.
SYBASE_SERVER	data_server_name	Especifica o nome do servidor de dados Sybase (-S opção no comando isql).por exemplo: A01

Parâmetro	* Definição*	Descrição
SYBASE_DATABASES	db_name:user_name/pas sword	Lista os bancos de dados dentro da instância para fazer backup. O banco de dados mestre é adicionado; por exemplo: DBAtest2:sa/53616c7404351e.se um banco de dados chamado "ALL" for usado, então a descoberta automática do banco de dados é usada, e os bancos de dados sybsyntax, sybssystemprocs, e tempdb são excluídos. Por exemplo: TODAS AS senhas criptografadas:sa/53616c71a6351e são suportadas se o parâmetro NTAP_PWD_PROTECTION estiver definido.
SYBASE_DATABASES_EXCLUDE	db_name	Permite que os bancos de dados sejam excluídos se o constructo "ALL" for usado. Você pode especificar vários bancos de dados usando uma lista separada por ponto-e-vírgula.por exemplo, pubs2;test_db1
SYBASE_TRAN_DUMP	db_name:directory_path	Permite que você execute um despejo de transação Sybase depois de criar uma cópia Snapshot.por exemplo: pubs2:/sybasedumps/pubs2 você deve especificar cada banco de dados que requer um despejo de transação.
SYBASE_TRAN_DUMP_FORMAT	%S_%D_%T.CMN	Permite especificar a convenção de nomenclatura dump. As seguintes chaves podem ser especificadas: %S Nome da instância DO SYBASE_SERVER %D base de dados DO SYBASE_DATABASES %T carimbo de data/hora único aqui está um exemplo: %S_%D_%T.log
SYBASE_TRAN_DUMP_COMPRESS	(Y / N)	Ativa ou desativa a compressão de despejo de transação Sybase nativa.
SYBASE	Exemplo: /Sybase	Especifica o local da instalação do Sybase.
SYBASE_MANIFEST	Exemplo: A01:/sybase/A01/sapdiag	Especifica os bancos de dados para os quais o arquivo de manifesto deve ser criado, juntamente com o local onde o arquivo de manifesto deve ser colocado.
SYBASE_MANIFEST_FORMAT	%S__%D_.exemplo de manifesto: %S_%D_.MANIFEST	Permite que você especifique a convenção de nomenclatura de arquivos MANIFEST. As seguintes chaves podem ser especificadas: %S Nome da instância DE SYBASE_SERVER %D base de dados DE SYBASE_DATABASES
SYBASE_MANIFEST_DELETE	(Y / N)	Permite que o manifesto seja excluído após a cópia Snapshot ter sido criada. O arquivo de manifesto deve ser capturado na cópia Snapshot para que ele esteja sempre disponível com o backup.
SYBASE_EXCLUDE_TEMPDB	(Y / N)	Permite a exclusão automática de bancos de dados temporários criados pelo usuário.

Sequência para recuperar o sistema A01

- 1. Pare o SAP System A01 (incluindo banco de dados), pare o sapinit
- 2. Sistemas de arquivos umount
- 3. Restaurar volumes A01-datalog (usando SnapCenter)
- 4. Montar sistemas de arquivos
- 5. Inicie o Banco de dados A01 (com opção -q, para evitar o acesso automático online e manter o banco de dados recuperável – de acordo com a SAP Note 1887068)
- 6. Inicie o BackupServer A01
- 7. saptools de banco de dados on-line, sybsecurity , sybmgmtldb
- 8. Recuperar Banco de dados A01 (usando isql)
- 9. Base de dados online A01
- 10. Inicie o sapinit, SAP System A01

Recuperar instância A01

- Pare o SAP System e o DB A01 no host vm-A01
 - Utilizador a01adm: Stopsap
 - Root do usuário: /Etc/init.d/sapinit stop
 - Root do usuário: Umount -a -t nfs
- Restaurar cópia de segurança
 - SnapCenter GUI: Selecione Backup necessário para Restauração

Manage Copies

6 Backups
0 Clones
Local copies

3 Backups
Backups

Summary Card

9 Backups
0 Clones

Primary Backup(s)

search

Restore
Clone Restore Delete

Backup Name	Snapshot Lock Expiration	Count	End Date
SnapCenter_sybase_ondemand_02-07-2025_13_23_21_3633		1	02/07/2025 1:23:58 PM
SnapCenter_sybase_daily_02-07-2025_11_08_28_9176		1	02/07/2025 11:09:07 AM
SnapCenter_sybase_ondemand_02-07-2025_09_31_42_2639		1	02/07/2025 9:32:23 AM
SnapCenter_sybase_daily_02-06-2025_16_35_19_5734		1	02/06/2025 4:36:32 PM
SnapCenter_sybase_ondemand_02-06-2025_16_34_01_6115		1	02/06/2025 4:34:36 PM
SnapCenter_sybase_ondemand_02-06-2025_15_41_33_6630		1	02/06/2025 3:42:21 PM

- Para implantação do ANF: Somente recurso completo está disponível

Restore from SnapCenter_sybase_ondemand_02-07-2025_13_23_21_3633

1 Restore scope

2 PreOps

3 PostOps

4 Notification

Select the restore types

☒ Complete Resource *i*



A seleção de recurso completo acionará uma Restauração Snap baseada em volume (VBSR). Dentro do Azure é chamado "[reverter volume](#)".

i Important

Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.



Para outros tipos de implantação (por exemplo, ANF no local), uma operação SFSR (Single File Snap Restore) pode ser orquestrada. Selecione File Level (nível de ficheiro) e o volume e marca de verificação "All" (todos) – consulte a seguinte captura de ecrã.

Restore from SnapCenter_sybase_ondemand_02-10-2025_18.16.17.1615

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Select the restore types

☐ Complete Resource

☒ File Level

Select files to restore

Volume/Qtree	All	File Path
☒ svm-sap01.muccbc.hq.netapp.com:/vol/A0...	☒	Provide one or more file paths separated by comma
☐ svm-sap01.muccbc.hq.netapp.com:/vol/A0...		

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

O resumo seria exibido e com concluir a restauração real é iniciada.

Restore from SnapCenter_sybase_ondemand_02-07-2025_13_23_21_3633

1 Restore scope
2 PreOps
3 PostOps
4 Notification
5 Summary

Summary

Backup Name	SnapCenter_sybase_ondemand_02-07-2025_13_23_21_3633
Backup date	02/07/2025 1:23:58 PM
Restore scope	Complete Resource
Pre restore command	
Unmount command	
Mount command	
Post restore command	
Send email	No

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Finish

- Montar sistemas de arquivos (vm-A01)
 - Raiz do usuário: Mount -a -t nfs
- Iniciar base de dados A01 e BackupServer
 - Modificar RUN_A01 e adicionar -q (de acordo com SAP Note 1887068)
 - Utilizador syba01: RUN_A01 &
 - Utilizador syba01: RUN_A01_BS&
- Bancos de dados on-line sapttools, sybsecurity , sybmgtmdb
 - Usuário syba01: Isql -S A01 -U sapsa -X -W 1024
 - sapttools de banco de dados on-line
 - vá
 - segurança de banco de dados on-line
 - vá
 - banco de dados online sybmtdb
 - vá

Documentação externa

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- "SAP Instalação Azure no ANF"
- "Pré-requisitos do SnapCenter para Plugins"
- "SnapCenter Instalar Plugins"
- "Sybase Infocenter - isql"
- "Sybase Infocenter - carregar despejo de log de transações"
- SAP Notes (login necessário)
 - 1887068 - SYB: Usando backup externo e restauração com SAP ASE: <https://me.sap.com/notes/1887068/E>
 - 1618817 - SYB: Como restaurar um servidor de banco de dados SAP ASE (UNIX): <https://me.sap.com/notes/1618817/E>
 - 1585981 - SYB: Garantindo recuperabilidade para SAP ASE: <https://me.sap.com/notes/1585981/E>
 - 1588316 - SYB: Configurar backups automáticos de banco de dados e log: <https://me.sap.com/notes/1588316/E>
 - Documentação do produto NetApp: <https://www.netapp.com/support-and-training/documentation/>
 - "Soluções SAP da NetApp – informações sobre casos de uso, práticas recomendadas e benefícios"

Histórico de versões

Versão	Data	* Histórico de versões do documento*
Versão 1,0	Abril de 2025	Versão inicial – backup / recuperação de banco de dados ASE

Integração do SnapCenter para o banco de dados IBM DB2

Este documento descreve as especificidades de integração do SnapCenter para o banco de dados IBM DB2 usado em um ambiente SAP.

Introdução

O documento não se destina a ser uma descrição passo a passo de como configurar o ambiente completo, mas abrange conceitos e detalhes relevantes relacionados com:

- Exemplo de visão geral da configuração
- Esquema da amostra
- Proteja o banco de dados DB2
- Restaurar e recuperar banco de dados DB2

Autor: Michael Schlosser, NetApp

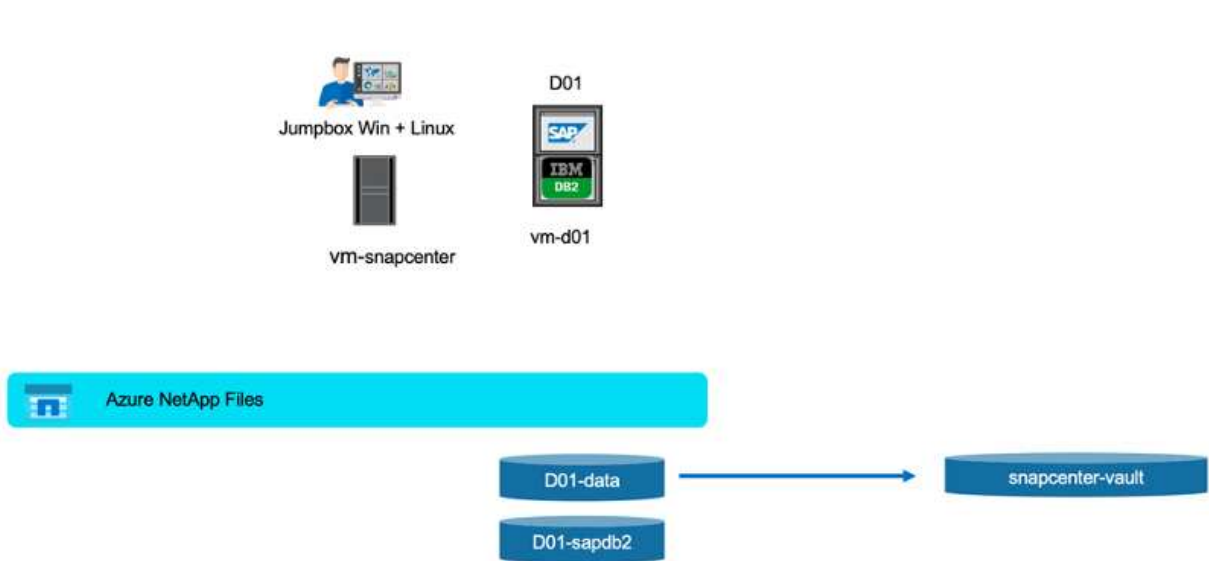
Exemplo de visão geral da configuração

Exemplo de implementação para o Plugin SnapCenter DB2 para um sistema SAP em execução na Plataforma Azure.



Esta implementação descreve a configuração mínima de volume necessária.

Alternativamente, a estrutura de volume descrita neste ["Blog da Comunidade Técnica MS"](#) documento pode ser usada.



Ambiente de demonstração

Versões de software

Software	Versão
OS do Linux	SLES PARA SAP 15 SP5
SAP	SAP NetWeaver 7,5
DB2	10.5.0.7
SnapCenter	6,1

DB2 Design de volume

O layout de menor volume a seguir deve ser usado para habilitar casos de uso de backup/recuperação e clonar para o banco de dados DB2. A configuração de exemplo usa <SID>: D01.

Nome do volume	Diretório (qtree) no volume	Ponto de montagem no servidor	Comentário
<SID>-sapdb2	db2	/db2	
		/DB2/<SID>	Diretório pai para arquivos relacionados ao DB2

Nome do volume	Diretório (qtree) no volume	Ponto de montagem no servidor	Comentário
		/db2/db2<sid>	Diretório base do usuário db2<sid> e software DB2
		/DB2/<SID>/db2dump	DB2 arquivos de log de diagnóstico e despejo
		/DB2/<SID>/backup	Dlocation de backup (pode ser colocado em um volume diferente)
		/DB2/<SID>/log_arch	Registos de remarcação offline (podem ser colocados num volume diferente – o instantâneo será acionado)
		/DB2/<SID>/log_dir	Registos de remarcação online (podem ser colocados num volume diferente – o instantâneo será acionado)
	<sid>.adm	/home/<sid>adm	Diretório base do usuário <sid>.adm
	sap<sid>	/home/sap<sid>	Diretório base do usuário sap<sid>
	usrsaptrans	/usr/sap/trans	Diretório de transporte
	Usrsap<SID>	/Usr/sap/<SID>	Usr SAP
	Sapmnt<SID>	/Sapmnt/<SID>	SAP GlobalHost dir
<SID>-data	sapdata1	/DB2/<SID>/sapdata1	Dados DB
	sapdata2	/DB2/<SID>/sapdata2	Dados DB
	sapdata3	/DB2/<SID>/sapdata3	Dados DB
	sapdata4	/DB2/<SID>/sapdata4	Dados DB
	saptmp1	/DB2/<SID>/saptmp1	Ficheiros Temp BD
	saptmp2	/DB2/<SID>/saptmp2	Ficheiros Temp BD
	saptmp3	/DB2/<SID>/saptmp3	Ficheiros Temp BD
	saptmp4	/DB2/<SID>/saptmp4	Ficheiros Temp BD
	db2<sid>	/DB2/<SID>/db2<sid>	Arquivos de instância

Como a descoberta automática está ativada por padrão para o plug-in DB2, um snapshot é criado para volumes que correspondem aos seguintes caminhos de arquivo.

```

Database StoragePath      /db2/D01/saptmp4/, /db2/D01/saptmp3/, /db2/D01/saptmp2/, /db2/D01/saptmp1/,
                          /db2/D01/sapdata4/, /db2/D01/sapdata3/, /db2/D01/sapdata2/, /db2/D01/sapdata1/

Database LogPath          /db2/D01/log_dir/NODE0000/LOGSTREAM0000/

Database Archive Path (Primary) DISK:/db2/D01/log_arch/

```


Passos para proteger banco de dados D01

- Verifique a distribuição do ficheiro, de acordo com o esquema da amostra
- Verificar pré-requisitos para o host (vm-D01)
- Verificar pré-requisitos para a base de dados (D01)
- Implantar / instalar o agente SnapCenter no host (vm-D01)
- Criar Configuração de recurso de instância do SnapCenter

Pré-requisitos no Host

Mais informações atuais podem estar disponíveis aqui:

- https://docs.netapp.com/us-en/snapcenter/protect-scu/reference_prerequisites_for_adding_hosts_and_installing_snapcenter_plug_ins_package_for_linux.html
- <https://docs.netapp.com/us-en/snapcenter/protect-db2/prerequisites-for-using-snapcenter-plug-in-for-ibm-db2.html>

Antes de adicionar um host e instalar o pacote de plug-ins para Linux, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você pode usar a autenticação baseada em senha para o usuário root ou não root ou autenticação baseada em chave SSH.
- O plug-in do SnapCenter para sistemas de arquivos Unix pode ser instalado por um usuário não-root. No entanto, você deve configurar o sudo Privileges para que o usuário não-root instale e inicie o processo de plug-in. Depois de instalar o plug-in, os processos serão executados como um usuário não-root eficaz.
- Crie credenciais com o modo de autenticação como Linux para o usuário de instalação.
- Você deve ter instalado o Java 11 em seu host Linux.
- Certifique-se de ter instalado apenas a edição certificada DO Java 11 no host Linux
- Para obter informações sobre O download DO JAVA, consulte: Downloads Java para todos os sistemas operacionais
- Você deve ter bash como o shell padrão para instalação de plug-in.

Pré-requisitos para a base de dados – Ativar registo e cópias de segurança



para ativar os registos offline, é necessário efetuar uma cópia de segurança completa offline da base de dados. Normalmente, ele já está habilitado para sistemas produtivos.

- Criar diretórios para backup e log_arch (/DB2/D01/backup, /sybase/D01/log_arch)
- Ativar logarchmeth1 (como os-user db2d01)
 - DB2 atualização dB cfg para D01 usando logarchmeth1 DISCO:/DB2/D01/log_arch/
- Criar cópia de segurança offline (como os-user db2d01)
 - db2stop força
 - db2start modo de administração acesso restrito
 - DB2 backup dB D01 para /DB2/D01/backup

- DB2 Ativar dB D01

Implante o agente do SnapCenter no host vm-D01

Mais informações podem ser encontradas no ["Documentação do SnapCenter"](#).

Selecione Plug-ins IBM DB2 e Unix File Systems.

Add Host

Host Type

Linux

Host Name

vm-d01

Credentials

linux-snapcenter

+

i

Select Plug-ins to Install

SnapCenter Plug-ins Package 6.1 for Linux

☒

IBM DB2

☐

MySQL

☐

Oracle Database

☐

PostgreSQL

☐

SAP HANA☒

☐

MongoDB☐

i

☐☐☐

i

⚙

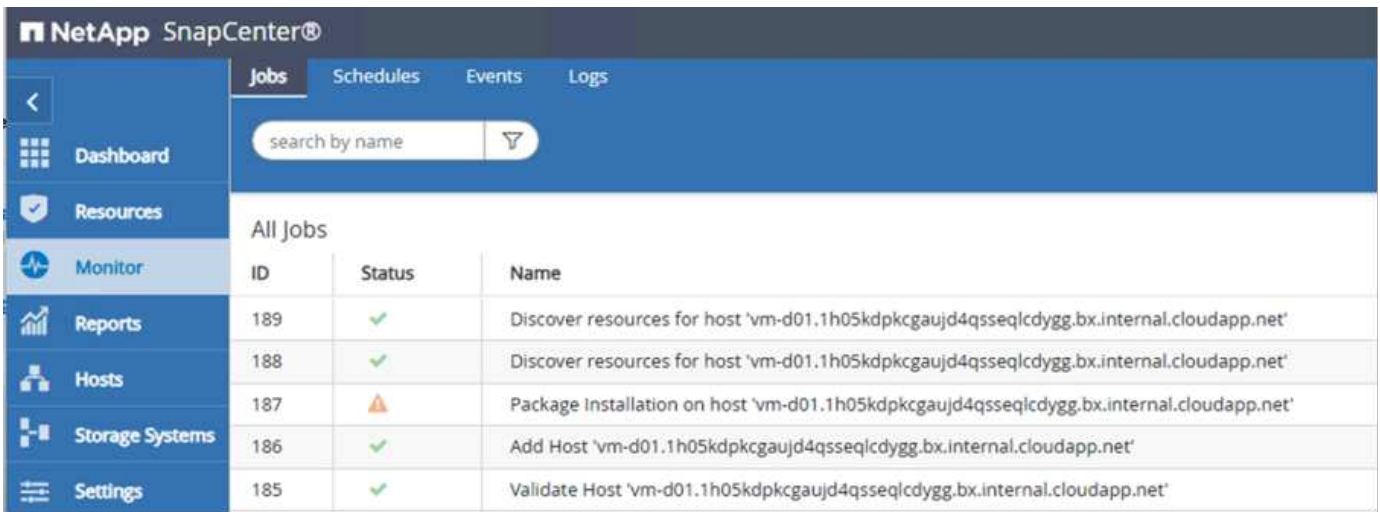
[More Options](#) : Port, Install Path, Custom Plug-Ins...

Submit

Cancel



Após a instalação, uma descoberta dos bancos de dados no host é acionada.



The screenshot shows the NetApp SnapCenter interface with the 'Jobs' tab selected. A sidebar on the left contains navigation links: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, and Settings. The main area displays a table of jobs with columns for ID, Status, and Name. The table lists five jobs, with the first two having a green checkmark status and the others having a yellow warning icon.

ID	Status	Name
189	✓	Discover resources for host 'vm-d01.1h05kdpkcgauj4qsseqldygg.bx.internal.cloudapp.net'
188	✓	Discover resources for host 'vm-d01.1h05kdpkcgauj4qsseqldygg.bx.internal.cloudapp.net'
187	⚠	Package Installation on host 'vm-d01.1h05kdpkcgauj4qsseqldygg.bx.internal.cloudapp.net'
186	✓	Add Host 'vm-d01.1h05kdpkcgauj4qsseqldygg.bx.internal.cloudapp.net'
185	✓	Validate Host 'vm-d01.1h05kdpkcgauj4qsseqldygg.bx.internal.cloudapp.net'

Criar Configuração de recursos para Banco de dados D01

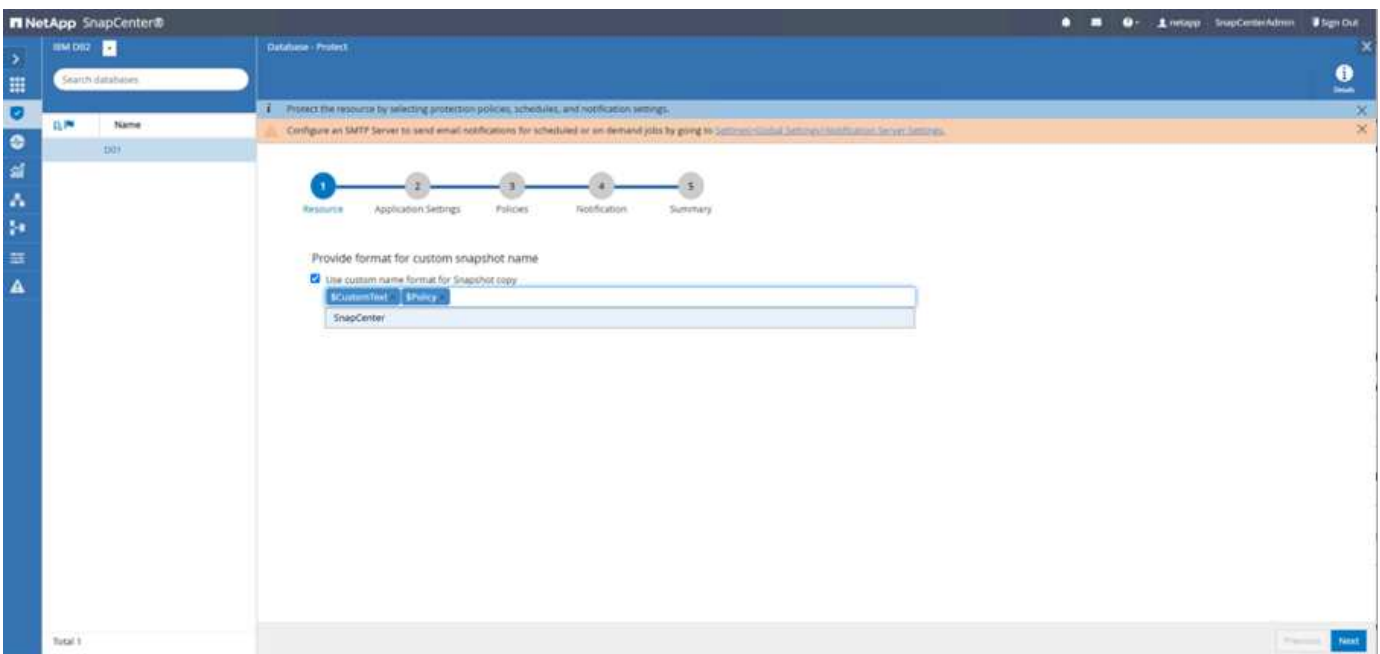
Selecione recurso descoberto D01



The screenshot shows the NetApp SnapCenter interface with the 'Resources' tab selected. A sidebar on the left contains navigation links: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, and Settings. The main area displays a table of resources with columns for Name, Type, Instance, Host, Resource Groups, Policies, Last backup, and Overall Status. The table lists one resource named 'D01' of type 'Database'.

Name	Type	Instance	Host	Resource Groups	Policies	Last backup	Overall Status
D01	Database	db2d01	vm-d01.1h05kdpkcgauj4qsseqldygg.bx.internal.cloudapp.net				Not protected

Configurar o Nome do Snapshot



The screenshot shows the NetApp SnapCenter interface with the 'Protect' tab selected. A sidebar on the left contains navigation links: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, and Settings. The main area displays a wizard for configuring protection for the resource 'D01'. The wizard has five steps: Resource, Application Settings, Policies, Notification, and Summary. The 'Policies' step is currently active. The 'Provide format for custom snapshot name' section is checked, and the format is set to '%Customized% %Policy%'. The 'SnapCenter' checkbox is also checked.

Protect the resource by selecting protection policies, schedules, and notification settings.

Configure an SMTP Server to send email notifications for scheduled or on-demand jobs by going to [Settings>Global Settings>Notification Server Settings](#).

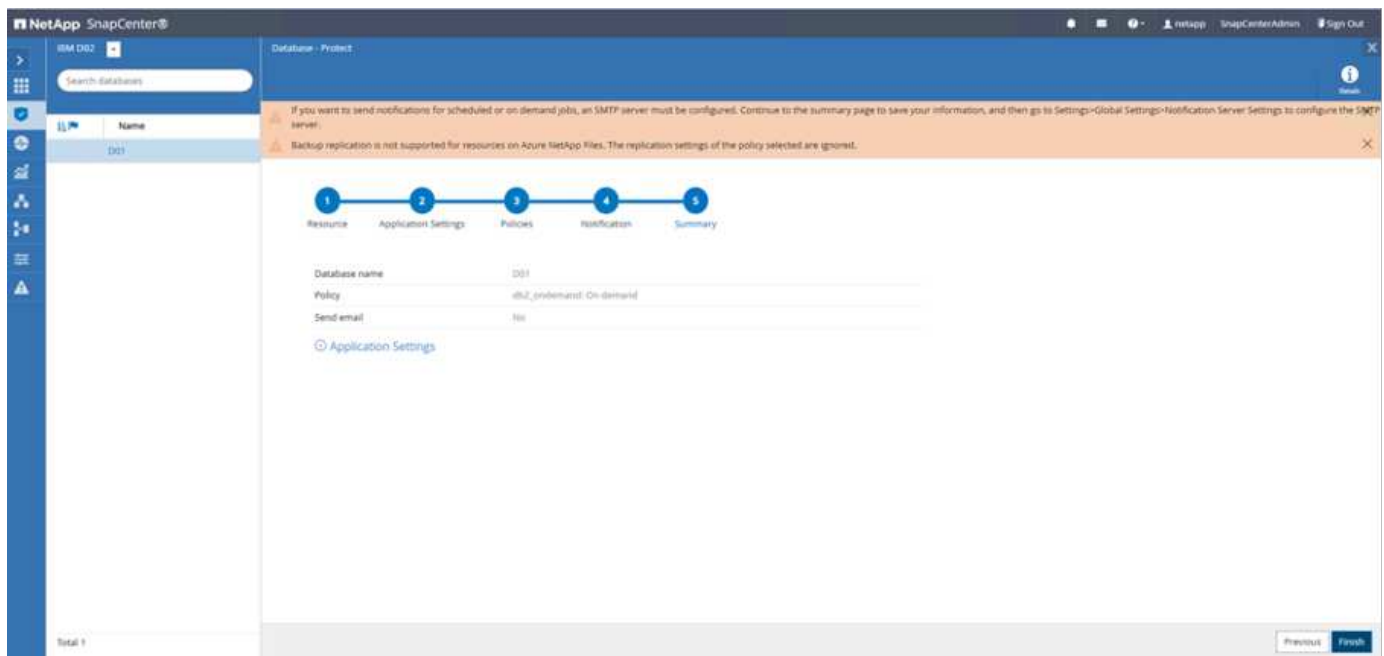
1 Resource 2 Application Settings 3 Policies 4 Notification 5 Summary

Provide format for custom snapshot name

☒ Use custom name format for Snapshot copy

☒ SnapCenter

Não são necessárias definições de aplicação específicas, configure as definições de política e notificação, conforme necessário.



E terminar a configuração.

Sequência para recuperar o sistema D01

1. Parar o SAP System D01 (incluindo banco de dados)
2. Restaurar backup do SnapCenter (volume D01-data)
 - a. Desmontar sistemas de arquivos
 - b. Restaurar volume
 - c. Montar sistemas de arquivos
 - d. Init banco de dados como espelho dB
3. Recuperar banco de dados D01 (usando o rollforward DB2)
4. Inicie o SAP System D01

Recuperar Banco de dados D01

- Pare o SAP System e o DB D01 no host vm-D01
 - Utilizador d01adm: Stopsap
- Restaurar cópia de segurança
 - SnapCenter GUI: Selecione Backup necessário para Restauração



- Para implantação do ANF: Somente recurso completo está disponível



O resumo seria exibido e com concluir a restauração real é iniciada.

Restore from SnapCenter_db2_ondemand_03-26-2025_14_42_07_4144 ✕

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Summary

Backup Name	SnapCenter_db2_ondemand_03-26-2025_14_42_07_4144
Backup date	03/26/2025 2:43:50 PM
Restore scope	Complete Resource without Volume Revert
Pre restore command	
Post restore command	
Send email	No

⚠ If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Finish



"db2inidb D01 como espelho" é feito como parte do fluxo de trabalho de restauração do SnapCenter.

- Verifique recuperar status Banco de dados D01 (como usuário db2d01)
 - DB2 rollforward db D01 status da consulta
- Recuperar banco de dados conforme necessário – aqui uma recuperação sem perda é iniciada (como usuário db2d01)
 - DB2 rollforward dB D01 para o fim dos logs
- Parar recuperação de banco de dados e banco de dados online D01 (como usuário db2d01)
 - DB2 dB rollforward D01 stop
- Iniciar o sistema SAP (como usuário d01adm)
 - startsap

Informações adicionais e histórico de versões

As seguintes demonstrações recodificadas estão disponíveis para suportar a documentação.

Restauração e recuperação de banco de dados DB2

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- "SAP em DB2 Instalação Azure no ANF"
- "Pré-requisitos do SnapCenter para Plugins"
- "SnapCenter Instalar Plugins"
- "Documentação do plug-in do SnapCenter DB2"
- SAP Notes (login necessário)
 - 83000 - DB2/390: Opções de backup e recuperação: <https://me.sap.com/notes/83000>
 - 594301 - DB6: Ferramentas de administração e espelho dividido: <https://me.sap.com/notes/594301>
- Documentação do produto NetApp: <https://www.netapp.com/support-and-training/documentation/>
- "Soluções SAP da NetApp – informações sobre casos de uso, práticas recomendadas e benefícios"

Histórico de versões

Versão	Data	* Histórico de versões do documento*
Versão 1,0	Abril de 2025	Versão inicial – backup / recuperação de banco de dados DB2

Integração SnapCenter para o banco de dados SAP MaxDB

Este documento descreve as especificidades de integração do SnapCenter para o banco de dados SAP MaxDB usado em um ambiente SAP.

Introdução

O documento não se destina a ser uma descrição passo a passo de como configurar o ambiente completo, mas abrange conceitos e detalhes relevantes relacionados com:

- Exemplo de visão geral da configuração
- Esquema da amostra
- Proteja a instância do SAP MaxDB
- Restaure e recupere a instância do SAP MaxDB

Exemplo de visão geral da configuração

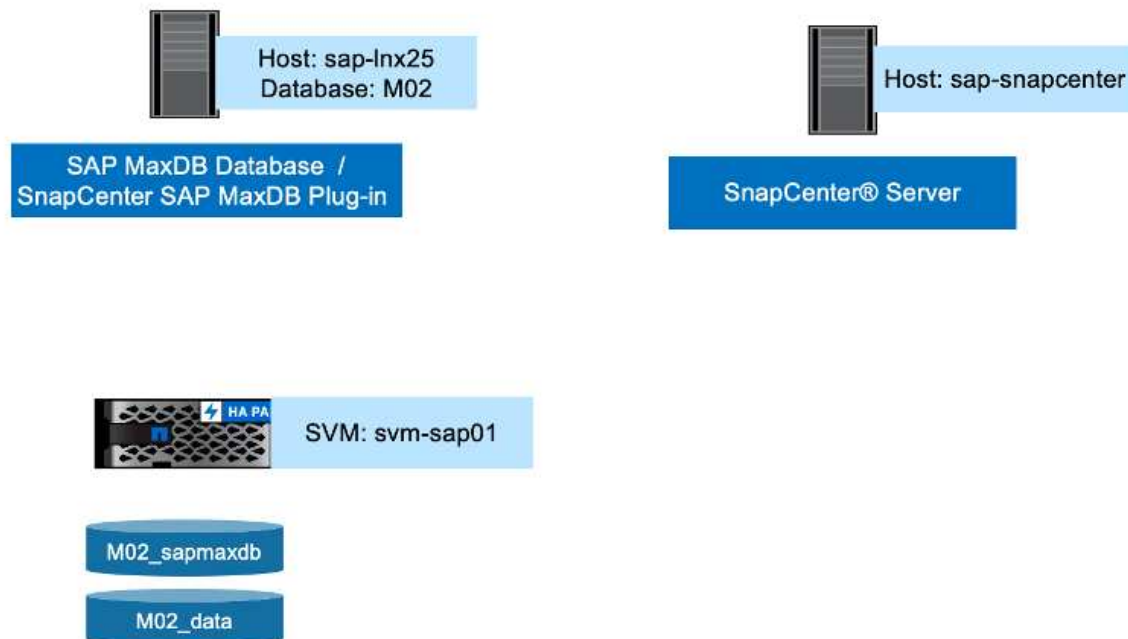
Exemplo de implementação para o Plugin SnapCenter MaxDB para um sistema SAP em execução no nosso Centro de demonstração.



Esta implementação descreve a configuração mínima de volume necessária. Backups de despejo de dados e backups de despejo de log, modelo de backup, etc. são configurados de acordo com SAP Note "1928060 - backup e recuperação de dados com backup do sistema de arquivos" e Notas referenciadas a partir daí.

Alternativamente, a estrutura de volume descrita em "[MS TechCommunity Blog](#)" pode ser usada.

Ambiente de demonstração



Versões de software

Software	Versão
OS do Linux	SLES PARA SAP 15 SP5
SAP	SAP NetWeaver 7,5
SAP MaxDB	DBMServer 7.9.10 build 004-123-265-969
SnapCenter	6,1

MaxDB volume Design

O layout de menor volume a seguir deve ser usado para habilitar casos de uso de backup / recuperação e clonar para o banco de dados SAP MaxDB. A configuração de exemplo usa <SID>: M02.

Nome do volume	Diretório (qtree) no volume	Ponto de montagem no servidor	Comentário
<SID>_sapmaxdb	sapdb	/sapdb	Diretório pai para arquivos relacionados ao MaxDB

Nome do volume	Diretório (qtree) no volume	Ponto de montagem no servidor	Comentário
		/Sapdb/<SID>/saplog	Refazer logs (pode ser colocado em um volume diferente)
		/Sapdb/<SID>/backup	Backups de despejo (dados e log) (podem ser colocados em um volume diferente)
	<sid>.adm	/home/<sid>adm	Diretório base do usuário <sid>.adm
	caixa de distribuição	/home/sdb	Diretório de base do usuário sdb
	<sid>	/home/<sid>	Diretório base do usuário <sid>
	usrsaptrans	/usr/sap/trans	Diretório de transporte
	Usrsap<SID>	/Utr/sap/<SID>	Utr SAP
	Sapmnt<SID>	/Sapmnt/<SID>	SAP GlobalHost dir
<SID>_data	sapdata	/Sapdb/<SID>/sapdata	Arquivos de dados DB (SID)

Passos para proteger banco de dados M02

- Verifique a distribuição do ficheiro, de acordo com o esquema da amostra
- Verificar pré-requisitos para o host (sap-lnx25HANA)
- Verificar pré-requisitos para a base de dados (M02)
- Implantar / instalar o agente SnapCenter no host (sap-lnx25HANA)
- Criar Configuração de recurso de instância do SnapCenter

Pré-requisitos no Host

Mais informações atuais podem estar disponíveis ["aqui"](#).

Antes de adicionar um host e instalar o pacote de plug-ins para Linux, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você pode usar a autenticação baseada em senha para o usuário root ou não root ou autenticação baseada em chave SSH.
- O plug-in do SnapCenter para sistemas de arquivos Unix pode ser instalado por um usuário não-root. No entanto, você deve configurar o sudo Privileges para que o usuário não-root instale e inicie o processo de plug-in. Depois de instalar o plug-in, os processos serão executados como um usuário não-root eficaz.
- Crie credenciais com o modo de autenticação como Linux para o usuário de instalação.
- Você deve ter instalado o Java 11 em seu host Linux.
- Certifique-se de ter instalado apenas a edição certificada DO Java 11 no host Linux
- Para obter informações sobre O download DO JAVA, consulte: Downloads Java para todos os sistemas operacionais
- Você deve ter bash como o shell padrão para instalação de plug-in.

Pré-requisitos para o banco de dados – criar modelos de backup, ativar Logbackup

- Criar diretórios para backups de dados e log (/sapdb/M02/backup/data, /sapdb/M02/backup/log – proprietário sdba – permissões 755)
- Conectar ao banco de dados M02 (como usuário do sistema operacional sqdm02)
 - Dbmcli -d M02 -u CONTROLE, <password>
- Criar modelo de backup de arquivo de dados (M02_DATA) de acordo com a SAP Note 1928060
 - Backup_template_create M02_DATA para ARQUIVAR DADOS DE conteúdo /sapdb/M02/backup/data/M02_DATA
- Criar modelo de backup de dados (M02_LOG) de acordo com a SAP Note 1928060
 - Backup_template_create M02_LOG para ARQUIVO /sapdb/M02/backup/log/M02_LOG LOG de conteúdo
- Criar modelo de backup de Snapshot de dados (M02_SNAP) de acordo com a SAP Note 1928060
 - Backup_template_create M02_SNAP para INSTANTÂNEO EXTERNO
- Criar Fake-Backup para habilitar o LOG Backup
 - util_connect
 - Backup_start M02_SNAP
 - Backup_finish M02_SNAP ExternalBackupID First_full_fake_backup
- Mudar o modo de registo da base de dados
 - autolog_off
 - autolog_on M02_LOG INTERVALO 300
 - autolog_show

Implante o agente do SnapCenter para hospedar o sap-Inx25HANA

Mais informações podem ser encontradas no ["Documentação do SnapCenter"](#).

Selecione Plug-ins SAP MaxDB e Unix File Systems.

Add Host

Host Type	Linux
Host Name	sap-lnx25
Credentials	linux-snapcenter  

Select Plug-ins to Install SnapCenter Plug-ins Package 6.1 for Linux

- | | |
|---|--|
| ☐ IBM DB2 | ☐ MongoDB |
| ☐ MySQL | ☐ Oracle Applications  |
| ☐ Oracle Database | ☐ SAP ASE |
| ☐ PostgreSQL | ☒ SAP MaxDB |
| ☐ SAP HANA | ☐ Storage  |
| ☒ Unix File Systems | |

 [More Options](#): Port, Install Path, Custom Plug-Ins...

Submit

Cancel

Criar Configuração de recursos do SnapCenter para Banco de dados M02

Recursos → SAP MaxDB → Adicionar recursos

Add SAP MaxDB Resource

1 Name
2 Storage Footprint
3 Resource Settings
4 Summary

Provide Resource Details

Name
M02

Host Name
sap-lnx25.muccbc.hq.netapp.com

Type
Database

Credential Name
None

Add information for the credential

Credential Name
control-M02

Username
control

Password

Add

Previous
Next



Se a Senha contiver caracteres especiais, eles devem ser mascarados com uma barra invertida (por exemplo, Test!123! → Teste!123!).

Add SAP MaxDB Resource

1 Name
2 Storage Footprint
3 Resource Settings
4 Summary

Provide Resource Details

Name
M02

Host Name
sap-lnx25.muccbc.hq.netapp.com

Type
Database

Credential Name
control-M02

Add SAP MaxDB Resource

1 Name

2 Storage Footprint

3 Resource Settings

4 Summary

Provide Storage Footprint Details

Storage Type ☒ ONTAP ☐ Azure NetApp Files

Add Storage Footprint

Storage System

svm-sap01.muccbc.hq.netapp.com

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name

M02_data

M02_sapmaxdb

LUNs or Qtrees

Default is 'None' or type to find

Default is 'None' or type to find

+

x

Save

Os pares de chave-valor personalizados devem ser feitos (pelo menos).

Add SAP MaxDB Resource

1 Name
2 Storage Footprint
3 Resource Settings
4 Summary

Resource Settings

Custom key-value pairs for SAP MaxDB plug-in

Name	Value	
DBMCLICMD	/sapdb/M02/db/bin/dbmcli	✕
SQLCLICMD	/sapdb/M02/db/bin/sqlcli	✕
MAXDB_UPDATE_HIST_LOG	Y	✕
MAXDB_BACKUP_TEMPLATES	M02:M02\$SNAP	+ ✕

Previous
Next

A tabela a seguir lista os parâmetros do plug-in MaxDB, fornece suas configurações e os descreve:

Parâmetro	* Definição*	Descrição
PEGA_LOGWRITER	(Y / N)	Executa suspender operações de logwriter (N) ou retomar o logwriter (Y).
DBMCLICMD	caminho_para_dbmcli_cm d	Especifica o caminho para o comando MaxDB dbmcli.se não estiver definido, dbmcli no caminho de pesquisa é usado.
SQLCLICMD	caminho_para_sqlcli_cmd	Especifica o caminho para o comando sqlcli MaxDB. Se não estiver definido, sqlcli é usado no caminho de pesquisa.
MAXDB_UPDATE_HIST_ LOG	(Y / N)	Instrui o programa de backup MaxDB se deseja ou não atualizar o log de histórico do MaxDB.

Parâmetro	* Definição*	Descrição
MAXDB_BACKUP_TEMP LATES	template_name (por exemplo M02_SNAP,)	Especifica um modelo de backup para cada banco de dados.o modelo já deve existir e ser um tipo externo de modelo de backup. Para ativar a integração de cópia Snapshot para MaxDB 7,8 e posterior, você deve ter a funcionalidade de servidor em segundo plano MaxDB e modelo de backup MaxDB já configurado.
MAXDB_BG_SERVER_P REFIX	bg_server_prefix (por exemplo na_bg,)	Especifica o prefixo para o nome do servidor em segundo plano. Se o parâmetro MAXDB_BACKUP_TEMPLATES estiver definido, você também deve definir o parâmetro MAXDB_BG_SERVER_PREFIX. Se você não definir o prefixo, o valor padrão na_bg_DATABASE será usado.

Add SAP MaxDB Resource

1 Name
2 Storage Footprint
3 Resource Settings
4 Summary

Summary

Name

M02

Type

Database

Host

sap-lnx25.muccbc.hq.netapp.com

Credential Name

control-M02

Storage Footprint

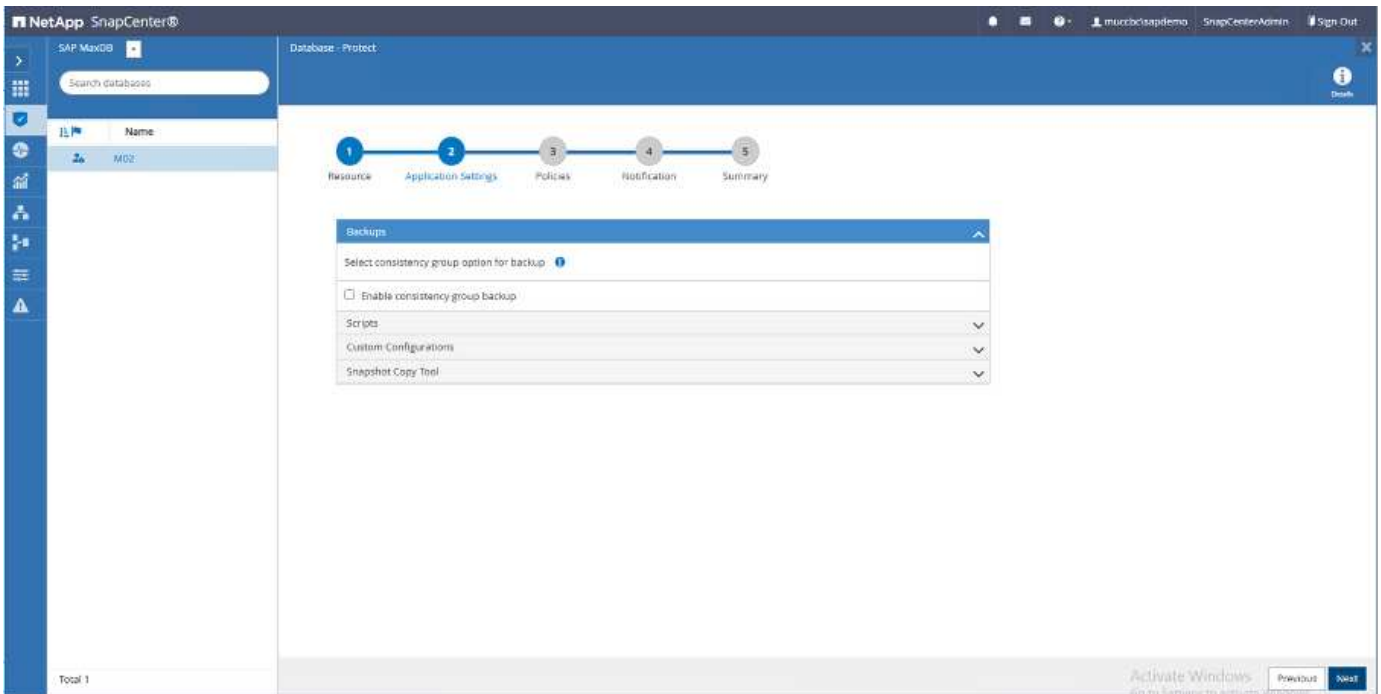
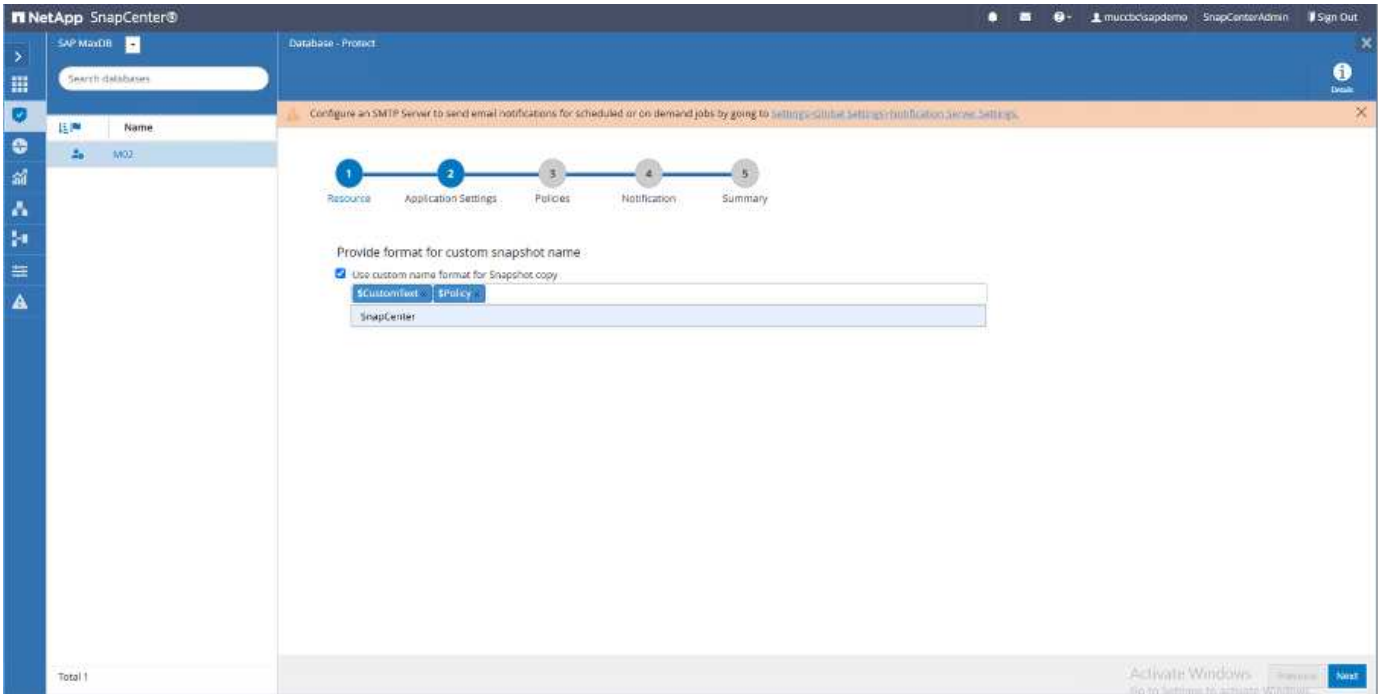
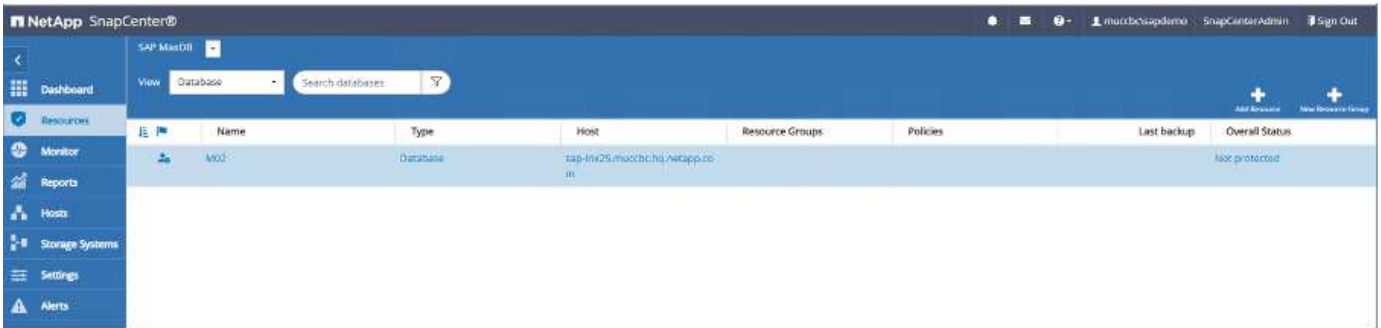
Storage System	Volume	LUN/Qtree
svm-sap01.muccbc.hq.netapp.com	M02_data	
	M02_sapmaxdb	

Custom Resource Parameters

Key	Value
DBMCLICMD	/sapdb/M02/db/bin/dbmcli
SQLCLICMD	/sapdb/M02/db/bin/sqlcli
MAXDB_UPDATE_HIST_LOG	Y
MAXDB_BACKUP_TEMPLATES	M02:M02_SNAP

Previous
Finish

Agora, a configuração poderia ser concluída e o Backup agendado de acordo com o conceito geral de proteção.



NetApp SnapCenter®

SAP MaxDB

Search databases

Database: Protect

1 Resource 2 Application Settings 3 Policies 4 Notification 5 Summary

Select one or more policies and configure schedules

maxdb_endemall + ⓘ

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules	Secondary Protection
maxdb_endemall	None	To schedule operations select a policy that has the appropriate schedule associated, or modify the selected policy to allow schedules.	No

Total 1

Activate Windows
Go to Settings to activate Windows.

Previous Next

NetApp SnapCenter®

SAP MaxDB

Search databases

Database: Protect

ⓘ If you want to send notifications for scheduled or on-demand jobs, an SMTP server must be configured. Continue to the summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Resource 2 Application Settings 3 Policies 4 Notification 5 Summary

Provide email settings ⓘ

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

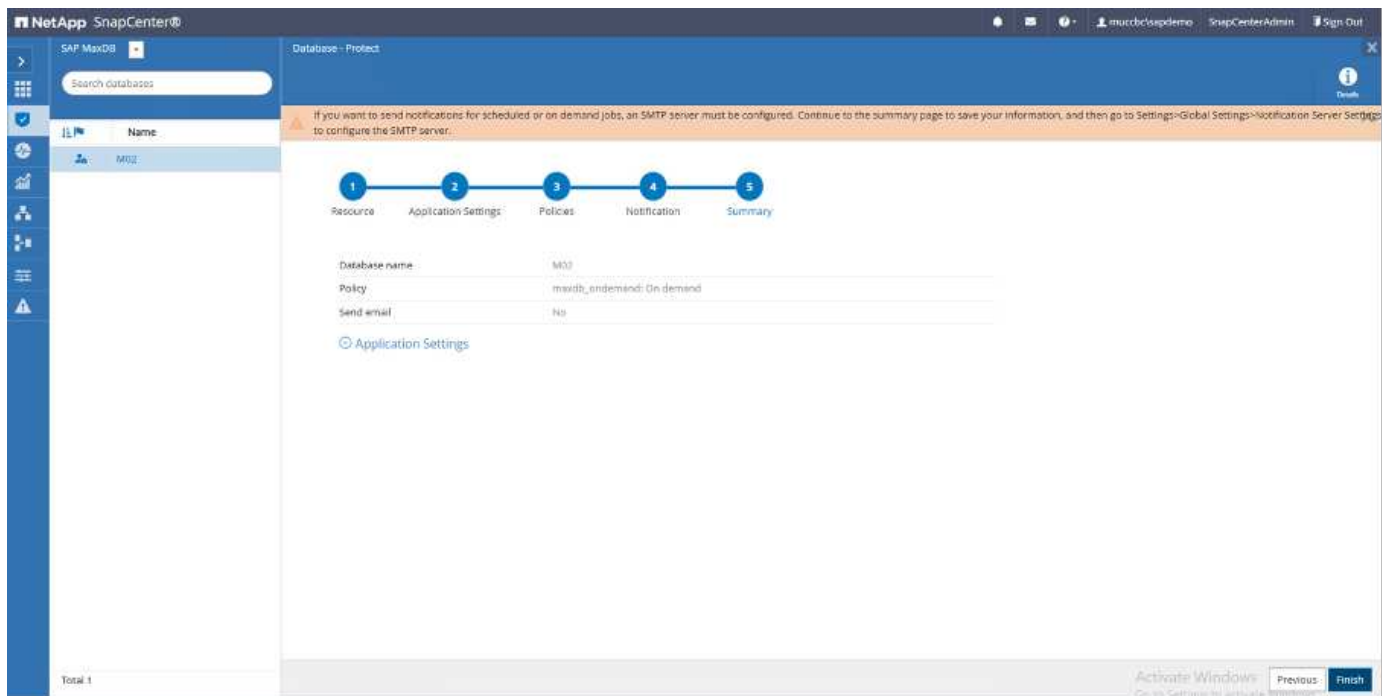
Subject: Notification

☐ Attach job report

Total 1

Activate Windows
Go to Settings to activate Windows.

Previous Next

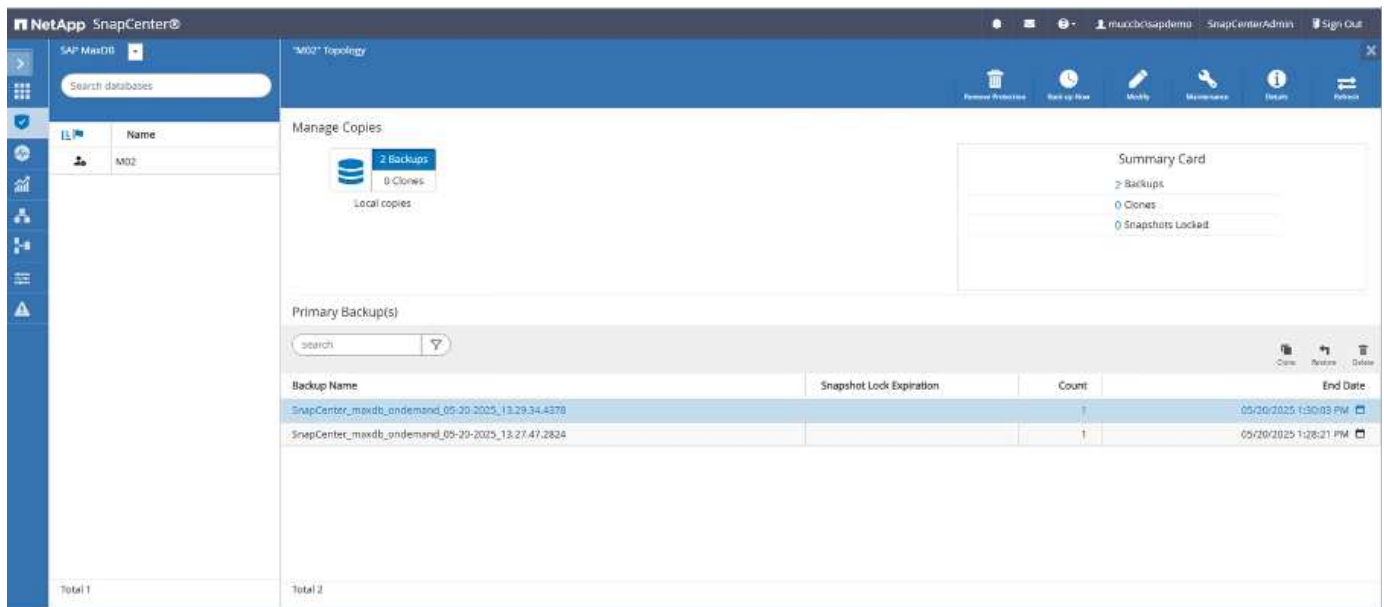


Sequência para recuperar o sistema M02

1. Pare o SAP System M02 (incluindo banco de dados), pare o sapinit
2. Sistema de arquivos Umount /sapdb/M02/sapdata
3. Restaurar volumes M02_data (usando SnapCenter)
4. Monte o sistema de arquivos /sapdb/M02/sapdata
5. Iniciar base de dados M02 e ligar (modo admin)
6. Reunir informações de cópia de Segurança
7. recuperar backup de dados de banco de dados
8. recuperar backups de log de banco de dados
9. parar a base de dados
10. Inicie o sapinit, SAP System M02

Recuperar instância M02

- Pare o SAP System e o DB M02 no host sap-Inx25HANA
 - Utilizador m02adm: Stopsap
 - Opcional – se a base de dados não tiver sido interrompida com êxito – Utilizador: sqdm02
 - Dbmcli -d M02 -u CONTROLE, <password>
 - db_offline
 - Root do usuário: /Etc/init.d/sapinit stop
 - Root do usuário: Umount /sapdb/M02/sapdata
- Restaurar cópia de segurança
 - SnapCenter GUI: Selecione Backup necessário para restaurar



A seleção de recurso completo acionará uma Restauração Snap baseada em volume (VBSR). Dentro do Azure é chamado "**reverter volume**". Para implantação do ANF **somente recurso completo está disponível**.

Important

Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.



Para outros tipos de implantação (por exemplo, ANF no local), uma operação SFSR (Single File Snap Restore) pode ser orquestrada. Selecione File Level (nível de ficheiro) e o volume e marca de verificação "All" (todos) – consulte a seguinte captura de ecrã.

Restore from SnapCenter_maxdb_ondemand_05-20-2025_13.29.34.4378

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Select the restore types

☐ Complete Resource

☒ File Level

Select files to restore

Volume/Qtree	All	File Path
☒ svm-sap01.muccbc.hq.netapp.com:/vol/M...	☒	Provide one or more file paths separated by comma
☐ svm-sap01.muccbc.hq.netapp.com:/vol/M...		

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next

O resumo seria exibido e com concluir a restauração real é iniciada.

Restore from SnapCenter_maxdb_ondemand_05-20-2025_13.29.34.4378

1 Restore scope
2 PreOps
3 PostOps
4 Notification
5 Summary

Summary

Backup Name	SnapCenter_maxdb_ondemand_05-20-2025_13.29.34.4378
Backup date	05/20/2025 1:30:03 PM
Restore scope	File Level
Pre restore command	
Unmount command	
Mount command	
Post restore command	
Send email	No

⚠ If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous
Finish

- Montar sistemas de arquivos (sap-Inx25)
 - Root do usuário: Mount /sapdb/M02/sapdata
- Inicie a base de dados M02 no modo de administração e ligue
 - Usuário: sqdm02: Dbmcli -d M02 -u CONTROL, <password>
 - db_admin
 - db_connect
- Reunir informações de cópia de Segurança
 - backup_history_open
 - backup_history_list -c label,action,pages,stop,media -r por último

```
[dbmcli on M02>backup_history_list -c label,action,pages,stop,media -r last
OK
END
DAT_000000008|SAVE WARM|          0|2025-05-20 13:29:50|M02_SNAP
---
```

- Recuperar banco de dados

- Recuperar backup de dados
 - Recover_start M02_SNAP data ExternalBackupID DAT_000000008

```
dbmcli on M02>recover_start M02_SNAP data ExternalBackupID DAT_000000008
OK
Returncode          0
Date                20250520
Time                00151550
Server              sap-lnx25
Database            M02
Kernel Version      Kernel    7.9.10    Build 004-123-265-969
Pages Transferred   0
Pages Left
Volumes
Medianame           M02_SNAP
Location
Error text
Label               DAT_000000008
Is Consistent       true
First LOG Page      512226
Last LOG Page
DB Stamp 1 Date     20250520
DB Stamp 1 Time     00132933
DB Stamp 2 Date
DB Stamp 2 Time
Page Count
Devices Used        0
Database ID         sap-lnx25:M02_20241203_104036
Max Used Data Page  3187892
Converter Page Count
---
```

- Recupere o backup de log conforme necessário
 - Por exemplo, Recover_start M02_LOG LOG LOG 147

```
[dbmccli on M02>recover_start M02_LOG LOG 147
OK
Returncode          0
Date                20250521
Time               00112001
Server              sap-lnx25
Database            M02
Kernel Version      Kernel    7.9.10    Build 004-123-265-969
Pages Transferred   24
Pages Left          0
Volumes            1
Medianame           M02_LOG
Location            /sapdb/M02/backup/log/M02_LOG.147
Errortext
Label               LOG_000000147
Is Consistent
First LOG Page      514072
Last LOG Page       514075
DB Stamp 1 Date     20250520
DB Stamp 1 Time     00180238
DB Stamp 2 Date     20250520
DB Stamp 2 Time     00180539
Page Count          4
Devices Used        1
Database ID         sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count
```

- Informações opcionais – recuperação automática para um carimbo de data/hora específico (sem necessidade de especificar dados dedicados / registo de backp
 - por exemplo, recuperação automática até 20250520 200000

```
---
[dbmccli on M02>autorecover until 20250520 200000
OK
Returncode          0
Date                20250521
Time               00131559
Server              sap-lnx25
Database            M02
Kernel Version      Kernel    7.9.10    Build 004-123-265-969
Pages Transferred   10096
Pages Left          0
Volumes            1
Medianame           M02_LOG
Location            /sapdb/M02/backup/log/M02_LOG.102
Errortext
Label               LOG_000000102
Is Consistent
First LOG Page      256227
Last LOG Page       341559
DB Stamp 1 Date     20241203
DB Stamp 1 Time     00190348
DB Stamp 2 Date     20241226
DB Stamp 2 Time     00193615
Page Count          85333
Devices Used        1
Database ID         sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count
---
```

- Terminar recuperação e parar base de dados

- db_offline



Mais informações sobre a recuperação estão disponíveis no ["Documentação do MaxDB"](#)

- Inicie o SAP System
 - Root do usuário: /Etc/init.d/sapinit start
 - Usuário m02adm: Startsap

Informações adicionais e histórico de versões

Demos gravadas

As seguintes demonstrações recodificadas estão disponíveis para suportar a documentação.

[Instalação MaxDB Plugin](#), [Configuração MaxDB Plugin](#), [Backup do banco de dados MaxDB](#)

[Restauração e recuperação de banco de dados MaxDB](#)

Documentação externa

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- ["SAP Instalação Azure no ANF"](#)
- ["Pré-requisitos do SnapCenter para Plugins"](#)
- ["SnapCenter Instalar Plugins"](#)
- ["Documentação do MaxDB Recovery"](#)
- SAP Notes (login necessário)
 - ["1928060 - Backup e recuperação de dados com backup do sistema de arquivos"](#)
 - ["2282054 - servidor DBM em segundo plano"](#)
 - ["616814 - suspender o gravador de registros para espelho dividido ou instantâneo"](#)
- ["HOWTO - SAP MaxDB Backup com Database Manager CLI"](#)
- ["HOWTO - SAP MaxDB recuperação com Database Manager CLI"](#)
- ["Documentação do produto NetApp"](#)
- ["Soluções SAP da NetApp – informações sobre casos de uso, práticas recomendadas e benefícios"](#)

Histórico de versões

Versão	Data	* Histórico de versões do documento*
Versão 1,0	Mai de 2025	Versão inicial – backup / recuperação de banco de dados MaxDB

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

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.