Backup e recovery SAP HANA con SnapCenter

NetApp solutions for SAP

NetApp
December 16, 2025

Sommario

Backup e recovery SAP HANA con SnapCenter

Proteggi i sistemi SAP HANA con SnapCenter su ONTAP, Azure NetApp Files e FSx per ONTAP

Proteggi i sistemi SAP HANA con NetApp SnapCenter utilizzando backup basati su snapshot e replica dei dati. Questa soluzione copre la configurazione SnapCenter e le best practice operative per i sistemi SAP HANA sui sistemi ONTAP AFF e ASA , Azure NetApp Files e Amazon FSx per ONTAP, comprese strategie di backup, controlli di coerenza e flussi di lavoro di ripristino.

Autore: Nils Bauer, NetApp

Ulteriori dettagli specifici sui casi d'uso relativi alle operazioni di aggiornamento del sistema SAP e alla replica del sistema SAP HANA sono disponibili all'indirizzo:

- "Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"
- "Replica di sistema SAP HANA - backup e recovery con SnapCenter"

Le migliori pratiche per combinare la protezione dei dati SnapCenter e la sincronizzazione attiva NetApp SnapMirror sono descritte in

- "Protezione dei dati SAP HANA e alta disponibilità con SnapCenter, SnapMirror ActiveSync e VMware Metro Storage Cluster"

Ulteriore documentazione sulle best practice specifiche della piattaforma è disponibile all'indirizzo

- "Protezione dei dati SAP HANA con SnapCenter con sistemi VMware VMFS e NetApp ASA"
- "SAP HANA su Amazon FSX per NetApp ONTAP - Backup e recovery con SnapCenter"
- "Data Protection SAP HANA su Azure NetApp Files con SnapCenter (blog e video)"
- "Operazioni di refresh e cloning di sistemi SAP su Azure NetApp Files con SnapCenter (blog e video)"

Scopri di più sulla protezione dei dati SAP HANA con la tecnologia NetApp Snapshot

Scopri come la tecnologia NetApp Snapshot protegge i database SAP HANA con backup che vengono completati in pochi minuti, indipendentemente dalle dimensioni del database. Scopri le strategie di backup e ripristino tramite copie Snapshot, SnapRestore per un ripristino rapido e replica con SnapVault o backup Azure NetApp Files per una protezione secondaria.

Oggi le aziende necessitano di una disponibilità continua e ininterrotta per le loro applicazioni SAP. Si aspettano livelli di prestazioni costanti e necessitano di operazioni quotidiane automatizzate a fronte di volumi di dati in costante aumento e della necessità di attività di manutenzione di routine, come i backup di sistema. L'esecuzione di backup dei database SAP è un'attività critica e può avere un impatto significativo sulle prestazioni del sistema SAP di produzione.

Le finestre di backup si stanno riducendo mentre la quantità di dati da sottoporre a backup sta aumentando.

Pertanto, è difficile trovare un momento in cui sia possibile eseguire backup con un impatto minimo sui processi aziendali. Il tempo necessario per ripristinare e recuperare i sistemi SAP è un problema, perché è necessario ridurre al minimo i tempi di inattività dei sistemi SAP di produzione e non di produzione per ridurre i costi aziendali.

Backup e ripristino tramite backup Snapshot

È possibile utilizzare la tecnologia NetApp Snapshot per creare backup del database in pochi minuti. Il tempo necessario per creare una copia Snapshot è indipendente dalle dimensioni del database, poiché una copia Snapshot non sposta alcun blocco di dati fisici sulla piattaforma di archiviazione. Inoltre, l'utilizzo della tecnologia Snapshot non ha alcun effetto sulle prestazioni del sistema SAP live, poiché tutte le operazioni vengono eseguite nel sistema di archiviazione. Pertanto, è possibile pianificare la creazione di copie Snapshot senza considerare i periodi di picco delle conversazioni o delle attività batch. In genere, i clienti SAP su NetApp pianificano più backup Snapshot online durante il giorno; ad esempio, è normale che vengano eseguiti ogni sei ore. Questi backup Snapshot vengono in genere conservati per tre-cinque giorni sul sistema di archiviazione primario prima di essere rimossi o trasferiti su un sistema di archiviazione più economico per la conservazione a lungo termine.

Le copie snapshot offrono inoltre vantaggi fondamentali per le operazioni di ripristino e recupero. Un'operazione di ripristino ripristina i dati nel file system in base allo stato di un backup. Un'operazione di ripristino viene utilizzata per riportare lo stato del database a un punto nel tempo utilizzando i backup del log del database.

La tecnologia NetApp SnapRestore consente il ripristino di un intero database o, in alternativa, solo di una parte di esso, in base ai backup Snapshot attualmente disponibili. Il processo di ripristino viene completato in pochi secondi, indipendentemente dalle dimensioni del database. Poiché è possibile creare più backup Snapshot online durante il giorno, il tempo necessario per il processo di ripristino è notevolmente ridotto rispetto a un approccio di backup tradizionale eseguito una volta al giorno. Poiché è possibile eseguire un ripristino con una copia Snapshot che risale al massimo a poche ore prima (anziché a 24 ore prima), è necessario applicare un numero inferiore di registri delle transazioni durante il ripristino in avanti. Il tempo necessario per il ripristino e il recupero è notevolmente ridotto rispetto ai tradizionali backup in streaming.

Poiché i backup Snapshot vengono archiviati sullo stesso sistema disco dei dati online attivi, NetApp consiglia di utilizzare i backup di copia Snapshot come integrazione anziché come sostituzione dei backup in una posizione secondaria. La maggior parte delle azioni di ripristino e recupero vengono gestite tramite SnapRestore sul sistema di archiviazione primario. I ripristini da una posizione secondaria sono necessari solo se il sistema di archiviazione primario contenente le copie Snapshot non è disponibile. È possibile utilizzare il backup secondario anche se è necessario ripristinare un backup non più disponibile nell'archivio primario.

Un backup in una posizione secondaria si basa su copie Snapshot create sullo storage primario. Pertanto i dati vengono letti direttamente dal sistema di archiviazione primario senza generare carico sul server del database SAP e sulla sua rete. L'archiviazione primaria comunica direttamente con l'archiviazione secondaria e replica i dati di backup nella destinazione utilizzando la funzionalità di backup SnapVault o ANF.

I backup SnapVault e ANF offrono notevoli vantaggi rispetto ai backup tradizionali. Dopo un trasferimento dati iniziale, in cui tutti i dati vengono trasferiti dall'origine alla destinazione, tutti i backup successivi replicano solo i blocchi modificati nell'archivio secondario. Pertanto, il carico sul sistema di archiviazione primario e il tempo necessario per un backup completo risultano notevolmente ridotti. Poiché nella destinazione vengono archiviati solo i blocchi modificati, qualsiasi backup completo del database aggiuntivo consuma molto meno spazio su disco.

Esecuzione delle operazioni di backup e ripristino Snapshot

La figura seguente mostra HANA Studio di un cliente che utilizza operazioni di backup Snapshot. L'immagine

mostra che il database HANA (di circa 4 TB) viene sottoposto a backup in 1 minuto e 20 secondi utilizzando la tecnologia di backup Snapshot e in più di 4 ore con un'operazione di backup basata su file.

La parte più consistente del tempo di esecuzione complessivo del flusso di lavoro di backup è il tempo necessario per eseguire l'operazione Snapshot del database HANA. Il backup dello snapshot di archiviazione viene completato in un paio di secondi, indipendentemente dalle dimensioni del database HANA.

[larghezza=624, altezza=267]

Confronto degli obiettivi del tempo di ripristino

Questa sezione fornisce un confronto tra gli obiettivi del tempo di ripristino (RTO) dei backup snapshot basati su file e quelli basati su storage. L'RTO è definito dalla somma del tempo necessario per ripristinare, recuperare e quindi avviare il database.

Tempo necessario per il ripristino del database

Con un backup basato su file, il tempo di ripristino dipende dalle dimensioni del database e dell'infrastruttura di backup, che definisce la velocità di ripristino in megabyte al secondo. Ad esempio, se l'infrastruttura supporta un'operazione di ripristino a una velocità di 250 MBps, occorrono circa 4.5 ore per ripristinare un database di 4 TB sulla persistenza.

Con i backup NetApp Snapshot, il tempo di ripristino è indipendente dalle dimensioni del database ed è sempre nell'ordine di un paio di secondi.

Tempo necessario per il ripristino del database

Il tempo di ripristino dipende dal numero di registri che devono essere applicati dopo il ripristino. Questo numero è determinato dalla frequenza con cui vengono eseguiti i backup dei dati.

Con i backup dei dati basati su file, la pianificazione del backup è generalmente una volta al giorno. In genere, non è possibile una frequenza di backup più elevata, poiché il backup diminuisce le prestazioni di produzione. Pertanto, nel peggiore dei casi, tutti i log scritti durante la giornata devono essere applicati durante il recupero in avanti.

I backup snapshot vengono in genere pianificati con una frequenza maggiore perché non hanno alcun impatto sulle prestazioni del database SAP HANA. Ad esempio, se i backup Snapshot sono programmati ogni sei ore, i registri dovranno essere applicati nel caso peggiore per le ultime sei ore, se l'errore si verifica immediatamente prima della creazione dello Snapshot successivo. Per un backup giornaliero basato su file, nel caso peggiore sarebbe necessario applicare i registri delle ultime 24 ore.

Tempo necessario per avviare il database

L'ora di inizio del database dipende dalle dimensioni del database e dal tempo necessario per caricare i dati in memoria. Negli esempi seguenti, si presuppone che i dati possano essere caricati con 1000 Mbps. Il caricamento di 4 TB in memoria richiede circa 1 ora e 10 minuti. L'ora di inizio è la stessa per le operazioni di ripristino e ripristino basate su file e Snapshot.

Calcolo del campione di ripristino e recupero

La figura seguente mostra un confronto tra le operazioni di ripristino e recupero con un backup giornaliero basato su file e backup Snapshot con pianificazioni diverse.

Le prime due barre mostrano che anche con un singolo backup Snapshot al giorno, il ripristino e il ripristino vengono ridotti al 43% a causa della velocità dell'operazione di ripristino da un backup Snapshot. Se vengono

creati più backup Snapshot al giorno, il runtime può essere ulteriormente ridotto perché è necessario applicare meno registri durante il forward recovery.

La figura seguente mostra anche che quattro o sei backup Snapshot al giorno sono i più sensati, perché una frequenza più elevata non influisce più in modo significativo sul runtime complessivo.

[larghezza=624, altezza=326]

Casi di utilizzo e valori delle operazioni di backup e cloning accelerate

L'esecuzione dei backup è una parte fondamentale di qualsiasi strategia di protezione dei dati. I backup vengono pianificati regolarmente per garantire che sia possibile eseguire il ripristino in caso di guasti del sistema. Questo è il caso di utilizzo più ovvio, ma esistono anche altre attività di gestione del ciclo di vita SAP, in cui l'accelerazione delle operazioni di backup e ripristino è fondamentale.

L'aggiornamento del sistema SAP HANA è un esempio in cui un backup su richiesta prima dell'aggiornamento e una possibile operazione di ripristino in caso di errore dell'aggiornamento hanno un impatto significativo sui tempi di inattività pianificati complessivi. Ad esempio, con un database da 4 TB, è possibile ridurre i tempi di inattività pianificati di 8 ore oppure disporre di altre 8 ore per analizzare e correggere gli errori utilizzando le operazioni di backup e ripristino basate su snapshot.

Un altro caso d'uso potrebbe essere un tipico ciclo di test, in cui i test devono essere eseguiti su più iterazioni con diversi set di dati o parametri. Utilizzando le operazioni di backup e ripristino rapide, è possibile creare facilmente punti di salvataggio all'interno del ciclo di test e ripristinare il sistema a uno qualsiasi di questi punti di salvataggio precedenti se un test fallisce o deve essere ripetuto. Ciò consente di terminare prima i test o di eseguirne più contemporaneamente, migliorandone i risultati.

[larghezza=618, altezza=279]

Una volta implementati, i backup Snapshot possono essere utilizzati per affrontare diversi altri casi d'uso che richiedono copie di un database HANA. È possibile creare un nuovo volume in base al contenuto di qualsiasi backup Snapshot disponibile. Il tempo di esecuzione di questa operazione è di pochi secondi, indipendentemente dalle dimensioni del volume.

Il caso d'uso più diffuso è l'aggiornamento del sistema SAP, in cui i dati del sistema di produzione devono essere copiati nel sistema di test o di controllo qualità. Sfruttando la funzionalità di clonazione ONTAP o ANF, è possibile predisporre il volume per il sistema di test da qualsiasi copia Snapshot del sistema di produzione in pochi secondi. Il nuovo volume deve quindi essere collegato al sistema di test e il database HANA deve essere ripristinato.

Il secondo caso d'uso è la creazione di un sistema di riparazione, utilizzato per risolvere i problemi di corruzione logica nel sistema di produzione. In questo caso, viene utilizzato un backup Snapshot precedente del sistema di produzione per avviare un sistema di riparazione, che è un clone identico del sistema di produzione con i dati precedenti al verificarsi del danneggiamento. Il sistema di riparazione viene quindi utilizzato per analizzare il problema ed esportare i dati necessari prima che vengano danneggiati.

L'ultimo caso d'uso è la possibilità di eseguire un test di failover di disaster recovery senza interrompere la replica e quindi senza influenzare l'RTO e l'obiettivo del punto di ripristino (RPO) della configurazione di disaster recovery. Quando si utilizza la replica ONTAP SnapMirror o la replica ANF tra regioni per replicare i dati sul sito di disaster recovery, i backup Snapshot di produzione sono disponibili anche sul sito di disaster recovery e possono quindi essere utilizzati per creare un nuovo volume per i test di disaster recovery.

[larghezza=627, altezza=328]

Scopri di più sull’architettura SnapCenter

Scopri di più sull’architettura SnapCenter per la protezione dei dati SAP HANA, inclusi il server SnapCenter , i componenti plug-in e le piattaforme di archiviazione supportate. SnapCenter fornisce una gestione centralizzata di backup, ripristino e clonazione per database SAP HANA su sistemi ONTAP , Azure NetApp Files e FSx per ONTAP.

SnapCenter è una piattaforma unificata per la protezione dei dati coerente con le applicazioni. SnapCenter fornisce controllo e supervisione centralizzati, delegando al contempo agli utenti la possibilità di gestire operazioni di backup, ripristino e clonazione specifiche per l’applicazione. NetApp SnapCenter è un singolo strumento che può essere utilizzato dagli amministratori di database e storage per gestire le operazioni di backup, ripristino e clonazione per una varietà di applicazioni e database. SnapCenter supporta i sistemi di archiviazione NetApp ONTAP , nonché Azure NetApp Files e FSx per ONTAP. È inoltre possibile utilizzare SnapCenter per replicare i dati tra ambienti on-premise, tra ambienti on-premise e cloud e tra cloud privati, ibridi o pubblici.

SnapCenter include il server SnapCenter e i plug-in SnapCenter . I plug-in sono disponibili per varie applicazioni e componenti infrastrutturali. Il server SnapCenter può essere eseguito sia su Windows che su Linux.

[larghezza=601, altezza=275]

Scopri di più sul backup e ripristino SnapCenter per SAP HANA

SnapCenter offre funzionalità complete di backup e ripristino per i database SAP HANA utilizzando copie Snapshot basate sull’archiviazione, gestione automatizzata della conservazione e integrazione con NetApp ONTAP, Azure NetApp Files e FSx per NetApp ONTAP. La soluzione supporta backup di database coerenti con l’applicazione, protezione di volumi non dati, controlli di integrità dei blocchi e replica su storage secondario tramite backup SnapVault o ANF.

La soluzione di backup SnapCenter per SAP HANA copre le seguenti aree:

- Operazioni di backup, pianificazione e gestione della conservazione
- Backup dei dati SAP HANA con copie Snapshot basate su storage
- Backup di volumi non dati con copie Snapshot basate su storage (ad esempio, /hana/shared)
- Operazioni di controllo dell’integrità dei blocchi del database
  - utilizzando un backup basato su file
  - utilizzando lo strumento hdbpersdiag di SAP HANA
- Replica del backup snapshot in una posizione di backup secondaria
  - utilizzando SnapVault/ SnapMirror
  - utilizzando il backup ANF Azure NetApp Files
- Manutenzione del catalogo di backup SAP HANA
  - per backup dei dati HANA (basati su snapshot e file)

    - per i backup dei log HANA
- Operazioni di ripristino e recovery
    - Ripristino e ripristino automatici
    - Operazioni di ripristino di un singolo tenant

I backup dei dati del database vengono eseguiti da SnapCenter in combinazione con il plug-in SnapCenter per SAP HANA. Il plug-in attiva uno snapshot del database interno SAP HANA in modo che gli snapshot, creati sul sistema di archiviazione, siano basati su un'immagine coerente con l'applicazione del database SAP HANA.

SnapCenter consente la replica di immagini di database coerenti in una posizione di backup o di ripristino di emergenza secondaria utilizzando SnapVault o la funzionalità SnapMirror. In genere, vengono definite policy di conservazione diverse per i backup nello storage primario e in quello secondario. SnapCenter gestisce la conservazione nello storage primario, mentre ONTAP gestisce la conservazione nello storage di backup secondario.

Per consentire un backup completo di tutte le risorse correlate a SAP HANA, SnapCenter consente inoltre di eseguire il backup di tutti i volumi non dati utilizzando il plug-in SAP HANA con copie Snapshot basate su storage. È possibile pianificare volumi diversi dai dati in modo indipendente dal backup dei dati del database per consentire policy di conservazione e protezione individuali.

SAP consiglia di combinare i backup Snapshot basati sull'archiviazione con un controllo settimanale della coerenza del livello di persistenza. È possibile eseguire il controllo di coerenza dei blocchi da SnapCenter eseguendo un backup basato su file oppure eseguendo lo strumento SAP hdbpersdiag.

In base ai criteri di conservazione configurati, SnapCenter gestisce la manutenzione dei backup dei file di dati nell'archivio primario, dei backup dei file di registro e del catalogo di backup SAP HANA.

SnapCenter gestisce la conservazione dello storage primario, mentre ONTAP gestisce la conservazione del backup secondario.

La figura seguente mostra una panoramica delle operazioni di backup e gestione della conservazione di SnapCenter.

Quando si esegue un backup Snapshot basato su storage del database SAP HANA, SnapCenter esegue le seguenti attività:

- Operazione di backup:
    - Attiva uno snapshot del database HANA interno per ottenere un'immagine coerente dell'applicazione sul livello di persistenza
    - Crea un backup Snapshot basato sull'archiviazione del volume di dati
    - Chiude lo snapshot del database HANA interno, conferma o abbandona l'operazione di backup. Questo passaggio registra il backup nel catalogo di backup HANA.
- Gestione della fidelizzazione:
    - Elimina i backup degli snapshot di archiviazione in base alla conservazione definita
    - Elimina gli snapshot sul livello di archiviazione
    - Elimina le voci del catalogo di backup SAP HANA
    - Elimina tutti i backup del registro più vecchi del backup dei dati più vecchio. I backup del log vengono eliminati nel file system e nel catalogo di backup SAP HANA

[larghezza=601, altezza=285]

Se è configurato un backup secondario, con SnapVault/ SnapMirror o con backup ANF, lo Snapshot creato nel volume primario viene replicato nell'archivio di backup secondario. SnapCenter gestisce il catalogo di backup HANA e la conservazione dei backup dei log in base alla disponibilità dei backup secondari.

[larghezza=601, altezza=278]

Scopri le configurazioni supportate da SnapCenter per SAP HANA

SnapCenter supporta un'ampia gamma di architetture di sistema e scenari di distribuzione SAP HANA su piattaforme di archiviazione on-premise e cloud. Scopri le configurazioni SAP HANA supportate, le combinazioni di piattaforme, i protocolli di archiviazione e le operazioni di backup e ripristino disponibili per ciascun ambiente.

Configurazioni SAP HANA supportate

SnapCenter supporta le seguenti configurazioni e funzionalità HANA:

- Sistemi host singoli SAP HANA
- Sistemi host multipli SAP HANA
  - Richiede una distribuzione centrale del plug-in come descritto in "Opzioni di distribuzione per il plug-in SnapCenter per SAP HANA".
- Sistemi SAP HANA MDC
  - con un singolo o più inquilini
- Sistemi SAP HANA con più partizioni
- Replica di sistema SAP HANA
- Crittografia SAP HANA (dati, log, backup)

Configurazioni di piattaforma e infrastruttura supportate

SnapCenter supporta le seguenti combinazioni di piattaforme host, file system e piattaforme di archiviazione.

Piattaforma host	Connessione di archiviazione e file system SAP HANA	Piattaforma di stoccaggio
VMware	Montaggi NFS in-guest	ONTAP AFF
VMware	Archivio dati FC con VMFS + VM con XFS con o senza Linux LVM	ONTAP AFF o ASA
KVM	Montaggi NFS in-guest	ONTAP AFF
Server bare metal	Montaggi NFS	ONTAP AFF
Server bare metal	FC SAN + e XFS con o senza Linux LVM	ONTAP AFF o ASA (*)
Macchina virtuale di Azure	Montaggi NFS	Azure NetApp Files
AWS EC2	Montaggi NFS	FSx per ONTAP

(*): supporto ASA disponibile a partire dalla versione SnapCenter 6.2

I plug-in HANA e Linux sono disponibili solo per la piattaforma CPU Intel. Per Linux su IBM Power è necessario configurare una distribuzione centrale del plug-in HANA come descritto in "Opzioni di distribuzione per il plug-in SnapCenter per SAP HANA".

Funzionalità e operazioni supportate

Spiegazione dell'abbreviazione

- VBSR: SnapRestore basato sul volume + Uno SnapRestore basato sul volume ripristina il volume allo stato dello Snapshot.
- SFSR: SnapRestore su singolo file + È possibile utilizzare uno SnapRestore su singolo file per ripristinare file o LUN specifici all'interno di un volume.

Vedi anche "Tipi di operazioni di ripristino per database SAP HANA rilevati automaticamente"

ONTAP AFF e FSx per ONTAP

Solo la colonna 1 (mount NFS) della tabella sottostante è rilevante per FSx per ONTAP.

Operazione	NFS monta Bare metal o in-guest con VMware o KVM	FC SAN + metallo nudo	Archivio dati FC VMware VMFS
Operazioni di backup e ripristino snapshot per il database HANA			
Backup snapshot	Sì	Sì	Sì
Istantanea a prova di manomissione	Sì	Sì	Sì
Ripristino completo	VBSR o SFSR (selezionabile)	SFSR del LUN completo	Clona, monta, copia
Ripristino di un singolo tenant	SFSR	Clona, monta, copia	Clona, monta, copia
* Operazioni di backup e ripristino SnapVault per il database HANA*			
Replica SnapVault	Sì	Sì	Sì
Istantanea a prova di manomissione	Sì	Sì	Sì
Ripristino completo	Sì	Sì	Clona, monta, copia
Ripristino di un singolo tenant	Sì	Clona, monta, copia	Clona, monta, copia
Operazione di ripristino HANA dalla destinazione Snapshot o SnapVault primaria			
Recupero automatizzato MDC tenant singolo	Sì	Sì	Sì
Recupero automatico MDC di più tenant	No	No	No
Backup e ripristino di volumi non dati			

Operazione	NFS monta Bare metal o in-guest con VMware o KVM	FC SAN + metallo nudo	Archivio dati FC VMware VMFS
Backup snapshot	Sì	Sì	SÌ (*)
Ripristina da snapshot	VBSR o SFSR (selezionabile)	SFSR del LUN completo	VBSR (*)
Replica SnapVault	Sì	Sì	SÌ (*)
Ripristina dalla destinazione SnapVault	Sì	Sì	SÌ (*)
Aggiornamento del sistema SAP			
Dall'istantanea primaria	Sì	SÌ (**)	SÌ (**)
Dal target SnapVault	Sì	SÌ (**)	SÌ (**)
HA e DR			
HSR supporta Snapshot e SnapVault	Sì	Sì	Sì
Aggiornamenti della replica SnapMirror con SC	Sì	Sì	Sì
Sincronizzazione attiva SnapMirror	NA	Sì	Sì

(*): Nessuna integrazione con VMware: snapshot dell'immagine in crash e ripristino completo del volume

(**): Soluzioni alternative richieste per le versioni SnapCenter < 6.2

ONTAP ASA

Operazione	FC SAN + Metallo nudo (*)	Archivio dati FC VMware VMFS
Operazioni di backup e ripristino snapshot per il database HANA		
Backup snapshot	Sì	Sì
Istantanea a prova di manomissione	No	No
Ripristino completo	SFSR del LUN completo	Clona, monta, copia
Ripristino di un singolo tenant	Clona, monta, copia	Clona, monta, copia
* Operazioni di backup e ripristino SnapVault per il database HANA*		
Replica SnapVault	Sì	Sì
Istantanea a prova di manomissione	No	No
Ripristino completo	Sì	Clona, monta, copia
Ripristino di un singolo tenant	Clona, monta, copia	Clona, monta, copia
Operazione di ripristino HANA dalla destinazione Snapshot o SnapVault primaria		

Operazione	FC SAN + Metallo nudo (*)	Archivio dati FC VMware VMFS
Recupero automatizzato MDC tenant singolo	Sì	Sì
Recupero automatico MDC di più tenant	No	No
Backup e ripristino di volumi non dati		
Backup snapshot	SÌ (*)	SÌ (*)
Ripristina da snapshot	SFSR del LUN completo (*)	SFSR del LUN completo (*)
Replica SnapVault	SÌ (*)	SÌ (*)
Ripristina dalla destinazione SnapVault	SÌ (*)	SÌ (*)
Aggiornamento del sistema SAP		
Dall'istantanea primaria	SÌ (**)	SÌ (**)
Dal target SnapVault	SÌ (**)	SÌ (**)
HA e DR		
HSR supporta Snapshot e SnapVault	Sì	Sì
Aggiornamenti della replica SnapMirror attivati da SnapCenter	Sì	Sì
Sincronizzazione attiva SnapMirror	Sì	Sì

(*): Supporto a partire dalla versione SnapCenter 6.2

(**): Soluzioni alternative richieste per le versioni SnapCenter < 6.2

Azure NetApp Files

Operazione	Montaggi NFS
Operazioni di backup e ripristino snapshot per il database HANA	
Backup snapshot	Sì
Istantanea a prova di manomissione	No
Ripristino completo sul posto	Ripristino del volume o SFSR (selezionabile)
Ripristino di un singolo tenant	SFSR
Operazioni di backup e ripristino ANF per il database HANA	
Replica di backup ANF	Sì
Istantanea a prova di manomissione	No
Ripristino completo sul posto	Sì
Ripristino di un singolo tenant	Sì

Operazione	Montaggi NFS
Operazione di ripristino HANA da snapshot primario o backup ANF	
Recupero automatizzato MDC tenant singolo	Sì
Recupero automatico MDC di più tenant	No
Backup e ripristino di volumi non dati	
Backup snapshot	Sì
Ripristina da snapshot	Ripristina volume
Replica di backup ANF	Sì
Ripristino completo sul posto dal backup ANF	NO (*)
Aggiornamento del sistema SAP	
Dall'istantanea primaria	Sì
Dal backup ANF	Sì
HA e DR	
Supporto HSR per snapshot e backup ANF	Sì
Aggiornamento della replica tra regioni attivato da SnapCenter	No

(*): Con la versione corrente, un'operazione di ripristino deve essere eseguita tramite il portale di Azure o la CLI

Scopri i concetti e le best practice sulla protezione dei dati SnapCenter

Scopri le opzioni di distribuzione SnapCenter , le strategie di protezione dei dati e la gestione della conservazione dei backup per gli ambienti SAP HANA. SnapCenter supporta la distribuzione di plug-in su host di database o host centrali, rilevamento automatico e configurazione manuale, controlli di coerenza dei blocchi tramite backup basati su file o hdbpersdiag e gestione completa della conservazione su storage primario e secondario.

Opzioni di distribuzione per il plug-in SnapCenter per SAP HANA

La figura seguente mostra la vista logica della comunicazione tra il server SnapCenter , il database SAP HANA e il sistema di archiviazione. Il server SnapCenter sfrutta i plug-in HANA e Linux per comunicare con il database HANA e i sistemi operativi Linux.

[larghezza=601, altezza=199]

L'opzione di distribuzione consigliata e predefinita per i plug-in SnapCenter è l'installazione sull'host del database HANA. Con questa opzione di distribuzione, tutte le configurazioni e le funzionalità descritte nel capitolo Configurazione supportata SnapCenter sono valide. Esistono alcune eccezioni in cui i plug-in SnapCenter non possono essere installati sull'host del database HANA, ma devono essere configurati su un host di plug-in centrale, che potrebbe essere il server SnapCenter stesso. Per i sistemi HANA con più host o

per i sistemi HANA in esecuzione sulla piattaforma IBM Power è necessario un host plug-in centrale. Entrambe le opzioni di distribuzione possono anche essere combinate, ad esempio utilizzando il server SnapCenter come host di plug-in centrale per un sistema host multiplo e distribuendo i plug-in sugli host del database HANA per tutti gli altri sistemi HANA con host singolo.

In SnapCenter una risorsa HANA può essere rilevata automaticamente o configurata manualmente. Per impostazione predefinita, un sistema HANA viene rilevato automaticamente non appena i plug-in HANA e Linux vengono distribuiti sull'host del database. La rilevazione automatica SnapCenter non supporta più installazioni HANA sullo stesso host. I sistemi HANA gestiti tramite un host plug-in centrale devono essere configurati manualmente in SnapCenter. Inoltre, i volumi non dati sono per impostazione predefinita risorse configurate manualmente.

	Plug-in distribuito a	**Risorsa SnapCenter**
Banca dati HANA	Host del database	Scoperto automaticamente
Banca dati HANA	Host plug-in centrale	Configurazione manuale
Volume non dati	N/A.	Configurazione manuale

Sebbene SnapCenter supporti la distribuzione centralizzata di plug-in per i sistemi HANA, vi sono limitazioni nel supporto di piattaforme e funzionalità. Le seguenti configurazioni e operazioni infrastrutturali non sono supportate per i sistemi HANA configurati con un host plug-in centrale:

- VMware con datastore FC
- Sincronizzazione attiva SnapMirror
- Alta disponibilità del server SnapCenter se utilizzato come host plug-in centrale
- Rilevamento automatico del sistema HANA
- Ripristino automatizzato del database HANA
- Aggiornamento automatico del sistema SAP
- Ripristino di un singolo tenant

Plug-in SnapCenter per HANA distribuito sull'host del database SAP HANA

Il server SnapCenter comunica tramite il plug-in HANA con i database HANA. Il plug-in HANA utilizza il software client HANA hdbsql per eseguire comandi SQL nei database HANA. L'archivio utenti hdb HANA viene utilizzato per fornire le credenziali utente, il nome host e le informazioni sulla porta per accedere ai database HANA. Il plug-in SnapCenter Linux viene utilizzato per coprire tutte le operazioni del file system host, nonché per il rilevamento automatico del file system e delle risorse di archiviazione.

Quando il plug-in HANA viene distribuito sull'host del database HANA, il sistema HANA viene rilevato automaticamente da SnapCenter e contrassegnato come risorsa rilevata automaticamente in SnapCenter.

[larghezza=601, altezza=304]

Server SnapCenter ad alta disponibilità

SnapCenter può essere configurato in una configurazione HA a due nodi. In una configurazione di questo tipo, viene utilizzato un bilanciatore del carico (ad esempio, F5) per accedere agli host SnapCenter . Il repository SnapCenter (il database MySQL) viene replicato da SnapCenter tra i due host in modo che i dati SnapCenter siano sempre sincronizzati.

L'HA del server SnapCenter non è supportato se il plug-in HANA è installato sul server SnapCenter . Maggiori

dettagli su SnapCenter HA sono disponibili all'indirizzo "Configurare i server SnapCenter per l'alta disponibilità".

[larghezza=601, altezza=307]

Host plug-in centrale

Come discusso nel capitolo precedente, è necessario un plug-in centrale per

- Sistemi host multipli HANA
- Sistemi HANA in esecuzione su IBM Power

Con un host plug-in centrale, il plug-in HANA e il client hdbsql SAP HANA devono essere installati su un host esterno agli host del database HANA. Questo host può essere qualsiasi host Windows o Linux, ad esempio il server SnapCenter .

> Quando esegui il server SnapCenter su Windows, puoi utilizzare il tuo sistema Windows come host plug-in centrale. Quando esegui il tuo server SnapCenter su Linux, devi utilizzare un host diverso come host del plug-in centrale.

Per un sistema HANA con più host, le chiavi di archiviazione utente SAP HANA per tutti gli host worker e standby devono essere configurate nell'host del plug-in centrale. SnapCenter tenta di connettersi al database utilizzando ciascuna delle chiavi fornite e può quindi funzionare indipendentemente da un failover del database di sistema (server dei nomi HANA) su un host diverso.

[larghezza=601, altezza=314]

Per più sistemi HANA con host singolo gestiti da un host plug-in centrale, tutte le singole chiavi di archivio utente SAP HANA dei sistemi HANA devono essere configurate nell'host plug-in centrale.

[larghezza=601, altezza=338]

Controllo di coerenza dei blocchi SAP HANA

SAP consiglia di includere controlli regolari della coerenza dei blocchi HANA nella strategia di backup complessiva. Con i backup tradizionali basati su file, questo controllo viene eseguito a ogni operazione di backup. Con i backup Snapshot, il controllo di coerenza deve essere eseguito oltre alle operazioni di backup Snapshot, ad esempio una volta alla settimana.

Tecnicamente ci sono due opzioni per eseguire il controllo di coerenza dei blocchi.

- Esecuzione di un backup standard basato su file o backint
- Esecuzione dello strumento HANA hdbpersdiag, vedere anche "Controllo della coerenza della persistenza | Portale di assistenza SAP"

Lo strumento HANA hdbpersdiag fa parte dell'installazione di HANA e consente di eseguire operazioni di controllo della coerenza dei blocchi su un database HANA offline. Pertanto è perfetto per essere utilizzato in combinazione con i backup Snapshot, dove i backup Snapshot esistenti possono essere presentati a hdbpersdiag.

Confrontando i due approcci, hdbpersdiag presenta notevoli vantaggi rispetto al backup basato su file per i controlli di coerenza dei blocchi HANA. Una dimensione è la capacità di archiviazione richiesta. Con i backup basati su file, per ogni sistema HANA deve essere disponibile almeno la dimensione di un backup. Ad esempio, se si dispone di 15 sistemi HANA con una dimensione di persistenza di 3 TB, sarebbero necessari

altri 45 TB solo per i controlli di coerenza. Con hdbpersdiag non è richiesta alcuna capacità di archiviazione aggiuntiva poiché l'operazione viene eseguita su un backup Snapshot esistente o su un FlexClone di un backup Snapshot esistente. La seconda dimensione è il carico della CPU sull'host HANA durante l'operazione di controllo della coerenza. Un backup basato su file richiederà cicli di CPU sull'host del database HANA, mentre l'elaborazione hdbpersdiag può essere completamente scaricata dall'host HANA se utilizzata in combinazione con un host di verifica centrale. La tabella seguente riassume le caratteristiche principali.

	Capacità di archiviazione richiesta	Carico di CPU e rete sull'host HANA
Backup basato su file	Dimensione minima del backup dei dati pari a 1 x per ogni sistema HANA	Alto
hdbpersdiag utilizzando la directory Snapshot sull'host HANA (solo NFS)	Nessuno	Medio
Host di verifica centrale utilizzato per eseguire hdbpersdiag con volumi FlexClone	Nessuno	Nessuno

NetApp consiglia di utilizzare hdbpersdiag per eseguire i controlli di coerenza dei blocchi HANA. Ulteriori dettagli sull'implementazione sono disponibili nel capitolo "Controlli di coerenza dei blocchi con SnapCenter".

Strategia di protezione dei dati

Prima di configurare SnapCenter e il plug-in SAP HANA, la strategia di protezione dei dati deve essere definita in base ai requisiti RTO e RPO dei vari sistemi SAP.

Un approccio comune consiste nella definizione di tipi di sistema quali produzione, sviluppo, test o sistemi sandbox. Tutti i sistemi SAP dello stesso tipo di sistema hanno in genere gli stessi parametri di protezione dei dati.

I parametri da definire sono:

- Con quale frequenza deve essere eseguito un backup Snapshot?
- Per quanto tempo i backup delle copie Snapshot devono essere conservati nel sistema di storage primario?
- Con quale frequenza deve essere eseguito un controllo dell'integrità dei blocchi?
- I backup primari devono essere replicati su un sito di backup secondario?
- Per quanto tempo i backup devono essere conservati nell'archivio di backup secondario?

La tabella seguente mostra un esempio di parametri di protezione dei dati per i tipi di sistema produzione, sviluppo e test. Per il sistema di produzione è stata definita un'elevata frequenza di backup e i backup vengono replicati su un sito di backup secondario una volta al giorno. I sistemi di test hanno requisiti inferiori e non richiedono la replica dei backup.

Parametri	Sistemi di produzione	Sistemi di sviluppo	Sistemi di test
Frequenza di backup	Ogni 6 ore	Ogni 6 ore	Ogni 12 ore
Conservazione primaria	3 giorni	3 giorni	6 giorni

Parametri	Sistemi di produzione	Sistemi di sviluppo	Sistemi di test
Controllo dell'integrità del blocco	Una volta alla settimana	Una volta alla settimana	No
Replica sul sito di backup secondario	Una volta al giorno	Una volta al giorno	No
Conservazione del backup secondario	2 settimane	2 settimane	No

Nella tabella seguente sono riportati i criteri e le pianificazioni che devono essere configurati per i parametri di protezione dei dati sopra indicati.

Politica	Tipo di backup	Frequenza di pianificazione	Conservazione primaria	Replica SnapVault	Ritenzione secondaria
LocalSnap	Basato su Snapshot	Ogni 6 ore	Conteggio=12	No	NA
LocalSnapAndSnapVault	Basato su Snapshot	Una volta al giorno	Conteggio=2	Sì	Conteggio=14
SnapAndCallHdbpersdiag	Basato su Snapshot	Una volta alla settimana	Conteggio=2	No	NA

Per il sistema ONTAP o FSx per ONTAP, è necessario configurare una relazione di protezione dei dati in ONTAP per la replica SnapVault , prima che SnapCenter possa eseguire le operazioni di aggiornamento SnapVault . La conservazione secondaria è definita all'interno della policy di protezione ONTAP .

Per il backup ANF non è richiesta alcuna configurazione aggiuntiva al di fuori di SnapCenter. La conservazione secondaria del backup ANF è gestita da SnapCenter.

Per questa configurazione di esempio, hdbpersdiag viene utilizzato per l'operazione di controllo dell'integrità del blocco. Maggiori dettagli possono essere trovati nel capitolo "Controlli di coerenza dei blocchi con SnapCenter".

La figura seguente riassume le pianificazioni e le conservazioni dei backup. Se si utilizza SnapCenter per gestire la conservazione dei backup dei log, tutti i backup dei log più vecchi del backup Snapshot più vecchio verranno eliminati. In altre parole, i backup del registro vengono conservati per tutto il tempo necessario a consentire il ripristino in tempo utile per ogni backup disponibile.

[larghezza=601, altezza=192]

Backup delle chiavi radice di crittografia

Quando si utilizza la crittografia persistente HANA, è fondamentale creare backup delle chiavi radice oltre ai backup dei dati standard. I backup della chiave radice sono necessari per ripristinare il database HANA nel caso in cui il volume di dati e il file system di installazione HANA vengano persi. Per maggiori informazioni vedere "Guida all'amministrazione di SAP HANA".

Tieni presente che se una chiave radice viene modificata, la nuova chiave radice non può essere utilizzata per ripristinare i vecchi backup del database HANA creati in precedenza. È sempre necessaria la chiave radice attiva al momento della creazione del backup.

Operazioni di backup

SnapCenter supporta le operazioni di backup Snapshot dei sistemi HANA MDC con uno o più tenant. SnapCenter supporta anche due diverse operazioni di ripristino di un sistema HANA MDC. È possibile ripristinare l'intero sistema, il database di sistema e tutti i tenant, oppure ripristinare solo un tenant. Per consentire a SnapCenter di eseguire queste operazioni, sono necessari alcuni prerequisiti.

In un sistema MDC, la configurazione del tenant non è necessariamente statica. È possibile aggiungere o eliminare inquilini. SnapCenter non può basarsi sulla configurazione rilevata quando il database HANA viene aggiunto a SnapCenter. Per abilitare un'operazione di ripristino di un singolo tenant, SnapCenter deve sapere quali tenant sono inclusi in ciascun backup Snapshot. Inoltre, deve sapere quali file e directory appartengono a ciascun tenant incluso nel backup Snapshot.

Pertanto, a ogni operazione di backup, SnapCenter identifica le informazioni sul tenant. Ciò include i nomi dei tenant e le informazioni corrispondenti sui file e sulle directory. Questi dati devono essere archiviati nei metadati del backup Snapshot per poter supportare un'operazione di ripristino di un singolo tenant.

Un altro passaggio del rilevamento automatico dell'applicazione è il rilevamento del nodo primario o secondario di HANA System Replication (HSR). Se un sistema HANA è configurato con HSR, SnapCenter deve identificare il nodo primario con ogni operazione di backup in modo che i comandi SQL di backup vengano eseguiti sul nodo primario HSR. Vedi anche "Replica di sistema SAP HANA - backup e recovery con SnapCenter".

SnapCenter rileva anche la configurazione del volume dati HANA e la mappa al file system e alle risorse di archiviazione. Con questo approccio, SnapCenter può gestire le modifiche alla configurazione del volume HANA, ad esempio più partizioni o modifiche alla configurazione dell'archiviazione come le migrazioni dei volumi.

Il passaggio successivo è l'operazione di backup Snapshot vera e propria. Questo passaggio include il comando SQL per attivare lo snapshot del database HANA, il backup dello snapshot di archiviazione e il comando SQL per chiudere l'operazione di snapshot HANA. Utilizzando il comando close, il database HANA aggiorna il catalogo di backup del DB di sistema e di ciascun tenant.

SAP non supporta le operazioni di backup Snapshot per i sistemi MDC quando uno o più tenant vengono arrestati.

Per la gestione della conservazione dei backup dei dati e della gestione del catalogo di backup HANA, SnapCenter deve eseguire le operazioni di eliminazione del catalogo per il database di sistema e per tutti i database tenant identificati nella prima fase. Allo stesso modo per i backup dei log, il flusso di lavoro di SnapCenter deve operare su ogni tenant che faceva parte dell'operazione di backup.

La figura seguente mostra una panoramica del flusso di lavoro di backup.

[larghezza=601, altezza=237]

Gestione della conservazione dei backup

La gestione della conservazione dei backup dei dati e la gestione del backup dei log possono essere suddivise in cinque aree principali, tra cui la gestione della conservazione di:

- Backup locali nello storage primario
- Backup basati su file
- Backup su storage secondario (backup SnapVault o ANF)
- Backup dei dati nel catalogo di backup SAP HANA
- Backup dei log nel catalogo di backup SAP HANA e sul file system

La figura seguente fornisce una panoramica dei diversi flussi di lavoro e delle dipendenze di ciascuna operazione. Le sezioni seguenti descrivono in dettaglio le diverse operazioni.

[larghezza=601, altezza=309]

Gestione della conservazione dei backup locali nello storage primario

SnapCenter gestisce la gestione dei backup del database SAP HANA e dei backup dei volumi non dati eliminando le copie Snapshot sullo storage primario e nel repository SnapCenter in base a una conservazione definita nella policy di backup SnapCenter . La gestione della conservazione è inclusa in ogni flusso di lavoro di backup in SnapCenter. I backup locali nell'archivio primario possono anche essere eliminati manualmente in SnapCenter.

Gestione della conservazione dei backup basati su file

SnapCenter gestisce la gestione dei backup basati su file eliminando i backup dal file system in base a una conservazione definita nei criteri di backup SnapCenter . La logica di gestione della conservazione viene eseguita con ogni flusso di lavoro di backup in SnapCenter.

Gestione della conservazione dei backup nello storage secondario (SnapVault)

La gestione della conservazione dei backup nell'archivio secondario (SnapVault) è gestita da ONTAP in base alla conservazione definita nella relazione di protezione ONTAP . Per sincronizzare queste modifiche sullo storage secondario nel repository SnapCenter , SnapCenter utilizza un processo di pulizia pianificato. Questo processo di pulizia sincronizza tutti i backup dell'archiviazione secondaria con il repository SnapCenter per tutti i plug-in SnapCenter e tutte le risorse.

Per impostazione predefinita, il lavoro di pulizia viene programmato una volta alla settimana. Questa pianificazione settimanale comporta un ritardo nell'eliminazione dei backup in SnapCenter e SAP HANA Studio rispetto ai backup già eliminati nell'archivio secondario. Per evitare questa incoerenza, i clienti possono modificare la programmazione impostando una frequenza maggiore, ad esempio una volta al giorno. Per i dettagli su come adattare la pianificazione del lavoro di pulizia o come attivare un aggiornamento manuale, fare riferimento al capitolo "Pulizia dei backup secondari".

Gestione della conservazione dei backup nello storage secondario (backup ANF)

La conservazione dei backup ANF è configurata e gestita da SnapCenter. SnapCenter gestisce la gestione dei backup ANF eliminandoli in base a una conservazione definita nei criteri di backup SnapCenter . La gestione della conservazione è inclusa in ogni flusso di lavoro di backup in SnapCenter.

Gestione della conservazione dei backup dei dati all'interno del catalogo di backup SAP HANA

Quando SnapCenter elimina un backup, uno snapshot locale o basato su file, oppure se SnapCenter identifica l'eliminazione di un backup nell'archivio secondario, questo backup dei dati viene eliminato anche nel catalogo dei backup SAP HANA. Prima di eliminare la voce del catalogo SAP HANA per un backup Snapshot locale nello storage primario, SnapCenter verifica se il backup esiste ancora nello storage secondario.

Gestione della conservazione dei backup dei log

Il database SAP HANA crea automaticamente backup dei log. Queste operazioni creano file di backup per ogni singolo servizio SAP HANA in una directory di backup configurata in SAP HANA. I backup del log più vecchi dell'ultimo backup dei dati non sono più necessari per il ripristino futuro e possono quindi essere eliminati. SnapCenter gestisce la gestione dei backup dei file di registro a livello di file system e nel catalogo di backup SAP HANA eseguendo i seguenti passaggi:

1. SnapCenter legge il catalogo di backup SAP HANA per ottenere l'ID del backup dei dati più vecchio eseguito correttamente.
2. SnapCenter elimina tutti i backup dei log nel catalogo SAP HANA e il file system che sono più vecchi di questo ID di backup.

> SnapCenter gestisce l'housekeeping solo per i backup creati da SnapCenter. Se vengono creati backup aggiuntivi basati su file al di fuori di SnapCenter, è necessario assicurarsi che i backup basati su file vengano eliminati dal catalogo di backup. Se tale backup dei dati non viene eliminato manualmente dal catalogo di backup, può diventare il backup dei dati meno recente e i backup dei log meno recenti non vengono cancellati fino a quando questo backup basato su file non viene eliminato.

> Anche se la conservazione è definita per i backup su richiesta nella configurazione della policy, la manutenzione viene eseguita solo quando viene eseguito un altro backup su richiesta. Pertanto, i backup on-demand devono in genere essere eliminati manualmente in SnapCenter per assicurarsi che vengano eliminati anche nel catalogo di backup SAP HANA e che la gestione dei backup dei log non si basi su un vecchio backup on-demand.

> La gestione della conservazione del backup del registro è abilitata per impostazione predefinita. Se necessario, è possibile disattivarlo come descritto nella sezione Disattivare la gestione automatica del backup dei log.

Scopri come configurare SnapCenter per gli ambienti SAP HANA

Configurare SnapCenter per gli ambienti SAP HANA utilizzando un approccio in due fasi: configurazione iniziale per le risorse condivise (credenziali, sistemi di archiviazione e policy) e configurazione specifica delle risorse per i singoli sistemi HANA (distribuzione host, rilevamento automatico e impostazioni di protezione).

La configurazione SnapCenter per un ambiente SAP HANA con più sistemi HANA può essere suddivisa in due aree principali:

- La configurazione iniziale
  - Configurazioni di credenziali, archiviazione e policy. + Queste impostazioni o risorse vengono in genere utilizzate da più sistemi HANA.
- Configurazione specifica delle risorse HANA
  - La configurazione dell'host, di HANA e della protezione delle risorse deve essere eseguita individualmente per ogni sistema HANA.

La figura seguente illustra i diversi componenti di configurazione e le relative dipendenze.

Tutti i passaggi della configurazione sono descritti in dettaglio negli argomenti seguenti.

> Le descrizioni e gli screenshot presenti nel documento si basano sui sistemi HANA rilevati automaticamente SnapCenter . Ulteriori o diversi passaggi di configurazione per le risorse configurate manualmente con un host plug-in centrale sono descritti in "Configurazione host del plug-in centrale".

[larghezza=601, altezza=319]

Configurare le impostazioni iniziali SnapCenter per SAP HANA

Configurare le impostazioni iniziali SnapCenter per gli ambienti SAP HANA impostando le credenziali per i principali servizi di Azure, aggiungendo sistemi di archiviazione e creando policy per i backup Snapshot, i controlli di integrità dei blocchi e la replica secondaria.

La configurazione iniziale SnapCenter include i seguenti passaggi:

1. Configurazione delle credenziali
   a. Per i sistemi HANA configurati con Azure NetApp Files (ANF), è necessario preparare un'entità servizio e quindi configurarla in SnapCenter.
   b. È necessario fornire le credenziali dell'host per consentire l'installazione automatica del plug-in HANA sugli host del database HANA.
2. Configurazione del sistema storage
   a. Per i sistemi HANA configurati con ANF, è possibile selezionare gli account NetApp richiesti e aggiungerli alla configurazione SnapCenter .
   b. Per i sistemi di storage ONTAP o FSx per ONTAP , è possibile aggiungere a SnapCenter sia le SVM che l'intero cluster di storage.
3. Configurazione dei criteri
   a. È possibile configurare policy per backup basati su snapshot e operazioni di controllo dell'integrità dei blocchi per ANF e per sistemi di archiviazione ONTAP e FSx per ONTAP .
   b. I criteri per snapshot a prova di manomissione e backup secondari con SnapVault o SnapMirror possono essere configurati solo per i sistemi di archiviazione ONTAP e FSx per ONTAP .
   c. Per i sistemi HANA configurati con ANF, una policy può includere "Backup ANF".

> Gli stessi criteri di backup Snapshot possono essere utilizzati per i database HANA e per i volumi non dati, ad esempio il volume condiviso HANA.

La figura seguente riassume le sezioni di configurazione.

[larghezza=601, altezza=158]

Nei capitoli seguenti vengono descritti i passaggi iniziali della configurazione.

Configurazione delle credenziali

Credenziali per la distribuzione del plug-in HANA

Le credenziali vengono configurate nella sezione Impostazioni e selezionando la scheda Credenziali. È possibile aggiungere le credenziali cliccando sull'icona +.

[larghezza=601, altezza=118]

NetApp consiglia di configurare un utente su tutti gli host del database HANA (ad esempio scuser) e di configurare i privilegi sudo come descritto in "Prerequisiti per l'aggiunta di host e l'installazione del plug-in SnapCenter per il database SAP HANA".

[larghezza=287, altezza=247]

Credenziali per Azure NetApp Files

È necessario preparare un'entità servizio di Azure che consenta a SnapCenter di eseguire le operazioni richieste per i volumi ANF. L'esempio seguente mostra le autorizzazioni minime richieste che devono essere incluse.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/latestRestoreStatus
/current/read",

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

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

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

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

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

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

Le credenziali vengono configurate nella sezione Impostazioni e selezionando la scheda Credenziali. Le credenziali vengono configurate cliccando sull'icona +.

[larghezza=601, altezza=116]

Nella schermata seguente, è necessario specificare un nome per le credenziali e selezionare la modalità di autenticazione Credenziali di Azure. Quindi è necessario configurare l'ID tenant, l'ID client e la chiave segreta

client.

[larghezza=252, altezza=246]

Configurazione del sistema storage

Sistemi ONTAP e FSx per ONTAP

Il sistema ONTAP o FSx per ONTAP può essere aggiunto a SnapCenter fornendo le credenziali del cluster o le credenziali per ogni SVM richiesta. Quando vengono fornite le credenziali del cluster, tutte le SVM del cluster vengono aggiunte a SnapCenter.

Nella configurazione del nostro laboratorio, abbiamo aggiunto i cluster di archiviazione a SnapCenter. I cluster ONTAP vengono configurati nella sezione Sistemi di archiviazione selezionando la scheda Archiviazione ONTAP e il tipo di cluster ONTAP . Per aggiungere un nuovo cluster, fare clic sull'icona +.

[larghezza=601, altezza=117]

Nella schermata seguente è necessario fornire le credenziali per un utente del cluster.

> Non si dovrebbe utilizzare l'utente admin del cluster. Invece dovrebbe essere creato un nuovo utente con i privilegi richiesti come descritto in "Creare ruoli cluster ONTAP con privilegi minimi"I privilegi richiesti per il sistema ASA possono essere trovati su "Creare ruoli cluster ONTAP per sistemi ASA r2".

[larghezza=299, altezza=176]

Gli SVM vengono configurati nella sezione Sistemi di archiviazione selezionando la scheda Archiviazione ONTAP e il tipo di SVMS ONTAP . Per aggiungere un nuovo SVM, fare clic sull'icona +.

Nella schermata seguente è necessario fornire le credenziali per un utente del cluster.

> L'utente SVM vsadmin non deve essere utilizzato. Invece dovrebbe essere creato un nuovo utente con i privilegi richiesti come descritto in "Creare ruoli SVM con privilegi minimi"I privilegi richiesti per il sistema ASA possono essere trovati su "Creare ruoli SVM per i sistemi ASA r2".

> Il nome DNS per l'SVM deve corrispondere al nome SVM configurato nel sistema ONTAP .

[larghezza=331, altezza=199]

Azure NetApp Files

Dopo aver configurato le credenziali ANF, è possibile aggiungere gli account ANF NetApp a SnapCenter. Gli account NetApp vengono configurati nella sezione Sistemi di archiviazione e selezionando la scheda Azure NetApp Files . Per aggiungere un nuovo account NetApp , fare clic sull'icona +.

[larghezza=601, altezza=117]

Dopo aver selezionato le credenziali ANF e l'abbonamento, è possibile aggiungere un account NetApp a SnapCenter.

[larghezza=401, altezza=176]

Configurazione dell'archiviazione quando si utilizza SnapMirror ActiveSync

I passaggi specifici della configurazione dell'archiviazione sono descritti in "Configurazione dell'archiviazione con SnapMirror ActiveSync".

Configurazione dei criteri

Come discusso nella sezione, le policy della strategia di protezione dei dati sono solitamente configurate indipendentemente dalla risorsa e possono essere utilizzate per più sistemi SAP HANA.

Una configurazione minima tipica è costituita dai seguenti criteri:

- Criterio per backup orari senza replica
- Criteri per i backup giornalieri con replica di backup SnapVault o ANF
- Politica per l'operazione di controllo settimanale dell'integrità dei blocchi
  - utilizzando un backup basato su file
  - utilizzando lo strumento HANA hdbpersdiag

Le sezioni seguenti descrivono la configurazione di questi tre criteri.

Le policy vengono configurate nella sezione Impostazioni e selezionando la scheda Policy. Per configurare una nuova policy, fare clic sull'icona +. I due screenshot seguenti mostrano l'elenco dei criteri per i sistemi HANA in esecuzione con Azure NetApp Files e un secondo per i sistemi HANA in esecuzione con sistemi di archiviazione ONTAP o FSx per ONTAP.

[larghezza=601, altezza=133]

[larghezza=601, altezza=138]

Backup snapshot con sistemi ONTAP e FSx per ONTAP

I criteri di backup degli snapshot per il sistema ONTAP o FSx per ONTAP possono combinare uno snapshot locale con operazioni di replica o di blocco degli snapshot (snapshot antimanomissione). Questo esempio mostra una policy con replica su un archivio secondario tramite SnapVault.

Fornire un nome per la policy e una descrizione facoltativa.

[larghezza=376, altezza=103]

Selezionare il tipo di archiviazione ONTAP e l'ambito della policy Snapshot.

[larghezza=385, altezza=97]

Per questa policy è stato configurato un tipo di pianificazione giornaliera. Verrà creato uno Snapshot giornaliero e i delta degli Snapshot verranno replicati nello storage secondario tramite SnapVault.

La pianificazione stessa è configurata con la configurazione di protezione delle risorse HANA individuale.

La conservazione configurata nella policy è valida solo per gli snapshot primari. La conservazione nella destinazione SnapVault è configurata con la relazione di replica ONTAP per i singoli volumi del database HANA come descritto nel capitolo "Operazioni di backup snapshot SAP HANA". L'etichetta Snapshot configurata nel criterio deve corrispondere all'etichetta configurata con la relazione di replica ONTAP .

Il blocco degli snapshot (snapshot antimanomissione) può essere abilitato facendo clic sulle caselle di controllo e definendo il periodo di blocco. Questa funzionalità richiede una licenza SnapLock sul sistema di archiviazione e la configurazione dell'orologio di conformità.

Una policy per gli Snapshot locali verrebbe configurata solo con una pianificazione oraria e disattivando la casella di controllo Aggiorna SnapVault .

[larghezza=378, altezza=352]

La schermata riepilogativa mostra i parametri configurati.

[larghezza=385, altezza=119]

Backup snapshot con Azure NetApp Files

I criteri di backup degli snapshot per Azure NetApp Files possono combinare uno snapshot locale con un backup ANF, che replica i dati dello snapshot nel BLOB di Azure. Questo esempio mostra una policy utilizzata per la replica con backup ANF.

Fornire un nome per la policy e una descrizione facoltativa.

[larghezza=356, altezza=95]

Selezionare il tipo di archiviazione Azure NetApp Files e l'ambito dei criteri Snapshot.

[larghezza=360, altezza=102]

Per questa policy è stato configurato un tipo di pianificazione giornaliera. Verrà creato uno snapshot giornaliero e i delta dello snapshot verranno replicati nel vault di backup utilizzando il backup ANF.

> La pianificazione stessa è configurata con la configurazione di protezione delle risorse HANA individuale.

La conservazione degli snapshot configurata nel criterio è valida per gli snapshot primari nel volume ANF. La conservazione per il backup ANF è configurata con le impostazioni di conservazione del backup.

Una policy per gli snapshot locali verrebbe configurata solo con una pianificazione oraria e disattivando la casella di controllo Abilita backup.

[larghezza=373, altezza=361]

La schermata riepilogativa mostra i parametri configurati.

[larghezza=376, altezza=138]

Operazioni di controllo dell'integrità dei blocchi per tutte le piattaforme

Strumento HANA hdbpersdiag

I dettagli sono descritti nel capitolo "Controlli di coerenza dei blocchi con SnapCenter".

Backup basato su file

Fornire un nome per la policy e una descrizione facoltativa.

[larghezza=346, altezza=95]

Selezionare il tipo di archiviazione ONTAP o Azure NetApp Files , a seconda della configurazione, e selezionare l'ambito dei criteri basati su file.

[larghezza=357, altezza=98]

Come detto, si consiglia di eseguire il controllo dell'integrità del blocco una volta alla settimana. Per questo motivo viene scelto un programma settimanale.

La pianificazione stessa è configurata con la configurazione di protezione delle risorse HANA individuale.

Il file system in cui viene scritto il backup basato su file deve fornire capacità sufficiente per un backup in più rispetto a quanto definito nelle impostazioni di conservazione, perché SnapCenter elimina il vecchio backup dopo la creazione di quello nuovo. In questo esempio è necessario spazio per due backup, con conservazione di uno. La conservazione minima configurabile è zero.

[larghezza=351, altezza=173]

La schermata riepilogativa mostra i parametri configurati.

[larghezza=366, altezza=101]

Configurazione dei criteri quando si utilizza SnapMirror ActiveSync

I passaggi specifici per la configurazione della policy sono descritti nel documento "Configurazione dei criteri SnapMirror ActiveSync".

Configurare le risorse SnapCenter per singoli database SAP HANA

Configurare singoli database SAP HANA in SnapCenter creando utenti di backup e chiavi di archiviazione utente, impostando la replicazione dell'archiviazione per i backup secondari, distribuendo il plug-in HANA per il rilevamento automatico e configurando la protezione delle risorse con policy e pianificazioni.

La configurazione di un database HANA in SnapCenter avviene tramite i seguenti passaggi:

1. Un utente di backup SnapCenter deve essere configurato nel database di sistema HANA e una chiave di archivio utente SAP HANA deve essere impostata nell'host del database HANA
2. Se è richiesta la replica dei dati su un archivio secondario, è necessario configurare la replica dell'archivio ONTAP per il volume di dati HANA
3. Il plug-in SnapCenter HANA deve essere distribuito sull'host del database HANA
    a. Il processo di rilevamento automatico viene avviato
    b. La chiave dell'archivio utente SAP HANA deve essere configurata in SnapCenter
    c. Viene avviata la seconda fase di rilevamento automatico e la risorsa HANA viene aggiunta automaticamente da SnapCenter

4. La protezione delle risorse HANA deve essere configurata per la nuova risorsa HANA aggiunta

La configurazione iniziale SnapCenter , come descritto nell'argomento precedente "Configurazione iniziale di SnapCenter" deve essere eseguita per prima, poiché durante la configurazione delle risorse del database HANA sono richieste credenziali, sistemi di archiviazione e policy. La figura seguente riassume i passaggi e le dipendenze.

La figura seguente visualizza i diversi componenti di configurazione e le dipendenze.

[larghezza=601, altezza=315] Le sezioni seguenti forniscono una descrizione dettagliata dei passaggi di configurazione richiesti.

Configurazione dell'utente di backup SAP HANA e dell'archivio utenti SAP HANA

NetApp consiglia di configurare un utente dedicato nel database HANA per eseguire le operazioni di backup con SnapCenter. Come secondo passaggio, viene configurata una chiave di archivio utente SAP HANA per questo utente di backup e la chiave di archivio utente SAP HANA viene fornita nella configurazione SnapCenter .

La figura seguente mostra SAP HANA Studio tramite il quale è possibile creare l'utente di backup, in questo esempio SNAPCENTER.

L'utente di backup deve essere configurato con i privilegi di amministratore di backup, lettura catalogo, amministratore di backup del database e operatore di ripristino del database.

L'utente di backup deve essere creato nel database di sistema perché tutti i comandi di backup per il sistema e i database tenant vengono eseguiti tramite il database di sistema.

[larghezza=601, altezza=382]

Configurazione dell'archivio utenti SAP HANA sull'host del database HANA

SnapCenter utilizza l'utente <sid>adm per comunicare con il database HANA. Pertanto, la chiave dell'archivio utenti SAP HANA deve essere configurata utilizzando l'utente <sid>adm sull'host del database.

hdbuserstore set <nome-chiave> <host>:<porta> <utente database> <password>

Per un sistema SAP HANA MDC, la porta del database di sistema HANA è 3<instanceNo>13.

Esempi di configurazione dell'archivio utenti SAP HANA

L'output mostra la chiave SS1KEY che è stata configurata per il sistema HANA con numero di istanza = 00.

```
ss1adm@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.
ss1adm@hana-1:/usr/sap/SS1/HDB00>
```

L'output mostra la chiave SM1KEY che è stata configurata per il sistema HANA con numero di istanza = 12.

```
sm1adm@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.
sm1adm@hana-2:/usr/sap/SM1/HDB12>
```

Configurazione della replicazione dello storage

La configurazione della relazione di protezione dei dati e il trasferimento iniziale dei dati devono essere eseguiti prima che gli aggiornamenti di replica possano essere gestiti da SnapCenter.

Gli screenshot seguenti mostrano una configurazione che utilizza il gestore di sistema ONTAP . Per i sistemi FSx per ONTAP la replica deve essere eseguita utilizzando l' ONTAP CLI come descritto in "Panoramica - replica di backup con SnapVault".

La figura seguente mostra la relazione di protezione configurata per il volume di dati del sistema SAP HANA

SS1. In questo esempio, il volume di origine SS1_data_mnt00001 nell'SVM hana-primary viene replicato nell'SVM hana-backup e nel volume di destinazione SS1_data_mnt00001_dst.

[larghezza=601, altezza=183]

La figura seguente mostra la policy di protezione creata per questa configurazione di laboratorio. La policy di protezione utilizzata per la relazione di protezione definisce l'etichetta SnapMirror , nonché la conservazione dei backup nell'archivio secondario. In questo esempio, l'etichetta utilizzata è Giornaliera e la conservazione è impostata su 5.

L'etichetta SnapMirror nella policy di replica deve corrispondere all'etichetta definita nella configurazione della policy SnapCenter .

La pianificazione della relazione deve essere impostata su Nessuno, perché SnapCenter attiva l'aggiornamento SnapVault come parte dell'operazione di backup in base allo Snapshot coerente con l'applicazione creato in precedenza.

La conservazione dei backup nell'archivio di backup secondario è definita nella policy e controllata da ONTAP.

[larghezza=601, altezza=180]

Configurazione di backup ANF

Per il backup ANF non è richiesta alcuna preparazione specifica. Non appena viene eseguito il primo backup con backup ANF abilitato, SnapCenter crea un vault di backup di Azure con il nome snapcenter-vault. Questo archivio di backup viene quindi utilizzato da tutte le successive operazioni di backup ANF eseguite da SnapCenter.

[larghezza=601, altezza=227]

Distribuzione del plug-in SnapCenter per SAP HANA

I requisiti dell'host sono elencati qui "Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux".

L'implementazione del plug-in HANA avviene facendo clic sul pulsante Aggiungi nella sezione Host dell'interfaccia utente di SnapCenter .

[larghezza=601, altezza=145]

Nella schermata Aggiungi host, è necessario fornire il tipo e il nome dell'host, nonché le credenziali da utilizzare per il processo di distribuzione. Inoltre, è necessario selezionare il plug-in SAP HANA. Cliccando su Invia si avvia il processo di distribuzione.

Per questa descrizione non abbiamo aggiunto un nuovo host, ma mostriamo la configurazione degli host esistenti in SnapCenter.

[larghezza=601, altezza=154]

Rilevamento automatico HANA

Una volta completata la distribuzione del plug-in HANA, viene avviato il processo di rilevamento automatico. Nella prima fase vengono rilevate solo le impostazioni di base e SnapCenter crea una nuova risorsa che viene elencata nella sezione Risorse dell'interfaccia utente ed è contrassegnata da un lucchetto rosso.

[larghezza=601, altezza=169]

Facendo clic sulla risorsa, verrà richiesta la chiave di archivio utente SAP HANA per questo database HANA.

[larghezza=316, altezza=180]

Dopo aver fornito la chiave, ha inizio la seconda fase del processo di rilevamento automatico. Il processo di rilevamento automatico rileva tutti i database tenant nel sistema HANA, i dettagli di configurazione del backup di log e cataloghi e i ruoli di replica del sistema HANA. Inoltre, i dettagli sull'ingombro dello storage vengono rilevati automaticamente. È possibile verificare queste impostazioni selezionando una risorsa e cliccando sul pulsante Dettagli.

Questo processo di rilevamento automatico viene eseguito a ogni operazione di backup, in modo che tutte le modifiche apportate al sistema HANA rilevanti per l'operazione di backup vengano rilevate automaticamente.

[larghezza=601, altezza=219]

Configurazione della protezione delle risorse

La schermata di configurazione della protezione delle risorse si apre facendo clic su una risorsa al termine del processo di rilevamento automatico. Gli screenshot presenti in questa documentazione mostrano la configurazione di protezione di una risorsa esistente.

Configura un formato di nome personalizzato per lo Snapshot. NetApp consiglia di utilizzare un nome Snapshot personalizzato per identificare facilmente quali backup sono stati creati con quale criterio e tipo di pianificazione.

Nella configurazione illustrata nella figura seguente, i nomi delle copie Snapshot e di backup hanno il seguente formato:

- Backup orario pianificato: + SnapCenter_<nome-host>_LocalSnap_Hourly_<time_stamp>
- Backup giornaliero pianificato: + SnapCenter_<nome-host>_LocalSnapAndSnapVault_Daily_<time_stamp>

[larghezza=601, altezza=294]

Nella schermata successiva è possibile configurare gli script che devono essere eseguiti in vari passaggi del flusso di lavoro di backup.

[larghezza=601, altezza=294]

Ora le policy sono associate alla risorsa e le pianificazioni sono definite.

In questo esempio abbiamo configurato

- Un controllo settimanale dell'integrità del blocco, ogni domenica

- Un backup Snapshot locale, ogni 4 ore
- Un backup Snapshot giornaliero con replica SnapVault una volta al giorno

[larghezza=601, altezza=294]

È possibile configurare la notifica via e-mail.

[larghezza=601, altezza=294]

Una volta completata la configurazione della protezione delle risorse, i backup pianificati verranno eseguiti in base alle impostazioni definite.

Configurare SnapCenter per eseguire il backup di volumi non dati

Configurare SnapCenter per eseguire il backup di volumi non dati, quali file eseguibili, file di configurazione, file di traccia e dati del server applicativo.

La protezione del volume di dati del database è sufficiente per ripristinare e ripristinare il database SAP HANA in un dato momento, a condizione che le risorse di installazione del database e i registri richiesti siano ancora disponibili.

Per ripristinare situazioni in cui è necessario ripristinare altri file non dati, NetApp consiglia di sviluppare una strategia di backup aggiuntiva per i volumi non dati per integrare il backup del database SAP HANA. A seconda delle esigenze specifiche, il backup di volumi non dati potrebbe variare in termini di frequenza di pianificazione e impostazioni di conservazione; è inoltre opportuno considerare la frequenza con cui vengono modificati i file non dati. Ad esempio, il volume HANA /hana/shared contiene file eseguibili, file di configurazione ma anche file di traccia SAP HANA. Sebbene gli eseguibili cambino solo quando il database SAP HANA viene aggiornato, i file di configurazione e traccia di SAP HANA potrebbero richiedere una frequenza di backup più elevata. Anche i volumi del server applicativo SAP possono essere protetti con SnapCenter utilizzando backup di volumi non dati.

Il backup di volumi non dati SnapCenter consente di creare copie Snapshot di tutti i volumi rilevanti in pochi secondi, con la stessa efficienza di spazio dei backup del database SAP HANA. La differenza è che non è richiesta alcuna interazione con il database SAP HANA.

Dalla scheda Resource, selezionare non-Data-Volume e fare clic su Add SAP HANA Database (Aggiungi database SAP HANA).

[larghezza=601, altezza=173]

[larghezza=601, altezza=112]

Nella fase uno della finestra di dialogo Add SAP HANA Database (Aggiungi database SAP HANA), nell'elenco Resource Type (tipo di risorsa), selezionare non-data Volumes (volumi non dati). Specificare un nome per la risorsa, il SID associato e l'host del plug-in SAP HANA che si desidera utilizzare per la risorsa, quindi fare clic su Avanti.

[larghezza=332, altezza=310]

Per i sistemi ONTAP e FSx per ONTAP , selezionare il tipo di storage ONTAP e aggiungere gli SVM e i volumi di storage come footprint di storage, quindi fare clic su Avanti.

[larghezza=332, altezza=312]

Per ANF selezionare il tipo di archiviazione Azure NetApp Files, selezionare l'account NetApp e il pool di capacità e aggiungere i volumi ANF come footprint di archiviazione, quindi fare clic su Avanti.

[larghezza=350, altezza=337]

Nella fase di riepilogo, fare clic su fine per salvare le impostazioni.

Ripetere questi passaggi per tutti i volumi non dati richiesti. Procedere con la configurazione della protezione della nuova risorsa.

La configurazione della protezione dei dati per le risorse non di volume dati è identica al flusso di lavoro per le risorse del database SAP HANA e può essere definita a livello di singola risorsa.

Configurare l'host del plug-in centrale SnapCenter per SAP HANA

Distribuire il plug-in SnapCenter HANA su un host centrale per supportare i sistemi SAP HANA multi-host o i sistemi HANA su IBM Power. Questa procedura include l'installazione del plug-in su un host Windows o Linux, la configurazione del client hdbsql SAP HANA e l'impostazione delle chiavi di archiviazione utente per ciascun sistema HANA protetto.

Come discusso in "Opzioni di distribuzione per il plug-in SnapCenter per SAP HANA", il plug-in HANA può essere distribuito al di fuori del database HANA per supportare una configurazione di plug-in centrale richiesta dai sistemi host multipli SAP HANA o dagli ambienti SAP HANA su IBM Power.

L'host centrale del plug-in può essere qualsiasi host Windows o Linux, ma in genere viene utilizzato come host centrale del plug-in il server SnapCenter stesso.

La configurazione di un host plug-in centrale consiste nei seguenti passaggi:

- Distribuzione del plug-in SnapCenter HANA
- Installazione e configurazione del client hdbsql SAP HANA
- Configurazione dell'archivio utenti SAP HANA per ciascun sistema HANA protetto dall'host plug-in centrale

Distribuzione del plug-in SnapCenter HANA

I requisiti dell'host sono elencati qui "Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux".

L'host del plug-in centrale viene aggiunto come host e il plug-in SAP HANA viene installato sull'host. Lo screenshot qui sotto mostra la distribuzione del plug-in su un server SnapCenter in esecuzione su Windows.

1. Accedere a hosts e fare clic su Add (Aggiungi).
2. Fornire le informazioni sull'host richieste. Fare clic su Invia.

[larghezza=601, altezza=166]

Installazione e configurazione del software client SAP HANA hdbsql

Il software client hdbsql di SAP HANA deve essere installato sullo stesso host su cui è installato il plug-in SAP HANA. Il software può essere scaricato dal sito "Portale di supporto SAP".

L'utente del sistema operativo hdbsql configurato durante la configurazione delle risorse HANA deve essere in grado di eseguire l'eseguibile hdbsql. Il percorso all'eseguibile hdbsql deve essere configurato nel file hana.properties o nei parametri del percorso di ricerca (%PATH%, $PATH) dell'utente del sistema operativo.

Host plug-in centrale su 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 centrale del plug-in su Linux:

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties

HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

Configurazione dell'archivio utenti SAP HANA per un host plug-in centrale

Per ogni sistema HANA gestito dall'host del plug-in centrale, è necessario configurare una chiave di archivio utente SAP HANA. Prima che la chiave possa essere configurata sull'host centrale del plug-in, è necessario creare un utente del database come descritto in "Configurazione dell'utente di backup SAP HANA e dell'archivio utenti SAP HANA".

Se il plug-in SAP HANA e il client SAP hdbsql sono installati su Windows, l'utente del sistema locale esegue i comandi hdbsql e viene configurato per impostazione predefinita nella configurazione delle risorse. Poiché l'utente di sistema non è un utente di accesso, la configurazione dell'archivio utenti SAP HANA deve essere eseguita con un utente diverso utilizzando l'opzione -u <Utente>.

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

Per una configurazione SAP HANA con più host, è necessario configurare le chiavi di archiviazione utente SAP HANA per tutti gli host. SnapCenter tenta di connettersi al database utilizzando ciascuna delle chiavi fornite e può quindi funzionare indipendentemente da un failover del database di sistema (server dei nomi HANA) su un host diverso. Una chiave di archivio utente SAP HANA è configurata per tutti i worker e per l'host di standby. L'utente del database HANA, in questo esempio SNAPCENTER, è l'utente che è stato configurato nel database di 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>
```

Configurazione manuale delle risorse HANA

Una risorsa di sistema HANA configurata manualmente viene creata in SnapCenter facendo clic sul pulsante Aggiungi nella vista delle risorse.

[larghezza=601, altezza=189]

Nella schermata successiva è necessario fornire un paio di parametri di sistema.

- Host del plug-in: deve essere selezionato l'host centrale del plug-in
- Chiave di archivio utente SAP HANA: per un sistema HANA con un singolo host, è necessario fornire il nome della chiave preparato nell'host del plug-in centrale. Per un sistema HANA con più host, è necessario fornire un elenco separato da virgole di tutte le chiavi del sistema.
- Utente del sistema operativo HDBSQL: se l'host del plug-in centrale è in esecuzione su Windows, l'utente verrà preselezionato come utente SYSTEM. In caso contrario, è necessario fornire l'utente utilizzato per la chiave di archivio utenti SAP HANA.

[larghezza=384, altezza=357]

Il passaggio successivo è la configurazione dello spazio di archiviazione. Qui devono essere aggiunti tutti i volumi ONTAP o ANF che appartengono al sistema HANA.

[larghezza=385, altezza=359]

La configurazione della protezione delle risorse può ora essere effettuata nello stesso modo dei sistemi HANA rilevati automaticamente.

Scopri di più sulle operazioni di backup per SAP HANA Snapshot in SnapCenter

Eseguire backup Snapshot SAP HANA utilizzando SnapCenter. Scopri di più sui backup Snapshot del database, sui controlli di integrità dei blocchi, sui backup di volumi non dati e sulla replica dei backup tramite SnapVault o Azure NetApp Files .

In SnapCenter, i backup del database vengono in genere eseguiti utilizzando le pianificazioni definite all'interno della configurazione di protezione delle risorse di ciascun database HANA.

Il backup del database on-demand può essere eseguito utilizzando l'interfaccia utente grafica di SnapCenter, una riga di comando PowerShell o API REST.

SnapCenter supporta le seguenti operazioni di backup.

- Operazioni di backup degli snapshot del database HANA
- Operazioni di controllo dell'integrità dei blocchi
- Backup snapshot di volumi non dati
- Replica di backup tramite SnapVault o backup ANF per database HANA o backup di volumi non dati

Le sezioni seguenti descrivono le diverse operazioni per i sistemi HANA a host singolo che sono stati rilevati automaticamente da SnapCenter (plug-in HANA distribuito sull'host del database HANA)

Backup snapshot SAP HANA in SnapCenter

La topologia delle risorse SnapCenter mostra l'elenco dei backup creati da SnapCenter. La figura seguente mostra i backup disponibili sullo storage primario ed evidenzia il backup più recente.

[larghezza=601, altezza=293]

I backup nell'archivio secondario possono essere elencati facendo clic sull'icona Copie Vault.

[larghezza=601, altezza=294]

La seguente schermata mostra l'elenco dei backup per il sistema SM1, in cui sono stati configurati gli snapshot antimanomissione.

[larghezza=601, altezza=293]

Backup snapshot SAP HANA in SAP HANA Studio

Quando si esegue un backup utilizzando gli snapshot di archiviazione per un sistema SAP HANA MDC, viene creata una copia snapshot del volume di dati. Questo volume di dati contiene i dati del database di sistema e i dati di tutti i database tenant. Per riflettere questa architettura fisica, SAP HANA esegue internamente uno snapshot combinato del database interno del database di sistema e di tutti i database tenant ogni volta che SnapCenter attiva un backup Snapshot. Ciò comporta la creazione di più voci di backup separate nel catalogo di backup SAP HANA: una per il database di sistema e una per ciascun database tenant.

Nel catalogo di backup SAP HANA, il nome del backup SnapCenter viene memorizzato come campo

Commento e come ID backup esterno (EBID). Ciò è mostrato nello screenshot seguente per il database di sistema e nello screenshot successivo per il database tenant SS1. Entrambe le figure evidenziano il nome del backup SnapCenter memorizzato nel campo dei commenti e l'EBID.

[larghezza=601, altezza=289]

[larghezza=601, altezza=296]

SnapCenter è a conoscenza solo dei propri backup. I backup aggiuntivi creati, ad esempio, con SAP HANA Studio sono visibili nel catalogo SAP HANA ma non in SnapCenter. Anche gli snapshot creati direttamente sul sistema di archiviazione non saranno visibili in SnapCenter,

Backup snapshot SAP HANA sul livello di archiviazione

Per visualizzare i backup sul livello di archiviazione, è possibile utilizzare NetApp System Manager e selezionare il volume del database. La seguente schermata mostra i backup disponibili per il volume del database SS1_data_mnt00001 nell'archivio primario. Il backup evidenziato è quello mostrato in SnapCenter e SAP HANA Studio nelle immagini precedenti e ha la stessa convenzione di denominazione.

[larghezza=601, altezza=294]

La seguente schermata mostra i backup disponibili per il volume di destinazione della replica hana_SS1_data_mnt00001_dest nel sistema di archiviazione secondario.

[larghezza=601, altezza=294]

Backup snapshot SAP HANA con ANF

La seguente schermata mostra la vista topologica di un sistema HANA utilizzando Azure NetApp Files. Per questo sistema HANA sono stati configurati backup Snapshot locali e replica di backup tramite backup ANF.

[larghezza=601, altezza=303]

I backup snapshot sul volume ANF possono essere elencati tramite il portale di Azure.

[larghezza=601, altezza=258]

Facendo clic sull'icona di backup, è possibile elencare i backup replicati con ANF Backup.

[larghezza=601, altezza=304]

I backup ANF possono essere elencati anche nel portale di Azure.

[larghezza=601, altezza=216]

Backup snapshot di volumi non dati

La topologia delle risorse SnapCenter mostra l'elenco dei backup per i volumi non dati. Nella figura seguente sono elencati i backup del volume condiviso HANA.

[larghezza=601, altezza=294]

Flusso di lavoro di backup per i backup del database HANA

Il flusso di lavoro di backup per un backup snapshot del database HANA è costituito da tre sezioni principali.

- Rilevamento automatico
  - Scoperta dell'applicazione, ad esempio
    - SnapCenter rileva eventuali modifiche alla configurazione del tenant
    - SnapCenter rileva il nodo primario di replicazione del sistema HANA
  - Rilevamento del file system e dell'archiviazione, ad esempio
    - SnapCenter rileva eventuali modifiche nella configurazione del volume
    - SnapCenter rileva la configurazione di più partizioni HANA
- Operazioni di backup HANA e Snapshot
  - Attiva lo snapshot del database HANA
  - Crea snapshot di archiviazione
  - Conferma lo snapshot del database HANA e registra il backup nel catalogo di backup HANA
- Gestione della conservazione
  - Elimina i backup degli snapshot in base alla conservazione definita in
    - Repository SnapCenter
    - Magazzinaggio
    - Catalogo di backup HANA
  - Gestione della conservazione del backup dei log
    - Elimina i backup del registro sul file system e sul catalogo di backup HANA

[larghezza=339, altezza=475]

Flusso di lavoro di backup per volumi non dati

Per un volume non di dati, il flusso di lavoro di backup è costituito dall'operazione Snapshot e dall'operazione di gestione della conservazione.

[larghezza=329, altezza=404]

Pulizia dei backup secondari

Come descritto in "Gestione della conservazione per i backup secondari", la gestione della conservazione dei backup dei dati su un archivio di backup secondario è gestita da ONTAP. SnapCenter verifica periodicamente se ONTAP ha eliminato i backup nell'archivio di backup secondario eseguendo un processo di pulizia con una pianificazione predefinita settimanale.

Il processo di pulizia SnapCenter elimina i backup nel repository SnapCenter e nel catalogo di backup di SAP HANA se sono stati identificati backup eliminati nell'archivio di backup secondario.

[larghezza=601, altezza=158]

[larghezza=267, altezza=330]

Finché questa pulizia programmata non sarà completata, SAP HANA e SnapCenter continueranno a mostrare

i backup che sono già stati eliminati dall'archivio di backup secondario. Ciò comporterà la conservazione di ulteriori backup del registro, anche se i backup Snapshot basati sull'archiviazione corrispondenti nell'archiviazione di backup secondaria sono già stati eliminati. NetApp consiglia di modificare la pianificazione da settimanale a giornaliera per evitare di conservare backup dei log, che non sono più necessari.

Modificare la frequenza del lavoro di pulizia SnapCenter

Per impostazione predefinita, SnapCenter esegue il processo di pulizia SnapCenter_RemoveSecondaryBackup per tutte le risorse su base settimanale. Questa impostazione può essere modificata utilizzando un cmdlet SnapCenter PowerShell.

```
SnapCenterPS C:\> Open-SmConnection

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

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

TaskName : SnapCenter_RemoveSecondaryBackup
Hosts : {}
StartTime : 8/25/2025 3:45:00 AM
DaysoftheMonth :
MonthsofTheYear :
DaysInterval : 1
DaysOfTheWeek :
AllowDefaults : False
ReplaceJobIfExist : 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:\>
```

La configurazione può essere verificata anche nella vista Monitor - Pianificazioni nell'interfaccia utente SnapCenter .

[larghezza=601, altezza=257]

Aggiornamento manuale a livello di risorse

Se necessario, è possibile eseguire anche una pulizia manuale dei backup secondari nella vista topologica di una risorsa. Quando si selezionano i backup secondari, SnapCenter visualizza i backup nell'archivio di backup secondario, come mostrato nella seguente schermata. SnapCenter esegue un'operazione di pulizia con l'icona Aggiorna per sincronizzare i backup per questa risorsa.

[larghezza=601, altezza=291]

Eseguire controlli di coerenza dei blocchi SAP HANA con SnapCenter

Eseguire controlli di coerenza dei blocchi SAP HANA utilizzando lo strumento SAP hdbpersdiag o eseguendo backup basati su file. Scopri le opzioni di configurazione, tra cui l'accesso alla directory Snapshot locale, gli host di verifica centrali con volumi FlexClone e l'integrazione SnapCenter per la pianificazione e l'automazione.

La tabella seguente riassume i parametri chiave che aiutano a decidere quale metodo di controllo della coerenza dei blocchi è più adatto al tuo ambiente.

	Strumento HANA hdbpersdiag che utilizza la directory Snapshot locale	Strumento HANA hdbpersdiag con host di verifica centrale	Backup basato su file
Configurazioni supportate	Solo NFS Montaggi in-guest bare metal, ANF, FSx ONTAP, VMware o KVM	Tutti i protocolli e le piattaforme	Tutti i protocolli e le piattaforme
Carico della CPU sull'host HANA	Medio	Nessuno	Alto
Utilizzo della rete presso l'host HANA	Alto	Nessuno	Alto
Durata	Sfrutta la piena capacità di lettura del volume di archiviazione	Sfrutta la piena capacità di lettura del volume di archiviazione	Tipicamente limitato dalla velocità di scrittura del sistema di destinazione
Requisiti di capacità	Nessuno	Nessuno	Almeno 1 x dimensione di backup per sistema HANA
Integrazione SnapCenter	Script di backup successivo	Clona crea e pubblica script di clonazione, clona elimina	Funzionalità integrata
Pianificazione	Pianificatore SnapCenter	Script di PowerShell per eseguire il flusso di lavoro di creazione ed eliminazione di cloni, pianificato esternamente	Pianificatore SnapCenter

Nei capitoli seguenti vengono descritte la configurazione e l'esecuzione delle diverse opzioni per le operazioni di controllo della coerenza dei blocchi.

Controlli di coerenza con hdbpersdiag utilizzando la directory snapshot locale

All'interno di SnapCenter viene creata una policy dedicata per le operazioni hdbpersdiag con una pianificazione giornaliera e una conservazione di due. Non utilizziamo la pianificazione settimanale, poiché in tal caso avremmo almeno 2 backup Snapshot (conservazione minima=2), uno dei quali risalirebbe a due settimane prima.

Nella configurazione di protezione delle risorse SnapCenter del sistema HANA, viene aggiunto uno script di post-backup che esegue lo strumento hdbpersdiag. Poiché lo script di post-backup verrà richiamato anche con qualsiasi altra policy configurata per la risorsa, dobbiamo verificare nello script quale policy è attualmente attiva. All'interno dello script controlliamo anche il giorno corrente della settimana ed eseguiamo l'operazione hdbpersdiag solo una volta alla settimana, la domenica. HANA hdbpersdiag viene quindi chiamato per ogni volume di dati nella directory hdb* corrispondente della directory di backup Snapshot corrente. Se il controllo di coerenza con hdbpersdiag segnala un errore, il processo SnapCenter verrà contrassegnato come non riuscito.

Lo script di esempio call-hdbpersdiag.sh viene fornito così com'è e non è coperto dal supporto NetApp . È possibile richiedere lo script via e-mail all'indirizzo ng-sapcc@netapp.com.

La figura seguente mostra il concetto di alto livello dell'implementazione del controllo di coerenza.

[larghezza=601, altezza=248]

Come primo passo è necessario consentire l'accesso alla directory snapshot, in modo che la directory """.snapshot" sia visibile sull'host del database HANA.

- Sistemi ONTAP e FSX per ONTAP: è necessario configurare il parametro del volume di accesso alla directory Snapshot
- ANF: È necessario configurare il parametro del volume Nascondi percorso snapshot.

Come passaggio successivo, è necessario configurare un criterio che corrisponda al nome utilizzato nello script di post-backup. Per il nostro esempio di script il nome deve essere SnapAndCallHdbpersdiag. Come discusso in precedenza, si utilizza una pianificazione giornaliera per evitare di conservare vecchi Snapshot con una pianificazione settimanale.

[larghezza=414, altezza=103]

[larghezza=424, altezza=108]

[larghezza=433, altezza=336]

Nella configurazione della protezione delle risorse, viene aggiunto lo script di post-backup e il criterio viene assegnato alla risorsa.[larghezza=601, altezza=294]

[larghezza=601, altezza=281]

Infine, lo script deve essere configurato nel file allowed_commands.config sull'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
```

L'operazione di backup Snapshot verrà ora eseguita una volta al giorno e lo script gestisce il controllo hdbpersdiag che verrà eseguito solo una volta alla settimana, la domenica.

> Lo script richiama hdbpersdiag con l'opzione della riga di comando "-e", necessaria per la crittografia del volume di dati. Se non viene utilizzata la crittografia del volume dati HANA, il parametro deve essere rimosso.

L'output seguente mostra il file di registro dello 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 'libhdblivecache'
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 'libhdblivecache'
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 'libhdblivecache'
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
```

Controlli di coerenza con hdbpersdiag utilizzando un host di verifica centrale

La figura seguente mostra una panoramica generale dell'architettura della soluzione e del flusso di lavoro. Con un host di verifica centrale, è possibile utilizzare l'host di verifica per verificare la coerenza di più sistemi HANA diversi. La soluzione sfrutta i flussi di lavoro di creazione ed eliminazione dei cloni SnapCenter per collegare un volume clonato dal sistema HANA che deve essere verificato sull'host di verifica. Per eseguire lo strumento hdbpersdiag di HANA viene utilizzato uno script di post-clone. Come secondo passaggio, il flusso di lavoro di eliminazione del clone SnapCenter viene utilizzato per smontare ed eliminare il volume clonato.

> Se i sistemi HANA sono configurati con la crittografia del volume di dati, le chiavi radice di crittografia del sistema HANA di origine devono essere importate nell'host di verifica prima dell'esecuzione di hdbpersdiag. Vedi anche "Importazione delle chiavi radice di backup prima del ripristino del database | Portale di assistenza SAP"

[larghezza=601, altezza=257]

Lo strumento HANA hdbpersdiag è incluso in ogni installazione HANA ma non è disponibile come strumento autonomo. Pertanto l'host di verifica centrale deve essere preparato installando un normale sistema HANA.

Fasi iniziali di preparazione una tantum:

- Installazione del sistema SAP HANA da utilizzare come host di verifica centrale
- Configurazione del sistema SAP HANA in SnapCenter
  - Distribuzione del plug-in SnapCenter SAP HANA sull'host di verifica. Il sistema SAP HANA viene rilevato automaticamente da SnapCenter.
- La prima operazione hdbpersdiag dopo l'installazione iniziale viene preparata con i seguenti passaggi:
  - Chiudi il sistema SAP HANA di destinazione
  - Disinstalla volume di dati SAP HANA.

È necessario aggiungere gli script che devono essere eseguiti sul sistema di destinazione al file di configurazione dei comandi consentiti da 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
```

Lo script di esempio call-hdbpersdiag-flexclone.sh viene fornito così com'è e non è coperto dal supporto NetApp . È possibile richiedere lo script via e-mail all'indirizzo ng-sapcc@netapp.com.

Esecuzione manuale del flusso di lavoro

Nella maggior parte dei casi, l'operazione di controllo della coerenza verrà eseguita come operazione pianificata, come descritto nel capitolo successivo. Tuttavia, conoscere il flusso di lavoro manuale è utile per comprendere i parametri utilizzati per il processo automatizzato.

Il flusso di lavoro per la creazione di cloni viene avviato selezionando un backup dal sistema che deve essere selezionato e facendo clic su Clona da backup.

[larghezza=601, altezza=247]

Nella schermata successiva è necessario fornire il nome host, il SID e l'interfaccia di rete di archiviazione dell'host di verifica.

È importante utilizzare sempre il SID del sistema HANA installato sull'host di verifica, altrimenti il flusso di lavoro non andrà a buon fine.

[larghezza=431, altezza=115]

Nella schermata successiva è necessario aggiungere lo script call-hdbpersdiag-fleclone.sh come comando post-clone.

[larghezza=442, altezza=169]

Una volta avviato il flusso di lavoro, SnapCenter creerà un volume clonato basato sul backup Snapshot selezionato e lo monterà sull'host di verifica.

Nota: l'output di esempio riportato di seguito si basa sui sistemi HANA che utilizzano NFS come protocollo di archiviazione. Per il sistema HANA che utilizza FC o VMware VMDK, il dispositivo verrà montato nello stesso modo su /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
```

L'output seguente mostra il file di registro del comando post-clone 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 'libhdblivecache'
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 'libhdblivecache'
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 'libhdblivecache'
```

```
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.
```

Lo script richiama hdbpersdiag con l'opzione della riga di comando "-e", necessaria per la crittografia del volume di dati. Se non viene utilizzata la crittografia del volume dati HANA, il parametro deve essere rimosso. Una volta terminato lo script di post-clone, anche il lavoro SnapCenter è terminato.

[larghezza=279, altezza=344]

Come passaggio successivo, eseguiremo il flusso di lavoro di eliminazione del clone SnapCenter per ripulire l'host di verifica ed eliminare il volume FlexClone .

Nella vista topologica del sistema sorgente, selezioniamo il clone e clicchiamo sul pulsante Elimina.

[larghezza=601, altezza=165]

SnapCenter ora smonterà il volume clonato dall'host di verifica ed eliminerà il volume clonato dal sistema di archiviazione.

Automazione del flusso di lavoro SnapCenter tramite script di PowerShell

Nella sezione precedente, i flussi di lavoro di creazione e eliminazione dei cloni sono stati eseguiti utilizzando l'interfaccia utente SnapCenter . Tutti i flussi di lavoro possono essere eseguiti anche con script PowerShell o chiamate API REST, consentendo un'ulteriore automazione. Nella sezione seguente viene descritto un

esempio di script PowerShell di base per eseguire i flussi di lavoro di creazione e eliminazione dei cloni SnapCenter .

> Gli script di esempio call-hdbpersdiag-flexclone.sh e clone-hdbpersdiag.ps1 vengono forniti così come sono e non sono coperti dal supporto NetApp . È possibile richiedere gli script via e-mail all'indirizzo ng-sapcc@netapp.com.

Lo script di esempio di PowerShell esegue il seguente flusso di lavoro.

- Cerca l'ultimo backup Snapshot in base al parametro della riga di comando SID e all'host di origine
- Esegue il flusso di lavoro di creazione del clone SnapCenter utilizzando il backup Snapshot definito nel passaggio precedente. Le informazioni sull'host di destinazione e le informazioni hdbpersdiag sono definite nello script. Lo script call-hdbpersdiag-flexclone.sh è definito come script post-clone e viene eseguito sull'host di destinazione.
  - $result = New-SmClone -AppPluginCode hana -BackupName $backupName -Resources @{"Host"="$sourceHost";"UID"="$uid"} -CloneToInstance "$verificationHost" -NFSExportIPs $exportIpTarget -CloneUid $targetUid -PostCloneCreateCommands $postCloneScript
- Esegue il flusso di lavoro di eliminazione del clone SnapCenter. Il testo seguente mostra l'output dello script di esempio eseguito sul server SnapCenter .

Il testo seguente mostra l'output dello script di esempio eseguito sul server 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>
```

Lo script richiama hdbpersdiag con l'opzione della riga di comando "-e", necessaria per la crittografia del volume di dati. Se non viene utilizzata la crittografia del volume dati HANA, il parametro deve essere rimosso.

L'output seguente mostra il file di registro dello 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 'libhdblivecache'
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 'libhdblivecache'
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 'libhdblivecache'
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 basato su file

SnapCenter supporta l'esecuzione di un controllo di integrità dei blocchi utilizzando un criterio in cui il backup basato su file viene selezionato come tipo di backup.

Quando si pianificano backup utilizzando questa policy, SnapCenter crea un backup standard dei file SAP HANA per il sistema e tutti i database tenant.

SnapCenter non visualizza il controllo dell'integrità del blocco allo stesso modo dei backup basati su copia Snapshot. La scheda di riepilogo mostra invece il numero di backup basati su file e lo stato del backup precedente.

[larghezza=601, altezza=293]

Il catalogo di backup SAP HANA mostra le voci per i database di sistema e tenant. La figura seguente mostra un controllo dell'integrità del blocco SnapCenter nel catalogo di backup del database di sistema.

[larghezza=601, altezza=293]

Un controllo di integrità del blocco riuscito crea file di backup dei dati SAP HANA standard.

[larghezza=351, altezza=433]

SnapCenter utilizza il percorso di backup configurato nel database HANA per le operazioni di backup dei dati basate su file.

```
hana-1:/hana/shared/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 3717564
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ss1adm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ss1adm 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 ss1adm 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 ss1adm 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 ss1adm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ss1adm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ss1adm 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 ss1adm sapsys 3405787136 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_1_1
```

Ripristina e recupera i database SAP HANA con SnapCenter

Ripristina e recupera i sistemi SAP HANA utilizzando SnapCenter con opzioni di ripristino automatiche o manuali. Ciò include ripristini completi del sistema, ripristini di tenant singoli per database HANA su ONTAP, Azure NetApp Files e FSx per ONTAP.

SnapCenter supporta le seguenti operazioni di ripristino e recupero.

- Sistemi SAP HANA MDC con un singolo tenant
  - Ripristino e recupero automatizzati end-to-end
  - Ripristino automatico end-to-end e recupero manuale (selezionabile)
- Sistemi SAP HANA MDC con più tenant
  - Ripristino automatizzato end-to-end, il ripristino deve essere eseguito manualmente
- Ripristino di un singolo tenant
  - Ripristino automatizzato end-to-end, il ripristino deve essere eseguito manualmente

Il ripristino automatico è supportato solo quando il plug-in HANA è distribuito sull'host del database HANA e il sistema HANA è stato rilevato automaticamente da SnapCenter. Con una configurazione host plug-in centrale, il ripristino deve essere eseguito manualmente dopo l'operazione di ripristino con SnapCenter.

È supportato il ripristino dal volume ANF primario. Il ripristino del backup ANF non è ancora supportato. Un ripristino sul posto o un ripristino su un nuovo volume da un backup ANF deve essere eseguito manualmente tramite il portale di Azure o l'interfaccia della riga di comando.

Ripristino e recupero automatizzati per sistemi SAP HANA MDC con un singolo tenant

Un'operazione di ripristino viene avviata selezionando un backup Snapshot nella vista topologia delle risorse e facendo clic su Ripristina.

[larghezza=601, altezza=294]

Per i sistemi HANA che utilizzano NFS su ANF, FSx per ONTAP o sistemi di archiviazione ONTAP è possibile selezionare il ripristino completo con o senza un'operazione di ripristino del volume per gli snapshot del volume primario.

- La risorsa completa senza ripristino del volume utilizza Single File SnapRestore (SFSR) per ripristinare tutti i file del database.
- La risorsa completa con ripristino del volume utilizza un'operazione di ripristino basata sul volume (VBSR) per ripristinare l'intero volume allo stato dello snapshot selezionato.

Il ripristino del volume non può essere utilizzato se è necessario ripristinare uno Snapshot precedente allo SnapVault attivo o SnapMirror Replication Snapshot.

Un'operazione di ripristino del volume eliminerà tutti i backup Snapshot più recenti dello Snapshot selezionato per l'operazione di ripristino.

Un ripristino con SFSR è quasi veloce quanto un'operazione di ripristino del volume, ma blocca qualsiasi operazione di snapshot finché il processo in background non ha completato le operazioni sui metadati.

[larghezza=300]

Per i sistemi HANA su host bare metal che utilizzano FC SAN, il ripristino del volume (VBSR) non è

supportato; al suo posto viene sempre utilizzato SFSR per l'operazione di ripristino. Per i sistemi HANA in esecuzione su VMware con VMFS verrà utilizzata un'operazione di clonazione, montaggio e copia.

[larghezza=345, altezza=325]

Per un ripristino da un backup secondario è necessario selezionare la posizione dell'archivio.

[larghezza=345, altezza=323]

Con l'ambito di ripristino è possibile selezionare un ripristino "allo stato più recente", "a un punto nel tempo" o un ripristino tramite punto di salvataggio senza utilizzare backup del registro. Se non si seleziona alcun ripristino, SnapCenter esegue solo l'operazione di ripristino e il ripristino deve essere eseguito manualmente come descritto "Ripristino manuale con HANA Studio".

> SnapCenter utilizza i percorsi configurati in SAP HANA per le posizioni di backup dei log e dei cataloghi. Se si dispone di backup a livelli in una posizione aggiuntiva, è possibile aggiungere questi percorsi aggiuntivi.

[larghezza=346, altezza=324]

Facoltativamente è possibile aggiungere script pre e post ripristino.

[larghezza=348, altezza=326]

[larghezza=359, altezza=335]

Facendo clic su Fine nella schermata di riepilogo, viene avviata l'operazione di ripristino e recupero.

[larghezza=361, altezza=336]

Il flusso di lavoro di ripristino e recupero può essere suddiviso in tre sezioni principali.

- Arresto del sistema HANA
- Ripristinare l'operazione
  - Preparazioni specifiche del file system, ad esempio operazione di smontaggio
  - Operazione di ripristino dello snapshot
  - Operazioni di post-operazioni specifiche del file system, ad esempio operazione di montaggio
- Recupero HANA
  - Recovery del database di sistema
  - Recovery del database tenant

[larghezza=357, altezza=439]

Ripristino manuale con HANA Studio

Per ripristinare e recuperare un sistema SAP HANA MDC con uno o più tenant utilizzando SAP HANA Studio e SnapCenter, completare i seguenti passaggi:

1. Preparare il processo di ripristino con SAP HANA Studio:
   a. Selezionare Recover System Database (Ripristina database di sistema) e confermare l'arresto del sistema SAP HANA.

b. Selezionare il tipo di ripristino e specificare il percorso del catalogo di backup.

c. Viene visualizzato l'elenco dei backup dei dati. Selezionare Backup per visualizzare l'ID del backup esterno.

2. Eseguire il processo di ripristino con SnapCenter:

a. Nella vista topologica della risorsa, selezionare Copie locali per ripristinare dall'archivio primario o Copie Vault se si desidera ripristinare da un archivio di backup secondario.

b. Selezionare il backup SnapCenter che corrisponde all'ID di backup esterno o al campo del commento di SAP HANA Studio.

c. Avviare il processo di ripristino.

3. Eseguire il processo di ripristino del database di sistema con SAP HANA Studio:

a. Fare clic su Refresh (Aggiorna) dall'elenco dei backup e selezionare il backup disponibile per il ripristino (indicato da un'icona verde).

b. Avviare il processo di ripristino. Al termine del processo di ripristino, viene avviato il database di sistema.

4. Eseguire il processo di ripristino del database tenant con SAP HANA Studio:

a. Selezionare Recover tenant Database (Ripristina database tenant) e selezionare il tenant da ripristinare.

b. Selezionare il tipo di ripristino e la posizione di backup del registro.

c. Viene visualizzato un elenco di backup dei dati. Poiché il volume di dati è già stato ripristinato, il backup del tenant viene indicato come disponibile (in verde).

d. Selezionare questo backup e avviare il processo di ripristino. Al termine del processo di ripristino, il database del tenant viene avviato automaticamente.

5. Per un sistema HANA con più tenant, ripetere il passaggio 4 per ciascun tenant.

Un ripristino manuale con SAP HANA Cockpit avviene seguendo gli stessi passaggi.

Nella sezione seguente vengono descritti i passaggi delle operazioni di ripristino e recupero di un sistema SAP HANA MDC con un singolo tenant.

In HANA Studio selezionare Backup e ripristino e Ripristina database di sistema.

[larghezza=450, altezza=368]

Conferma l'operazione di spegnimento; richiesta solo se il sistema HANA è ancora in esecuzione.

[larghezza=349, altezza=83]

Selezionare l'operazione di ripristino. In questo esempio vogliamo ripristinare lo stato più recente.

[larghezza=345, altezza=359]

Fornire la posizione del catalogo di backup.

[larghezza=343, altezza=356]

HANA Studio elenca i backup più recenti archiviati nel catalogo dei backup HANA.

Viene visualizzato un elenco dei backup disponibili in base al contenuto del catalogo dei backup. Selezionare il

backup richiesto e annotare l'ID del backup esterno: in questo esempio, il backup più recente.

[larghezza=391, altezza=283]

Dall'interfaccia utente grafica SnapCenter , selezionare la vista della topologia delle risorse e selezionare il backup da ripristinare, in questo esempio il backup primario più recente. Fare clic sull'icona Ripristina per avviare il ripristino.

[larghezza=601, altezza=294]

Viene avviata la procedura guidata di ripristino SnapCenter . Selezionare il tipo di ripristino Risorsa completa e Ripristino volume per utilizzare un ripristino basato sul volume.

[larghezza=346, altezza=325]

Selezionare "Nessun ripristino" per escludere le operazioni di ripristino dal flusso di lavoro SnapCenter .

[larghezza=358, altezza=336]

Fare clic su Fine per avviare l'operazione di ripristino.

[larghezza=361, altezza=339]

SnapCenter sta ora eseguendo l'operazione di ripristino.

- Preparazioni specifiche del file system, ad esempio operazione di smontaggio
- Operazione di ripristino dello snapshot
- Operazioni post specifiche del file system, ad esempio operazione di montaggio

[larghezza=322, altezza=398]

Quando lo Snapshot viene ripristinato da SnapCenter , un file snapshot_databackup_0_1 è disponibile nella sottodirectory del database di sistema e del tenant del volume dati HANA. Questo file è stato creato dal database HANA durante la creazione dello snapshot del database HANA. HANA elimina il file al termine dell'operazione di backup, in modo che i file siano visibili solo all'interno del backup Snapshot. Questi file sono necessari per qualsiasi operazione di recupero. Dopo il ripristino, i file vengono eliminati dal database HANA.

```
hana-1:~ # cd /hana/data/SS1/mnt00001/
hana-1:/hana/data/SS1/mnt00001 # ls -al *
-rw-r--r-- 1 ss1adm sapsys 16 Aug 26 06:00 nameserver.lck
hdb00001:
total 4992236
drwxr-x--- 2 ss1adm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r----- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 ss1adm sapsys 5100273664 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ss1adm sapsys 36 Aug 25 10:30 landscape.id
-rw-r----- 1 ss1adm sapsys 163840 Aug 26 06:00 snapshot_databackup_0_1
hdb00002.00003:
total 201420
drwxr-xr-- 2 ss1adm sapsys 4096 Nov 3 2020 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ss1adm sapsys 335544320 Aug 26 06:00 datavolume_0000.dat
hdb00003.00003:
total 4803140
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ss1adm sapsys 4898947072 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ss1adm sapsys 159744 Aug 26 06:00 snapshot_databackup_0_1
hana-1:/hana/data/SS1/mnt00001 #
```

Vai a SAP HANA Studio e fai clic su Aggiorna per aggiornare l'elenco dei backup disponibili. Il backup ripristinato con SnapCenter viene ora visualizzato con un'icona verde nell'elenco dei backup. Selezionare il backup e fare clic su Avanti.

[larghezza=400, altezza=290]

Fornire la posizione dei backup del registro. Fare clic su Avanti.

> SAP HANA Studio utilizza i percorsi configurati in SAP HANA per le posizioni di backup dei log e dei cataloghi. Se si dispone di backup a livelli in una posizione aggiuntiva, è possibile aggiungere questi percorsi aggiuntivi.

[larghezza=465, altezza=296]

Selezionare le altre impostazioni desiderate. Assicurarsi che l'opzione Usa backup delta non sia selezionata. Fare clic su Avanti.

[larghezza=466, altezza=296]

Rivedere le impostazioni di ripristino e fare clic su fine.

Facendo clic su Mostra istruzione SQL, HANA Studio mostra il comando SQL che viene eseguito per l'operazione di ripristino.

[larghezza=464, altezza=295]

Inizia il processo di recupero. Attendere il completamento del ripristino del database di sistema.

[larghezza=376, altezza=239]

In SAP HANA Studio, selezionare la voce per il database di sistema e avviare Backup Recovery - Recover Tenant Database.

[larghezza=476, altezza=315]

Selezionare il tenant da ripristinare e fare clic su Next (Avanti).

[larghezza=342, altezza=355]

Specificare il tipo di ripristino e fare clic su Next (Avanti).

[larghezza=343, altezza=356]

Confermare la posizione del catalogo di backup e fare clic su Next (Avanti).

[larghezza=342, altezza=355]

Confermare l'arresto del database tenant.

[larghezza=348, altezza=85]

Poiché il ripristino del volume di dati è stato eseguito prima del ripristino del database di sistema, il backup del tenant è immediatamente disponibile. Selezionare il backup evidenziato in verde e fare clic su Avanti.

[larghezza=433, altezza=349]

Fornire la posizione dei backup del registro. Fare clic su Avanti.

> SAP HANA Studio utilizza i percorsi configurati in SAP HANA per le posizioni di backup dei log e dei cataloghi. Se si dispone di backup a livelli in una posizione aggiuntiva, è possibile aggiungere questi percorsi aggiuntivi.

[larghezza=384, altezza=310]

Selezionare le altre impostazioni desiderate. Assicurarsi che l'opzione Usa backup delta non sia selezionata. Fare clic su Avanti.

[larghezza=384, altezza=310]

Rivedere le impostazioni di ripristino e fare clic su fine.

Facendo clic su Mostra istruzione SQL, HANA Studio mostra il comando SQL che viene eseguito per l'operazione di ripristino.

[larghezza=380, altezza=307]

Attendere il completamento del ripristino e l'avvio del database tenant.

[larghezza=378, altezza=305]

Una volta completato il ripristino del tenant, il sistema SAP HANA è attivo e funzionante.

Per un sistema SAP HANA MDC con più tenant, è necessario ripetere il ripristino del tenant per ciascun tenant.

Ripristino manuale con comandi SQL

È anche possibile utilizzare istruzioni SQL per il ripristino del sistema HANA.

Per prima cosa è necessario ripristinare il database di 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"
```

Come secondo passaggio è necessario connettersi al database di sistema e avviare il ripristino del/i database del tenant. In questo esempio il database tenant è 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
```

Ripristino e recupero di un singolo tenant

Un'operazione di ripristino e recupero di un singolo tenant con SnapCenter è molto simile al flusso di lavoro descritto nell'argomento precedente "Ripristino manuale con HANA Studio".

Per ripristinare e ripristinare un sistema single-tenant SAP HANA MDC utilizzando SAP HANA Studio e SnapCenter, attenersi alla seguente procedura:

1. Preparare il processo di ripristino con SAP HANA Studio:
   a. Selezionare Recupera database tenant e confermare l'arresto del database tenant.
   b. Selezionare il tipo di ripristino e specificare il percorso del catalogo di backup.
   c. Viene visualizzato l'elenco dei backup dei dati. Selezionare Backup per visualizzare l'ID del backup esterno.
2. Eseguire il processo di ripristino con SnapCenter:
   a. Nella vista topologica della risorsa, selezionare Copie locali per ripristinare dall'archivio primario o Copie Vault se si desidera ripristinare da un archivio di backup secondario.
   b. Selezionare il backup SnapCenter che corrisponde all'ID di backup esterno o al campo del commento di SAP HANA Studio.
   c. Avviare il processo di ripristino del tenant.

3. Eseguire il processo di ripristino del database tenant con SAP HANA Studio:
    a. Fare clic su Refresh (Aggiorna) dall'elenco dei backup e selezionare il backup disponibile per il ripristino (indicato da un'icona verde).
    b. Avviare il processo di recupero. Una volta completato il processo di ripristino, viene avviato il database del tenant.

Ripristino di volumi non dati

Un'operazione di ripristino per un volume non dati viene avviata selezionando un backup Snapshot nella vista topologica della risorsa del volume non dati e facendo clic su Ripristina.

[larghezza=601, altezza=294]

Per i volumi non dati con NFS è possibile selezionare un'operazione di ripristino completa delle risorse (VBSR) o a livello di file (SFSR). Per il ripristino a livello di file è possibile definire per l'operazione di ripristino tutti i file o singoli file.

[larghezza=369, altezza=344]

Configurare le opzioni avanzate SnapCenter per SAP HANA

Configurare le impostazioni avanzate SnapCenter per gli ambienti SAP HANA, tra cui la soppressione dei messaggi di avviso VMware per i montaggi NFS in-guest, la disabilitazione della gestione automatica dei backup dei log e l'abilitazione della crittografia SSL per le connessioni al database HANA.

Messaggio di avviso con ambienti virtualizzati e montaggi in-guest

Ad esempio, quando si utilizza VMware con montaggi NFS in-guest, SnapCenter emetterà un messaggio di avviso che indica di utilizzare il plug-in SnapCenter VMware. Poiché il plug-in VMWare non è necessario per i montaggi in-guest, il messaggio di avviso può essere ignorato e disattivato. Per configurare SnapCenter in modo da eliminare questo avviso, è necessario applicare la seguente configurazione:

1. Dalla scheda Settings (Impostazioni), selezionare Global Settings (Impostazioni globali).
2. Per le impostazioni dell'hypervisor, selezionare VM con iSCSI Direct Attached Disk o NFS per tutti gli host e aggiornare le impostazioni.

[larghezza=601, altezza=176]

Disattivare l'housekeeping automatico del backup dei log

La gestione del backup dei log è abilitata per impostazione predefinita e può essere disabilitata a livello di host del plug-in HANA. Utilizzare il comando PowerShell:

Il comando Set- SmConfigSettings -Plugin - HostName <pluginhostname> - PluginCode hana - configSettings @{"LOG_CLEANUP_DISABLE" = "Y"} disabilita la gestione del backup del log per questo host SAP HANA.

Abilitare la comunicazione sicura con il database HANA

Se i database HANA sono configurati con comunicazione sicura, il comando hdbsql eseguito da SnapCenter deve utilizzare opzioni della riga di comando aggiuntive.

Esistono diverse opzioni per configurare la comunicazione SSL. Per impostazione predefinita, SnapCenter utilizza l'opzione della riga di comando -e ssltrustcert hdbsql. Con questa opzione viene effettuata la comunicazione SSL senza convalida del certificato del server e funziona anche per i sistemi HANA in cui SSL non è abilitato.

Se è richiesta la convalida del certificato sul lato server e/o client, sono necessarie diverse opzioni della riga di comando hdbsql ed è necessario configurare l'ambiente PSE di conseguenza, come descritto nella Guida alla sicurezza di SAP HANA.

Ciò può essere ottenuto utilizzando uno script wrapper che richiama hdbsql con le opzioni richieste. Invece di configurare l'eseguibile hdbsql nei file hana.properties, viene aggiunto lo script wrapper.

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

Lo script wrapper hdbsqls richiama hdbsql con le opzioni della riga di comando richieste.

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

Disattivare la funzione di rilevamento automatico sull'host del plug-in HANA

Per disabilitare il rilevamento automatico sull'host del plug-in HANA, completare i seguenti passaggi:

1. Sul server SnapCenter , aprire PowerShell. Connettersi al server SnapCenter eseguendo il comando Open-SmConnection e specificare il nome utente e la password nella finestra di accesso iniziale.
2. Per disattivare il rilevamento automatico, eseguire il comando Set-SmConfigSettings.

Per un host HANA hana-2, il comando è il seguente:

```
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>
```

La configurazione viene scritta nel file di configurazione dell'agente sull'host ed è ancora disponibile dopo un aggiornamento del plug-in con 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 #
```

Informazioni sul copyright

Informazioni sul marchio commerciale