Documentazione software SnapCenter

SnapCenter Software 5.0

NetApp
November 13, 2024

Sommario

Documentazione software SnapCenter

Note di rilascio

Fornisce importanti informazioni su questa versione del server SnapCenter e sui pacchetti di plug-in SnapCenter, inclusi problemi risolti, problemi noti, precauzioni e limitazioni.

Per ulteriori informazioni, vedere "Note sulla versione del software SnapCenter 5,0".

Concetti

Panoramica di SnapCenter

Il software SnapCenter è una piattaforma semplice, centralizzata e scalabile che offre una protezione dei dati coerente con l'applicazione per applicazioni, database, file system host e macchine virtuali in esecuzione su sistemi ONTAP in qualsiasi punto del cloud ibrido.

SnapCenter sfrutta le tecnologie NetApp Snapshot, SnapRestore, FlexClone, SnapMirror e SnapVault per fornire quanto segue:

- Backup rapidi, efficienti in termini di spazio, coerenti con le applicazioni e basati su disco
- Ripristino rapido e granulare e ripristino coerente con l'applicazione
- Cloning rapido ed efficiente in termini di spazio

SnapCenter include sia il server SnapCenter che singoli plug-in leggeri. È possibile automatizzare la distribuzione dei plug-in agli host delle applicazioni remote, pianificare le operazioni di backup, verifica e clonazione e monitorare tutte le operazioni di protezione dei dati.

SnapCenter può essere implementato nei seguenti modi:

- On-premise per proteggere:
  - Dati presenti nei sistemi primari ONTAP FAS, AFF o All SAN Array (ASA) e replicati nei sistemi secondari ONTAP FAS, AFF o ASA
  - Dati sui sistemi primari ONTAP Select
  - Dati presenti nei sistemi primari e secondari ONTAP FAS, AFF o ASA e protetti nello storage a oggetti StorageGRID locale
- On-premise in un cloud ibrido per proteggere:
  - Dati presenti nei sistemi primari ONTAP FAS, AFF o ASA e replicati in Cloud Volumes ONTAP
  - Dati su sistemi primari e secondari ONTAP FAS, AFF o ASA e protetti per lo storage di oggetti e archivi nel cloud (utilizzando l'integrazione di backup e ripristino BlueXP)
- In un cloud pubblico per proteggere:
  - Dati presenti nei sistemi primari Cloud Volumes ONTAP (in precedenza cloud ONTAP)
  - Dati presenti su Amazon FSX per ONTAP
  - I dati che sono sul Azure NetApp Files primario (Oracle, Microsoft SQL e SAP HANA)

SnapCenter include le seguenti funzionalità principali:

- Protezione dei dati centralizzata e coerente con l'applicazione

  La protezione dei dati è supportata per i database Microsoft Exchange Server, Microsoft SQL Server, Oracle su Linux o AIX, il database SAP HANA e i file system host Windows in esecuzione sui sistemi ONTAP.

  La protezione dei dati è supportata anche per altre applicazioni e database standard o personalizzati fornendo un framework per creare plug-in SnapCenter definiti dall'utente. Ciò consente la protezione dei

dati per altre applicazioni e database dallo stesso singolo pannello di controllo. Sfruttando questo framework, NetApp ha rilasciato plug-in personalizzati SnapCenter per IBM DB2, MongoDB, MySQL e così via sul NetApp Automation Store.

- Backup basati su policy

  I backup basati su policy sfruttano la tecnologia NetApp Snapshot per creare backup rapidi, efficienti in termini di spazio, coerenti con l'applicazione e basati su disco. Facoltativamente, è possibile automatizzare la protezione di questi backup nello storage secondario mediante aggiornamenti alle relazioni di protezione esistenti.

- Backup di più risorse

  Utilizzando i gruppi di risorse SnapCenter è possibile eseguire contemporaneamente il backup di più risorse (applicazioni, database o file system host) dello stesso tipo.

- Ripristino e ripristino

  SnapCenter offre ripristini rapidi e granulari dei backup e recovery basato sul tempo e coerente con l'applicazione. È possibile eseguire il ripristino da qualsiasi destinazione nel cloud ibrido.

- Cloning

  SnapCenter offre una clonazione rapida, efficiente in termini di spazio e coerente con le applicazioni, che consente uno sviluppo software accelerato. Puoi clonare su qualsiasi destinazione nel cloud ibrido.

- Interfaccia grafica utente (GUI) di gestione utente singola

  L'interfaccia grafica di SnapCenter offre un'unica interfaccia per la gestione di backup e cloni di una risorsa in qualsiasi destinazione nel cloud ibrido.

- API REST, cmdlet Windows, comandi UNIX

  SnapCenter include API REST per la maggior parte delle funzionalità per l'integrazione con qualsiasi software di orchestrazione e l'utilizzo di cmdlet e interfaccia a riga di comando di Windows PowerShell.

  Per ulteriori informazioni sulle API REST, vedere "Panoramica delle API REST".

  Per ulteriori informazioni sui cmdlet di Windows, vedere "Guida di riferimento al cmdlet del software SnapCenter".

  Per ulteriori informazioni sui comandi UNIX, vedere "Guida di riferimento al comando software SnapCenter".

- Data Protection centralizzata Dashboard e reporting
- RBAC (Role-Based Access Control) per la sicurezza e la delega.
- Database di repository con disponibilità elevata

  SnapCenter offre un database repository integrato con alta disponibilità per memorizzare tutti i metadati di backup.

- Installazione push automatica dei plug-in

  È possibile automatizzare un push remoto dei plug-in SnapCenter dall'host del server SnapCenter agli host delle applicazioni.

- Alta disponibilità

  L'alta disponibilità per SnapCenter viene impostata utilizzando un bilanciamento del carico esterno (F5). Nello stesso data center sono supportati fino a due nodi.

- Disaster Recovery (DR)

  È possibile ripristinare il server SnapCenter in caso di disastri come danneggiamento delle risorse o crash del server.

- SnapLock

  SnapLock è una soluzione per la compliance dalle performance elevate per le organizzazioni che utilizzano lo storage WORM (Write Once, Read Many) per conservare i file in forma non modificata a scopi normativi e di governance.

  Per ulteriori informazioni su SnapLock, fare riferimento a. "Che cos'è SnapLock"

- Continuità aziendale SnapMirror (SM-BC)

  SnapMirror Business Continuity (SM-BC) consente ai servizi di business di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Per attivare un failover con SM-BC non sono richiesti né interventi manuali né script aggiuntivi.

  I plug-in supportati per questa funzionalità sono il plug-in SnapCenter per SQL Server, il plug-in SnapCenter per Windows e il plug-in SnapCenter per database Oracle.

  Per ulteriori informazioni su SM-BC, fare riferimento a. "Continuità aziendale SnapMirror (SM-BC)"

  Per SM-BC, assicurarsi di aver soddisfatto i vari requisiti di configurazione di hardware, software e sistema. Per ulteriori informazioni, fare riferimento a. "Prerequisiti"

- Mirroring sincrono

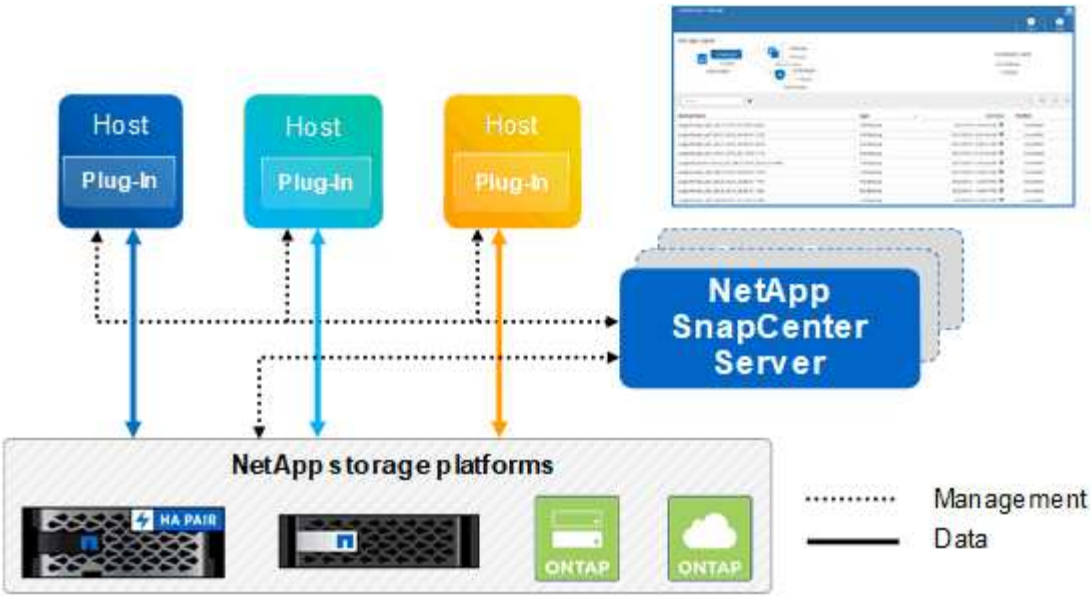
  La funzionalità di mirroring sincrono offre replica dei dati online e in tempo reale tra storage array su una distanza remota.

  Per ulteriori informazioni sul mirror della sincronizzazione, fare riferimento a. "Panoramica del mirroring sincrono"

Architettura SnapCenter

La piattaforma SnapCenter è basata su un'architettura a più livelli che include un server di gestione centralizzato (server SnapCenter) e un host plug-in SnapCenter.

SnapCenter supporta data center multisito. Il server SnapCenter e l'host plug-in possono trovarsi in diverse posizioni geografiche.



Componenti SnapCenter

SnapCenter è costituito dal server SnapCenter e dai plug-in SnapCenter. Installare solo i plug-in appropriati per i dati che si desidera proteggere.

- Server SnapCenter
- Pacchetto di plug-in SnapCenter per Windows, che include i seguenti plug-in:
  - Plug-in SnapCenter per Microsoft SQL Server
  - Plug-in SnapCenter per Microsoft Windows
  - Plug-in SnapCenter per server Microsoft Exchange
  - Plug-in SnapCenter per database SAP HANA
- Pacchetto plug-in SnapCenter per Linux, che include i seguenti plug-in:
  - Plug-in SnapCenter per database Oracle
  - Plug-in SnapCenter per database SAP HANA
  - Plug-in SnapCenter per file system UNIX
- Pacchetto plug-in SnapCenter per AIX, che include i seguenti plug-in:
  - Plug-in SnapCenter per database Oracle
  - Plug-in SnapCenter per file system UNIX
- Plug-in personalizzati di SnapCenter

Il plug-in SnapCenter per VMware vSphere, in precedenza NetApp Data Broker, è un'appliance virtuale standalone che supporta le operazioni di protezione dei dati SnapCenter su database e file system virtualizzati.

Server SnapCenter

Il server SnapCenter include un server Web, un'interfaccia utente centralizzata basata su HTML5, cmdlet PowerShell, API REST e il repository SnapCenter.

SnapCenter consente l'alta disponibilità e la scalabilità orizzontale su più server SnapCenter all'interno di una singola interfaccia utente. È possibile ottenere una disponibilità elevata utilizzando un bilanciamento del carico

esterno (F5). Per ambienti di grandi dimensioni con migliaia di host, l'aggiunta di più server SnapCenter può contribuire a bilanciare il carico.

- Se si utilizza il pacchetto di plug-in SnapCenter per Windows, l'agente host viene eseguito sul server SnapCenter e sull'host del plug-in Windows. L'agente host esegue le pianificazioni in modo nativo sull'host remoto di Windows oppure, per Microsoft SQL Server, la pianificazione viene eseguita sull'istanza SQL locale.

  Il server SnapCenter comunica con i plug-in di Windows tramite l'agente host.

- Se si utilizza il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX, le pianificazioni vengono eseguite sul server SnapCenter come pianificazioni delle attività di Windows.
  - Per il plug-in SnapCenter per database Oracle, l'agente host in esecuzione sull'host del server SnapCenter comunica con il caricatore plug-in (SPL) SnapCenter in esecuzione sull'host Linux o AIX per eseguire diverse operazioni di protezione dei dati.
  - Per il plug-in SnapCenter per il database SAP HANA e i plug-in personalizzati SnapCenter, il server SnapCenter comunica con questi plug-in tramite l'agente SCCore in esecuzione sull'host.

Il server SnapCenter e i plug-in comunicano con l'agente host utilizzando HTTPS. Le informazioni sulle operazioni SnapCenter vengono memorizzate nel repository SnapCenter.

SnapCenter supporta lo spazio dei nomi disgiunto per gli host Windows. Se si verificano problemi durante l'utilizzo dello spazio dei nomi disgiunto, fare riferimento a "SnapCenter non è in grado di rilevare le risorse quando si utilizza uno spazio dei nomi disgiunto".

Plug-in SnapCenter

Ogni plug-in SnapCenter supporta ambienti, database e applicazioni specifici.

Nome del plug-in	Incluso nel pacchetto di installazione	Richiede altri plug-in	Installato sull'host	Piattaforma supportata
Plug-in per SQL Server	Plug-in Package per Windows	Plug-in per Windows	Host di SQL Server	Windows
Plug-in per Windows	Plug-in Package per Windows		Host Windows	Windows
Plug-in per Exchange	Plug-in Package per Windows	Plug-in per Windows	Host di Exchange Server	Windows
Plug-in per Oracle Database	Plug-in Package for Linux and Plug-ins Package for AIX	Plug-in per UNIX	Host Oracle	Linux o AIX
Plug-in per SAP HANA Database	Pacchetto plug-in per Linux e pacchetto plug-in per Windows	Plug-in per UNIX o Plug-in per Windows	Host client HDBSQL	Linux o Windows

Nome del plug-in	Incluso nel pacchetto di installazione	Richiede altri plug-in	Installato sull'host	Piattaforma supportata
Plug-in personalizzati		Per i backup del file system, plug-in per Windows	Host applicativo personalizzato	Linux o Windows

Il plug-in SnapCenter per VMware vSphere supporta operazioni di backup e ripristino coerenti con il crash e le macchine virtuali per macchine virtuali (VM), datastore e dischi macchine virtuali (VMDK) e supporta i plug-in specifici dell'applicazione SnapCenter per proteggere le operazioni di backup e ripristino coerenti con l'applicazione per database e file system virtualizzati.

Per gli utenti di SnapCenter 4.1.1, la documentazione del plug-in SnapCenter per VMware vSphere 4.1.1 contiene informazioni sulla protezione dei database e dei file system virtualizzati. Per gli utenti di SnapCenter 4.2.x, NetApp Data Broker 1.0 e 1.0.1, la documentazione contiene informazioni sulla protezione dei database virtualizzati e dei file system mediante il plug-in SnapCenter per VMware vSphere fornito dall'appliance virtuale NetApp Data Broker basata su Linux (formato di appliance virtuale aperta). Per gli utenti che utilizzano SnapCenter 4,3 o versioni successive, "Plug-in SnapCenter per la documentazione di VMware vSphere" dispone di informazioni sulla protezione di database e file system virtualizzati mediante il plug-in SnapCenter basato su Linux per l'appliance virtuale VMware vSphere (formato Open Virtual Appliance).

Plug-in SnapCenter per le funzionalità di Microsoft SQL Server

- Automatizza le operazioni di backup, ripristino e clonazione application-aware per i database Microsoft SQL Server nel tuo ambiente SnapCenter.
- Supporta i database Microsoft SQL Server su LUN VMDK e RDM (Raw Device Mapping) quando si implementa il plug-in SnapCenter per VMware vSphere e si registra il plug-in con SnapCenter
- Supporta solo il provisioning delle condivisioni SMB. Non viene fornito il supporto per il backup dei database SQL Server sulle condivisioni SMB.
- Supporta l'importazione di backup da SnapManager per Microsoft SQL Server a SnapCenter.

Plug-in SnapCenter per le funzionalità di Microsoft Windows

- Abilita la protezione dei dati application-aware per altri plug-in in in esecuzione negli host Windows nell'ambiente SnapCenter
- Automatizza le operazioni di backup, ripristino e clonazione application-aware per i file system Microsoft nel tuo ambiente SnapCenter
- Supporta provisioning dello storage, coerenza Snapshot e recupero dello spazio per host Windows

Il plug-in per Windows fornisce condivisioni SMB e file system Windows su LUN fisici e RDM, ma non supporta operazioni di backup per file system Windows su condivisioni SMB.

Plug-in SnapCenter per le funzionalità di Microsoft Exchange Server

- Automatizza le operazioni di backup e ripristino application-aware per i database Microsoft Exchange Server e i gruppi di disponibilità dei database (DAG) nel tuo ambiente SnapCenter
- Supporta Exchange Server virtualizzati su LUN RDM quando si implementa il plug-in SnapCenter per

VMware vSphere e si registra il plug-in con SnapCenter

Plug-in SnapCenter per le funzionalità di database Oracle

- Automatizza backup, ripristino, ripristino, verifica, montaggio e ripristino basati sulle applicazioni Smontare e clonare le operazioni per i database Oracle nel tuo ambiente SnapCenter
- Supporta i database Oracle per SAP, tuttavia non viene fornita l'integrazione SAP BR*Tools

Funzionalità del plug-in SnapCenter per UNIX

- Consente al plug-in per database Oracle di eseguire operazioni di protezione dei dati sui database Oracle gestendo lo stack di storage host sottostante sui sistemi Linux o AIX
- Supporta i protocolli NFS (Network file System) e SAN (Storage Area Network) su un sistema storage che esegue ONTAP.
- Per i sistemi Linux, i database Oracle su LUN VMDK e RDM sono supportati quando si implementa il plug-in SnapCenter per VMware vSphere e si registra il plug-in con SnapCenter.
- Supporta Mount Guard per AIX su file system SAN e layout LVM.
- Supporta Enhanced Journaled file System (JFS2) con logging inline su file system SAN e layout LVM solo per sistemi AIX.

  Sono supportati i dispositivi nativi SAN, i file system e i layout LVM costruiti sui dispositivi SAN.

- Automatizza le operazioni di backup, ripristino e clonazione integrate con l'applicazione per file system UNIX nel tuo ambiente SnapCenter

Plug-in SnapCenter per le funzionalità del database SAP HANA

- Automatizza il backup, il ripristino e la clonazione application-aware dei database SAP HANA nel tuo ambiente SnapCenter

Funzionalità dei plug-in personalizzati di SnapCenter

- Supporta plug-in personalizzati per gestire applicazioni o database non supportati da altri plug-in SnapCenter. I plug-in personalizzati non vengono forniti come parte dell'installazione di SnapCenter.
- Supporta la creazione di copie mirror dei set di backup su un altro volume ed esecuzione della replica del backup disk-to-disk.
- Supporta ambienti Windows e Linux. Negli ambienti Windows, le applicazioni personalizzate tramite plug-in personalizzati possono utilizzare il plug-in SnapCenter per Microsoft Windows per eseguire backup coerenti del file system.

I plug-in personalizzati MySQL, DB2 e MongoDB sono supportati solo dalle community NetApp.

NetApp supporta la possibilità di creare e utilizzare plug-in personalizzati; tuttavia, i plug-in personalizzati creati non sono supportati da NetApp.

Per ulteriori informazioni, vedere "Sviluppare un plug-in per l'applicazione"

Repository SnapCenter

Il repository SnapCenter, a volte chiamato database NSM, memorizza informazioni e metadati per ogni operazione SnapCenter.

Il database del repository MySQL Server viene installato per impostazione predefinita quando si installa il server SnapCenter. Se MySQL Server è già installato e si sta eseguendo una nuova installazione di SnapCenter Server, è necessario disinstallare MySQL Server.

SnapCenter supporta MySQL Server 5.7.25 o versione successiva come database repository SnapCenter. Se si utilizza una versione precedente di MySQL Server con una release precedente di SnapCenter, durante l'aggiornamento di SnapCenter, MySQL Server viene aggiornato alla versione 5.7.25 o successiva.

Il repository SnapCenter memorizza le seguenti informazioni e metadati:

- Backup, clonazione, ripristino e verifica dei metadati
- Informazioni su reporting, lavoro ed eventi
- Informazioni su host e plug-in
- Dettagli su ruolo, utente e permesso
- Informazioni sulla connessione del sistema di storage

Funzionalità di sicurezza

SnapCenter utilizza rigide funzionalità di sicurezza e autenticazione per garantire la sicurezza dei dati.

SnapCenter include le seguenti funzioni di sicurezza:

- Tutte le comunicazioni con SnapCenter utilizzano HTTP su SSL (HTTPS).
- Tutte le credenziali in SnapCenter sono protette mediante la crittografia AES (Advanced Encryption Standard).
- SnapCenter utilizza algoritmi di sicurezza conformi allo standard FIPS (Federal Information Processing Standard).
- SnapCenter supporta l'utilizzo dei certificati CA autorizzati forniti dal cliente.
- SnapCenter 4.1.1 o versioni successive supporta TLS (Transport Layer Security) 1,2 per la comunicazione con ONTAP. È inoltre possibile utilizzare TLS 1,2 per le comunicazioni tra client e server.

  A partire da 5,0, SnapCenter supporta (TLS) 1,3 per le comunicazioni con ONTAP.

- SnapCenter supporta un determinato set di suite di crittografia SSL per garantire la sicurezza delle comunicazioni di rete.

  Per ulteriori informazioni, vedere "Come configurare la suite di crittografia SSL supportata".

- SnapCenter viene installato all'interno del firewall aziendale per consentire l'accesso al server SnapCenter e la comunicazione tra il server SnapCenter e i plug-in.
- L'API SnapCenter e l'accesso alle operazioni utilizzano token crittografati con crittografia AES, che scadono dopo 24 ore.
- SnapCenter si integra con Windows Active Directory per l'accesso e il RBAC (role-based access control) che regolano le autorizzazioni di accesso.
- IPSec è supportato con SnapCenter su ONTAP per computer host Windows e Linux. "Scopri di più"
- I cmdlet PowerShell di SnapCenter sono protetti da sessione.
- Dopo un periodo di inattività predefinito di 15 minuti, SnapCenter avvisa che l'utente verrà disconnesso tra

5 minuti. Dopo 20 minuti di inattività, SnapCenter si disconnette ed è necessario effettuare nuovamente l'accesso. È possibile modificare il periodo di disconnessione.

- L'accesso viene temporaneamente disattivato dopo 5 o più tentativi di accesso non corretti.
- Supporta l'autenticazione del certificato CA tra il server SnapCenter e ONTAP. "Scopri di più"
- Integrity Verifier viene aggiunto al server SnapCenter e ai plug-in e convalida tutti i file binari forniti durante le nuove operazioni di installazione e aggiornamento.

Panoramica del certificato CA

Il programma di installazione del server SnapCenter abilita il supporto centralizzato dei certificati SSL durante l'installazione. Per migliorare la comunicazione protetta tra il server e il plug-in, SnapCenter supporta l'utilizzo dei certificati CA autorizzati forniti dal cliente.

È necessario implementare i certificati CA dopo aver installato il server SnapCenter e i relativi plug-in. Per ulteriori informazioni, vedere "Generare il file CSR del certificato CA".

È inoltre possibile implementare il certificato CA per il plug-in SnapCenter per VMware vSphere. Per ulteriori informazioni, vedere "Creare e importare certificati".

Comunicazione SSL bidirezionale

La comunicazione SSL bidirezionale protegge la comunicazione reciproca tra il server SnapCenter e i plug-in.

Panoramica dell'autenticazione basata su certificato

L'autenticazione basata su certificato verifica l'autenticità dei rispettivi utenti che tentano di accedere all'host del plug-in SnapCenter. L'utente deve esportare il certificato del server SnapCenter senza chiave privata e importarlo nell'archivio attendibile dell'host del plug-in. L'autenticazione basata su certificato funziona solo se è attivata la funzione SSL bidirezionale.

Autenticazione a più fattori (MFA)

MFA utilizza un provider di identità (IdP) di terze parti tramite SAML (Security Assertion Markup Language) per gestire le sessioni degli utenti. Questa funzionalità migliora la sicurezza dell'autenticazione grazie alla possibilità di utilizzare diversi fattori come TOTP, biometria, notifiche push e così via, oltre al nome utente e alla password esistenti. Inoltre, consente al cliente di utilizzare i propri provider di identità utente per ottenere un accesso utente unificato (SSO) nel proprio portfolio.

MFA è applicabile solo per l'accesso all'interfaccia utente del server SnapCenter. Gli accessi vengono autenticati tramite IdP Active Directory Federation Services (ad FS). È possibile configurare diversi fattori di autenticazione in ad FS. SnapCenter è il provider di servizi ed è necessario configurare SnapCenter come parte di base in ad FS. Per attivare l'MFA in SnapCenter, sono necessari i metadati di ad FS.

Per informazioni sull'abilitazione dell'MFA, vedere "Abilitare l'autenticazione a più fattori".

RBAC (Role-Based Access Control) di SnapCenter

Tipi di RBAC

Le autorizzazioni RBAC (Role-Based Access Control) e ONTAP di SnapCenter consentono agli amministratori di SnapCenter di delegare il controllo delle risorse

SnapCenter a diversi utenti o gruppi di utenti. Questo accesso gestito centralmente consente agli amministratori delle applicazioni di lavorare in modo sicuro all'interno degli ambienti delegati.

È possibile creare e modificare i ruoli e aggiungere l'accesso alle risorse agli utenti in qualsiasi momento, ma quando si imposta SnapCenter per la prima volta, è necessario almeno aggiungere utenti o gruppi Active Directory ai ruoli, quindi aggiungere l'accesso alle risorse a tali utenti o gruppi.

> Non è possibile utilizzare SnapCenter per creare account utente o di gruppo. È necessario creare account utente o di gruppo in Active Directory del sistema operativo o del database.

SnapCenter utilizza i seguenti tipi di controllo degli accessi in base al ruolo:

- SnapCenter RBAC
- Plug-in SnapCenter RBAC (per alcuni plug-in)
- RBAC a livello applicativo
- Permessi ONTAP

SnapCenter RBAC

Ruoli e autorizzazioni

SnapCenter viene fornito con ruoli predefiniti con autorizzazioni già assegnate. È possibile assegnare utenti o gruppi di utenti a questi ruoli. È inoltre possibile creare nuovi ruoli e gestire autorizzazioni e utenti.

Assegnazione delle autorizzazioni a utenti o gruppi

È possibile assegnare autorizzazioni a utenti o gruppi per accedere a oggetti SnapCenter come host, connessioni di storage e gruppi di risorse. Non è possibile modificare le autorizzazioni del ruolo SnapCenterAdmin.

È possibile assegnare le autorizzazioni RBAC a utenti e gruppi all'interno della stessa foresta e a utenti appartenenti a foreste diverse. Non è possibile assegnare autorizzazioni RBAC agli utenti appartenenti a gruppi nidificati tra foreste.

> Se si crea un ruolo personalizzato, deve contenere tutte le autorizzazioni del ruolo di amministratore di SnapCenter. Se si copiano solo alcune delle autorizzazioni, ad esempio aggiunta host o rimozione host, non è possibile eseguire tali operazioni.

Autenticazione

Gli utenti devono fornire l'autenticazione durante l'accesso, tramite l'interfaccia grafica utente (GUI) o utilizzando i cmdlet PowerShell. Se gli utenti sono membri di più ruoli, dopo aver immesso le credenziali di accesso, viene richiesto di specificare il ruolo che si desidera utilizzare. Gli utenti devono inoltre fornire l'autenticazione per eseguire le API.

RBAC a livello applicativo

SnapCenter utilizza le credenziali per verificare che gli utenti SnapCenter autorizzati dispongano anche delle autorizzazioni a livello di applicazione.

Ad esempio, se si desidera eseguire operazioni di snapshot e protezione dei dati in un ambiente SQL Server, è

necessario impostare le credenziali con le credenziali Windows o SQL appropriate. Il server SnapCenter autentica il set di credenziali utilizzando uno dei due metodi. Per eseguire operazioni di Snapshot e data Protection in un ambiente file system Windows sullo storage ONTAP, il ruolo di amministratore SnapCenter deve disporre dei privilegi di amministratore sull'host Windows.

Allo stesso modo, se si desidera eseguire operazioni di protezione dei dati su un database Oracle e se l'autenticazione del sistema operativo (OS) è disattivata nell'host del database, è necessario impostare le credenziali con il database Oracle o con le credenziali ASM Oracle. Il server SnapCenter autentica il set di credenziali utilizzando uno di questi metodi, a seconda dell'operazione.

Plug-in SnapCenter per VMware vSphere RBAC

Se si utilizza il plug-in VMware di SnapCenter per la protezione dei dati coerente con le macchine virtuali, il server vCenter fornisce un livello aggiuntivo di RBAC. Il plug-in VMware di SnapCenter supporta sia vCenter Server RBAC che Data ONTAP RBAC.

Per informazioni, vedere "Plug-in SnapCenter per VMware vSphere RBAC"

Permessi ONTAP

È necessario creare un account vsadmin con le autorizzazioni necessarie per accedere al sistema di storage.

Per informazioni sulla creazione dell'account e l'assegnazione delle autorizzazioni, vedere "Creare un ruolo di cluster ONTAP con privilegi minimi"

Autorizzazioni e ruoli RBAC

Il RBAC (Role-Based Access Control) di SnapCenter consente di creare ruoli e assegnare autorizzazioni a tali ruoli, quindi assegnare utenti o gruppi di utenti ai ruoli. Ciò consente agli amministratori di SnapCenter di creare un ambiente gestito centralmente, mentre gli amministratori delle applicazioni possono gestire i processi di protezione dei dati. SnapCenter viene fornito con alcuni ruoli e autorizzazioni predefiniti.

Ruoli di SnapCenter

SnapCenter viene fornito con i seguenti ruoli predefiniti. È possibile assegnare utenti e gruppi a questi ruoli o creare nuovi ruoli.

Quando si assegna un ruolo a un utente, nella pagina lavori sono visibili solo i lavori pertinenti a tale utente, a meno che non sia stato assegnato il ruolo Amministratore SnapCenter.

- Backup dell'app e amministratore del clone
- Visualizzatore di backup e cloni
- Amministratore dell'infrastruttura
- SnapCenterAdmin

Plug-in SnapCenter per i ruoli di VMware vSphere

Per la gestione della protezione dei dati coerente con le macchine virtuali di macchine virtuali, VMDK e datastore, i seguenti ruoli vengono creati in vCenter dal plug-in SnapCenter per VMware vSphere:

- Amministratore di SCV

- Vista dei distributori idraulici
- SCV di backup
- Ripristino dei distributori idraulici
- Ripristino del file ospite SCV

Per ulteriori informazioni, vedere "Tipi di plug-in RBAC per SnapCenter per utenti di VMware vSphere"

Best practice: NetApp consiglia di creare un ruolo ONTAP per il plug-in SnapCenter per le operazioni VMware vSphere e assegnargli tutti i privilegi richiesti.

Permessi SnapCenter

SnapCenter fornisce le seguenti autorizzazioni:

- Gruppo di risorse
- Policy
- Backup
- Host
- Connessione storage
- Clonare
- Provisioning (solo per database Microsoft SQL)
- Dashboard
- Report
- Ripristinare
  - Full Volume Restore (solo per plug-in personalizzati)
- Risorsa

  L'amministratore deve disporre dei privilegi del plug-in per consentire ai non amministratori di eseguire l'operazione di rilevamento delle risorse.

- Installazione o disinstallazione del plug-in

  Quando si abilitano le autorizzazioni per l'installazione del plug-in, è necessario modificare anche l'autorizzazione host per abilitare le letture e gli aggiornamenti.

- Migrazione
- Montare (solo per database Oracle)
- Smontare (solo per database Oracle)
- Monitoraggio del processo

  L'autorizzazione Job Monitor consente ai membri di diversi ruoli di visualizzare le operazioni su tutti gli oggetti a cui sono assegnati.

Ruoli e autorizzazioni SnapCenter predefiniti

SnapCenter viene fornito con ruoli predefiniti, ciascuno con un set di autorizzazioni già attivate. Quando si imposta e si amministra RBAC (role-based access control), è possibile utilizzare questi ruoli predefiniti o crearne di nuovi.

SnapCenter include i seguenti ruoli predefiniti:

- Ruolo di amministratore di SnapCenter
- Backup dell'app e ruolo di amministratore del clone
- Ruolo di Backup e Clone Viewer
- Ruolo di amministratore dell'infrastruttura

Quando si aggiunge un utente a un ruolo, è necessario assegnare l'autorizzazione StorageConnection per abilitare la comunicazione SVM (Storage Virtual Machine) o assegnare una SVM all'utente per abilitare l'autorizzazione all'utilizzo di SVM. L'autorizzazione connessione storage consente agli utenti di creare connessioni SVM.

Ad esempio, un utente con il ruolo di amministratore SnapCenter può creare connessioni SVM e assegnarle a un utente con il ruolo di backup dell'applicazione e amministratore clone, che per impostazione predefinita non dispone dell'autorizzazione per creare o modificare connessioni SVM. Senza una connessione SVM, gli utenti non possono completare alcuna operazione di backup, clonazione o ripristino.

Ruolo di amministratore di SnapCenter

Il ruolo di amministratore di SnapCenter ha tutte le autorizzazioni attivate. Non è possibile modificare le autorizzazioni per questo ruolo. È possibile aggiungere utenti e gruppi al ruolo o rimuoverli.

Backup dell'app e ruolo di amministratore del clone

Il ruolo App Backup and Clone Admin dispone delle autorizzazioni necessarie per eseguire azioni amministrative per i backup delle applicazioni e le attività correlate ai cloni. Questo ruolo non dispone di autorizzazioni per la gestione degli host, il provisioning, la gestione della connessione dello storage o l'installazione remota.

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Gruppo di risorse	Non applicabile	Sì	Sì	Sì	Sì
Policy	Non applicabile	Sì	Sì	Sì	Sì
Backup	Non applicabile	Sì	Sì	Sì	Sì
Host	Non applicabile	Sì	Sì	Sì	Sì
Connessione storage	Non applicabile	No	Sì	No	No
Clonare	Non applicabile	Sì	Sì	Sì	Sì

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Provisioning	Non applicabile	No	Sì	No	No
Dashboard	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Report	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristinare	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Risorsa	Sì	Sì	Sì	Sì	Sì
Installazione/disinstallazione del plug-in	No	Non applicabile		Non applicabile	Non applicabile
Migrazione	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Montare	Sì	Sì	Non applicabile	Non applicabile	Non applicabile
Smontare	Sì	Sì	Non applicabile	Non applicabile	Non applicabile
Ripristino completo del volume	No	No	Non applicabile	Non applicabile	Non applicabile
Monitoraggio del processo	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Ruolo di Backup e Clone Viewer

Il ruolo Backup and Clone Viewer (Visualizzatore di backup e clonazione) dispone di una vista in sola lettura di tutte le autorizzazioni. Questo ruolo dispone anche di autorizzazioni abilitate per il rilevamento, la creazione di report e l'accesso al dashboard.

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Gruppo di risorse	Non applicabile	No	Sì	No	No
Policy	Non applicabile	No	Sì	No	No
Backup	Non applicabile	No	Sì	No	No
Host	Non applicabile	No	Sì	No	No

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Connessione storage	Non applicabile	No	Sì	No	No
Clonare	Non applicabile	No	Sì	No	No
Provisioning	Non applicabile	No	Sì	No	No
Dashboard	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Report	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristinare	No	No	Non applicabile	Non applicabile	Non applicabile
Risorsa	No	No	Sì	Sì	No
Installazione/disinstallazione del plug-in	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Migrazione	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Montare	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Smontare	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristino completo del volume	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Monitoraggio del processo	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Ruolo di amministratore dell'infrastruttura

Il ruolo Infrastructure Admin (Amministratore dell'infrastruttura) dispone di autorizzazioni abilitate per la gestione degli host, la gestione dello storage, il provisioning, i gruppi di risorse, i report di installazione remota, E l'accesso alla dashboard.

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Gruppo di risorse	Non applicabile	Sì	Sì	Sì	Sì
Policy	Non applicabile	No	Sì	Sì	Sì

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Backup	Non applicabile	Sì	Sì	Sì	Sì
Host	Non applicabile	Sì	Sì	Sì	Sì
Connessione storage	Non applicabile	Sì	Sì	Sì	Sì
Clonare	Non applicabile	No	Sì	No	No
Provisioning	Non applicabile	Sì	Sì	Sì	Sì
Dashboard	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Report	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristinare	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Risorsa	Sì	Sì	Sì	Sì	Sì
Installazione/disinstallazione del plug-in	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Migrazione	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Montare	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Smontare	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristino completo del volume	No	No	Non applicabile	Non applicabile	Non applicabile
Monitoraggio del processo	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Disaster recovery SnapCenter

È possibile ripristinare il server SnapCenter in caso di disastri come il danneggiamento delle risorse o il crash del server utilizzando la funzione di disaster recovery (DR) di SnapCenter. È possibile ripristinare il repository SnapCenter, le pianificazioni dei server e i componenti di configurazione dei server. È inoltre possibile ripristinare il plug-in SnapCenter per SQL Server e il plug-in SnapCenter per lo storage SQL Server.

In questa sezione vengono descritti i due tipi di disaster recovery (DR) in SnapCenter:

Dr. Server SnapCenter

- Viene eseguito il backup dei dati del server SnapCenter e possono essere ripristinati senza alcun plug-in aggiunto o gestito dal server SnapCenter.
- Il server SnapCenter secondario deve essere installato nella stessa directory di installazione e sulla stessa porta del server SnapCenter primario.
- Per l'autenticazione a più fattori (MFA), durante il DR del server SnapCenter, chiudere tutte le schede del browser e riaprire un browser per effettuare nuovamente l'accesso. In questo modo, i cookie di sessione esistenti o attivi verranno salvati e verranno aggiornati i dati di configurazione corretti.
- La funzionalità di disaster recovery di SnapCenter utilizza API REST per il backup del server SnapCenter. Vedere "Flussi di lavoro API REST per il disaster recovery del server SnapCenter".
- Il backup del file di configurazione relativo alle impostazioni di controllo non viene eseguito nel backup DR e nel server DR dopo l'operazione di ripristino. Ripetere manualmente le impostazioni del registro di controllo.

Plug-in SnapCenter e DR storage

DR è supportato solo per il plug-in SnapCenter per SQL Server. Quando il plug-in SnapCenter per SQL Server è inattivo, passare a un host SQL diverso e ripristinare i dati eseguendo pochi passaggi. Vedere "Disaster recovery del plug-in SnapCenter per SQL Server".

SnapCenter utilizza la tecnologia SnapMirror di ONTAP per replicare i dati. Può essere utilizzato per replicare i dati su un sito secondario per il DR e mantenerli sincronizzati. È possibile avviare un failover interrompendo la relazione di replica in SnapMirror. Durante il failback, la sincronizzazione può essere invertita e i dati dal sito di DR possono essere replicati nuovamente nella posizione principale.

Risorse, gruppi di risorse e policy

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- **Le risorse** sono generalmente database, file system Windows o condivisioni di file di cui si esegue il backup o la clonazione con SnapCenter.

  Tuttavia, a seconda dell'ambiente in uso, le risorse potrebbero essere istanze di database, gruppi di disponibilità di Microsoft SQL Server, database Oracle, database Oracle RAC, file system Windows o un gruppo di applicazioni personalizzate.

- Un **gruppo di risorse** è un insieme di risorse su un host o cluster. Il gruppo di risorse può anche contenere risorse provenienti da più host e da più cluster.

  Quando si esegue un'operazione su un gruppo di risorse, questa operazione viene eseguita su tutte le risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È inoltre possibile configurare backup pianificati per singole risorse e gruppi di risorse.

  > Se si attiva la modalità di manutenzione di un host di un gruppo di risorse condiviso e sono presenti pianificazioni associate allo stesso gruppo di risorse condivise, tutte le operazioni pianificate verranno sospese per tutti gli altri host del gruppo di risorse condiviso.

È necessario utilizzare un plug-in del database per il backup dei database, un plug-in del file system per il backup dei file system e il plug-in SnapCenter per VMware vSphere per il backup di macchine virtuali e datastore.

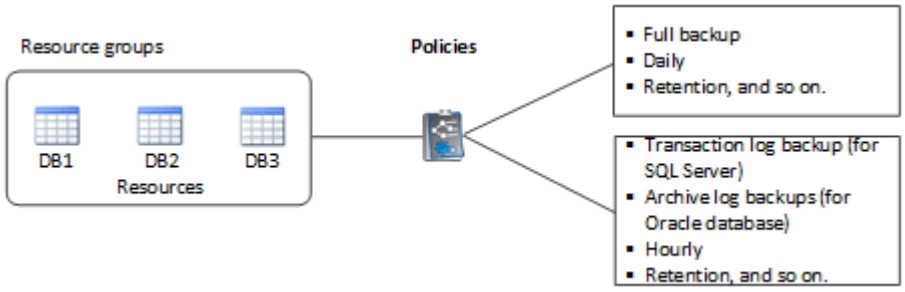
- **Policy** specifica la frequenza di backup, la conservazione delle copie, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano uno o più criteri per tale gruppo. È inoltre possibile selezionare un criterio quando si esegue un backup su richiesta.

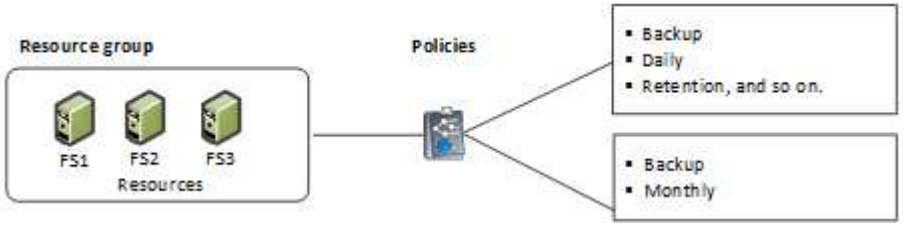
Un gruppo di risorse definisce *cosa* si desidera proteggere e quando si desidera proteggerlo in termini di giorno e ora. Pensa a una policy come a definire *come* la vuoi proteggere. Ad esempio, se si esegue il backup di tutti i database o di tutti i file system di un host, è possibile creare un gruppo di risorse che includa tutti i database o tutti i file system dell'host. È quindi possibile associare due criteri al gruppo di risorse: Una policy giornaliera e una policy oraria.

Quando si crea il gruppo di risorse e si allegano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno e un altro programma che esegua i backup del registro ogni ora.

L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i database:



L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i file system Windows:



Prescrizioni e post-script

È possibile utilizzare prescritture e postscript personalizzati come parte delle operazioni di protezione dei dati. Questi script consentono l'automazione prima o dopo il lavoro di protezione dei dati. Ad esempio, è possibile includere uno script che notifica automaticamente gli errori o gli avvisi dei processi di protezione dei dati. Prima di impostare le prescrizioni e i postscript, è necessario comprendere alcuni dei requisiti per la creazione di questi script.

Tipi di script supportati

Per Windows sono supportati i seguenti tipi di script:

- File batch
- Script PowerShell
- Script Perl

Sono supportati i seguenti tipi di script per UNIX:

- Script Perl
- Script Python
- Script shell

> Insieme alla shell bash di default sono supportate anche altre shell come sh-shell, k-shell e c-shell.

Percorso dello script

Tutte le prescritture e i postscript eseguiti come parte delle operazioni SnapCenter, su sistemi storage non virtualizzati e virtualizzati, vengono eseguiti sull'host plug-in.

- Gli script di Windows devono essere posizionati sull'host del plug-in.

> Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

- Gli script UNIX devono essere posizionati sull'host del plug-in.

> Il percorso dello script viene convalidato al momento dell'esecuzione.

Dove specificare gli script

Gli script sono specificati nelle policy di backup. Quando viene avviato un processo di backup, il criterio associa automaticamente lo script alle risorse di cui viene eseguito il backup. Quando si crea un criterio di backup, è possibile specificare gli argomenti prescrittt e postscript.

> Non è possibile specificare più script.

Timeout dello script

Per impostazione predefinita, il timeout è impostato su 60 secondi. È possibile modificare il valore di timeout.

Output dello script

La directory predefinita per i file di output delle prescrizioni e dei post-script di Windows è Windows System32.

Non esiste una posizione predefinita per le prescrizioni e i postscript UNIX. È possibile reindirizzare il file di output in qualsiasi posizione preferita.

Automazione SnapCenter con API REST

È possibile utilizzare le API REST per eseguire diverse operazioni di gestione di SnapCenter. Le API REST sono esposte attraverso la pagina web di Swagger. È possibile accedere alla pagina Web di Swagger per visualizzare la documentazione API REST e per eseguire manualmente una chiamata API. È possibile utilizzare le API REST per gestire il server SnapCenter o l'host SnapCenter vSphere.

Le API REST per…	**Si trovano in…**
Server SnapCenter	Https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/
Plug-in SnapCenter per VMware vSphere	Https://<OVA_IP_address_or_host_name>:<scv_plugin_port>/api/swagger-ui.html n.

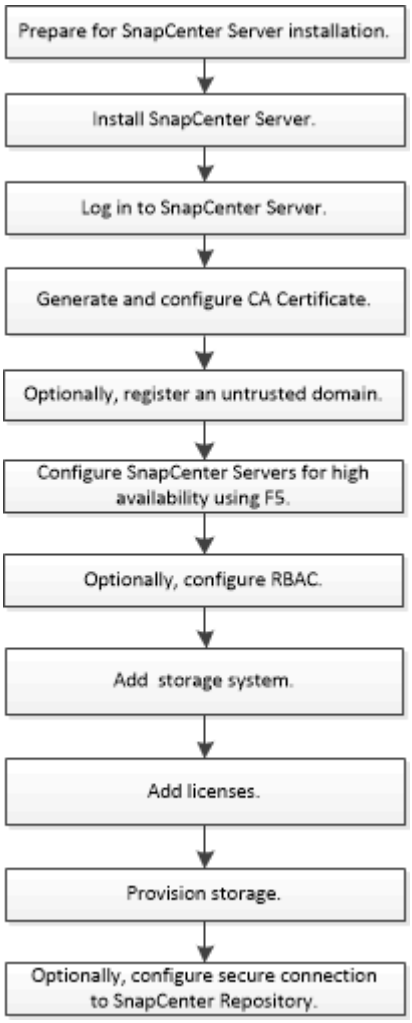
Per informazioni sulle API REST SnapCenter, vedere "Panoramica delle API REST"

Per informazioni sul plug-in SnapCenter per le API REST VMware vSphere, vedere "Plug-in SnapCenter per le API REST di VMware vSphere"

Installazione del server SnapCenter

Workflow di installazione

Il flusso di lavoro mostra le diverse attività necessarie per installare e configurare il server SnapCenter.



Preparazione per l'installazione del server SnapCenter

Requisiti di dominio e gruppo di lavoro

Il server SnapCenter può essere installato su sistemi che si trovano in un dominio o in un gruppo di lavoro. L'utente utilizzato per l'installazione deve disporre dei privilegi di amministratore sul computer in caso di gruppo di lavoro e dominio.

Per installare il server SnapCenter e i plug-in SnapCenter su host Windows, è necessario utilizzare uno dei seguenti elementi:

- **Dominio Active Directory**

  È necessario utilizzare un utente di dominio con diritti di amministratore locale. L'utente di dominio deve

essere membro del gruppo Administrator locale sull'host Windows.

- **Gruppi di lavoro**

  È necessario utilizzare un account locale con diritti di amministratore locale.

Sebbene siano supportati trust di dominio, foreste di domini multipli e trust tra domini, i domini tra foreste non sono supportati. La documentazione Microsoft sui domini e trust di Active Directory contiene ulteriori informazioni.

> Dopo aver installato il server SnapCenter, non modificare il dominio in cui si trova l'host SnapCenter. Se si rimuove l'host del server SnapCenter dal dominio in cui si trovava quando è stato installato il server SnapCenter e si tenta di disinstallare il server SnapCenter, l'operazione di disinstallazione non riesce.

Requisiti di spazio e dimensionamento

Prima di installare il server SnapCenter, è necessario conoscere i requisiti di spazio e dimensionamento. È inoltre necessario applicare gli aggiornamenti di sicurezza e di sistema disponibili.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Sono supportate solo le versioni in inglese, tedesco, giapponese e cinese semplificato dei sistemi operativi. Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".
Numero minimo di CPU	4 core
RAM minima	8 GB Il pool di buffer di MySQL Server utilizza il 20% della RAM totale.
Spazio minimo su disco rigido per il software e i registri del server SnapCenter	4 GB Se il repository SnapCenter si trova nello stesso disco in cui è installato il server SnapCenter, si consiglia di utilizzare 10 GB.

Elemento	Requisiti
Spazio minimo su disco rigido per il repository SnapCenter	6 GB NOTA: Se il server SnapCenter si trova nello stesso disco in cui è installato il repository SnapCenter, si consiglia di utilizzare 10 GB.
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet".

Requisiti degli host SAN

Se l'host SnapCenter fa parte di un ambiente FC/iSCSI, potrebbe essere necessario installare software aggiuntivo sul sistema per consentire l'accesso allo storage ONTAP.

SnapCenter non include le utility host o un DSM. Se l'host SnapCenter fa parte di un ambiente SAN, potrebbe essere necessario installare e configurare il seguente software:

- Utility host

  Le utility host supportano FC e iSCSI e consentono di utilizzare MPIO sui server Windows. Per informazioni, vedere "Documentazione delle utility host".

- Microsoft DSM per Windows MPIO

  Questo software funziona con i driver MPIO di Windows per gestire percorsi multipli tra i computer host NetApp e Windows.

  Per le configurazioni ad alta disponibilità è necessario un DSM.

  Se si utilizza ONTAP DSM, è necessario eseguire la migrazione a Microsoft DSM. Per ulteriori informazioni, vedere "Come migrare da ONTAP DSM a Microsoft DSM".

Sistemi e applicazioni storage supportati

È necessario conoscere il sistema di storage, le applicazioni e i database supportati.

- SnapCenter supporta ONTAP 9.8 e versioni successive per proteggere i dati.
- SnapCenter supporta Amazon FSX per NetApp ONTAP per proteggere i dati dalla versione della patch P1

del software SnapCenter 4.5.

Se si utilizza Amazon FSX per NetApp ONTAP, assicurarsi che i plug-in host del server SnapCenter siano aggiornati alla versione 4.5 P1 o successiva per eseguire le operazioni di protezione dei dati.

Per informazioni su Amazon FSX per NetApp ONTAP, vedere "Documentazione di Amazon FSX per NetApp ONTAP".

- SnapCenter supporta la protezione di diverse applicazioni e database.

  Per informazioni dettagliate sulle applicazioni e i database supportati, vedere "Tool di matrice di interoperabilità NetApp".

- SnapCenter 4,9 P1 e versioni successive supporta la protezione dei carichi di lavoro Oracle e Microsoft SQL in ambienti VMware Cloud su Amazon Web Services (AWS) Software-Defined Data Center (SDDC).

  Per ulteriori informazioni, vedere "Proteggi i carichi di lavoro Oracle e MS SQL utilizzando NetApp SnapCenter in VMware Cloud su ambienti SDDC AWS".

Browser supportati

Il software SnapCenter può essere utilizzato su più browser.

- Cromo

  Se si utilizza la versione 66, potrebbe non essere possibile avviare l'interfaccia grafica di SnapCenter.

- Microsoft Edge 110.0.1587.17 e versioni successive

Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Requisiti di connessione e porta

Prima di installare il server SnapCenter e i plug-in dell'applicazione o del database, assicurarsi che i requisiti di connessione e porte siano soddisfatti.

- Le applicazioni non possono condividere una porta.

  Ciascuna porta deve essere dedicata all'applicazione appropriata.

- Per le porte personalizzabili, è possibile selezionare una porta personalizzata durante l'installazione se non si desidera utilizzare la porta predefinita.

  È possibile modificare una porta del plug-in dopo l'installazione utilizzando la procedura guidata Modify host (Modifica host).

- Per le porte fisse, accettare il numero di porta predefinito.
- Firewall
  - Firewall, proxy o altri dispositivi di rete non devono interferire con le connessioni.
  - Se si specifica una porta personalizzata quando si installa SnapCenter, è necessario aggiungere una regola firewall sull'host del plug-in per tale porta per il caricatore plug-in SnapCenter.

La tabella seguente elenca le diverse porte e i relativi valori predefiniti.

Tipo di porta	Porta predefinita
Porta SnapCenter	8146 (HTTPS), bidirezionale, personalizzabile, come nell'URL *https://server:8146* Utilizzato per la comunicazione tra il client SnapCenter (l'utente SnapCenter) e il server SnapCenter. Utilizzato anche per la comunicazione dagli host plug-in al server SnapCenter. Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Porta di comunicazione SMCore SnapCenter	8145 (HTTPS), bidirezionale, personalizzabile La porta viene utilizzata per la comunicazione tra il server SnapCenter e gli host in cui sono installati i plug-in SnapCenter. Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Porta MySQL	3306 (HTTPS), bidirezionale La porta viene utilizzata per la comunicazione tra SnapCenter e il database del repository MySQL. È possibile creare connessioni protette dal server SnapCenter al server MySQL. "Scopri di più" Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Host plug-in Windows	135, 445 (TCP) Oltre alle porte 135 e 445, dovrebbe essere aperto anche l'intervallo di porte dinamiche specificato da Microsoft. Le operazioni di installazione remota utilizzano il servizio WMI (Windows Management Instrumentation), che ricerca dinamicamente questo intervallo di porte. Per informazioni sull'intervallo di porte dinamiche supportato, consultare la sezione "Panoramica del servizio e requisiti della porta di rete per Windows" Le porte vengono utilizzate per la comunicazione tra il server SnapCenter e l'host su cui viene installato il plug-in. Per inviare i binari dei pacchetti plug-in agli host plug-in di Windows, le porte devono essere aperte solo sull'host plug-in e possono essere chiuse dopo l'installazione.

Tipo di porta	Porta predefinita
Host plug-in Linux o AIX	22 (SSH) Le porte vengono utilizzate per la comunicazione tra il server SnapCenter e l'host in cui viene installato il plug-in. Le porte vengono utilizzate da SnapCenter per copiare i binari dei pacchetti plug-in su host plug-in Linux o AIX e devono essere aperte o escluse dal firewall o da iptables.
Pacchetto plug-in SnapCenter per Windows, pacchetto plug-in SnapCenter per Linux o pacchetto plug-in SnapCenter per AIX	8145 (HTTPS), bidirezionale, personalizzabile La porta viene utilizzata per la comunicazione tra SMCore e gli host in cui è installato il pacchetto plug-in. Il percorso di comunicazione deve essere aperto anche tra la LIF di gestione SVM e il server SnapCenter. Per personalizzare la porta, vedere "Aggiungere host e installare il plug-in SnapCenter per Microsoft Windows" o. "Aggiungere host e installare il pacchetto di plug-in SnapCenter per Linux o AIX."
Plug-in SnapCenter per database Oracle	27216, personalizzabile La porta JDBC predefinita viene utilizzata dal plug-in per Oracle per la connessione al database Oracle. Per personalizzare la porta, vedere "Aggiungere host e installare il pacchetto di plug-in SnapCenter per Linux o AIX."
Plug-in personalizzati per SnapCenter	9090 (HTTPS), fisso Si tratta di una porta interna che viene utilizzata solo sull'host plug-in personalizzato; non è richiesta alcuna eccezione firewall. La comunicazione tra il server SnapCenter e i plug-in personalizzati viene instradata attraverso la porta 8145.

Tipo di porta	Porta predefinita
Porta di comunicazione SVM o cluster ONTAP	443 (HTTPS), bidirezionale (HTTP), bidirezionale La porta viene utilizzata da SAL (Storage Abstraction Layer) per la comunicazione tra l'host che esegue il server SnapCenter e SVM. La porta viene attualmente utilizzata anche dagli host plug-in SAL on SnapCenter per Windows per la comunicazione tra l'host plug-in SnapCenter e SVM.
Plug-in SnapCenter per database SAP HANA vCode controllo ortografico	3instance_number13 o 3instance_number15, HTTP o HTTPS, bidirezionale e personalizzabile Per un singolo tenant MDC (Multitenant Database Container), il numero di porta termina con 13; per i non MDC, il numero di porta termina con 15. Ad esempio, 32013 è il numero della porta, ad esempio 20 e 31015 è il numero della porta, ad esempio 10. Per personalizzare la porta, vedere "Aggiungere host e installare pacchetti plug-in su host remoti."
Porta di comunicazione del controller di dominio	Consultare la documentazione Microsoft per identificare le porte che devono essere aperte nel firewall di un controller di dominio affinché l'autenticazione funzioni correttamente. È necessario aprire le porte richieste da Microsoft sul controller di dominio in modo che il server SnapCenter, gli host plug-in o altri client Windows possano autenticare gli utenti.

Per modificare i dettagli della porta, vedere "Modificare gli host dei plug-in".

Licenze SnapCenter

SnapCenter richiede diverse licenze per consentire la protezione dei dati di applicazioni, database, file system e macchine virtuali. Il tipo di licenze SnapCenter installate dipende dall'ambiente di storage e dalle funzionalità che si desidera utilizzare.

Licenza	Dove richiesto
Basato su controller standard SnapCenter	Richiesto per FAS, AFF, All SAN Array (ASA) La licenza standard di SnapCenter è una licenza basata su controller ed è inclusa nel pacchetto premium. Se si dispone della licenza della suite SnapManager, si ottiene anche il diritto di licenza standard SnapCenter. Se si desidera installare SnapCenter in prova con storage FAS, AFF o ASA, è possibile ottenere una licenza di valutazione Premium Bundle contattando il rappresentante commerciale. SnapCenter è anche offerto come parte del bundle per la protezione dei dati. Se hai acquistato A400 o versioni successive, devi acquistare il bundle per la protezione dei dati.
SnapCenter basato sulla capacità standard	Richiesto con ONTAP Select e Cloud Volumes ONTAP Se sei un cliente Cloud Volumes ONTAP o ONTAP Select, devi procurarti una licenza per TB basata sulla capacità in base ai dati gestiti da SnapCenter. Per impostazione predefinita, SnapCenter fornisce una licenza di prova integrata per SnapCenter standard da 100 TB, valida 90 giorni. Per ulteriori informazioni, contattare il rappresentante commerciale.
SnapMirror o SnapVault	ONTAP Se la replica è attivata in SnapCenter, è necessario disporre di una licenza SnapMirror o SnapVault.
SnapRestore	Necessario per ripristinare e verificare i backup. Sui sistemi storage primari • Necessario sui sistemi di destinazione SnapVault per eseguire la verifica remota e il ripristino da un backup. • Necessario sui sistemi di destinazione SnapMirror per eseguire la verifica in remoto.

Licenza	Dove richiesto
FlexClone	Necessario per clonare i database e le operazioni di verifica. Sui sistemi di storage primario e secondario • Necessario sui sistemi di destinazione SnapVault per creare cloni dal backup del vault secondario. • Necessario sui sistemi di destinazione SnapMirror per creare cloni dal backup SnapMirror secondario.
Protocolli	• Licenza iSCSI o FC per LUN • Licenza CIFS per le condivisioni SMB • Licenza NFS per VMDK di tipo NFS • Licenza iSCSI o FC per VMFS tipo VMDK Necessario sui sistemi di destinazione SnapMirror per la distribuzione dei dati se un volume di origine non è disponibile.
Licenze standard SnapCenter (opzionali)	Destinazioni secondarie Si consiglia, ma non è necessario, di aggiungere le licenze standard di SnapCenter alle destinazioni secondarie. Se le licenze standard di SnapCenter non sono abilitate sulle destinazioni secondarie, non è possibile utilizzare SnapCenter per eseguire il backup delle risorse sulla destinazione secondaria dopo aver eseguito un'operazione di failover. Tuttavia, è necessaria una licenza FlexClone sulle destinazioni secondarie per eseguire operazioni di cloning e verifica.

Le licenze servizi file NAS SnapCenter e SnapCenter sono obsolete e non sono più disponibili.

Installare una o più licenze SnapCenter. Per informazioni su come aggiungere le licenze, vedere "Aggiunta di licenze SnapCenter basate su controller standard" o "Aggiunta di licenze SnapCenter basate sulla capacità standard".

Licenze SMBR (Single Mailbox Recovery)

Se si utilizza il plug-in SnapCenter per Exchange per gestire i database e il ripristino di una singola casella postale (SMBR), è necessaria una licenza aggiuntiva per SMBR che deve essere acquistata separatamente in base alla casella postale dell'utente.

Il ripristino di una singola casella postale di NetApp® è giunto alla fine della disponibilità (EOA) il 12 maggio 2023. Per ulteriori informazioni, fare riferimento a "CPC-00507". NetApp continuerà a supportare i clienti che hanno acquistato capacità, manutenzione e supporto della casella postale attraverso i codici marketing introdotti il 24 giugno 2020, per tutta la durata del diritto al supporto.

Il servizio di ripristino di una singola casella postale di NetApp è un prodotto partner fornito da Ontrack. Ontrack PowerControl offre funzionalità simili a quelle del ripristino di una singola casella postale di NetApp. I clienti possono acquistare nuove licenze software Ontrack PowerControls e rinnovi di assistenza e manutenzione Ontrack PowerControls da Ontrack (fino al licensingteam@ontrack.com) per il ripristino granulare della mailbox dopo la data EOA del 12 maggio 2023.

Metodi di autenticazione per le credenziali

Le credenziali utilizzano metodi di autenticazione diversi a seconda dell'applicazione o dell'ambiente. Le credenziali autenticano gli utenti in modo che possano eseguire operazioni SnapCenter. È necessario creare un set di credenziali per l'installazione dei plug-in e un altro set per le operazioni di protezione dei dati.

Autenticazione di Windows

Il metodo di autenticazione di Windows esegue l'autenticazione con Active Directory. Per l'autenticazione di Windows, Active Directory viene configurato al di fuori di SnapCenter. SnapCenter esegue l'autenticazione senza alcuna configurazione aggiuntiva. È necessaria una credenziale Windows per eseguire attività come l'aggiunta di host, l'installazione di pacchetti plug-in e la pianificazione dei processi.

Autenticazione di dominio non attendibile

SnapCenter consente la creazione di credenziali Windows utilizzando utenti e gruppi appartenenti a domini non attendibili. Affinché l'autenticazione abbia esito positivo, è necessario registrare i domini non attendibili con SnapCenter.

Autenticazione del gruppo di lavoro locale

SnapCenter consente la creazione di credenziali Windows con utenti e gruppi di lavoro locali. L'autenticazione di Windows per gli utenti e i gruppi di lavoro locali non avviene al momento della creazione delle credenziali di Windows, ma viene posticipata fino a quando non vengono eseguite la registrazione dell'host e altre operazioni dell'host.

Autenticazione di SQL Server

Il metodo di autenticazione SQL esegue l'autenticazione con un'istanza di SQL Server. Ciò significa che un'istanza di SQL Server deve essere rilevata in SnapCenter. Pertanto, prima di aggiungere una credenziale SQL, è necessario aggiungere un host, installare pacchetti plug-in e aggiornare le risorse. È necessaria l'autenticazione di SQL Server per eseguire operazioni come la pianificazione su SQL Server o il rilevamento delle risorse.

Autenticazione Linux

Il metodo di autenticazione Linux esegue l'autenticazione su un host Linux. L'autenticazione Linux è necessaria durante la fase iniziale di aggiunta dell'host Linux e installazione del pacchetto di plug-in SnapCenter per Linux in remoto dall'interfaccia grafica di SnapCenter.

Autenticazione AIX

Il metodo di autenticazione AIX esegue l'autenticazione su un host AIX. È necessaria l'autenticazione AIX durante la fase iniziale di aggiunta dell'host AIX e installazione del pacchetto di plug-in SnapCenter per AIX in remoto dalla GUI di SnapCenter.

Autenticazione del database Oracle

Il metodo di autenticazione del database Oracle esegue l'autenticazione su un database Oracle. Se l'autenticazione del sistema operativo (OS) è disattivata sull'host del database, è necessaria un'autenticazione del database Oracle per eseguire operazioni sul database Oracle. Pertanto, prima di aggiungere una credenziale di database Oracle, è necessario creare un utente Oracle nel database Oracle con privilegi sysdba.

Autenticazione Oracle ASM

Il metodo di autenticazione Oracle ASM esegue l'autenticazione con un'istanza di Oracle Automatic Storage Management (ASM). Se viene richiesto di accedere all'istanza di Oracle ASM e se l'autenticazione del sistema operativo (OS) è disattivata sull'host del database, è necessaria un'autenticazione Oracle ASM. Pertanto, prima di aggiungere una credenziale Oracle ASM, è necessario creare un utente Oracle con privilegi sysasm nell'istanza di ASM.

Autenticazione del catalogo RMAN

Il metodo di autenticazione del catalogo RMAN viene autenticato nel database del catalogo Oracle Recovery Manager (RMAN). Se è stato configurato un meccanismo di catalogo esterno e il database è stato registrato nel database del catalogo, è necessario aggiungere l'autenticazione del catalogo RMAN.

Connessioni e credenziali dello storage

Prima di eseguire operazioni di protezione dei dati, è necessario configurare le connessioni di storage e aggiungere le credenziali utilizzate dal server SnapCenter e dai plug-in SnapCenter.

- **Connessioni storage**

  Le connessioni storage consentono al server SnapCenter e ai plug-in SnapCenter di accedere allo storage ONTAP. L'impostazione di queste connessioni comporta anche la configurazione delle funzionalità di AutoSupport e del sistema di gestione degli eventi (EMS).

- **Credenziali**

  - Amministratore di dominio o qualsiasi membro del gruppo di amministratori

    Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono:

    - *NetBIOS/nome utente*
    - *Dominio FQDN/nome utente*
    - *Nome utente@upn*
  - Amministratore locale (solo per gruppi di lavoro)

    Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato

nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host.

Il formato valido per il campo Nome utente è: *Nome utente*

- Credenziali per singoli gruppi di risorse

  Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup al nome utente.

Autenticazione a più fattori (MFA)

Gestire l'autenticazione a più fattori (MFA)

È possibile gestire la funzionalità di autenticazione multifattore (MFA) nel server del servizio di federazione Active Directory (ad FS) e nel server SnapCenter.

Attiva autenticazione a più fattori (MFA)

È possibile attivare la funzionalità MFA per il server SnapCenter utilizzando i comandi PowerShell.

A proposito di questa attività

- SnapCenter supporta gli accessi basati su SSO quando altre applicazioni sono configurate nello stesso ad FS. In alcune configurazioni di ad FS, SnapCenter potrebbe richiedere l'autenticazione dell'utente per motivi di sicurezza, a seconda della persistenza della sessione di ad FS.
- Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name`. In alternativa, è anche possibile vedere "Guida di riferimento al cmdlet del software SnapCenter".

Prima di iniziare

- Windows Active Directory Federation Service (ad FS) deve essere attivo e in esecuzione nel rispettivo dominio.
- È necessario disporre di un servizio di autenticazione multifattore supportato da ad FS, ad esempio Azure MFA, Cisco Duo e così via.
- L'indicatore di data e ora del server SnapCenter e ad FS deve essere lo stesso indipendentemente dal fuso orario.
- Procurarsi e configurare il certificato CA autorizzato per il server SnapCenter.

  Il certificato CA è obbligatorio per i seguenti motivi:

  - Garantisce che le comunicazioni ADFS-F5 non si interrangano perché i certificati autofirmati sono univoci a livello di nodo.
  - Garantisce che durante l'upgrade, la riparazione o il disaster recovery (DR) in una configurazione standalone o ad alta disponibilità, il certificato autofirmato non venga ricreato, evitando così la riconfigurazione MFA.
  - Garantisce risoluzioni IP-FQDN.

    Per informazioni sul certificato CA, vedere "Generare il file CSR del certificato CA".

Fasi

1. Connettersi all'host Active Directory Federation Services (ad FS).
2. Scaricare il file di metadati della federazione ad FS da "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copiare il file scaricato sul server SnapCenter per attivare la funzione MFA.
4. Accedere al server SnapCenter come utente amministratore di SnapCenter tramite PowerShell.
5. Utilizzando la sessione PowerShell, generare il file di metadati MFA di SnapCenter utilizzando il cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

   Il parametro path specifica il percorso per salvare il file di metadati MFA nell'host del server SnapCenter.
6. Copiare il file generato nell'host ad FS per configurare SnapCenter come entità client.
7. Attivare MFA per il server SnapCenter utilizzando il `Set-SmMultiFactorAuthentication` cmdlet.
8. (Facoltativo) controllare lo stato e le impostazioni della configurazione MFA utilizzando il `Get-SmMultiFactorAuthentication` cmdlet.
9. Accedere alla console di gestione Microsoft (MMC) ed effettuare le seguenti operazioni:
   a. Fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
   b. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
   c. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
   d. Fare clic su **Directory principale console** > **certificati – computer locale** > **personale** > **certificati**.
   e. Fare clic con il pulsante destro del mouse sul certificato CA associato a SnapCenter, quindi selezionare **tutte le attività** > **Gestisci chiavi private**.
   f. Nella procedura guidata delle autorizzazioni, attenersi alla seguente procedura:
      i. Fare clic su **Aggiungi**.
      ii. Fare clic su **Locations** (posizioni) e selezionare l'host desiderato (in cima alla gerarchia).
      iii. Fare clic su **OK** nella finestra a comparsa **Locations**.
      iv. Nel campo Object name (Nome oggetto), immettere 'IIS_IUSRS', fare clic su **Check Names** (Controlla nomi) e fare clic su **OK**.

      Se il controllo ha esito positivo, fare clic su **OK**.
10. Nell'host ad FS, aprire la procedura guidata di gestione di ad FS ed eseguire le seguenti operazioni:
    a. Fare clic con il pulsante destro del mouse su **Trust di parte affidabile** > **Aggiungi Trust di parte affidabile** > **Start**.
    b. Selezionare la seconda opzione, sfogliare il file di metadati MFA di SnapCenter e fare clic su **Avanti**.
    c. Specificare un nome visualizzato e fare clic su **Avanti**.
    d. Scegliere un criterio di controllo degli accessi come richiesto e fare clic su **Avanti**.
    e. Selezionare le impostazioni predefinite nella scheda successiva.
    f. Fare clic su **fine**.

    SnapCenter si riflette ora come parte di base con il nome visualizzato fornito.
11. Selezionare il nome ed effettuare le seguenti operazioni:

a. Fare clic su **Edit Claim Issuance Policy** (Modifica policy di emissione richieste
b. Fare clic su **Add Rule** (Aggiungi regola) e fare clic su **Next** (Avanti).
c. Specificare un nome per la regola di richiesta di rimborso.
d. Selezionare **Active Directory** come archivio di attributi.
e. Selezionare l'attributo **User-Principal-Name** e il tipo di richiesta di rimborso in uscita come **Name-ID**.
f. Fare clic su **fine**.

12. Eseguire i seguenti comandi PowerShell sul server ADFS.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. Attenersi alla seguente procedura per confermare che i metadati sono stati importati correttamente.
    a. Fare clic con il pulsante destro del mouse sul trust della parte che si basa e selezionare **Proprietà**.
    b. Assicurarsi che i campi Endpoint, Identifier e Firma siano compilati.
14. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

La funzionalità MFA di SnapCenter può anche essere attivata utilizzando API REST.

Per informazioni sulla risoluzione dei problemi, fare riferimento alla "I tentativi di accesso simultanei in più schede mostrano un errore MFA".

Aggiornare i metadati di ad FS MFA

È necessario aggiornare i metadati MFA di ad FS in SnapCenter ogni volta che si verifica una modifica nel server di ad FS, ad esempio aggiornamento, rinnovo del certificato CA, DR e così via.

Fasi

1. Scaricare il file di metadati della federazione ad FS da "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copiare il file scaricato sul server SnapCenter per aggiornare la configurazione MFA.
3. Aggiornare i metadati di ad FS in SnapCenter eseguendo il seguente cmdlet:

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

Aggiornare i metadati MFA di SnapCenter

È necessario aggiornare i metadati MFA di SnapCenter in ad FS ogni volta che si verifica una modifica nel server ADFS, ad esempio riparazione, rinnovo del certificato CA, DR e così via.

Fasi

1. Nell'host ad FS, aprire la procedura guidata di gestione di ad FS ed eseguire le seguenti operazioni:

a. Fare clic su **Trust di parte**.
b. Fare clic con il pulsante destro del mouse sul trust della parte di base creato per SnapCenter e fare clic su **Elimina**.

   Viene visualizzato il nome definito dall'utente del trust della parte che si basa.

c. Attivare l'autenticazione a più fattori (MFA).

   Vedere "Abilitare l'autenticazione a più fattori".

2. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

Disattiva autenticazione a più fattori (MFA)

Fasi

1. Disattivare MFA e pulire i file di configurazione creati quando MFA è stato attivato utilizzando il `Set-SmMultiFactorAuthentication` cmdlet.
2. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

Gestisci l'autenticazione a più fattori (MFA) utilizzando REST API, PowerShell e SCCLI

L'accesso MFA è supportato da browser, REST API, PowerShell e SCCLI. MFA è supportato tramite un Identity manager di ad FS. È possibile attivare MFA, disattivare MFA e configurare MFA da GUI, REST API, PowerShell e SCCLI.

Impostare ad FS come OAuth/OIDC

Configurare ad FS utilizzando la GUI di Windows

1. Accedere a **Server Manager Dashboard** > **Tools** > **ADFS Management**.
2. Accedere a **ADFS** > **gruppi di applicazioni**.
   a. Fare clic con il pulsante destro del mouse su **gruppi di applicazioni**.
   b. Selezionare **Add Application group** (Aggiungi gruppo di applicazioni) e immettere **Application Name** (Nome applicazione).
   c. Selezionare **applicazione server**.
   d. Fare clic su **Avanti**.
3. Copia **identificatore del client**.

   ID client. .. Aggiungere l'URL di richiamata (URL del server SnapCenter) nell'URL di reindirizzamento. .. Fare clic su **Avanti**.

4. Selezionare **generate shared secret**.

   Copiare il valore segreto. Questo è il segreto del cliente. .. Fare clic su **Avanti**.

5. Nella pagina **Riepilogo**, fare clic su **Avanti**.
   a. Nella pagina **complete**, fare clic su **Close** (Chiudi).

6. Fare clic con il pulsante destro del mouse sul nuovo **Application Group** e selezionare **Properties**.
7. Selezionare **Aggiungi applicazione** da Proprietà applicazione.
8. Fare clic su **Aggiungi applicazione**.

   Selezionare API Web e fare clic su **Avanti**.

9. Nella pagina Configura API web, inserire l'URL del server SnapCenter e l'identificativo client creati nel passaggio precedente nella sezione identificativo.
   a. Fare clic su **Aggiungi**.
   b. Fare clic su **Avanti**.
10. Nella pagina **Choose Access Control Policy** (Scegli policy di controllo dell'accesso), selezionare la policy di controllo in base ai requisiti (ad esempio, Permit Everyone and Request MFA) e fare clic su **Next** (Avanti).
11. Nella pagina **Configure Application Permission** (Configura autorizzazione applicazione), per impostazione predefinita openid è selezionato come ambito, fare clic su **Next** (Avanti).
12. Nella pagina **Riepilogo**, fare clic su **Avanti**.

    Nella pagina **complete**, fare clic su **Close** (Chiudi).

13. Nella pagina **Proprietà applicazione di esempio**, fare clic su **OK**.
14. Token JWT emesso da un server di autorizzazione (ad FS) e destinato ad essere utilizzato dalla risorsa.

    La richiesta "aud" o di pubblico di questo token deve corrispondere all'identificatore della risorsa o dell'API Web.

15. Modificare l'API Web selezionata e verificare che l'URL di richiamata (URL del server SnapCenter) e l'identificatore del client siano stati aggiunti correttamente.

    Configurare OpenID Connect in modo da fornire un nome utente come rivendicato.

16. Aprire lo strumento **ad FS Management** situato nel menu **Tools** in alto a destra di Server Manager.
    a. Selezionare la cartella **Application Groups** dalla barra laterale sinistra.
    b. Selezionare l'API Web e fare clic su **EDIT**.
    c. Accedere alla scheda Issuance Transform Rules (regole di trasformazione emissione)
17. Fare clic su **Add Rule** (Aggiungi regola).
    a. Selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) nell'elenco a discesa Claim Rule template (
    b. Fare clic su **Avanti**.
18. Inserire il nome **Claim rule**.
    a. Selezionare **Active Directory** nell'elenco a discesa dell'archivio degli attributi.
    b. Selezionare **User-Principal-Name** nel menu a discesa **LDAP Attribute** e **UPN** nel menu a discesa o*utgoing Claim Type*.
    c. Fare clic su **fine**.

Creare un gruppo di applicazioni utilizzando i comandi PowerShell

È possibile creare il gruppo di applicazioni, l'API Web e aggiungere l'ambito e le attestazioni utilizzando i comandi PowerShell. Questi comandi sono disponibili in formato script automatizzato. Per ulteriori informazioni, vedere <link to KB article>.

1. Creare il nuovo gruppo di applicazioni in ad FS utilizzando la seguente comand.

   ```
   New-AdfsApplicationGroup -Name $ClientRoleIdentifier
   -ApplicationGroupIdentifier $ClientRoleIdentifier
   ```

   `ClientRoleIdentifier` nome del gruppo di applicazioni

   `redirectURL` URL valido per il reindirizzamento dopo l'autorizzazione

2. Creare l'applicazione server di ad FS e generare il segreto del client.

   ```
   Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
   -ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
   -Identifier $identifier -GenerateClientSecret
   ```

3. Creare l'applicazione API Web ADFS e configurare il nome del criterio da utilizzare.

   ```
   $identifier = (New-Guid).Guid

   Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
   -Name "App Web API"

   -Identifier $identifier -AccessControlPolicyName "Permit everyone"
   ```

4. Ottenere l'ID client e il client secret dall'output dei seguenti comandi perché vengono visualizzati una sola volta.

   ```
   "client_id = $identifier"

   "client_secret: "$($ADFSApp.ClientSecret)
   ```

5. Concedere all'applicazione ad FS le autorizzazioni Allatclaims e openid.

   ```
   Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
   -ServerRoleIdentifier $identifier -ScopeNames @('openid')

   $transformrule = @"

   @RuleTemplate = "LdapClaims"

   @RuleName = "AD User properties and Groups"

   c:[Type ==
   "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
   Issuer ==

   "AD AUTHORITY"]
   ```

```
⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. Annotare il file di regole di trasformazione.

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii
$relativePath = Get-Item .\issueancetransformrules.tmp
```

7. Assegnare un nome all'applicazione API Web e definirne le regole di conversione mediante un file esterno.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Aggiornare il tempo di scadenza del token di accesso

È possibile aggiornare il tempo di scadenza del token di accesso utilizzando il comando PowerShell.

A proposito di questa attività

- Un token di accesso può essere utilizzato solo per una combinazione specifica di utente, client e risorsa. I token di accesso non possono essere revocati e sono validi fino alla scadenza.
- Per impostazione predefinita, la scadenza di un token di accesso è di 60 minuti. Questo tempo di scadenza minimo è sufficiente e scalabile. Devi fornire un valore sufficiente per evitare qualsiasi lavoro business-critical in corso.

Passo

Per aggiornare il tempo di scadenza del token di accesso per un gruppo di applicazioni WebAPI, utilizzare il seguente comando nel server ad FS.

+

```
Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

Ottenere il token del bearer da ad FS

Inserire i parametri indicati di seguito in qualsiasi client REST (come Postman) e richiedere di inserire le credenziali dell'utente. Inoltre, è necessario immettere l'autenticazione a secondo fattore (qualcosa che si ha e qualcosa che si è) per ottenere il token portante.

+ la validità del token portante è configurabile dal server ad FS per applicazione e il periodo di validità predefinito è di 60 minuti.

Campo	Valore

Tipo di concessione	Codice di autorizzazione
URL di richiamata	Se non si dispone di un URL di richiamata, immettere l'URL di base dell'applicazione.
URL di autenticazione	[adfs-domain-name]/adfs/oauth2/authorize
URL token di accesso	[adfs-domain-name]/adfs/oauth2/token
ID client	Inserire l'ID del client ad FS
Segreto del client	Inserire il segreto del client ad FS
Scopo	OpenID
Autenticazione del client	Invia come intestazione AUTH di base
Risorsa	Nella scheda **Opzioni avanzate**, aggiungere il campo risorsa con lo stesso valore dell'URL di richiamata, che viene fornito come valore "aud" nel token JWT.

Configurare MFA nel server SnapCenter utilizzando PowerShell, SCCLI e REST API

È possibile configurare MFA nel server SnapCenter utilizzando PowerShell, SCCLI e REST API.

Autenticazione SnapCenter MFA CLI

In PowerShell e SCCLI, il cmdlet esistente (Open-SmConnection) viene esteso con un altro campo chiamato "AccessToken" per utilizzare il token bearer per autenticare l'utente.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

Una volta eseguito il cmdlet sopra indicato, viene creata una sessione per consentire al rispettivo utente di eseguire ulteriori cmdlet SnapCenter.

Autenticazione API REST MFA SnapCenter

Utilizzare il token bearer nel formato *Authorization=bearer <access token>* nel client API REST (come Postman o swagger) e citare il nome del ruolo dell'utente nell'intestazione per ottenere una risposta corretta da SnapCenter.

Flusso di lavoro API REST MFA

Quando MFA è configurato con ad FS, è necessario eseguire l'autenticazione utilizzando un token di accesso (bearer) per accedere all'applicazione SnapCenter da qualsiasi API REST.

A proposito di questa attività

- Puoi utilizzare qualsiasi client REST come Postman, Swagger UI o FireCamp.
- Ottenere un token di accesso e utilizzarlo per autenticare le richieste successive (API REST SnapCenter) per eseguire qualsiasi operazione.

Fasi

Per l'autenticazione tramite ad FS MFA

1. Configurare il client REST per chiamare l'endpoint ad FS per ottenere il token di accesso.

   Quando si preme il pulsante per ottenere un token di accesso per un'applicazione, si viene reindirizzati alla pagina SSO di ad FS, dove è necessario fornire le credenziali ad e autenticare con MFA. 1. Nella pagina SSO di ad FS, digitare il nome utente o l'indirizzo e-mail nella casella di testo Nome utente.

   + i nomi utente devono essere formattati come utente@dominio o dominio\utente.

2. Digitare la password nella casella di testo Password.
3. Fare clic su **Log in** (Accedi).
4. Nella sezione **Opzioni di accesso**, selezionare un'opzione di autenticazione e autenticare (a seconda della configurazione).
   - Push: Consente di approvare la notifica push inviata al telefono.
   - Codice QR: Utilizza l'app mobile AUTH Point per eseguire la scansione del codice QR, quindi digita il codice di verifica visualizzato nell'app
   - Password monouso: Digitare la password monouso per il token.
5. Una volta completata l'autenticazione, viene visualizzata una finestra a comparsa contenente Access, ID e Refresh Token.

   Copiare il token di accesso e utilizzarlo nell'API REST di SnapCenter per eseguire l'operazione.

6. Nell'API REST, passare il token di accesso e il nome del ruolo nella sezione dell'intestazione.
7. SnapCenter convalida questo token di accesso da ad FS.

   Se si tratta di un token valido, SnapCenter lo decodifica e ottiene il nome utente.

8. Utilizzando il nome utente e il nome ruolo, SnapCenter autentica l'utente per un'esecuzione API.

   Se l'autenticazione ha esito positivo, SnapCenter restituisce il risultato, altrimenti viene visualizzato un messaggio di errore.

Attivare o disattivare la funzionalità MFA di SnapCenter per API REST, CLI e GUI

GUI

Fasi

1. Accedere al server SnapCenter come amministratore SnapCenter.
2. Fare clic su **Impostazioni** > **Impostazioni globali** > **Impostazioni MultiFactorAuthentication(MFA)**
3. Selezionare l'interfaccia (GUI/RST API/CLI) per attivare o disattivare l'accesso MFA.

Interfaccia PowerShell

Fasi

1. Eseguire i comandi PowerShell o CLI per abilitare MFA per GUI, REST API, PowerShell e SCCLI.

   ```
   Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
   -IsCliMFAEnabled -Path
   ```

   Il parametro path specifica la posizione del file xml di metadati di ad FS MFA.

   Abilita MFA per GUI SnapCenter, API REST, PowerShell e SCCLI configurati con il percorso file di metadati ad FS specificato.

2. Controllare lo stato e le impostazioni della configurazione MFA utilizzando il `Get-SmMultiFactorAuthentication` cmdlet.

INTERFACCIA SCCLI

Fasi

1. `# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
2. `# sccli Get-SmMultiFactorAuthentication`

API REST

1. Eseguire la seguente API post per abilitare MFA per GUI, REST API, PowerShell e SCCLI.

Parametro	Valore
URL richiesto	/api/4.9/settings/autenticazione multifattoriale
Metodo HTTP	Post
Corpo della richiesta	{ "IsGuiMFAEnabled": False, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }
Corpo di risposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSHostName": "win-adfs-sc49.winscedom2.com" }

2. Controllare lo stato e le impostazioni della configurazione MFA utilizzando la seguente API.

Parametro	Valore
URL richiesto	/api/4.9/settings/autenticazione multifattoriale

Metodo HTTP	Ottieni
Corpo di risposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSHostName": "win-adfs-sc49.winscedom2.com" }

Installare il server SnapCenter

È possibile eseguire il programma di installazione del server SnapCenter per installare il server SnapCenter.

È possibile eseguire diverse procedure di installazione e configurazione utilizzando i cmdlet PowerShell.

L'installazione automatica del server SnapCenter dalla riga di comando non è supportata.

Prima di iniziare

- L'host del server SnapCenter deve essere aggiornato con gli aggiornamenti di Windows senza riavvii di sistema in sospeso.
- È necessario assicurarsi che MySQL Server non sia installato sull'host in cui si intende installare il server SnapCenter.
- Dovrebbe essere stato attivato il debug del programma di installazione di Windows.

  Per informazioni sull'attivazione di , consultare il sito Web Microsoft "Registrazione del programma di installazione di Windows".

  Non installare il server SnapCenter su un host che dispone di server Exchange, Active Directory o server dei nomi di dominio.

Fasi

1. Scaricare il pacchetto di installazione del server SnapCenter da "Sito di supporto NetApp".
2. Avviare l'installazione del server SnapCenter facendo doppio clic sul file .exe scaricato.

   Dopo aver avviato l'installazione, vengono eseguiti tutti i controlli preliminari e, se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

   È possibile ignorare i messaggi di avviso e procedere con l'installazione; tuttavia, gli errori dovrebbero essere corretti.

3. Esaminare i valori precompilati richiesti per l'installazione del server SnapCenter e modificarli, se necessario.

   Non è necessario specificare la password per il database del repository MySQL Server. Durante l'installazione del server SnapCenter, la password viene generata automaticamente.

Il carattere speciale “%” is not supported in the custom path for the repository database. If you include "`%"" nel percorso, l’installazione non riesce.

4. Fare clic su **Installa ora**.

   Se sono stati specificati valori non validi, vengono visualizzati i messaggi di errore appropriati. Immettere nuovamente i valori e avviare l’installazione.

   Se si fa clic sul pulsante **Annulla**, la fase in corso di esecuzione viene completata e quindi viene avviata l’operazione di rollback. Il server SnapCenter verrà completamente rimosso dall’host.

   Tuttavia, se si fa clic su **Annulla** durante l’esecuzione delle operazioni "riavvio del server SnapCenter" o "in attesa dell’avvio del server SnapCenter", l’installazione proseguirà senza annullare l’operazione.

   I file di log sono sempre elencati (per primi quelli meno recenti) nella cartella %temp% dell’utente amministratore. Se si desidera reindirizzare le posizioni del registro, avviare l’installazione del server SnapCenter dal prompt dei comandi eseguendo:`C:\installer_location\installer_name.exe /log"C:\"`

Accedere a SnapCenter utilizzando l’autorizzazione RBAC

SnapCenter supporta il RBAC (role-based access control). L’amministratore di SnapCenter assegna ruoli e risorse tramite SnapCenter RBAC a un utente nel gruppo di lavoro o in Active Directory o a gruppi in Active Directory. L’utente RBAC può ora accedere a SnapCenter con i ruoli assegnati.

Prima di iniziare

- Attivare il servizio di attivazione del processo Windows (WAS) in Windows Server Manager.
- Se si desidera utilizzare Internet Explorer come browser per accedere al server SnapCenter, assicurarsi che la modalità protetta sia disattivata.

A proposito di questa attività

Durante l’installazione, l’installazione guidata del server SnapCenter crea un collegamento e lo posiziona sul desktop e nel menu Start dell’host in cui è installato SnapCenter. Inoltre, al termine dell’installazione, la procedura guidata di installazione visualizza l’URL SnapCenter in base alle informazioni fornite durante l’installazione, che è possibile copiare se si desidera effettuare l’accesso da un sistema remoto.

Se nel browser Web sono aperte più schede, la chiusura della scheda del browser SnapCenter non consente di disconnettersi da SnapCenter. Per terminare la connessione con SnapCenter, è necessario disconnettersi da SnapCenter facendo clic sul pulsante **Esci** o chiudendo l’intero browser Web.

Best practice: per motivi di sicurezza, si consiglia di non abilitare il browser per il salvataggio della password SnapCenter.

L’URL GUI predefinito è una connessione sicura alla porta predefinita 8146 sul server in cui è installato il server SnapCenter (*https://server:8146*). Se durante l’installazione di SnapCenter è stata fornita una porta server diversa, viene utilizzata tale porta.

Per l'implementazione ad alta disponibilità (ha), è necessario accedere a SnapCenter utilizzando l'IP *https://Virtual_Cluster_IP_or_FQDN:8146*. del cluster virtuale Se l'interfaccia utente di SnapCenter non viene visualizzata quando si seleziona *https://Virtual_Cluster_IP_or_FQDN:8146* in Internet Explorer (IE), è necessario aggiungere l'indirizzo IP del cluster virtuale o l'FQDN come sito attendibile in IE su ciascun host plug-in oppure disattivare la protezione avanzata di IE su ciascun host plug-in. Per ulteriori informazioni, vedere "Impossibile accedere all'indirizzo IP del cluster dall'esterno della rete".

Oltre a utilizzare l'interfaccia grafica di SnapCenter, è possibile utilizzare i cmdlet PowerShell per creare script per eseguire operazioni di configurazione, backup e ripristino. Alcuni cmdlet potrebbero essere stati modificati con ogni release di SnapCenter. La "Guida di riferimento al cmdlet del software SnapCenter" contiene i dettagli.

Se si effettua l'accesso a SnapCenter per la prima volta, è necessario effettuare l'accesso utilizzando le credenziali fornite durante il processo di installazione.

Fasi

1. Avviare SnapCenter dal collegamento situato sul desktop host locale, dall'URL fornito al termine dell'installazione o dall'URL fornito dall'amministratore di SnapCenter.
2. Immettere le credenziali dell'utente.

Per specificare quanto segue…	Utilizzare uno di questi formati…
Amministratore di dominio	• NetBIOS/nome utente • Nome utente@suffisso UPN Ad esempio, username@netapp.com • Nome utente FQDN del dominio
Amministratore locale	Nome utente

3. Se si dispone di più ruoli, selezionare il ruolo che si desidera utilizzare per questa sessione di accesso dalla casella ruolo.

   L'utente corrente e il ruolo associato vengono visualizzati nella parte superiore destra di SnapCenter dopo l'accesso.

Risultato

Viene visualizzata la pagina Dashboard.

Se la registrazione non riesce e viene visualizzato l'errore che indica che il sito non può essere raggiunto, è necessario mappare il certificato SSL a SnapCenter. "Scopri di più"

Al termine

Dopo aver effettuato l'accesso al server SnapCenter come utente RBAC per la prima volta, aggiornare l'elenco delle risorse.

Se si dispone di domini Active Directory non attendibili che si desidera supportare da SnapCenter, è necessario registrare tali domini con SnapCenter prima di configurare i ruoli per gli utenti in domini non

attendibili. "Scopri di più"

Accedere a SnapCenter utilizzando l'autenticazione multifattore (MFA)

Il server SnapCenter supporta MFA per l'account di dominio, che fa parte di Active Directory.

Prima di iniziare

- Dovrebbe essere stata attivata l'autenticazione MFA.

  Per informazioni su come attivare l'MFA, vedere "Abilitare l'autenticazione a più fattori"

A proposito di questa attività

- È supportato solo il nome FQDN
- Gli utenti di gruppi di lavoro e di più domini non possono accedere utilizzando MFA

Fasi

1. Avviare SnapCenter dal collegamento situato sul desktop host locale, dall'URL fornito al termine dell'installazione o dall'URL fornito dall'amministratore di SnapCenter.
2. Nella pagina di accesso ad FS, immettere il nome utente e la password.

   Quando il messaggio di errore nome utente o password non valida viene visualizzato nella pagina ad FS, verificare quanto segue:

   - Se il nome utente o la password sono validi

     L'account utente deve esistere in Active Directory (ad)

   - Se è stato superato il numero massimo di tentativi consentito impostato in ad
   - Se ad e ad FS sono attivi e in esecuzione

Modificare il timeout della sessione GUI predefinita di SnapCenter

È possibile modificare il periodo di timeout della sessione GUI di SnapCenter in modo che sia inferiore o superiore al periodo di timeout predefinito di 20 minuti.

Come funzione di sicurezza, dopo un periodo di inattività predefinito di 15 minuti, SnapCenter avvisa che la sessione della GUI verrà disconnessa in 5 minuti. Per impostazione predefinita, SnapCenter disconnette l'utente dalla sessione GUI dopo 20 minuti di inattività ed è necessario effettuare nuovamente l'accesso.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni** > **Impostazioni globali**.
2. Nella pagina Global Settings (Impostazioni globali), fare clic su **Configuration Settings** (Impostazioni di configurazione).
3. Nel campo Timeout sessione, immettere il timeout della nuova sessione in minuti, quindi fare clic su **Salva**.

Proteggere il server Web SnapCenter disattivando SSL 3.0

Per motivi di sicurezza, è necessario disattivare il protocollo SSL (Secure Socket Layer) 3.0 in Microsoft IIS, se attivato sul server Web SnapCenter.

Il protocollo SSL 3.0 presenta difetti che un utente malintenzionato può utilizzare per causare errori di connessione o per eseguire attacchi man-in-the-middle e osservare il traffico di crittografia tra il sito Web e i relativi visitatori.

Fasi

1. Per avviare l'editor del Registro di sistema sull'host del server Web di SnapCenter, fare clic su **Start** > **Esegui**, quindi digitare regedit.
2. Nell'Editor del Registro di sistema, accedere a HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/SecurityProviders/SCHANNEL/Protocols/SSL 3.0.
   - Se la chiave Server esiste già:
     i. Selezionare il DWORD abilitato, quindi fare clic su **Modifica** > **Modifica**.
     ii. Impostare il valore su 0, quindi fare clic su **OK**.
   - Se la chiave Server non esiste:
     i. Fare clic su **Modifica** > **nuovo** > **chiave**, quindi assegnare un nome al server delle chiavi.
     ii. Con la nuova chiave Server selezionata, fare clic su **Edit** > **New** > **DWORD**.
     iii. Assegnare un nome al nuovo DWORD abilitato, quindi immettere 0 come valore.
3. Chiudere l'Editor del Registro di sistema.

Configurare il certificato CA

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare una CSR, vedere "Come generare il file CSR del certificato CA".

Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di

Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato del file di importazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

> Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
   c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
   d. Copiare i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

      Get-ChildItem -Path Certate: LocalMachine/My

   b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

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

   Ad esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in
   dell'host Windows eseguendo i seguenti comandi:
   ```

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

   Ad esempio:

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

Configurare il certificato CA con il sito SnapCenter

È necessario configurare il certificato CA con il sito SnapCenter sull'host Windows.

Fasi

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter.
2. Nel riquadro di navigazione a sinistra, fare clic su **connessioni**.
3. Espandere il nome del server e **Sites**.
4. Selezionare il sito Web di SnapCenter su cui si desidera installare il certificato SSL.
5. Accedere a **azioni** > **Modifica sito**, fare clic su **associazioni**.
6. Nella pagina binding, selezionare **binding for https**.
7. Fare clic su **Edit** (Modifica).
8. Dall'elenco a discesa SSL certificate (certificato SSL), selezionare il certificato SSL importato di recente.
9. Fare clic su **OK**.

Se il certificato CA distribuito di recente non è elencato nel menu a discesa, controllare se il certificato CA è associato alla chiave privata.

Assicurarsi che il certificato venga aggiunto utilizzando il seguente percorso: **Root console > certificati – computer locale > autorità di certificazione root attendibili > certificati**.

Abilitare i certificati CA per SnapCenter

È necessario configurare i certificati CA e attivare la convalida del certificato CA per il server SnapCenter.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Set-SmCertificateSettings.
- È possibile visualizzare lo stato del certificato per il server SnapCenter utilizzando il cmdlet Get-SmCertificateSettings.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nella pagina Settings (Impostazioni), selezionare **Settings** (Impostazioni) > **Global Settings** (Impostazioni globali) > **CA Certificate Settings** (Impostazioni certificato CA).
2. Selezionare **attiva convalida certificato**.
3. Fare clic su **Apply** (Applica).

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- * * Indica che non è stato attivato o assegnato alcun certificato CA all'host del plug-in.
- * * Indica che il certificato CA è stato convalidato correttamente.
- * * Indica che il certificato CA non può essere convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Configurare e abilitare la comunicazione SSL bidirezionale

Configurare la comunicazione SSL bidirezionale

È necessario configurare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra il server SnapCenter e i plug-in.

Prima di iniziare

- Il file CSR del certificato CA dovrebbe essere stato generato con la lunghezza minima supportata della chiave di 3072.
- Il certificato CA deve supportare l'autenticazione del server e l'autenticazione del client.
- È necessario disporre di un certificato CA con chiave privata e dettagli di identificazione personale.
- La configurazione SSL unidirezionale dovrebbe essere stata attivata.

  Per ulteriori informazioni, vedere "Sezione Configure CA certificate (Configura certificato CA)."

- È necessario attivare la comunicazione SSL bidirezionale su tutti gli host plug-in e sul server SnapCenter.

  L'ambiente con alcuni host o server non abilitati per la comunicazione SSL bidirezionale non è supportato.

Fasi

1. Per eseguire il binding della porta, attenersi alla seguente procedura sull'host del server SnapCenter per la porta 8146 del server Web IIS SnapCenter (impostazione predefinita) e ancora per la porta 8145 SMCore (impostazione predefinita) utilizzando i comandi PowerShell.

   a. Rimuovere il binding della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
      ```

      Ad esempio,

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145

      > netsh http delete sslcert ipport=0.0.0.0:8146
      ```

   b. Associare il certificato CA appena procurato al server SnapCenter e alla porta SMCore.

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

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

      > netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
      certhash=$cert appid="$guid" clientcertnegotiation=enable
      verifyclientcertrevocation=disable
      ```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

Ad esempio,

```
> $cert = "abc123abc123abc123abc123"

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

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

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

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145
```

2. Per accedere all'autorizzazione al certificato CA, aggiungere l'utente predefinito del server Web IIS di SnapCenter "**IIS AppPool/SnapCenter**" nell'elenco delle autorizzazioni del certificato eseguendo la procedura seguente per accedere al certificato CA appena procurato.
   a. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi SnapIn**.
   b. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
   c. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
   d. Fare clic su **Directory principale console** > **certificati – computer locale** > **personale** > **certificati**.
   e. Selezionare il certificato SnapCenter.
   f. Per avviare l'aggiunta guidata autorizzazioni utente, fare clic con il pulsante destro del mouse sul certificato CA e selezionare **tutte le attività** > **Gestisci chiavi private**.
   g. Fare clic su **Aggiungi**, nella procedura guidata Seleziona utenti e gruppi modificare la posizione in Nome computer locale (in alto nella gerarchia)
   h. Aggiungere l'utente di IIS AppPool/SnapCenter, assegnare autorizzazioni di controllo complete.
3. Per l'autorizzazione IIS * del certificato CA, aggiungere la nuova voce delle chiavi di registro DWORD nel server SnapCenter dal seguente percorso:

   Nell'editor del Registro di sistema di Windows, passare al percorso indicato di seguito,

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv
   ders\SCHANNEL
   ```

4. Creare una nuova voce della chiave del Registro di sistema DWORD nel contesto della configurazione DEL Registro DI sistema SCHANNEL.

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

Configurare il plug-in Windows di SnapCenter per la comunicazione SSL bidirezionale

È necessario configurare il plug-in Windows di SnapCenter per la comunicazione SSL bidirezionale utilizzando i comandi PowerShell.

Prima di iniziare

Assicurarsi che il thumbprint del certificato CA sia disponibile.

Fasi

1. Per collegare la porta, eseguire le seguenti operazioni sull'host plug-in di Windows per la porta SMCore 8145 (impostazione predefinita).

   a. Rimuovere il binding della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

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

      Ad esempio,

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145
      ```

   b. Associare il certificato CA appena procurato alla porta SMCore.

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

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

      > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
      appid="$guid"
      clientcertnegotiation=enable verifyclientcertrevocation=disable

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

      Ad esempio,

      ```
      > $cert = "abc123abc123abc123abc123"

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

      > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
      clientcertnegotiation=enable verifyclientcertrevocation=disable

    > netsh http show sslcert ipport=0.0.0.0:8145
      ```

Abilitare la comunicazione SSL bidirezionale

È possibile abilitare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra il server SnapCenter e i plug-in utilizzando i comandi PowerShell.

Prima di iniziare

Eseguire i comandi per tutti i plug-in e l'agente SMCore prima e poi per il server.

Fasi

1. Per attivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi sul server SnapCenter per i plug-in, il server e per ciascuno degli agenti per i quali è richiesta la comunicazione SSL bidirezionale.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando.
   `> Restart-WebAppPool -Name "SnapCenter"`
3. Per i plug-in di Windows, riavviare il servizio SMCore eseguendo il seguente comando PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Disattiva la comunicazione SSL bidirezionale

È possibile disattivare la comunicazione SSL bidirezionale utilizzando i comandi PowerShell.

A proposito di questa attività

- Eseguire i comandi per tutti i plug-in e l'agente SMCore prima e poi per il server.
- Quando si disattiva la comunicazione SSL bidirezionale, il certificato CA e la relativa configurazione non vengono rimossi.
- Per aggiungere un nuovo host al server SnapCenter, è necessario disattivare il protocollo SSL bidirezionale per tutti gli host plug-in.
- NLB e F5 non sono supportati.

Fasi

1. Per disattivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi sul server SnapCenter per tutti gli host plug-in e l'host SnapCenter.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando.
   `> Restart-WebAppPool -Name "SnapCenter"`
3. Per i plug-in di Windows, riavviare il servizio SMCore eseguendo il seguente comando PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Configurare l'autenticazione basata su certificato

Esportare i certificati dell'autorità di certificazione (CA) dal server SnapCenter

È necessario esportare i certificati CA dal server SnapCenter agli host plug-in utilizzando la console di gestione Microsoft.

Prima di iniziare

Il protocollo SSL bidirezionale dovrebbe essere stato configurato.

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra Snap-in certificati, selezionare l'opzione **computer account**, quindi fare clic su **fine**.
4. Fare clic su **Console root** > **certificati - computer locale** > **personale** > **certificati**.
5. Fare clic con il pulsante destro del mouse sul certificato CA procurato, utilizzato per il server SnapCenter, quindi selezionare **tutte le attività** > **Esporta** per avviare l'esportazione guidata.
6. Eseguire le seguenti operazioni nella procedura guidata.

Per questa opzione…	Effettuare le seguenti operazioni…
Esporta chiave privata	Selezionare **No, non esportare la chiave privata**, quindi fare clic su **Avanti**.
Formato file di esportazione	Fare clic su **Avanti**.
Nome file	Fare clic su **Browse** (Sfoglia) e specificare il percorso del file per il salvataggio del certificato, quindi fare clic su **Next** (Avanti).
Completamento dell'esportazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'esportazione.

L'autenticazione basata su certificato non è supportata per le configurazioni SnapCenter ha e il plug-in SnapCenter per VMware vSphere.

Importa certificato CA (Certificate Authority) negli host plug-in di Windows

Per utilizzare il certificato della CA del server SnapCenter esportato, è necessario importare il certificato correlato negli host dei plug-in di SnapCenter utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra Snap-in certificati, selezionare l'opzione **computer account**, quindi fare clic su **fine**.
4. Fare clic su **Console root** > **certificati - computer locale** > **personale** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Personal", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Eseguire le seguenti operazioni nella procedura guidata.

Per questa opzione…	Effettuare le seguenti operazioni…
Ubicazione del negozio	Fare clic su **Avanti**.
File da importare	Selezionare il certificato del server SnapCenter che termina con l'estensione .cer.
Archivio certificati	Fare clic su **Avanti**.
Completamento dell'esportazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

Importare il certificato CA nei plug-in host UNIX e configurare i certificati root o intermedi nell'archivio di fiducia SPL

Importa certificato CA negli host plug-in UNIX

È necessario importare il certificato CA negli host plug-in UNIX.

A proposito di questa attività

- È possibile gestire la password per l'archivio chiavi SPL e l'alias della coppia di chiavi firmate CA in uso.
- La password per l'archivio chiavi SPL e per tutte le password alias associate della chiave privata deve essere la stessa.

Fasi

1. È possibile recuperare la password predefinita del keystore SPL dal file di proprietà SPL. È il valore corrispondente alla chiave `SPL_KEYSTORE_PASS`.
2. Modificare la password dell'archivio chiavi:
   `$ keytool -storepasswd -keystore keystore.jks`
3. Modificare la password per tutti gli alias delle voci di chiave privata nel keystore con la stessa password utilizzata per l'archivio chiavi:
   `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS nel `spl.properties` file.
5. Riavviare il servizio dopo aver modificato la password.

Configurare i certificati root o intermedi per l'archivio di trust SPL

È necessario configurare i certificati root o intermedi in SPL trust-store. Aggiungere il certificato CA principale e i certificati CA intermedi.

Fasi

1. Passare alla cartella contenente il keystore SPL: `/var/opt/snapcenter/spl/etc`.
2. Individuare il file `keystore.jks`.
3. Elencare i certificati aggiunti nell'archivio chiavi:
   `$ keytool -list -v -keystore keystore.jks`
4. Aggiungere un certificato root o intermedio:
   `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Riavviare il servizio dopo aver configurato i certificati root o intermedi in SPL trust-store.

Configurare la coppia di chiavi con firma CA nell'archivio di trust SPL

È necessario configurare la coppia di chiavi firmate della CA in SPL trust-store.

Fasi

1. Passare alla cartella contenente il keystore di SPL `/var/opt/snapcenter/spl/etc`.
2. Individuare il file `keystore.jks`.
3. Elencare i certificati aggiunti nell'archivio chiavi:
   `$ keytool -list -v -keystore keystore.jks`
4. Aggiungere il certificato CA con chiave pubblica e privata.
   `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. Elencare i certificati aggiunti nel keystore.
   `$ keytool -list -v -keystore keystore.jks`
6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita dell'archivio chiavi SPL è il valore della chiave SPL_KEYSTORE_PASS nel `spl.properties` file.

   `$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
8. Se il nome dell'alias nel certificato CA è lungo e contiene spazi o caratteri speciali ("*",","), modificare il nome dell'alias con un nome semplice:
   `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. Configurare il nome alias dall'archivio chiavi presente nel `spl.properties` file. Aggiornare questo valore con la chiave SPL_CERTIFICATE_ALIAS.
10. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA in SPL trust-store.

Abilitare l'autenticazione basata su certificato

Per abilitare l'autenticazione basata su certificato per il server SnapCenter e gli host plug-in Windows, eseguire il seguente cmdlet PowerShell. Per gli host plug-in Linux, l'autenticazione basata su certificato viene attivata quando si attiva il protocollo SSL bidirezionale.

- Per attivare l'autenticazione basata su certificati client:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- Per disattivare l'autenticazione basata su certificato del client:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

Configurare Active Directory, LDAP e LDAPS

Registrare domini Active Directory non attendibili

È necessario registrare Active Directory con il server SnapCenter per gestire host, utenti e gruppi di più domini Active Directory non attendibili.

Prima di iniziare

Protocolli LDAP e LDAPS

- È possibile registrare i domini Active Directory non attendibili utilizzando il protocollo LDAP o LDAPS.
- La comunicazione bidirezionale tra gli host plug-in e il server SnapCenter dovrebbe essere stata attivata.
- La risoluzione DNS deve essere impostata dal server SnapCenter agli host plug-in e viceversa.

Protocollo LDAP

- Il nome di dominio completo (FQDN) deve essere risolvibile dal server SnapCenter.

  È possibile registrare un dominio non attendibile con l'FQDN. Se l'FQDN non è risolvibile dal server SnapCenter, è possibile registrarsi con un indirizzo IP del controller di dominio, che dovrebbe essere risolvibile dal server SnapCenter.

Protocollo LDAPS

- I certificati CA sono necessari affinché LDAPS fornisca la crittografia end-to-end durante la comunicazione Active Directory.

  "Configurare il certificato del client CA per LDAPS"

- I nomi host dei controller di dominio (nome host DC) devono essere raggiungibili dal server SnapCenter.

A proposito di questa attività

- È possibile utilizzare l'interfaccia utente di SnapCenter, i cmdlet PowerShell o l'API REST per registrare un dominio non attendibile.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.
3. Nella pagina Global Settings (Impostazioni globali), fare clic su **Domain Settings** (Impostazioni dominio).
4. Fare clic su  per registrare un nuovo dominio.
5. Nella pagina Registra nuovo dominio, selezionare **LDAP** o **LDAPS**.
   a. Se si seleziona **LDAP**, specificare le informazioni necessarie per la registrazione del dominio non attendibile per LDAP:

Per questo campo…	Eseguire questa operazione…
Domain Name (Nome dominio)	Specificare il nome NetBIOS per il dominio.
FQDN del dominio	Specificare l'FQDN e fare clic su **Resolve** (Risolvi).
Indirizzi IP dei controller di dominio	Se l'FQDN del dominio non è risolvibile dal server SnapCenter, specificare uno o più indirizzi IP del controller di dominio. Per ulteriori informazioni, vedere "Aggiungere l'IP del controller di dominio per il dominio non attendibile dalla GUI".

   b. Se si seleziona **LDAPS**, specificare le informazioni necessarie per la registrazione del dominio non attendibile per LDAPS:

Per questo campo…	Eseguire questa operazione…
Domain Name (Nome dominio)	Specificare il nome NetBIOS per il dominio.
FQDN del dominio	Specificare l'FQDN.
Nomi dei controller di dominio	Specificare uno o più nomi di controller di dominio e fare clic su **Risolvi**.
Indirizzi IP dei controller di dominio	Se i nomi dei controller di dominio non sono risolvibili dal server SnapCenter, correggere le risoluzioni DNS.

6. Fare clic su **OK**.

Configurare il certificato del client CA per LDAPS

È necessario configurare il certificato del client CA per LDAPS sul server SnapCenter quando quest'ultimo è configurato con i certificati CA.

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Nella seconda pagina della procedura guidata	Fare clic su **Browse** (Sfoglia), selezionare *Root Certificate* (certificato principale) e fare clic su **Next** (Avanti).
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

7. Ripetere i passaggi 5 e 6 per i certificati intermedi.

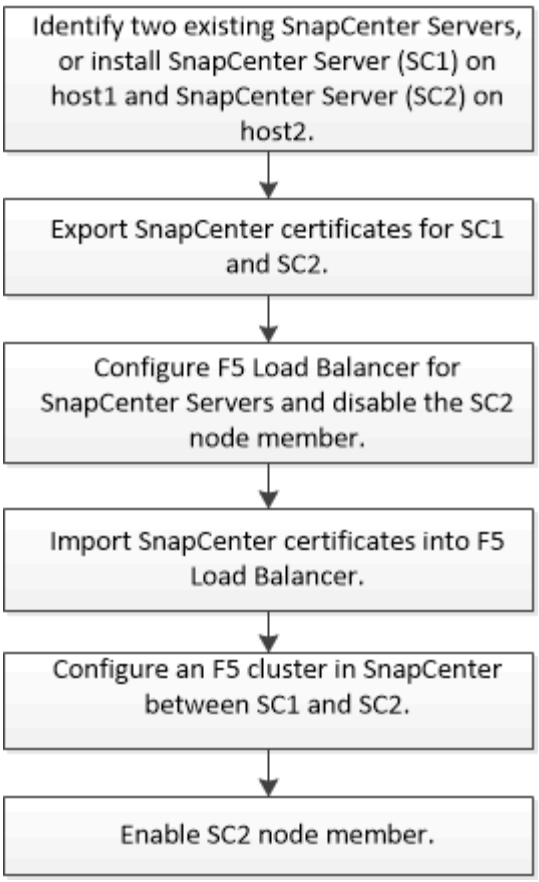
Configurare la disponibilità elevata

Configurare i server SnapCenter per l'alta disponibilità utilizzando F5

Per supportare l'alta disponibilità (ha) in SnapCenter, è possibile installare il bilanciamento del carico F5. F5 consente al server SnapCenter di supportare configurazioni Active-passive in un massimo di due host che si trovano nella stessa posizione. Per utilizzare F5 Load Balancer in SnapCenter, è necessario configurare i server SnapCenter e il bilanciamento del carico F5.

> Se è stato eseguito l'aggiornamento da SnapCenter 4.2.x e in precedenza si utilizzava il bilanciamento del carico di rete (NLB), è possibile continuare a utilizzare tale configurazione o passare a F5.

L'immagine del flusso di lavoro elenca i passaggi per configurare i server SnapCenter per l'alta disponibilità utilizzando il bilanciamento del carico F5. Per istruzioni dettagliate, vedere "Come configurare i server SnapCenter per l'alta disponibilità utilizzando F5 Load Balancer".



Per aggiungere e rimuovere i cluster F5, è necessario essere membri del gruppo amministratori locali sui server SnapCenter (oltre che essere assegnati al ruolo SnapCenterAdmin):

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

  Per ulteriori informazioni, vedere "Guida di riferimento al cmdlet del software SnapCenter".

Ulteriori informazioni sulla configurazione di F5

- Dopo aver installato e configurato SnapCenter per la disponibilità elevata, modificare il collegamento al desktop di SnapCenter in modo che punti all'IP del cluster F5.
- Se si verifica un failover tra i server SnapCenter e se esiste anche una sessione SnapCenter, chiudere il browser e accedere nuovamente a SnapCenter.
- Nella configurazione del bilanciamento del carico (NLB o F5), se si aggiunge un nodo parzialmente risolto dal nodo NLB o F5 e se il nodo SnapCenter non è in grado di raggiungere questo nodo, la pagina host SnapCenter passa spesso dallo stato di inattività a quello di esecuzione. Per risolvere questo problema, assicurarsi che entrambi i nodi SnapCenter siano in grado di risolvere l'host nel nodo NLB o F5.
- I comandi SnapCenter per le impostazioni MFA devono essere eseguiti su tutti i nodi. La configurazione della parte di base deve essere eseguita nel server Active Directory Federation Services (ad FS) utilizzando i dettagli del cluster F5. L'accesso all'interfaccia utente SnapCenter a livello di nodo viene bloccato dopo l'attivazione dell'MFA.
- Durante il failover, le impostazioni del registro di controllo non si rifletteranno sul secondo nodo. Pertanto, è necessario ripetere manualmente le impostazioni del registro di controllo sul nodo F5 passivo quando

diventa attivo.

Configurare Microsoft Network Load Balancer manualmente

È possibile configurare il bilanciamento del carico di rete Microsoft per impostare la disponibilità elevata SnapCenter. A partire da SnapCenter 4.2, è necessario configurare manualmente NLB al di fuori dell'installazione di SnapCenter per ottenere una disponibilità elevata.

Per informazioni su come configurare il bilanciamento del carico di rete (NLB) con SnapCenter, vedere "Come configurare NLB con SnapCenter".

SnapCenter 4.1.1 o versioni precedenti supportava la configurazione del bilanciamento del carico di rete (NLB) durante l'installazione di SnapCenter.

Passa da NLB a F5 per ottenere alta disponibilità

È possibile modificare la configurazione SnapCenter ha da bilanciamento del carico di rete (NLB) per utilizzare bilanciamento del carico F5.

Fasi

1. Configurare i server SnapCenter per la disponibilità elevata utilizzando F5. "Scopri di più"
2. Sull'host del server SnapCenter, avviare PowerShell.
3. Avviare una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
4. Aggiornare il server SnapCenter in modo che punti all'indirizzo IP del cluster F5 utilizzando il cmdlet Update-SmServerCluster.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Alta disponibilità per il repository MySQL di SnapCenter

La replica MySQL è una funzionalità di MySQL Server che consente di replicare i dati da un server database MySQL (master) a un altro server database MySQL (slave). SnapCenter supporta la replica MySQL per l'alta disponibilità solo su due nodi abilitati per il bilanciamento del carico di rete (abilitati per NLB).

SnapCenter esegue operazioni di lettura o scrittura sul repository master e instrada la connessione al repository slave in caso di errore nel repository master. Il repository slave diventa quindi il repository master. SnapCenter supporta inoltre la replica inversa, che viene attivata solo durante il failover.

Se si desidera utilizzare la funzionalità di disponibilità elevata (ha) di MySQL, è necessario configurare Network Load Balancer (NLB) sul primo nodo. Il repository MySQL viene installato su questo nodo come parte dell'installazione. Durante l'installazione di SnapCenter sul secondo nodo, è necessario unirsi alla F5 del primo nodo e creare una copia del repository MySQL sul secondo nodo.

SnapCenter fornisce i cmdlet *Get-SmRepositoryConfig* e *Set-SmRepositoryConfig* PowerShell per gestire la replica MySQL.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

È necessario conoscere le limitazioni relative alla funzionalità MySQL ha:

- NLB e MySQL ha non sono supportati oltre due nodi.
- Il passaggio da un'installazione standalone SnapCenter a un'installazione NLB o viceversa e il passaggio da un'installazione standalone MySQL a MySQL ha non sono supportati.
- Il failover automatico non è supportato se i dati del repository slave non sono sincronizzati con i dati del repository master.

  È possibile avviare un failover forzato utilizzando il cmdlet *set-SmRepositoryConfig*.

- Quando viene avviato il failover, i processi in esecuzione potrebbero non riuscire.

  Se il failover si verifica perché il server MySQL o SnapCenter non è attivo, i processi in esecuzione potrebbero non riuscire. Dopo aver eseguito il failover sul secondo nodo, tutti i processi successivi vengono eseguiti correttamente.

Per informazioni sulla configurazione della disponibilità elevata, vedere "Come configurare NLB e ARR con SnapCenter".

Esportare i certificati SnapCenter

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account utente**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **Certificates - Current User** > **Trusted Root Certification Authorities** > **Certificates**.
5. Fare clic con il pulsante destro del mouse sul certificato con il nome descrittivo SnapCenter, quindi selezionare **tutte le attività** > **Esporta** per avviare l'esportazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Esporta chiave privata	Selezionare l'opzione **Sì, esportare la chiave privata**, quindi fare clic su **Avanti**.
Formato file di esportazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
File da esportare	Specificare un nome di file per il certificato esportato (è necessario utilizzare .pfx), quindi fare clic su **Avanti**.

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Completamento dell'esportazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'esportazione.

Risultato

I certificati vengono esportati in formato .pfx.

Configurare RBAC (role-based access control)

Aggiungere un utente o un gruppo e assegnare ruolo e risorse

Per configurare il controllo degli accessi basato sui ruoli per gli utenti SnapCenter, è possibile aggiungere utenti o gruppi e assegnare un ruolo. Il ruolo determina le opzioni a cui gli utenti SnapCenter possono accedere.

Prima di iniziare

- È necessario aver effettuato l'accesso come ruolo "SnapCenterAdmin".
- È necessario aver creato gli account utente o di gruppo in Active Directory nel sistema operativo o nel database. Non è possibile utilizzare SnapCenter per creare questi account.

> Da SnapCenter 4.5, è possibile includere solo i seguenti caratteri speciali nei nomi utente e nei nomi dei gruppi: Spazio ( ), trattino (-), carattere di sottolineatura (_) e due punti (:). Se si desidera utilizzare un ruolo creato in una release precedente di SnapCenter con questi caratteri speciali, è possibile disattivare la convalida del nome del ruolo modificando il valore del parametro "DisableSQLInjectionValidation" su true nel file web.config in cui è installata l'applicazione web di SnapCenter. Dopo aver modificato il valore, non è necessario riavviare il servizio.

- SnapCenter include diversi ruoli predefiniti.

  È possibile assegnare questi ruoli all'utente o crearne di nuovi.

- Gli utenti AD e i gruppi ad aggiunti a RBAC SnapCenter devono disporre dell'autorizzazione DI LETTURA sul container utenti e sul container computer in Active Directory.
- Dopo aver assegnato un ruolo a un utente o a un gruppo che contiene le autorizzazioni appropriate, è necessario assegnare all'utente l'accesso alle risorse SnapCenter, ad esempio host e connessioni storage.

  In questo modo, gli utenti possono eseguire le azioni per le quali dispongono delle autorizzazioni per le risorse ad essi assegnate.

- È necessario assegnare un ruolo all'utente o al gruppo per sfruttare le autorizzazioni e le efficienze RBAC.
- È possibile assegnare risorse come host, gruppi di risorse, policy, connessione allo storage, plug-in, e all'utente durante la creazione dell'utente o del gruppo.
- Le risorse minime che è necessario assegnare a un utente per eseguire determinate operazioni sono le seguenti:

Operazione	Assegnazione delle risorse
Proteggere le risorse	host, policy
Backup	host, gruppo di risorse, policy
Ripristinare	host, gruppo di risorse
Clonare	host, gruppo di risorse, policy
Ciclo di vita dei cloni	host
Creare un gruppo di risorse	host

- Quando un nuovo nodo viene aggiunto a un cluster Windows o a una risorsa DAG (Exchange Server Database Availability Group) e se questo nuovo nodo viene assegnato a un utente, è necessario riassegnare la risorsa all'utente o al gruppo per includere il nuovo nodo all'utente o al gruppo.

  È necessario riassegnare l'utente o il gruppo RBAC al cluster o al DAG per includere il nuovo nodo all'utente o al gruppo RBAC. Ad esempio, si dispone di un cluster a due nodi ed è stato assegnato un utente o un gruppo RBAC al cluster. Quando si aggiunge un altro nodo al cluster, è necessario riassegnare l'utente o il gruppo RBAC al cluster per includere il nuovo nodo per l'utente o il gruppo RBAC.

- Se si intende replicare le istantanee, è necessario assegnare la connessione di archiviazione per il volume di origine e di destinazione all'utente che esegue l'operazione.

  Aggiungere le risorse prima di assegnare l'accesso agli utenti.

Se si utilizza il plug-in SnapCenter per le funzioni di VMware vSphere per proteggere macchine virtuali, VMDK o datastore, è necessario utilizzare l'interfaccia utente di VMware vSphere per aggiungere un utente vCenter a un plug-in SnapCenter per il ruolo di VMware vSphere. Per informazioni sui ruoli VMware vSphere, vedere "Ruoli predefiniti in pacchetto con il plug-in SnapCenter per VMware vSphere".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **utenti e accesso** > * *.
3. Nella pagina Add Users/Groups from Active Directory or Workgroup (Aggiungi utenti/gruppi da Active Directory o Workgroup):

Per questo campo…	Eseguire questa operazione…
Tipo di accesso	Selezionare Domain (dominio) o Workgroup (gruppo di lavoro) Per il tipo di autenticazione dominio, specificare il nome di dominio dell'utente o del gruppo a cui si desidera aggiungere l'utente a un ruolo. Per impostazione predefinita, viene compilato con il nome di dominio connesso. È necessario registrare il dominio non attendibile nella pagina **Impostazioni** > **Impostazioni globali** > **Impostazioni dominio**.
Tipo	Selezionare User (utente) o Group (Gruppo) SnapCenter supporta solo il gruppo di sicurezza e non il gruppo di distribuzione.
Nome utente	a. Digitare il nome utente parziale, quindi fare clic su **Aggiungi**. Il nome utente fa distinzione tra maiuscole e minuscole. b. Selezionare il nome utente dall'elenco di ricerca. Quando si aggiungono utenti da un dominio diverso o da un dominio non attendibile, è necessario digitare completamente il nome utente, in quanto non esiste un elenco di ricerca per gli utenti di più domini. Ripetere questo passaggio per aggiungere altri utenti o gruppi al ruolo selezionato.
Ruoli	Selezionare il ruolo a cui si desidera aggiungere l'utente.

4. Fare clic su **Assegna**, quindi nella pagina Assegna risorse:
   a. Selezionare il tipo di risorsa dall'elenco a discesa **risorsa**.
   b. Nella tabella Asset, selezionare la risorsa.

      Le risorse vengono elencate solo se l'utente ha aggiunto le risorse a SnapCenter.

c. Ripetere questa procedura per tutte le risorse richieste.

d. Fare clic su **Save** (Salva).

5. Fare clic su **Invia**.

Dopo aver aggiunto utenti o gruppi e aver assegnato ruoli, aggiornare l'elenco delle risorse.

Creare un ruolo

Oltre a utilizzare i ruoli SnapCenter esistenti, è possibile creare i propri ruoli e personalizzare le autorizzazioni.

Dovresti aver effettuato l'accesso come ruolo "SnapCenterAdmin".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **ruoli**.
3. Fare clic su .
4. Nella pagina Add role (Aggiungi ruolo), specificare un nome e una descrizione per il nuovo ruolo.

> Da SnapCenter 4.5, è possibile includere solo i seguenti caratteri speciali nei nomi utente e nei nomi dei gruppi: Spazio ( ), trattino (-), carattere di sottolineatura (_) e due punti (:). Se si desidera utilizzare un ruolo creato in una release precedente di SnapCenter con questi caratteri speciali, è possibile disattivare la convalida del nome del ruolo modificando il valore del parametro "DisableSQLInjectionValidation" su true nel file web.config in cui è installata l'applicazione web di SnapCenter. Dopo aver modificato il valore, non è necessario riavviare il servizio.

5. Selezionare **tutti i membri di questo ruolo possono visualizzare gli oggetti degli altri membri** per consentire agli altri membri del ruolo di visualizzare risorse come volumi e host dopo l'aggiornamento dell'elenco delle risorse.

   Deselezionare questa opzione se non si desidera che i membri di questo ruolo vedano gli oggetti a cui sono assegnati altri membri.

> Quando questa opzione è attivata, l'assegnazione dell'accesso degli utenti agli oggetti o alle risorse non è necessaria se gli utenti appartengono allo stesso ruolo dell'utente che ha creato gli oggetti o le risorse.

6. Nella pagina autorizzazioni, selezionare le autorizzazioni che si desidera assegnare al ruolo o fare clic su **Seleziona tutto** per concedere tutte le autorizzazioni al ruolo.
7. Fare clic su **Invia**.

Aggiungere un ruolo RBAC ONTAP utilizzando i comandi di accesso di sicurezza

È possibile utilizzare i comandi di accesso di sicurezza per aggiungere un ruolo RBAC ONTAP quando i sistemi storage eseguono Clustered ONTAP.

Prima di iniziare

- Prima di creare un ruolo RBAC ONTAP per i sistemi storage che eseguono Clustered ONTAP, è necessario identificare quanto segue:
  - L'attività (o le attività) che si desidera eseguire
  - I privilegi richiesti per eseguire queste attività
- La configurazione di un ruolo RBAC richiede l'esecuzione delle seguenti azioni:
  - Concedere privilegi alle directory dei comandi e/o dei comandi.

    Esistono due livelli di accesso per ogni directory di comando: All-access e Read-only.

    È sempre necessario assegnare prima i privilegi di accesso completo.
  - Assegnare ruoli agli utenti.
  - Modificare la configurazione a seconda che i plug-in SnapCenter siano collegati all'IP dell'amministratore del cluster per l'intero cluster o direttamente a una SVM all'interno del cluster.

A proposito di questa attività

Per semplificare la configurazione di questi ruoli nei sistemi storage, è possibile utilizzare il tool RBAC User Creator for Data ONTAP, disponibile nel forum delle community NetApp.

Questo strumento gestisce automaticamente la corretta impostazione dei privilegi ONTAP. Ad esempio, lo strumento RBAC User Creator for Data ONTAP aggiunge automaticamente i privilegi nell'ordine corretto in modo che i privilegi di accesso completo vengano visualizzati per primi. Se si aggiungono prima i privilegi di sola lettura e poi i privilegi di accesso completo, ONTAP contrassegna i privilegi di accesso completo come duplicati e li ignora.

Se in seguito si aggiorna SnapCenter o ONTAP, eseguire nuovamente lo strumento RBAC User Creator for Data ONTAP per aggiornare i ruoli utente creati in precedenza. I ruoli utente creati per una versione precedente di SnapCenter o ONTAP non funzionano correttamente con le versioni aggiornate. Quando si esegue di nuovo, lo strumento gestisce automaticamente l'aggiornamento. Non è necessario ricreare i ruoli.

Per ulteriori informazioni sull'impostazione dei ruoli RBAC di ONTAP, vedere "Autenticazione amministratore di ONTAP 9 e guida all'alimentazione RBAC".

Per coerenza, la documentazione di SnapCenter fa riferimento ai ruoli come all'utilizzo dei privilegi. L'interfaccia utente grafica di Gestore di sistema di OnCommand utilizza il termine *attribute* invece di *Privilege*. Quando si impostano i ruoli RBAC di ONTAP, entrambi questi termini significano la stessa cosa.

Fasi

1. Nel sistema di storage, creare un nuovo ruolo immettendo il seguente comando:

```
security login role create <role_name\> -cmddirname "command" -access all
–vserver <svm_name\>
```

   - nome_svm è il nome della SVM. Se si lascia questo campo vuoto, per impostazione predefinita viene visualizzato l'amministratore del cluster.
   - role_name è il nome specificato per il ruolo.

- Command è la funzionalità ONTAP.

> È necessario ripetere questo comando per ogni autorizzazione. Tenere presente che i comandi all-access devono essere elencati prima dei comandi di sola lettura.

Per informazioni sull'elenco delle autorizzazioni, vedere "Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli e l'assegnazione delle autorizzazioni".

2. Creare un nome utente immettendo il seguente comando:

```
security login create -username <user_name\> -application ontapi -authmethod
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
"user_description"
```

   - user_name è il nome dell'utente che si sta creando.
   - <password> è la tua password. Se non si specifica una password, il sistema ne richiederà una.
   - nome_svm è il nome della SVM.

3. Assegnare il ruolo all'utente immettendo il seguente comando:

```
security login modify username <user_name\> -vserver <svm_name\> -role
<role_name\> -application ontapi -application console -authmethod <password\>
```

   - <user_name> è il nome dell'utente creato al punto 2. Questo comando consente di modificare l'utente per associarlo al ruolo.
   - <svm_name> è il nome della SVM.
   - <role_name> è il nome del ruolo creato nella fase 1.
   - <password> è la tua password. Se non si specifica una password, il sistema ne richiederà una.

4. Verificare che l'utente sia stato creato correttamente immettendo il seguente comando:

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

   User_name è il nome dell'utente creato nel passaggio 3.

Creare ruoli SVM con privilegi minimi

Quando si crea un ruolo per un nuovo utente SVM in ONTAP, è necessario eseguire diversi comandi dell'interfaccia utente di ONTAP. Questo ruolo è necessario se si configurano le SVM in ONTAP per l'utilizzo con SnapCenter e non si desidera utilizzare il ruolo vsadmin.

Fasi

1. Nel sistema di storage, creare un ruolo e assegnare tutte le autorizzazioni al ruolo.

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```

> Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

```
security login create -user <user_name\> -vserver <svm_name\> -application
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. Liberare l'utente.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli SVM e l'assegnazione delle autorizzazioni

Esistono diversi comandi dell'interfaccia utente di ONTAP da eseguire per creare ruoli SVM e assegnare autorizzazioni.

> A partire da SnapCenter 5,0, gli utenti amministratori dei vserver sono supportati solo con API REST. Se si desidera creare ruoli utilizzando un amministratore non vserver, è necessario utilizzare ZAPI.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"snapmirror update-ls-set" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```
"volume managed-feature" -access all
```

Creare ruoli cluster ONTAP con privilegi minimi

È necessario creare un ruolo di cluster ONTAP con privilegi minimi in modo da non dover utilizzare il ruolo di amministratore di ONTAP per eseguire operazioni in SnapCenter. È possibile eseguire diversi comandi dell'interfaccia utente di ONTAP per creare il ruolo del cluster ONTAP e assegnare privilegi minimi.

Fasi

1. Nel sistema di storage, creare un ruolo e assegnare tutte le autorizzazioni al ruolo.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   ontapi -authmethod password -role <role_name\>
   ```

3. Liberare l'utente.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli cluster e l'assegnazione delle autorizzazioni

Esistono diversi comandi dell'interfaccia utente di ONTAP da eseguire per creare ruoli cluster e assegnare autorizzazioni.

A partire da SnapCenter 5,0, gli utenti degli amministratori dei cluster sono supportati solo con API REST. Se si desidera creare ruoli utilizzando un amministratore non cluster, è necessario utilizzare ZAPI.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"cluster show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"snapmirror show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"vserver cifs delete" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all

Configurare i pool di applicazioni IIS per abilitare le autorizzazioni di lettura di Active Directory

È possibile configurare Internet Information Services (IIS) sul server Windows per creare

un account pool di applicazioni personalizzato quando è necessario attivare le autorizzazioni di lettura di Active Directory per SnapCenter.

Fasi

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter.
2. Nel riquadro di spostamento di sinistra, fare clic su **Application Pools**.
3. Selezionare SnapCenter nell'elenco Pool di applicazioni, quindi fare clic su **Impostazioni avanzate** nel riquadro delle azioni.
4. Selezionare identità, quindi fare clic su **…** per modificare l'identità del pool di applicazioni SnapCenter.
5. Nel campo Custom account (account personalizzato), immettere un nome utente di dominio o un nome account admin di dominio con l'autorizzazione di lettura di Active Directory.
6. Fare clic su OK.

   L'account personalizzato sostituisce l'account ApplicationPoolIdentity incorporato per il pool di applicazioni SnapCenter.

Configurare le impostazioni del registro di controllo

I registri di audit vengono generati per ogni attività del server SnapCenter. Per impostazione predefinita, i registri di controllo sono protetti nella posizione predefinita installata _C: File di programma/NetApp/SnapCenter WebApp/audit.

I registri di audit sono protetti mediante la generazione di digest con firma digitale per ogni evento di audit per proteggerlo da modifiche non autorizzate. I digest generati vengono mantenuti nel file checksum di audit separato e vengono sottoposti a controlli di integrità periodici per garantire l'integrità del contenuto.

Dovresti aver effettuato l'accesso come ruolo "SnapCenterAdmin".

A proposito di questa attività

- Gli avvisi vengono inviati nei seguenti scenari:
  - Il programma di controllo dell'integrità del registro di controllo o il server Syslog sono attivati o disattivati
  - Controllo dell'integrità del registro di controllo, registro di controllo o errore del registro del server Syslog
  - Spazio su disco insufficiente
- L'e-mail viene inviata solo quando il controllo dell'integrità non riesce.
- È necessario modificare insieme la directory del registro di controllo e i percorsi della directory del registro di controllo. Non è possibile modificarne solo uno.
- Quando vengono modificati i percorsi delle directory dei log di audit e dei log di checksum, non è possibile eseguire il controllo dell'integrità dei log di audit presenti nella posizione precedente.
- I percorsi delle directory dei log di audit e dei log di checksum devono trovarsi sul disco locale del server SnapCenter.

  I dischi condivisi o montati in rete non sono supportati.

- Se nelle impostazioni del server Syslog viene utilizzato il protocollo UDP, gli errori dovuti alla porta non sono attivi o non disponibili non possono essere acquisiti come errore o avviso in SnapCenter.
- È possibile utilizzare i comandi Set-SmAuditSettings e Get-SmAuditSettings per configurare i registri di controllo.

  Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo Get-Help command_name. In alternativa, è anche possibile fare riferimento a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nella pagina **Impostazioni**, selezionare **Impostazioni** > **Impostazioni globali** > **Impostazioni registro di controllo**.
2. Nella sezione Registro di controllo, immettere i dettagli.
3. Inserire la directory **Registro audit** e la directory **Registro checksum audit**
   a. Inserire la dimensione massima del file
   b. Immettere il numero massimo di file di log
   c. Immettere la percentuale di utilizzo dello spazio su disco per inviare un avviso
4. (Facoltativo) attiva **Log UTC Time**.
5. (Facoltativo) attivare **Audit Log Integrity Check Schedule** e fare clic su **Start Integrity Check** per il controllo dell'integrità on-demand.

   È inoltre possibile eseguire il comando **Start-SmAuditIntegrityCheck** per avviare il controllo dell'integrità on-demand.

6. (Facoltativo) attivare i registri di controllo inoltrati al server syslog remoto e immettere i dettagli del server Syslog.

   È necessario importare il certificato dal server Syslog nel protocollo "Trusted Root" per TLS 1.2.

   a. Immettere Syslog Server host
   b. Immettere la porta del server Syslog
   c. Immettere il protocollo del server Syslog
   d. Inserire il formato RFC
7. Fare clic su **Save** (Salva).
8. È possibile visualizzare i controlli di integrità e lo spazio su disco facendo clic su **Monitor** > **Jobs**.

Aggiungere sistemi storage

È necessario configurare il sistema storage che consente a SnapCenter di accedere allo storage ONTAP o ad Amazon FSX per NetApp ONTAP per eseguire operazioni di provisioning e protezione dei dati.

È possibile aggiungere una SVM standalone o un cluster composto da più SVM. Se si utilizza Amazon FSX per NetApp ONTAP, è possibile aggiungere FSX admin LIF composto da più SVM utilizzando l'account fsxadmin o aggiungere FSX SVM in SnapCenter.

Prima di iniziare

- Per creare le connessioni storage, è necessario disporre delle autorizzazioni necessarie nel ruolo Infrastructure Admin.
- Assicurarsi che le installazioni dei plug-in non siano in corso.

  Le installazioni dei plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage perché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nella GUI di SnapCenter come "non disponibile per il backup" o "non su storage NetApp".

- I nomi dei sistemi di storage devono essere univoci.

  SnapCenter non supporta più sistemi storage con lo stesso nome su cluster diversi. Ogni sistema storage supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dei dati univoco.

A proposito di questa attività

- Quando si configurano i sistemi storage, è possibile attivare anche le funzioni del sistema di gestione degli eventi (EMS) e AutoSupport. Lo strumento AutoSupport raccoglie i dati sullo stato di salute del sistema e li invia automaticamente al supporto tecnico NetApp, consentendo loro di eseguire il troubleshooting del sistema.

  Se si abilitano queste funzioni, SnapCenter invia informazioni AutoSupport al sistema di storage e messaggi EMS al syslog del sistema di storage quando una risorsa viene protetta, un'operazione di ripristino o clonazione viene completata correttamente o un'operazione non riesce.

- Se hai intenzione di replicare Snapshot su una destinazione SnapMirror o su una destinazione SnapVault, devi impostare connessioni del sistema storage per la SVM o il cluster di destinazione così come la SVM o il cluster di origine.

> Se si modifica la password del sistema di storage, i processi pianificati, il backup su richiesta e le operazioni di ripristino potrebbero non riuscire. Dopo aver modificato la password del sistema di storage, è possibile aggiornarla facendo clic su **Modify** (Modifica) nella scheda Storage (archiviazione).

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Systems**.
2. Nella pagina Storage Systems (sistemi storage), fare clic su **New** (nuovo).
3. Nella pagina Add Storage System (Aggiungi sistema di storage), fornire le seguenti informazioni:

Per questo campo…	Eseguire questa operazione…
Sistema storage	Inserire il nome del sistema di storage o l'indirizzo IP. I nomi dei sistemi di storage, che non includono il nome di dominio, devono contenere un massimo di 15 caratteri e devono essere risolutibili. Per creare connessioni al sistema di storage con nomi che hanno più di 15 caratteri, è possibile utilizzare il cmdlet Add-SmStorageConnectionPowerShell. Per i sistemi storage con configurazione MetroCluster (MCC), si consiglia di registrare cluster locali e peer per operazioni senza interruzioni. SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM supportata da SnapCenter deve avere un nome univoco. Dopo aver aggiunto la connessione allo storage a SnapCenter, non rinominare la SVM o il cluster utilizzando ONTAP. Se SVM viene aggiunto con un nome breve o FQDN, deve essere risolvibile sia da SnapCenter che dall'host del plug-in.
Nome utente/Password	Inserire le credenziali dell'utente dello storage che dispone dei privilegi necessari per accedere al sistema di storage.

Per questo campo…	Eseguire questa operazione…
Sistema di gestione degli eventi (EMS) e impostazioni AutoSupport	Se si desidera inviare messaggi EMS al syslog del sistema di storage o inviare messaggi AutoSupport al sistema di storage per la protezione applicata, le operazioni di ripristino completate o le operazioni non riuscite, selezionare la casella di controllo appropriata. Quando si seleziona la casella di controllo **Invia notifica AutoSupport per operazioni non riuscite al sistema di storage**, viene selezionata anche la casella di controllo **Registra eventi server SnapCenter su syslog**, in quanto è necessaria la messaggistica EMS per attivare le notifiche AutoSupport.

4. Fare clic su **altre opzioni** per modificare i valori predefiniti assegnati a piattaforma, protocollo, porta e timeout.

   a. In Platform (piattaforma), selezionare una delle opzioni dall'elenco a discesa.

      Se SVM è il sistema di storage secondario in una relazione di backup, selezionare la casella di controllo **secondario**. Quando si seleziona l'opzione **secondario**, SnapCenter non esegue immediatamente un controllo della licenza.

   Se è stata aggiunta una SVM in SnapCenter, l'utente deve selezionare manualmente il tipo di piattaforma dal menu a discesa.

   a. In Protocol (protocollo), selezionare il protocollo configurato durante l'installazione di SVM o Cluster, in genere HTTPS.
   b. Inserire la porta accettata dal sistema di storage.

      La porta predefinita 443 in genere funziona.

   c. Inserire il tempo, espresso in secondi, che deve trascorrere prima dell'arresto dei tentativi di comunicazione.

      Il valore predefinito è 60 secondi.

   d. Se SVM dispone di più interfacce di gestione, selezionare la casella di controllo **Preferred IP** (IP preferito), quindi immettere l'indirizzo IP preferito per le connessioni SVM.
   e. Fare clic su **Save** (Salva).
5. Fare clic su **Invia**.

Risultato

Nella pagina Storage Systems (sistemi storage), dal menu a discesa **Type** (tipo), eseguire una delle seguenti operazioni:

- Selezionare **ONTAP SVM** per visualizzare tutte le SVM aggiunte.

  Se sono state aggiunte le SVM FSX, le SVM FSX sono elencate qui.

- Selezionare **ONTAP Clusters** per visualizzare tutti i cluster aggiunti.

  Se sono stati aggiunti cluster FSX utilizzando fsxadmin, i cluster FSX sono elencati qui.

  Quando si fa clic sul nome del cluster, tutte le SVM che fanno parte del cluster vengono visualizzate nella sezione Storage Virtual Machines (macchine virtuali di storage).

  Se una nuova SVM viene aggiunta al cluster ONTAP utilizzando l'interfaccia grafica di ONTAP, fare clic su **riscopri** per visualizzare la nuova SVM aggiunta.

Se i sistemi di storage FAS o AFF sono stati aggiornati a tutti gli array SAN (ASA), è necessario aggiornare la connessione di storage nel server SnapCenter in modo che rifletta il nuovo tipo di storage in SnapCenter.

Al termine

Un amministratore del cluster deve abilitare AutoSupport su ciascun nodo del sistema di storage per inviare notifiche e-mail da tutti i sistemi di storage a cui SnapCenter ha accesso, eseguendo il seguente comando dalla riga di comando del sistema di storage:

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
-to enable -noteto enable
```

L'amministratore della macchina virtuale per lo storage (SVM) non ha accesso a AutoSupport.

Aggiunta di licenze SnapCenter basate su controller standard

È necessaria una licenza basata su controller standard SnapCenter se si utilizzano controller di storage FAS, AFF o All SAN Array (ASA).

La licenza basata su controller ha le seguenti caratteristiche:

- Diritto standard SnapCenter incluso con l'acquisto di bundle premium o flash (non con il pacchetto base)
- Utilizzo illimitato dello storage
- È possibile aggiungerlo direttamente al controller di storage FAS, AFF o ASA utilizzando Gestione di sistema di ONTAP o la riga di comando del cluster di storage

  Non inserire alcuna informazione di licenza nell'interfaccia grafica di SnapCenter per le licenze basate su controller SnapCenter.

- Bloccato sul numero di serie del controller

Per informazioni sulle licenze richieste, vedere "Licenze SnapCenter".

Fase 1: Verificare che la licenza della suite SnapManager sia installata

È possibile utilizzare l'interfaccia grafica di SnapCenter per verificare se una licenza della suite SnapManager è installata su sistemi di storage primari FAS, AFF o ASA e per identificare i sistemi di storage che potrebbero richiedere licenze della suite SnapManager. Le licenze della suite SnapManager sono valide solo per SVM

FAS, AFF e ASA o per cluster su sistemi storage primari.

> Se si dispone già di una licenza della suite SnapManager sul controller, il diritto alla licenza basata su controller standard SnapCenter viene fornito automaticamente. I nomi licenza SnapManagerSuite e licenza basata su controller standard SnapCenter vengono utilizzati in modo intercambiabile, ma si riferiscono alla stessa licenza.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **Storage Systems**.
2. Nella pagina Storage Systems (sistemi storage), dal menu a discesa **Type** (tipo), selezionare se visualizzare tutte le SVM o i cluster aggiunti:
   - Per visualizzare tutte le SVM aggiunte, selezionare **ONTAP SVM**.
   - Per visualizzare tutti i cluster aggiunti, selezionare **ONTAP Clusters**.

     Quando si seleziona il nome del cluster, tutte le SVM che fanno parte del cluster vengono visualizzate nella sezione Storage Virtual Machines (macchine virtuali di storage).
3. Nell'elenco Storage Connections (connessioni storage), individuare la colonna Controller License (licenza controller).

   La colonna Controller License (licenza controller) visualizza il seguente stato:

   -  Indica che una licenza della suite SnapManager è installata su un sistema di storage primario FAS, AFF o ASA.
   -  Indica che una licenza della suite SnapManager non è installata su un sistema di storage primario FAS, AFF o ASA.
   - Non applicabile indica che una licenza della suite SnapManager non è applicabile perché lo storage controller si trova su piattaforme di storage Cloud Volumes ONTAP, ONTAP Select o secondarie.

Fase 2: Identificare le licenze installate sul controller

È possibile utilizzare la riga di comando ONTAP per visualizzare tutte le licenze installate sul controller. È necessario essere un amministratore del cluster nel sistema FAS, AFF o ASA.

> La licenza basata su controller standard SnapCenter viene visualizzata come licenza SnapManagerSuite sul controller.

Fasi

1. Accedere al controller NetApp utilizzando la riga di comando ONTAP.
2. Immettere il comando License show, quindi visualizzare l'output per determinare se la licenza SnapManagerSuite è installata.

Output di esempio

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
Base              site     Cluster Base License     -

Serial Number: 1-81-00000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

Nell'esempio, la licenza SnapManagerSuite è installata, pertanto non sono richieste ulteriori azioni di licenza SnapCenter.

Fase 3: Recuperare il numero di serie del controller

Per recuperare il numero di serie della licenza basata su controller, è necessario disporre del numero di serie del controller. È possibile recuperare il numero di serie del controller utilizzando la riga di comando ONTAP. È necessario essere un amministratore del cluster nel sistema FAS, AFF o ASA.

Fasi

1. Accedere al controller utilizzando la riga di comando ONTAP.
2. Immettere il comando show -instance del sistema, quindi esaminare l'output per individuare il numero di serie del controller.

Output di esempio

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. Annotare i numeri di serie.

Fase 4: Recuperare il numero di serie della licenza basata su controller

Se si utilizza lo storage FAS o AFF, è possibile recuperare la licenza basata su controller SnapCenter dal sito di supporto NetApp prima di poterla installare utilizzando la riga di comando ONTAP.

Prima di iniziare

- È necessario disporre di credenziali di accesso al sito di supporto NetApp valide.

  Se non si inseriscono credenziali valide, non vengono restituite informazioni per la ricerca.

- Il numero di serie del controller dovrebbe essere disponibile.

Fasi

1. Accedere a "Sito di supporto NetApp".
2. Accedere a **sistemi** > **licenze software**.
3. Nell'area Selection Criteria (Criteri di selezione), assicurarsi che sia selezionato Serial Number (numero di serie) (situato sul retro dell'unità), inserire il numero di serie del controller, quindi selezionare **Go!** (Vai).

   Viene visualizzato un elenco di licenze per il controller specificato.

4. Individuare e registrare la licenza di SnapCenter o SnapManagerSuite.

Fase 5: Aggiungere una licenza basata su controller

È possibile utilizzare la riga di comando ONTAP per aggiungere una licenza basata su controller SnapCenter quando si utilizzano sistemi FAS, AFF o ASA e si dispone di una licenza SnapCenter o SnapManagerSuite.

Prima di iniziare

- È necessario essere un amministratore del cluster nel sistema FAS, AFF o ASA.
- È necessario disporre della licenza standard o SnapManagerSuite di SnapCenter.

A proposito di questa attività

Se si desidera installare SnapCenter in prova con storage FAS, AFF o ASA, è possibile ottenere una licenza di valutazione Premium Bundle da installare sul controller.

Se si desidera installare SnapCenter in prova, contattare il rappresentante commerciale per ottenere una licenza di valutazione del bundle Premium da installare sul controller.

Fasi

1. Accedere al cluster NetApp utilizzando la riga di comando ONTAP.
2. Aggiungere la chiave di licenza SnapManagerSuite:

   ```
   system license add -license-code license_key
   ```

   Questo comando è disponibile a livello di privilegio admin.

3. Verificare che la licenza SnapManagerSuite sia installata:

   ```
   license show
   ```

Fase 6: Rimuovere la licenza di prova

Se si utilizza una licenza standard SnapCenter basata su controller e si deve rimuovere la licenza di prova basata su capacità (numero di serie che termina con “50”), utilizzare i comandi MySQL per rimuovere manualmente la licenza di prova. La licenza di prova non può essere eliminata utilizzando l’interfaccia grafica di SnapCenter.

> La rimozione manuale di una licenza di prova è necessaria solo se si utilizza una licenza basata su controller standard SnapCenter. Se si è acquistata una licenza basata sulla capacità standard di SnapCenter e la si è aggiunta nella GUI di SnapCenter, la licenza di prova viene sovrascritta automaticamente.

Fasi

1. Sul server SnapCenter, aprire una finestra PowerShell per reimpostare la password MySQL.
   a. Eseguire il cmdlet Open-SmConnection per avviare una sessione di connessione con il server SnapCenter per un account SnapCenterAdmin.
   b. Eseguire Set-SmRepositoryPassword per reimpostare la password MySQL.

      Per informazioni sui cmdlet, vedere "Guida di riferimento al cmdlet del software SnapCenter".
2. Aprire il prompt dei comandi ed eseguire mysql -u root -p per accedere a MySQL.

   MySQL richiede la password. Immettere le credenziali fornite durante la reimpostazione della password.
3. Rimuovere la licenza di prova dal database:

   ```
   use nsm;``DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
   ```

Aggiunta di licenze SnapCenter basate sulla capacità standard

Si utilizza una licenza SnapCenter con capacità standard per proteggere i dati sulle piattaforme ONTAP Select e Cloud Volumes ONTAP.

Una licenza di capacità ha le seguenti caratteristiche:

- Composto da un numero di serie di nove cifre con il formato 51xxxxxxx

  Per attivare la licenza utilizzando l’interfaccia grafica di SnapCenter, utilizzare il numero di serie della licenza e le credenziali di accesso al sito di supporto NetApp valide.
- Disponibile come licenza perpetua separata, con il costo basato sulla capacità di storage utilizzata o sulla dimensione dei dati che si desidera proteggere, a seconda di quale sia inferiore, e i dati sono gestiti da SnapCenter
- Disponibile per terabyte

  Ad esempio, è possibile ottenere una licenza basata sulla capacità per 1 TB, 2 TB, 4 TB e così via.
- Disponibile come licenza di prova per 90 giorni con capacità di 100 TB

  Per informazioni sulle licenze richieste, vedere "Licenze SnapCenter".

SnapCenter calcola automaticamente l'utilizzo della capacità una volta al giorno a mezzanotte sullo storage ONTAP Select e Cloud Volumes ONTAP gestito. Quando si utilizza una licenza con capacità standard, SnapCenter calcola la capacità inutilizzata deducendo la capacità utilizzata su tutti i volumi dalla capacità totale concessa in licenza. Se la capacità utilizzata supera la capacità concessa in licenza, viene visualizzato un avviso di utilizzo eccessivo nella dashboard di SnapCenter. Se sono state configurate soglie di capacità e notifiche in SnapCenter, viene inviata un'e-mail quando la capacità utilizzata raggiunge la soglia specificata.

Fase 1: Calcolo dei requisiti di capacità

Prima di ottenere una licenza SnapCenter basata sulla capacità, è necessario calcolare la capacità di un host che deve essere gestito da SnapCenter.

L'utente deve essere un amministratore del cluster nel sistema Cloud Volumes ONTAP o ONTAP Select.

A proposito di questa attività

SnapCenter calcola la capacità effettiva utilizzata. Se la dimensione del file system o del database è di 1 TB, ma vengono utilizzati solo 500 GB di spazio, SnapCenter calcola 500 GB di capacità utilizzata. La capacità del volume viene calcolata dopo la deduplica e la compressione e si basa sulla capacità utilizzata dell'intero volume.

Fasi

1. Accedere al controller NetApp utilizzando la riga di comando ONTAP.
2. Per visualizzare la capacità del volume utilizzata, immettere il comando.

```
select::> vol show -fields used -volume Engineering,Marketing
vserver volume       used
------- ------       ------
VS1     Engineering  2.13TB
VS1     Marketing    2.62TB

2   entries were displayed.
```

La capacità combinata utilizzata per i due volumi è inferiore a 5 TB; pertanto, se si desidera proteggere tutti i 5 TB di dati, il requisito minimo di licenza SnapCenter basato sulla capacità è di 5 TB.

Tuttavia, se si desidera proteggere solo 2 TB dei 5 TB di capacità totale utilizzata, è possibile acquistare una licenza basata sulla capacità da 2 TB.

Fase 2: Recuperare il numero di serie della licenza basata sulla capacità

Il numero di serie della licenza SnapCenter basata sulla capacità è disponibile nella conferma dell'ordine o nella documentazione; tuttavia, se non si dispone di questo numero di serie, è possibile recuperarlo dal sito del supporto NetApp.

È necessario disporre di credenziali di accesso al sito di supporto NetApp valide.

Fasi

1. Accedere a "Sito di supporto NetApp".
2. Accedere a **sistemi** > **licenze software**.

3. Nell'area Selection Criteria (Criteri di selezione), scegliere **SC_STANDARD** dal menu a discesa Show Me All: Serial Numbers and Licenses (Mostra tutti: Numeri di serie e licenze).

4. Digitare il nome della società, quindi selezionare **Go!**.

   Viene visualizzato il numero di serie di nove cifre della licenza SnapCenter, con il formato 51xxxxxxx.

5. Annotare il numero di serie.

Fase 3: Generare un file di licenza NetApp

Se non si desidera inserire le credenziali del sito di supporto NetApp e il numero di serie della licenza SnapCenter nell'interfaccia grafica di SnapCenter o se non si dispone dell'accesso a Internet al sito di supporto NetApp da SnapCenter, è possibile generare un file di licenza NetApp (NLF). È quindi possibile scaricare e memorizzare il file in una posizione accessibile dall'host SnapCenter.

Prima di iniziare

- SnapCenter deve essere utilizzato con ONTAP Select o Cloud Volumes ONTAP.
- È necessario disporre di credenziali di accesso al sito di supporto NetApp valide.
- Il numero seriale a nove cifre della licenza deve essere in formato 51xxxxxxx.

Fasi

1. Passare a "NetApp License file Generator".
2. Inserire le informazioni richieste.
3. Nel campo linea di prodotti, selezionare **SnapCenter standard (basato sulla capacità)** dal menu a discesa.
4. Nel campo Product Serial Number (numero di serie del prodotto), inserire il numero di serie della licenza SnapCenter
5. Leggere e accettare la direttiva sulla privacy dei dati di NetApp, quindi selezionare **Invia**.
6. Salvare il file di licenza, quindi registrare la posizione del file.

Fase 4: Aggiunta di una licenza basata sulla capacità

Se si utilizza SnapCenter con piattaforme ONTAP Select o Cloud Volumes ONTAP, è necessario installare una o più licenze SnapCenter basate sulla capacità.

Prima di iniziare

- Accedere come utente amministratore di SnapCenter.

- È necessario disporre di credenziali di accesso al sito di supporto NetApp valide.
- Il numero seriale a nove cifre della licenza deve essere in formato 51xxxxxxx.

  Se si utilizza un file di licenza NetApp (NLF) per aggiungere la licenza, è necessario conoscere la posizione del file di licenza.

A proposito di questa attività

Nella pagina Impostazioni è possibile eseguire le seguenti operazioni:

- Aggiungere una licenza.
- Visualizzare i dettagli della licenza per individuare rapidamente le informazioni relative a ciascuna licenza.
- Modificare una licenza quando si desidera sostituire la licenza esistente, ad esempio per aggiornare la capacità della licenza o per modificare le impostazioni di notifica della soglia.
- Eliminare una licenza quando si desidera sostituire una licenza esistente o quando la licenza non è più necessaria.

La licenza di prova (numero di serie che termina con 50) non può essere eliminata utilizzando l'interfaccia grafica di SnapCenter. La licenza di prova viene sovrascritta automaticamente quando si aggiunge una licenza basata sulla capacità dello standard SnapCenter procurato.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **Impostazioni**.
2. Nella pagina Impostazioni, selezionare **Software**.
3. Nella sezione licenza della pagina Software, selezionare **Aggiungi** (+).
4. Nella procedura guidata Aggiungi licenza SnapCenter, selezionare uno dei seguenti metodi per ottenere la licenza che si desidera aggiungere:

Per questo campo…	Eseguire questa operazione…
Immettere le credenziali di accesso al NetApp Support Site (NSS) per importare le licenze	a. Immettere il nome utente NSS. b. Inserire la password NSS. c. Inserire il numero di serie della licenza basata su controller.
File di licenza NetApp	a. Individuare il percorso del file di licenza, quindi selezionarlo. b. Selezionare **Apri**.

5. Nella pagina Notifiche, immettere la soglia di capacità alla quale SnapCenter invia le notifiche di posta elettronica, EMS e AutoSupport.

   La soglia predefinita è 90 percento.

6. Per configurare il server SMTP per le notifiche e-mail, selezionare **Impostazioni** > **Impostazioni globali** > **Impostazioni server di notifica**, quindi immettere i seguenti dettagli:

Per questo campo…	Eseguire questa operazione…
Preferenza e-mail	Scegliere **sempre** o **mai**.
Fornire le impostazioni e-mail	Se si seleziona **sempre**, specificare quanto segue: • Indirizzo e-mail del mittente • Indirizzo e-mail del destinatario • Facoltativo: Consente di modificare la riga dell'oggetto predefinita Il soggetto predefinito è il seguente: "Notifica della capacità della licenza SnapCenter".

7. Se si desidera che i messaggi del sistema di gestione degli eventi (EMS) vengano inviati al sistema di storage syslog o che i messaggi AutoSupport vengano inviati al sistema di storage per le operazioni non riuscite, selezionare le caselle di controllo appropriate. Si consiglia di attivare AutoSupport per risolvere eventuali problemi.
8. Selezionare **Avanti**.
9. Esaminare il riepilogo, quindi selezionare **fine**.

Eseguire il provisioning del sistema storage

Eseguire il provisioning dello storage su host Windows

Configurare lo storage LUN

È possibile utilizzare SnapCenter per configurare un LUN connesso a FC o a iSCSI. È inoltre possibile utilizzare SnapCenter per connettere un LUN esistente a un host Windows.

I LUN sono l'unità di storage di base in una configurazione SAN. L'host Windows vede le LUN del sistema come dischi virtuali. Per ulteriori informazioni, vedere "Guida alla configurazione SAN di ONTAP 9".

Stabilire una sessione iSCSI

Se si utilizza iSCSI per connettersi a un LUN, è necessario stabilire una sessione iSCSI prima di creare il LUN per abilitare la comunicazione.

Prima di iniziare

- È necessario aver definito il nodo del sistema di storage come destinazione iSCSI.
- È necessario aver avviato il servizio iSCSI sul sistema di archiviazione. "Scopri di più"

A proposito di questa attività

È possibile stabilire una sessione iSCSI solo tra le stesse versioni IP, da IPv6 a IPv6 o da IPv4 a IPv4.

È possibile utilizzare un indirizzo IPv6 link-local per la gestione della sessione iSCSI e per la comunicazione

tra un host e una destinazione solo quando entrambi si trovano nella stessa subnet.

Se si modifica il nome di un iSCSI Initiator, l'accesso alle destinazioni iSCSI viene compromesso. Dopo aver modificato il nome, potrebbe essere necessario riconfigurare le destinazioni a cui ha accesso l'iniziatore in modo che possano riconoscere il nuovo nome. Dopo aver modificato il nome di un iSCSI Initiator, è necessario riavviare l'host.

Se l'host dispone di più interfacce iSCSI, una volta stabilita una sessione iSCSI su SnapCenter utilizzando un indirizzo IP sulla prima interfaccia, non è possibile stabilire una sessione iSCSI da un'altra interfaccia con un indirizzo IP diverso.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iSCSI Session** (sessione iSCSI).
3. Dall'elenco a discesa **Storage Virtual Machine** (macchina virtuale di storage), selezionare la macchina virtuale di storage (SVM) per la destinazione iSCSI.
4. Dall'elenco a discesa **host**, selezionare l'host per la sessione.
5. Fare clic su **Definisci sessione**.

   Viene visualizzata la procedura guidata per stabilire la sessione.

6. Nella procedura guidata per stabilire la sessione, identificare la destinazione:

In questo campo…	Inserisci…
Nome del nodo di destinazione	Il nome del nodo della destinazione iSCSI Se esiste un nome di nodo di destinazione, il nome viene visualizzato in formato di sola lettura.
Indirizzo del portale di destinazione	L'indirizzo IP del portale di rete di destinazione
Porta del portale di destinazione	La porta TCP del portale di rete di destinazione
Indirizzo del portale iniziatore	L'indirizzo IP del portale di rete dell'iniziatore

7. Quando si è soddisfatti delle voci immesse, fare clic su **Connect** (Connetti).

   SnapCenter stabilisce la sessione iSCSI.

8. Ripetere questa procedura per stabilire una sessione per ogni destinazione.

Disconnettere una sessione iSCSI

A volte, potrebbe essere necessario disconnettere una sessione iSCSI da una destinazione con cui si hanno più sessioni.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.

2. Nella pagina host, fare clic su **iSCSI Session** (sessione iSCSI).
3. Dall'elenco a discesa **Storage Virtual Machine** (macchina virtuale di storage), selezionare la macchina virtuale di storage (SVM) per la destinazione iSCSI.
4. Dall'elenco a discesa **host**, selezionare l'host per la sessione.
5. Dall'elenco delle sessioni iSCSI, selezionare la sessione che si desidera disconnettere e fare clic su **Disconnetti sessione**.
6. Nella finestra di dialogo Disconnetti sessione, fare clic su **OK**.

   SnapCenter disconnette la sessione iSCSI.

Creare e gestire igroups

È possibile creare gruppi di iniziatori (igroups) per specificare gli host che possono accedere a una determinata LUN sul sistema di storage. È possibile utilizzare SnapCenter per creare, rinominare, modificare o eliminare un igroup su un host Windows.

Creare un igroup

È possibile utilizzare SnapCenter per creare un igroup su un host Windows. L'igroup sarà disponibile nella procedura guidata Create Disk (Crea disco) o Connect Disk (Connetti disco) quando si esegue la mappatura dell'igroup a un LUN.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iGroup**.
3. Nella pagina Initiator Groups (gruppi iniziatori), fare clic su **New** (nuovo).
4. Nella finestra di dialogo Create iGroup (Crea iGroup), definire il campo igroup:

In questo campo…	Eseguire questa operazione…
Sistema storage	Selezionare la SVM per il LUN da mappare all'igroup.
Host	Selezionare l'host su cui si desidera creare l'igroup.
Nome iGroup	Immettere il nome dell'igroup.
Iniziatori	Selezionare l'iniziatore.
Tipo	Selezionare il tipo di iniziatore, iSCSI, FCP o misto (FCP e iSCSI).

5. Quando si è soddisfatti delle voci immesse, fare clic su **OK**.

   SnapCenter crea l'igroup sul sistema storage.

Rinominare un igroup

È possibile utilizzare SnapCenter per rinominare un igroup esistente.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iGroup**.
3. Nella pagina Initiator Groups (gruppi iniziatori), fare clic nel campo **Storage Virtual Machine** (macchina virtuale di storage) per visualizzare un elenco di SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera rinominare.
4. Nell'elenco di igroups per SVM, selezionare l'igroup che si desidera rinominare e fare clic su **Rename** (Rinomina).
5. Nella finestra di dialogo Rinomina igroup, immettere il nuovo nome per igroup e fare clic su **Rinomina**.

Modificare un igroup

È possibile utilizzare SnapCenter per aggiungere gli iniziatori igroup a un igroup esistente. Durante la creazione di un igroup è possibile aggiungere un solo host. Se si desidera creare un igroup per un cluster, è possibile modificare il igroup per aggiungere altri nodi a tale igroup.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iGroup**.
3. Nella pagina Initiator Groups (gruppi di iniziatori), fare clic nel campo **Storage Virtual Machine** (macchina virtuale di storage) per visualizzare un elenco a discesa delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera modificare.
4. Nell'elenco di igroups, selezionare un igroup e fare clic su **Add Initiator to igroup**.
5. Selezionare un host.
6. Selezionare gli iniziatori e fare clic su **OK**.

Eliminare un igroup

È possibile utilizzare SnapCenter per eliminare un igroup quando non è più necessario.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iGroup**.
3. Nella pagina Initiator Groups (gruppi iniziatori), fare clic nel campo **Storage Virtual Machine** (macchina virtuale di storage) per visualizzare un elenco a discesa delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera eliminare.
4. Nell'elenco di igroups per SVM, selezionare l'igroup che si desidera eliminare e fare clic su **Delete** (Elimina).
5. Nella finestra di dialogo Delete igroup (Elimina igroup), fare clic su **OK**.

   SnapCenter elimina l'igroup.

Creare e gestire i dischi

L'host Windows vede le LUN del sistema storage come dischi virtuali. È possibile utilizzare SnapCenter per creare e configurare un LUN connesso a FC o iSCSI.

- SnapCenter supporta solo dischi di base. I dischi dinamici non sono supportati.
- Per GPT è consentita una sola partizione di dati e per MBR una partizione primaria con un volume formattato con NTFS o CSVFS e un percorso di montaggio.
- Stili di partizione supportati: GPT, MBR; in una macchina virtuale VMware UEFI, sono supportati solo i dischi iSCSI

SnapCenter non supporta la ridenominazione di un disco. Se un disco gestito da SnapCenter viene rinominato, le operazioni SnapCenter non avranno esito positivo.

Visualizzare i dischi su un host

È possibile visualizzare i dischi su ciascun host Windows gestito con SnapCenter.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.

   I dischi sono elencati.

Visualizzare i dischi in cluster

È possibile visualizzare i dischi in cluster nel cluster gestito con SnapCenter. I dischi in cluster vengono visualizzati solo quando si seleziona il cluster dall'elenco a discesa host.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare il cluster dall'elenco a discesa **host**.

   I dischi sono elencati.

Creazione di LUN o dischi connessi a FC o iSCSI

L'host Windows vede le LUN del sistema storage come dischi virtuali. È possibile utilizzare SnapCenter per creare e configurare un LUN connesso a FC o iSCSI.

Se si desidera creare e formattare dischi al di fuori di SnapCenter, sono supportati solo i file system NTFS e CSVFS.

Prima di iniziare

- È necessario aver creato un volume per il LUN sul sistema storage.

  Il volume deve contenere solo LUN e solo LUN creati con SnapCenter.

Non è possibile creare un LUN su un volume clone creato da SnapCenter a meno che il clone non sia già stato diviso.

- È necessario aver avviato il servizio FC o iSCSI sul sistema di storage.
- Se si utilizza iSCSI, è necessario aver stabilito una sessione iSCSI con il sistema di storage.
- Il pacchetto di plug-in SnapCenter per Windows deve essere installato solo sull'host su cui si sta creando il disco.

A proposito di questa attività

- Non è possibile connettere un LUN a più di un host a meno che il LUN non sia condiviso dagli host in un cluster di failover di Windows Server.
- Se un LUN viene condiviso dagli host in un cluster di failover di Windows Server che utilizza CSV (Cluster Shared Volumes), è necessario creare il disco sull'host proprietario del gruppo di cluster.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.
4. Fare clic su **nuovo**.

   Viene visualizzata la procedura guidata Create Disk (Crea disco).

5. Nella pagina LUN Name (Nome LUN), identificare il LUN:

In questo campo…	Eseguire questa operazione…
Sistema storage	Selezionare la SVM per il LUN.
Percorso LUN	Fare clic su **Browse** (Sfoglia) per selezionare il percorso completo della cartella contenente il LUN.
Nome LUN	Immettere il nome del LUN.
Dimensione del cluster	Selezionare la dimensione di allocazione del blocco LUN per il cluster. Le dimensioni del cluster dipendono dal sistema operativo e dalle applicazioni.
Etichetta LUN	Se si desidera, inserire un testo descrittivo per il LUN.

6. Nella pagina Disk Type (tipo di disco), selezionare il tipo di disco:

Selezionare…	Se…
Disco dedicato	È possibile accedere al LUN solo da un host. Ignorare il campo **Gruppo di risorse**.
Disco condiviso	Il LUN è condiviso dagli host in un cluster di failover di Windows Server. Inserire il nome del gruppo di risorse del cluster nel campo **Gruppo di risorse**. È necessario creare il disco su un solo host nel cluster di failover.
Volume condiviso del cluster (CSV)	Il LUN è condiviso dagli host di un cluster di failover di Windows Server che utilizza CSV. Inserire il nome del gruppo di risorse del cluster nel campo **Gruppo di risorse**. Assicurarsi che l'host su cui si sta creando il disco sia il proprietario del gruppo di cluster.

7. Nella pagina Drive Properties, specificare le proprietà del disco:

Proprietà	Descrizione
Assegnazione automatica del punto di montaggio	SnapCenter assegna automaticamente un punto di montaggio del volume in base al disco di sistema. Ad esempio, se il disco di sistema è C:, l'assegnazione automatica crea un punto di montaggio del volume sotto l'unità C:. L'assegnazione automatica non è supportata per i dischi condivisi.
Assegnare la lettera dell'unità	Montare il disco sull'unità selezionata nell'elenco a discesa adiacente.
Utilizzare il punto di montaggio del volume	Montare il disco sul percorso specificato nel campo adiacente. La directory principale del punto di montaggio del volume deve essere di proprietà dell'host su cui si sta creando il disco.
Non assegnare la lettera del disco o il punto di montaggio del volume	Scegliere questa opzione se si preferisce montare il disco manualmente in Windows.
Dimensioni LUN	Specificare la dimensione del LUN; almeno 150 MB. Selezionare MB, GB o TB nell'elenco a discesa adiacente.

Proprietà	Descrizione
Utilizzare il thin provisioning per il volume che ospita questo LUN	Eseguire il thin provisioning del LUN. Il thin provisioning alloca solo lo spazio di storage necessario alla volta, consentendo al LUN di crescere in modo efficiente fino alla massima capacità disponibile. Assicurarsi che sul volume sia disponibile spazio sufficiente per ospitare tutto lo storage LUN che si ritiene necessario.
Scegliere il tipo di partizione	Selezionare la partizione GPT per una tabella di partizione GUID o la partizione MBR per un record di avvio principale. Le partizioni MBR potrebbero causare problemi di disallineamento nei cluster di failover di Windows Server. I dischi di partizione UEFI (Unified Extensible firmware Interface) non sono supportati.

8. Nella pagina Map LUN (LUN mappa), selezionare iSCSI o FC Initiator (iniziatore iSCSI o FC) sull'host:

In questo campo…	Eseguire questa operazione…
Host	Fare doppio clic sul nome del gruppo di cluster per visualizzare un elenco a discesa che mostra gli host che appartengono al cluster, quindi selezionare l'host per l'iniziatore. Questo campo viene visualizzato solo se il LUN è condiviso dagli host in un cluster di failover di Windows Server.
Scegliere l'iniziatore host	Selezionare **Fibre Channel** o **iSCSI**, quindi selezionare l'iniziatore sull'host. È possibile selezionare più iniziatori FC se si utilizza FC con multipath i/o (MPIO).

9. Nella pagina Group Type (tipo gruppo), specificare se si desidera mappare un igroup esistente al LUN o creare un nuovo igroup:

Selezionare…	Se…
Creare un nuovo igroup per gli iniziatori selezionati	Si desidera creare un nuovo igroup per gli iniziatori selezionati.

Selezionare…	Se…
Scegliere un igroup esistente o specificare un nuovo igroup per gli iniziatori selezionati	Si desidera specificare un igroup esistente per gli iniziatori selezionati o creare un nuovo igroup con il nome specificato. Digitare il nome dell'igroup nel campo **igroup name**. Digitare le prime lettere del nome igroup esistente per completare automaticamente il campo.

10. Nella pagina Summary (Riepilogo), rivedere le selezioni e fare clic su **Finish** (fine).

    SnapCenter crea il LUN e lo connette all'unità o al percorso del disco specificato sull'host.

Ridimensionare un disco

È possibile aumentare o ridurre le dimensioni di un disco in base alle esigenze del sistema di storage.

A proposito di questa attività

- Per i LUN con thin provisioning, la dimensione della geometria del lun ONTAP viene visualizzata come dimensione massima.
- Per i LUN con thick provisioning, la dimensione espandibile (dimensione disponibile nel volume) viene visualizzata come dimensione massima.
- Le LUN con partizioni di tipo MBR hanno una dimensione massima di 2 TB.
- Le LUN con partizioni di tipo GPT hanno un limite di dimensioni del sistema storage di 16 TB.
- È consigliabile creare un'istantanea prima di ridimensionare un LUN.
- Per ripristinare una LUN da una Snapshot creata prima del ridimensionamento della LUN, SnapCenter ridimensiona automaticamente il LUN alla dimensione della Snapshot.

  Dopo l'operazione di ripristino, i dati aggiunti al LUN dopo il ridimensionamento devono essere ripristinati da una Snapshot creata dopo il ridimensionamento.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa host.

   I dischi sono elencati.

4. Selezionare il disco che si desidera ridimensionare, quindi fare clic su **Ridimensiona**.
5. Nella finestra di dialogo Ridimensiona disco, utilizzare lo strumento a scorrimento per specificare le nuove dimensioni del disco oppure inserire le nuove dimensioni nel campo dimensione.

   Se si inserisce la dimensione manualmente, è necessario fare clic all'esterno del campo dimensione prima che il pulsante Riduci o Espandi sia attivato correttamente. Inoltre, è necessario fare clic su MB, GB o TB per specificare l'unità di misura.

6. Quando si è soddisfatti delle voci immesse, fare clic su **Riduci** o **Espandi**, a seconda dei casi.

   SnapCenter ridimensiona il disco.

Collegare un disco

È possibile utilizzare la procedura guidata Connect Disk per connettere un LUN esistente a un host o per riconnettere un LUN disconnesso.

Prima di iniziare

- È necessario aver avviato il servizio FC o iSCSI sul sistema di storage.
- Se si utilizza iSCSI, è necessario aver stabilito una sessione iSCSI con il sistema di storage.
- Non è possibile connettere un LUN a più di un host a meno che il LUN non sia condiviso dagli host in un cluster di failover di Windows Server.
- Se il LUN è condiviso da host in un cluster di failover di Windows Server che utilizza CSV (Cluster Shared Volumes), è necessario collegare il disco all'host proprietario del gruppo di cluster.
- Il plug-in per Windows deve essere installato solo sull'host su cui si sta collegando il disco.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.
4. Fare clic su **Connect** (Connetti).

   Viene visualizzata la procedura guidata Connect Disk.

5. Nella pagina LUN Name (Nome LUN), identificare il LUN a cui connettersi:

In questo campo…	Eseguire questa operazione…
Sistema storage	Selezionare la SVM per il LUN.
Percorso LUN	Fare clic su **Browse** (Sfoglia) per selezionare il percorso completo del volume contenente il LUN.
Nome LUN	Immettere il nome del LUN.
Dimensione del cluster	Selezionare la dimensione di allocazione del blocco LUN per il cluster. Le dimensioni del cluster dipendono dal sistema operativo e dalle applicazioni.
Etichetta LUN	Se si desidera, inserire un testo descrittivo per il LUN.

6. Nella pagina Disk Type (tipo di disco), selezionare il tipo di disco:

Selezionare…	Se…
Disco dedicato	È possibile accedere al LUN solo da un host.
Disco condiviso	Il LUN è condiviso dagli host in un cluster di failover di Windows Server. È necessario connettere il disco a un solo host nel cluster di failover.
Volume condiviso del cluster (CSV)	Il LUN è condiviso dagli host di un cluster di failover di Windows Server che utilizza CSV. Assicurarsi che l'host su cui ci si connette al disco sia il proprietario del gruppo di cluster.

7. Nella pagina Drive Properties, specificare le proprietà del disco:

Proprietà	Descrizione
Assegnazione automatica	Consentire a SnapCenter di assegnare automaticamente un punto di montaggio del volume in base al disco di sistema. Ad esempio, se il disco di sistema è C:, la proprietà di assegnazione automatica crea un punto di montaggio del volume sotto l'unità C:. La proprietà di assegnazione automatica non è supportata per i dischi condivisi.
Assegnare la lettera dell'unità	Montare il disco sull'unità selezionata nell'elenco a discesa adiacente.
Utilizzare il punto di montaggio del volume	Montare il disco sul percorso specificato nel campo adiacente. La directory principale del punto di montaggio del volume deve essere di proprietà dell'host su cui si sta creando il disco.
Non assegnare la lettera del disco o il punto di montaggio del volume	Scegliere questa opzione se si preferisce montare il disco manualmente in Windows.

8. Nella pagina Map LUN (LUN mappa), selezionare iSCSI o FC Initiator (iniziatore iSCSI o FC) sull'host:

In questo campo…	Eseguire questa operazione…
Host	Fare doppio clic sul nome del gruppo di cluster per visualizzare un elenco a discesa che mostra gli host che appartengono al cluster, quindi selezionare l'host per l'iniziatore. Questo campo viene visualizzato solo se il LUN è condiviso dagli host in un cluster di failover di Windows Server.
Scegliere l'iniziatore host	Selezionare **Fibre Channel** o **iSCSI**, quindi selezionare l'iniziatore sull'host. È possibile selezionare più iniziatori FC se si utilizza FC con MPIO.

9. Nella pagina Group Type (tipo di gruppo), specificare se si desidera mappare un igroup esistente al LUN o creare un nuovo igroup:

Selezionare…	Se…
Creare un nuovo igroup per gli iniziatori selezionati	Si desidera creare un nuovo igroup per gli iniziatori selezionati.
Scegliere un igroup esistente o specificare un nuovo igroup per gli iniziatori selezionati	Si desidera specificare un igroup esistente per gli iniziatori selezionati o creare un nuovo igroup con il nome specificato. Digitare il nome dell'igroup nel campo **igroup name**. Digitare le prime lettere del nome igroup esistente per completare automaticamente il campo.

10. Nella pagina Summary (Riepilogo), rivedere le selezioni e fare clic su **Finish** (fine).

    SnapCenter connette il LUN all'unità o al percorso del disco specificato sull'host.

Scollegare un disco

È possibile disconnettere un LUN da un host senza influire sul contenuto del LUN, con un'eccezione: Se si disconnette un clone prima che sia stato separato, il contenuto del clone viene perso.

Prima di iniziare

- Assicurarsi che il LUN non sia in uso da nessuna applicazione.
- Assicurarsi che il LUN non venga monitorato con il software di monitoraggio.
- Se il LUN è condiviso, assicurarsi di rimuovere le dipendenze delle risorse del cluster dal LUN e verificare che tutti i nodi del cluster siano accesi, funzionino correttamente e disponibili per SnapCenter.

A proposito di questa attività

Se si disconnette un LUN in un volume FlexClone creato da SnapCenter e non sono connessi altri LUN sul volume, SnapCenter elimina il volume. Prima di disconnettere il LUN, SnapCenter visualizza un messaggio che avvisa che il volume FlexClone potrebbe essere stato eliminato.

Per evitare l'eliminazione automatica del volume FlexClone, rinominare il volume prima di disconnettere l'ultimo LUN. Quando si rinomina il volume, assicurarsi di modificare più caratteri rispetto all'ultimo carattere del nome.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.

   I dischi sono elencati.

4. Selezionare il disco che si desidera disconnettere, quindi fare clic su **Disconnetti**.
5. Nella finestra di dialogo Disconnetti disco, fare clic su **OK**.

   SnapCenter disconnette il disco.

Eliminare un disco

È possibile eliminare un disco quando non è più necessario. Una volta eliminato un disco, non è possibile annullarlo.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.

   I dischi sono elencati.

4. Selezionare il disco che si desidera eliminare, quindi fare clic su **Delete** (Elimina).
5. Nella finestra di dialogo Delete Disk (Elimina disco), fare clic su **OK**.

   SnapCenter elimina il disco.

Creare e gestire le condivisioni SMB

Per configurare una condivisione SMB3 su una macchina virtuale di storage (SVM), è possibile utilizzare l'interfaccia utente di SnapCenter o i cmdlet PowerShell.

Procedura consigliata: l'utilizzo dei cmdlet è consigliato in quanto consente di sfruttare i modelli forniti con SnapCenter per automatizzare la configurazione delle condivisioni.

I modelli incapsulano le Best practice per la configurazione di volumi e condivisioni. I modelli sono disponibili nella cartella modelli della cartella di installazione del pacchetto di plug-in SnapCenter per Windows.

Se ti senti a tuo agio, puoi creare i tuoi modelli seguendo i modelli forniti. Prima di creare un modello personalizzato, esaminare i parametri contenuti nella documentazione del cmdlet.

Creare una condivisione SMB

È possibile utilizzare la pagina condivisioni SnapCenter per creare una condivisione SMB3 su una macchina virtuale di storage (SVM).

Non è possibile utilizzare SnapCenter per eseguire il backup dei database sulle condivisioni SMB. Il supporto SMB è limitato solo al provisioning.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **shares**.
3. Selezionare la SVM dall'elenco a discesa **Storage Virtual Machine** (macchina virtuale di storage).
4. Fare clic su **nuovo**.

   Viene visualizzata la finestra di dialogo Nuova condivisione.

5. Nella finestra di dialogo New Share (Nuova condivisione), definire la condivisione:

In questo campo…	Eseguire questa operazione…
Descrizione	Inserire un testo descrittivo per la condivisione.
Nome di condivisione	Inserire il nome della condivisione, ad esempio test_share. Il nome immesso per la condivisione verrà utilizzato anche come nome del volume. Il nome della condivisione: • Deve essere una stringa UTF-8. • Non deve includere i seguenti caratteri: Caratteri di controllo da 0x00 a 0x1F (entrambi compresi), 0x22 (virgolette doppie) e i caratteri speciali `\ / [ ] : (vertical bar) < > + = ; , ?`
Percorso di condivisione	• Fare clic nel campo per immettere un nuovo percorso del file system, ad esempio /. • Fare doppio clic nel campo per selezionare da un elenco di percorsi del file system esistenti.

6. Quando si è soddisfatti delle voci immesse, fare clic su **OK**.

   SnapCenter crea la condivisione SMB sulla SVM.

Eliminare una condivisione SMB

È possibile eliminare una condivisione SMB quando non è più necessaria.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **shares**.
3. Nella pagina Shares (condivisioni), fare clic nel campo **Storage Virtual Machine** (macchina virtuale di storage) per visualizzare un elenco a discesa con un elenco di macchine virtuali di storage disponibili (SVM), quindi selezionare la SVM per la condivisione che si desidera eliminare.
4. Dall'elenco delle condivisioni di SVM, selezionare la condivisione che si desidera eliminare e fare clic su **Delete** (Elimina).
5. Nella finestra di dialogo Elimina condivisione, fare clic su **OK**.

   SnapCenter elimina la condivisione SMB dalla SVM.

Recuperare spazio sul sistema storage

Sebbene NTFS rilevi lo spazio disponibile su un LUN quando i file vengono cancellati o modificati, non riporta le nuove informazioni al sistema di storage. È possibile eseguire il cmdlet PowerShell per la rigenerazione dello spazio nel plug-in per l'host Windows per assicurarsi che i blocchi appena liberati siano contrassegnati come disponibili nello storage.

Se si esegue il cmdlet su un host plug-in remoto, è necessario eseguire il cmdlet SnapCenterOpen-SMConnection per aprire una connessione al server SnapCenter.

Prima di iniziare

- Prima di eseguire un'operazione di ripristino, assicurarsi che il processo di recupero dello spazio sia stato completato.
- Se il LUN è condiviso da host in un cluster di failover di Windows Server, è necessario eseguire la rigenerazione dello spazio sull'host proprietario del gruppo di cluster.
- Per ottenere performance di storage ottimali, è necessario eseguire il recupero dello spazio il più spesso possibile.

  Assicurarsi che sia stata eseguita la scansione dell'intero file system NTFS.

A proposito di questa attività

- Il recupero di spazio richiede tempo e richiede molta CPU, quindi è consigliabile eseguire l'operazione quando l'utilizzo del sistema storage e dell'host Windows è basso.
- La bonifica dello spazio recupera quasi tutto lo spazio disponibile, ma non il 100%.
- Non eseguire la deframmentazione del disco contemporaneamente alla rigenerazione dello spazio.

  In questo modo, il processo di recupero può rallentare.

Passo

Dal prompt dei comandi PowerShell del server applicativo, immettere il seguente comando:

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

Drive_path è il percorso del disco mappato al LUN.

Eseguire il provisioning dello storage utilizzando i cmdlet PowerShell

Se non si desidera utilizzare l'interfaccia grafica di SnapCenter per eseguire il provisioning host e i processi di recupero dello spazio, è possibile utilizzare i cmdlet PowerShell forniti dal plug-in SnapCenter per Microsoft Windows. È possibile utilizzare i cmdlet direttamente o aggiungerli agli script.

Se si eseguono i cmdlet su un host plug-in remoto, è necessario eseguire il cmdlet SnapCenter Open-SMConnection per aprire una connessione al server SnapCenter.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Se i cmdlet di SnapCenter PowerShell non sono più validi a causa della rimozione di SnapDrive per Windows dal server, fare riferimento a "I cmdlet di SnapCenter sono guasti quando SnapDrive per Windows viene disinstallato".

Eseguire il provisioning dello storage in ambienti VMware

È possibile utilizzare il plug-in SnapCenter per Microsoft Windows in ambienti VMware per creare e gestire LUN e Snapshot.

Piattaforme del sistema operativo guest VMware supportate

- Versioni supportate di Windows Server
- Configurazioni cluster Microsoft

  Supporto per un massimo di 16 nodi supportati su VMware quando si utilizza Microsoft iSCSI Software Initiator o fino a due nodi utilizzando FC

- LUN RDM

  Supporto per un massimo di 56 LUN RDM con quattro controller LSI Logic SCSI per RDMS normale o 42 LUN RDM con tre controller LSI Logic SCSI su un plug-in box-to-box MSCS VMware per configurazione Windows

  Supporta il controller SCSI paravirtuale VMware. È possibile supportare 256 dischi sui dischi RDM.

Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Limitazioni relative al server VMware ESXi

- L'installazione del plug-in per Windows su un cluster Microsoft su macchine virtuali che utilizzano le credenziali ESXi non è supportata.

  Utilizzare le credenziali vCenter per installare il plug-in per Windows su macchine virtuali in cluster.

- Tutti i nodi in cluster devono utilizzare lo stesso ID di destinazione (sull'adattatore SCSI virtuale) per lo stesso disco in cluster.
- Quando si crea un LUN RDM all'esterno del plug-in per Windows, è necessario riavviare il servizio plug-in per consentire il riconoscimento del disco appena creato.
- Non è possibile utilizzare gli iniziatori iSCSI e FC contemporaneamente su un sistema operativo guest VMware.

Privilegi minimi vCenter richiesti per le operazioni RDM di SnapCenter

Per eseguire operazioni RDM in un sistema operativo guest, è necessario disporre dei seguenti privilegi vCenter sull'host:

- Datastore: Rimuovere il file
- Host: Configuration > Storage Partition Configuration (Configurazione > Configurazione partizione storage)
- Macchina virtuale: Configurazione

È necessario assegnare questi privilegi a un ruolo a livello di Virtual Center Server. Il ruolo a cui si assegnano questi privilegi non può essere assegnato a nessun utente senza privilegi root.

Dopo aver assegnato questi privilegi, è possibile installare il plug-in per Windows sul sistema operativo guest.

Gestire LUN RDM FC in un cluster Microsoft

È possibile utilizzare il plug-in per Windows per gestire un cluster Microsoft utilizzando LUN RDM FC, ma è necessario prima creare il quorum RDM condiviso e lo storage condiviso all'esterno del plug-in, quindi aggiungere i dischi alle macchine virtuali del cluster.

A partire da ESXi 5.5, è possibile utilizzare anche l'hardware ESX iSCSI e FCoE per gestire un cluster Microsoft. Il plug-in per Windows include il supporto immediato per i cluster Microsoft.

Requisiti

Il plug-in per Windows fornisce il supporto per i cluster Microsoft che utilizzano LUN RDM FC su due macchine virtuali diverse che appartengono a due server ESX o ESXi diversi, noti anche come cluster tra le diverse caselle, quando si soddisfano requisiti di configurazione specifici.

- Le macchine virtuali (VM) devono eseguire la stessa versione di Windows Server.
- Le versioni dei server ESX o ESXi devono essere le stesse per ogni host VMware principale.
- Ogni host principale deve disporre di almeno due adattatori di rete.
- Deve essere presente almeno un datastore VMware Virtual Machine file System (VMFS) condiviso tra i due server ESX o ESXi.
- VMware consiglia di creare il datastore condiviso su una SAN FC.

  Se necessario, il datastore condiviso può essere creato anche su iSCSI.

- Il LUN RDM condiviso deve essere in modalità di compatibilità fisica.
- Il LUN RDM condiviso deve essere creato manualmente all'esterno del plug-in per Windows.

  Non è possibile utilizzare dischi virtuali per lo storage condiviso.

- È necessario configurare un controller SCSI su ciascuna macchina virtuale del cluster in modalità di

compatibilità fisica:

Windows Server 2008 R2 richiede la configurazione del controller SCSI SAS LSI Logic su ciascuna macchina virtuale. I LUN condivisi non possono utilizzare il controller SAS LSI Logic esistente se ne esiste uno solo e se è già collegato all'unità C.

I controller SCSI di tipo paravirtuale non sono supportati dai cluster VMware Microsoft.

> Quando si aggiunge un controller SCSI a un LUN condiviso su una macchina virtuale in modalità di compatibilità fisica, è necessario selezionare l'opzione **Raw Device Mapping** (RDM) e non l'opzione **Create a new disk** (Crea nuovo disco) in VMware Infrastructure Client.

- I cluster di macchine virtuali Microsoft non possono far parte di un cluster VMware.
- Quando si installa il plug-in per Windows su macchine virtuali appartenenti a un cluster Microsoft, è necessario utilizzare le credenziali vCenter e non le credenziali ESX o ESXi.
- Il plug-in per Windows non può creare un singolo igroup con iniziatori da più host.

  L'igroup contenente gli iniziatori di tutti gli host ESXi deve essere creato sul controller dello storage prima di creare le LUN RDM che verranno utilizzate come dischi del cluster condivisi.

- Assicurarsi di creare un LUN RDM su ESXi 5.0 utilizzando un iniziatore FC.

  Quando si crea un LUN RDM, viene creato un gruppo iniziatore con ALUA.

Limitazioni

Il plug-in per Windows supporta cluster Microsoft che utilizzano LUN RDM FC/iSCSI su macchine virtuali diverse appartenenti a server ESX o ESXi diversi.

> Questa funzione non è supportata nelle versioni precedenti a ESX 5.5i.

- Il plug-in per Windows non supporta cluster su datastore ESX iSCSI e NFS.
- Il plug-in per Windows non supporta gli iniziatori misti in un ambiente cluster.

  Gli iniziatori devono essere FC o Microsoft iSCSI, ma non entrambi.

- Gli iniziatori iSCSI ESX e gli HBA non sono supportati sui dischi condivisi in un cluster Microsoft.
- Il plug-in per Windows non supporta la migrazione delle macchine virtuali con vMotion se la macchina virtuale fa parte di un cluster Microsoft.
- Il plug-in per Windows non supporta MPIO su macchine virtuali in un cluster Microsoft.

Creare un LUN FC RDM condiviso

Prima di poter utilizzare le LUN RDM FC per condividere lo storage tra i nodi di un cluster Microsoft, è necessario creare il disco di quorum condiviso e il disco di storage condiviso, quindi aggiungerli a entrambe le macchine virtuali del cluster.

Il disco condiviso non viene creato utilizzando il plug-in per Windows. Creare e aggiungere il LUN condiviso a ciascuna macchina virtuale del cluster. Per informazioni, vedere "Cluster di macchine virtuali tra host fisici".

Configura connessioni MySQL protette con il server SnapCenter

È possibile generare certificati SSL (Secure Sockets Layer) e file di chiavi se si desidera proteggere la comunicazione tra server SnapCenter e MySQL in configurazioni standalone o di bilanciamento del carico di rete (NLB).

Configurare connessioni MySQL protette per configurazioni standalone del server SnapCenter

È possibile generare certificati SSL (Secure Sockets Layer) e file di chiavi, se si desidera proteggere la comunicazione tra il server SnapCenter e MySQL. È necessario configurare i certificati e i file delle chiavi nel server MySQL e nel server SnapCenter.

Vengono generati i seguenti certificati:

- Certificato CA
- Certificato pubblico del server e file di chiave privata
- Certificato pubblico del client e file di chiave privata

Fasi

1. Impostare i certificati SSL e i file delle chiavi per i server e i client MySQL su Windows utilizzando il comando openssl.

   Per informazioni, vedere "MySQL versione 5.7: Creazione di certificati e chiavi SSL con openssl"

   > Il valore del nome comune utilizzato per il certificato del server, il certificato del client e i file delle chiavi deve essere diverso dal valore del nome comune utilizzato per il certificato CA. Se i valori dei nomi comuni sono gli stessi, i file dei certificati e delle chiavi non funzionano per i server compilati utilizzando OpenSSL.

   Procedura consigliata: utilizzare il nome di dominio completo (FQDN) del server come nome comune per il certificato del server.

2. Copiare i certificati SSL e i file delle chiavi nella cartella MySQL Data.

   Il percorso predefinito della cartella MySQL Data è `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Aggiornare il certificato CA, il certificato pubblico del server, il certificato pubblico del client, la chiave privata del server e i percorsi delle chiavi private del client nel file di configurazione del server MySQL (my.ini).

   Il percorso predefinito del file di configurazione del server MySQL (my.ini) è `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   > Specificare il certificato CA, il certificato pubblico del server e i percorsi delle chiavi private del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

Specificare il certificato CA, il certificato pubblico del client e i percorsi delle chiavi private del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

L'esempio seguente mostra i certificati e i file chiave copiati nella sezione [mysqld] del file my.ini nella cartella predefinita `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. Arrestare l'applicazione Web del server SnapCenter nel server di informazioni Internet (IIS).
5. Riavviare il servizio MySQL.
6. Aggiornare il valore della chiave MySQLProtocol nel file web.config.

   Nell'esempio seguente viene illustrato il valore della chiave MySQLProtocol aggiornata nel file web.config.

   ```
   <add key="MySQLProtocol" value="SSL" />
   ```

7. Aggiornare il file web.config con i percorsi forniti nella sezione [client] del file my.ini.

   L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

   ```
   <add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
   ```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

8. Avviare l'applicazione Web del server SnapCenter in IIS.

Configurare connessioni MySQL protette per le configurazioni ha

È possibile generare certificati SSL (Secure Sockets Layer) e file di chiavi per i nodi ad alta disponibilità (ha) se si desidera proteggere la comunicazione tra server SnapCenter e server MySQL. È necessario configurare i certificati e i file delle chiavi nei server MySQL e nei nodi ha.

Vengono generati i seguenti certificati:

- Certificato CA

  Un certificato CA viene generato su uno dei nodi ha e questo certificato CA viene copiato nell'altro nodo ha.

- File di certificati pubblici e chiavi private del server per entrambi i nodi ha
- File di certificato pubblico del client e di chiave privata del client per entrambi i nodi ha

Fasi

1. Per il primo nodo ha, impostare i certificati SSL e i file delle chiavi per i server e i client MySQL su Windows utilizzando il comando openssl.

   Per informazioni, vedere "MySQL versione 5.7: Creazione di certificati e chiavi SSL con openssl"

   > Il valore del nome comune utilizzato per il certificato del server, il certificato del client e i file delle chiavi deve essere diverso dal valore del nome comune utilizzato per il certificato CA. Se i valori dei nomi comuni sono gli stessi, i file dei certificati e delle chiavi non funzionano per i server compilati utilizzando OpenSSL.

   Procedura consigliata: utilizzare il nome di dominio completo (FQDN) del server come nome comune per il certificato del server.

2. Copiare i certificati SSL e i file delle chiavi nella cartella MySQL Data.

   Il percorso predefinito della cartella MySQL Data è C: ProgramData/NetApp/SnapCenter/MySQL Data/Data.

3. Aggiornare il certificato CA, il certificato pubblico del server, il certificato pubblico del client, la chiave privata del server e i percorsi delle chiavi private del client nel file di configurazione del server MySQL (my.ini).

   Il percorso predefinito del file di configurazione del server MySQL (my.ini) è C:

ProgramData/NetApp/SnapCenter/MySQL Data/my.ini.

> Specificare il certificato CA, il certificato pubblico del server e i percorsi delle chiavi private del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

Specificare il certificato CA, il certificato pubblico del client e i percorsi delle chiavi private del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

L'esempio seguente mostra i certificati e i file delle chiavi copiati nella sezione [mysqld] del file my.ini nella cartella predefinita C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. Per il secondo nodo ha, copiare il certificato CA e generare il certificato pubblico del server, i file delle chiavi private del server, il certificato pubblico del client e i file delle chiavi private del client. attenersi alla procedura illustrata di seguito:

   a. Copiare il certificato CA generato sul primo nodo ha nella cartella MySQL Data del secondo nodo NLB.

      Il percorso predefinito della cartella MySQL Data è C: ProgramData/NetApp/SnapCenter/MySQL Data/Data.

      > Non è necessario creare nuovamente un certificato CA. Creare solo il certificato pubblico del server, il certificato pubblico del client, il file della chiave privata del server e il file della chiave privata del client.

b. Per il primo nodo ha, impostare i certificati SSL e i file delle chiavi per i server e i client MySQL su Windows utilizzando il comando openssl.

   "MySQL versione 5.7: Creazione di certificati e chiavi SSL con openssl"

   > Il valore del nome comune utilizzato per il certificato del server, il certificato del client e i file delle chiavi deve essere diverso dal valore del nome comune utilizzato per il certificato CA. Se i valori dei nomi comuni sono gli stessi, i file dei certificati e delle chiavi non funzionano per i server compilati utilizzando OpenSSL.

   Si consiglia di utilizzare l'FQDN del server come nome comune per il certificato del server.

c. Copiare i certificati SSL e i file delle chiavi nella cartella MySQL Data.

d. Aggiornare il certificato CA, il certificato pubblico del server, il certificato pubblico del client, la chiave privata del server e i percorsi delle chiavi private del client nel file di configurazione del server MySQL (my.ini).

   > Specificare il certificato CA, il certificato pubblico del server e i percorsi delle chiavi private del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

   Specificare il certificato CA, il certificato pubblico del client e i percorsi delle chiavi private del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

   L'esempio seguente mostra i certificati e i file delle chiavi copiati nella sezione [mysqld] del file my.ini nella cartella predefinita C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

   L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
key.pem"
```

5. Arrestare l'applicazione Web del server SnapCenter in IIS su entrambi i nodi ha.
6. Riavviare il servizio MySQL su entrambi i nodi ha.
7. Aggiornare il valore della chiave MySQLProtocol nel file web.config per entrambi i nodi ha.

   Nell'esempio seguente viene illustrato il valore della chiave MySQLProtocol aggiornata nel file web.config.

```
<add key="MySQLProtocol" value="SSL" />
```

8. Aggiornare il file web.config con i percorsi specificati nella sezione [client] del file my.ini per entrambi i nodi ha.

   L'esempio seguente mostra i percorsi aggiornati nella sezione [client] dei file my.ini.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

9. Avviare l'applicazione Web del server SnapCenter in IIS su entrambi i nodi ha.
10. Utilizzare il cmdlet Set-SmRepositoryConfig -RebuildSlave -Force PowerShell con l'opzione -Force su uno dei nodi ha per stabilire una replica MySQL sicura su entrambi i nodi ha.

    Anche se lo stato della replica è integro, l'opzione -Force consente di ricostruire il repository slave.

Funzionalità abilitate sull'host Windows durante l'installazione

Il programma di installazione del server SnapCenter abilita le funzionalità e i ruoli di Windows sull'host durante l'installazione. Questi potrebbero essere di interesse per la risoluzione dei problemi e la manutenzione del sistema host.

Categoria	Funzione
Server Web	• Internet Information Services • World Wide Web Services • Funzionalità HTTP comuni ◦ Documento predefinito ◦ Navigazione nelle directory ◦ Errori HTTP ◦ Reindirizzamento HTTP ◦ Contenuto statico ◦ Pubblicazione WebDAV • Salute e diagnostica ◦ Registrazione personalizzata ◦ Registrazione HTTP ◦ Strumenti di logging ◦ Richiedi Monitor ◦ Tracciamento • Caratteristiche delle performance ◦ Compressione del contenuto statico • Sicurezza ◦ Sicurezza IP ◦ Autenticazione di base ◦ Supporto centralizzato dei certificati SSL ◦ Autenticazione del mapping dei certificati client ◦ Autenticazione mapping certificati client IIS ◦ Limitazioni di dominio e IP ◦ Filtraggio delle richieste ◦ Autorizzazione URL ◦ Autenticazione di Windows • Funzionalità di sviluppo delle applicazioni ◦ Estendibilità di .NET 4.5 ◦ Inizializzazione dell’applicazione ◦ ASP.NET 4.7.2 ◦ Include lato server ◦ Protocollo WebSocket • Strumenti di gestione ◦ Console di gestione IIS

Categoria	Funzione
Script e strumenti di gestione IIS	• Servizio di gestione IIS • Strumenti di gestione Web
.funzionalità di NET Framework 4.7.2	• .NET Framework 4.7.2 • ASP.NET 4.7.2 • Attivazione HTTP di Windows Communication Foundation (WCF) 45 ◦ Attivazione TCP ◦ Attivazione HTTP ◦ Attivazione di message Queuing (MSMQ) Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet".
Accodamento messaggi	• Servizi di Accodamento messaggi Assicurarsi che nessun'altra applicazione utilizzi il servizio MSMQ creato e gestito da SnapCenter. • Server MSMQ
Servizio di attivazione del processo di Windows	• Modello di processo
API di configurazione	Tutto

Proteggere i database Microsoft SQL Server

Plug-in SnapCenter per Microsoft SQL Server

Panoramica del plug-in SnapCenter per Microsoft SQL Server

Il plug-in SnapCenter per Microsoft SQL Server è un componente sul lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati basata sulle applicazioni dei database Microsoft SQL Server. Il plug-in per SQL Server automatizza le operazioni di backup, verifica, ripristino e clonazione del database SQL Server nell'ambiente SnapCenter.

Una volta installato il plug-in per SQL Server, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror dei set di backup su un altro volume e con la tecnologia NetApp SnapVault per eseguire la replica del backup disk-to-disk a scopo di conformità agli standard o di archiviazione.

Operazioni che è possibile eseguire con il plug-in SnapCenter per Microsoft SQL Server

Una volta installato il plug-in SnapCenter per Microsoft SQL Server nell'ambiente, è possibile utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei database.

È possibile eseguire le seguenti attività che supportano le operazioni di backup, ripristino e clonazione dei database e delle risorse di database di SQL Server:

- Eseguire il backup dei database SQL Server e dei log delle transazioni associati

  Non è possibile creare un backup del registro per i database master e del sistema msdb. Tuttavia, è possibile creare backup di log per il database del modello di sistema.

- Ripristinare le risorse del database
  - È possibile ripristinare i database del sistema master, i database del sistema msdb e i database del sistema modello.
  - Non è possibile ripristinare più database, istanze e gruppi di disponibilità.
  - Non è possibile ripristinare il database di sistema su un percorso alternativo.
- Crea cloni point-in-time di database di produzione

  Non è possibile eseguire operazioni di backup, ripristino, clonazione e ciclo di vita dei cloni sui database del sistema tempdb.

- Verificare immediatamente le operazioni di backup o rinviare la verifica a un secondo momento

  La verifica del database di sistema di SQL Server non è supportata. SnapCenter clona i database per eseguire le operazioni di verifica. SnapCenter non è in grado di clonare i database del sistema SQL Server, pertanto la verifica di questi database non è supportata.

- Pianificazione delle operazioni di backup e clonazione

- Monitorare le operazioni di backup, ripristino e clonazione

> Il plug-in per SQL Server non supporta il backup e il ripristino dei database SQL Server sulle condivisioni SMB.

Plug-in SnapCenter per le funzionalità di Microsoft SQL Server

Il plug-in per SQL Server si integra con Microsoft SQL Server sull'host Windows e con la tecnologia Snapshot NetApp nel sistema storage. Per utilizzare il plug-in per SQL Server, utilizzare l'interfaccia SnapCenter.

Il plug-in per SQL Server include le seguenti funzionalità principali:

- **Interfaccia utente grafica unificata con tecnologia SnapCenter**

  L'interfaccia SnapCenter offre standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia di SnapCenter consente di completare processi di backup e ripristino coerenti tra i plug-in, utilizzare report centralizzati, utilizzare visualizzazioni dashboard a colpo d'occhio, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi in tutti i plug-in. SnapCenter offre inoltre la pianificazione centralizzata e la gestione delle policy per supportare le operazioni di backup e clonazione.

- **Amministrazione centrale automatizzata**

  È possibile pianificare backup di routine di SQL Server, configurare la conservazione dei backup basata su policy e impostare operazioni di ripristino point-in-time e up-to-the-minute. È inoltre possibile monitorare in modo proattivo l'ambiente SQL Server configurando SnapCenter per l'invio di avvisi e-mail.

- **Tecnologia istantanea NetApp senza interruzioni**

  Il plug-in per SQL Server utilizza la tecnologia Snapshot di NetApp con il plug-in NetApp SnapCenter per Microsoft Windows. In questo modo è possibile eseguire il backup dei database in pochi secondi e ripristinarli rapidamente senza interrompere la linea di SQL Server. Le snapshot consumano una quantità minima di spazio storage.

Oltre a queste funzionalità principali, il plug-in per SQL Server offre i seguenti vantaggi:

- Supporto del workflow di backup, ripristino, clonazione e verifica
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli
- Creazione di copie point-in-time efficienti in termini di spazio dei database di produzione per il test o l'estrazione dei dati utilizzando la tecnologia NetApp FlexClone

  È richiesta una licenza FlexClone sul sistema storage che contiene il clone.

- Verifica del backup automatica e senza interruzioni
- Possibilità di eseguire più backup contemporaneamente su più server
- Cmdlet PowerShell per lo scripting delle operazioni di backup, verifica, ripristino e clonazione
- Supporto per gruppi di disponibilità AlwaysOn (AGS) in SQL Server per accelerare le operazioni di setup AG, backup e ripristino
- Database in-memory e buffer Pool Extension (BPE) come parte di SQL Server 2014
- Supporto per il backup di LUN e dischi di macchine virtuali (VMDK)

- Supporto per infrastrutture fisiche e virtualizzate
- Supporto per iSCSI, Fibre Channel, FCoE, RDM (raw device mapping) e VMDK su NFS e VMFS

> I volumi NAS devono disporre di una policy di esportazione predefinita in SVM (Storage Virtual Machine).

- Supporto per FileStream e file group nei database standalone di SQL Server.

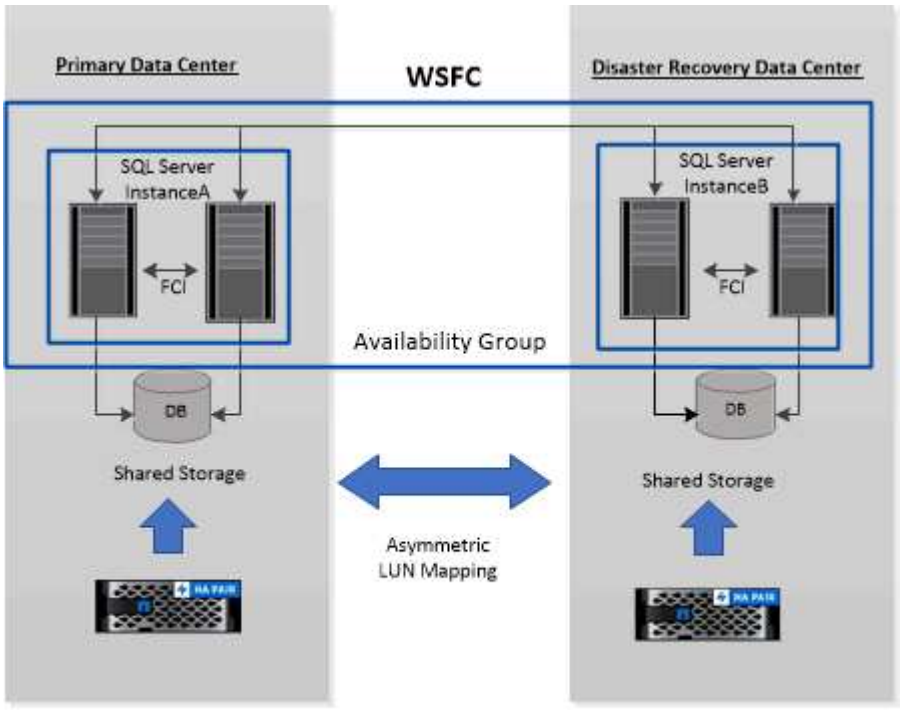
Supporto della mappatura LUN asimmetrica nei cluster Windows

Il plug-in SnapCenter per Microsoft SQL Server supporta il rilevamento in SQL Server 2012 e versioni successive, configurazioni ALM (Asymmetric LUN Mapping) per alta disponibilità e gruppi di disponibilità per il disaster recovery. Durante il rilevamento delle risorse, SnapCenter rileva i database sugli host locali e sugli host remoti nelle configurazioni ALM.

Una configurazione ALM è un singolo cluster di failover del server Windows che contiene uno o più nodi in un data center primario e uno o più nodi in un centro di disaster recovery.

Di seguito è riportato un esempio di configurazione ALM:

- Due istanze di cluster di failover (FCI) in un data center multi-sito
- FCI per ha (Local High Availability) e AG (Availability Group) per il disaster recovery con un'istanza standalone nel sito di disaster recovery



WSFC----Windows Server Failover Cluster

Lo storage nel data center primario è condiviso tra i nodi FCI presenti nel data center primario. Lo storage nel data center per il disaster recovery è condiviso tra i nodi FCI presenti nel data center per il disaster recovery.

Lo storage nel data center primario non è visibile ai nodi del data center per il disaster recovery e viceversa.

L'architettura ALM combina due soluzioni di storage condiviso utilizzate da FCI, con una soluzione di storage non condivisa o dedicata utilizzata da SQL AG. La soluzione AG utilizza lettere di unità identiche per le risorse disco condivise nei data center. Questa disposizione dello storage, in cui un disco del cluster è condiviso tra un sottoinsieme di nodi all'interno di un WSFC, viene definita ALM.

Tipi di storage supportati dai plug-in SnapCenter per Microsoft Windows e Microsoft SQL Server

SnapCenter supporta un'ampia gamma di tipi di storage su macchine fisiche e virtuali. Prima di installare il pacchetto per l'host, è necessario verificare se il supporto è disponibile per il tipo di storage in uso.

Il provisioning SnapCenter e il supporto per la protezione dei dati sono disponibili su Windows Server. Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Macchina	Tipo di storage	Eseguire il provisioning utilizzando	Note di supporto
Server fisico	LUN connessi a FC	Interfaccia grafica utente (GUI) o cmdlet PowerShell di SnapCenter	
Server fisico	LUN connessi a iSCSI	GUI SnapCenter o cmdlet PowerShell	
Server fisico	Condivisioni SMB3 (CIFS) che risiedono su una macchina virtuale di storage (SVM)	GUI SnapCenter o cmdlet PowerShell	Supporto solo per il provisioning. Non è possibile utilizzare SnapCenter per eseguire il backup di dati o condivisioni utilizzando il protocollo SMB.
Macchina virtuale VMware	LUN RDM collegati da un HBA FC o iSCSI	Cmdlet PowerShell	
Macchina virtuale VMware	LUN iSCSI collegati direttamente al sistema guest dall'iniziatore iSCSI	GUI SnapCenter o cmdlet PowerShell	
Macchina virtuale VMware	Virtual Machine file Systems (VMFS) o datastore NFS	VMware vSphere	

Macchina	Tipo di storage	Eseguire il provisioning utilizzando	Note di supporto
Macchina virtuale VMware	Un sistema guest connesso alle condivisioni SMB3 che risiedono su una SVM	GUI SnapCenter o cmdlet PowerShell	Supporto solo per il provisioning. Non è possibile utilizzare SnapCenter per eseguire il backup di dati o condivisioni utilizzando il protocollo SMB.
Macchina virtuale Hyper-V.	LUN Virtual FC (VFC) collegate da uno switch Fibre Channel virtuale	GUI SnapCenter o cmdlet PowerShell	È necessario utilizzare Hyper-V Manager per eseguire il provisioning dei LUN Virtual FC (VFC) collegati da uno switch Fibre Channel virtuale. I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti sullo storage NetApp non sono supportati.
Macchina virtuale Hyper-V.	LUN iSCSI collegati direttamente al sistema guest dall'iniziatore iSCSI	GUI SnapCenter o cmdlet PowerShell	I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti sullo storage NetApp non sono supportati.

Macchina	Tipo di storage	Eseguire il provisioning utilizzando	Note di supporto
Macchina virtuale Hyper-V.	Un sistema guest connesso alle condivisioni SMB3 che risiedono su una SVM	GUI SnapCenter o cmdlet PowerShell	Supporto solo per il provisioning. Non è possibile utilizzare SnapCenter per eseguire il backup di dati o condivisioni utilizzando il protocollo SMB. I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti sullo storage NetApp non sono supportati.

Consigli sul layout dello storage per il plug-in SnapCenter per Microsoft SQL Server

Un layout di storage ben progettato consente al server SnapCenter di eseguire il backup dei database per soddisfare gli obiettivi di recovery. Durante la definizione del layout dello storage, è necessario prendere in considerazione diversi fattori, tra cui la dimensione del database, la velocità di modifica del database e la frequenza con cui vengono eseguiti i backup.

Le sezioni seguenti definiscono le raccomandazioni e le restrizioni relative al layout dello storage per LUN e dischi di macchine virtuali (VMDK) con il plug-in SnapCenter per Microsoft SQL Server installato nell'ambiente in uso.

In questo caso, le LUN possono includere dischi VMware RDM e LUN iSCSI direct-attached mappati al guest.

Requisiti di LUN e VMDK

È possibile utilizzare facoltativamente LUN o VMDK dedicati per ottenere performance e gestione ottimali per i seguenti database:

- Database di sistema master e modello
- Tempdb
- File di database degli utenti (.mdf e .ndf)
- File di log delle transazioni del database utenti (.ldf)

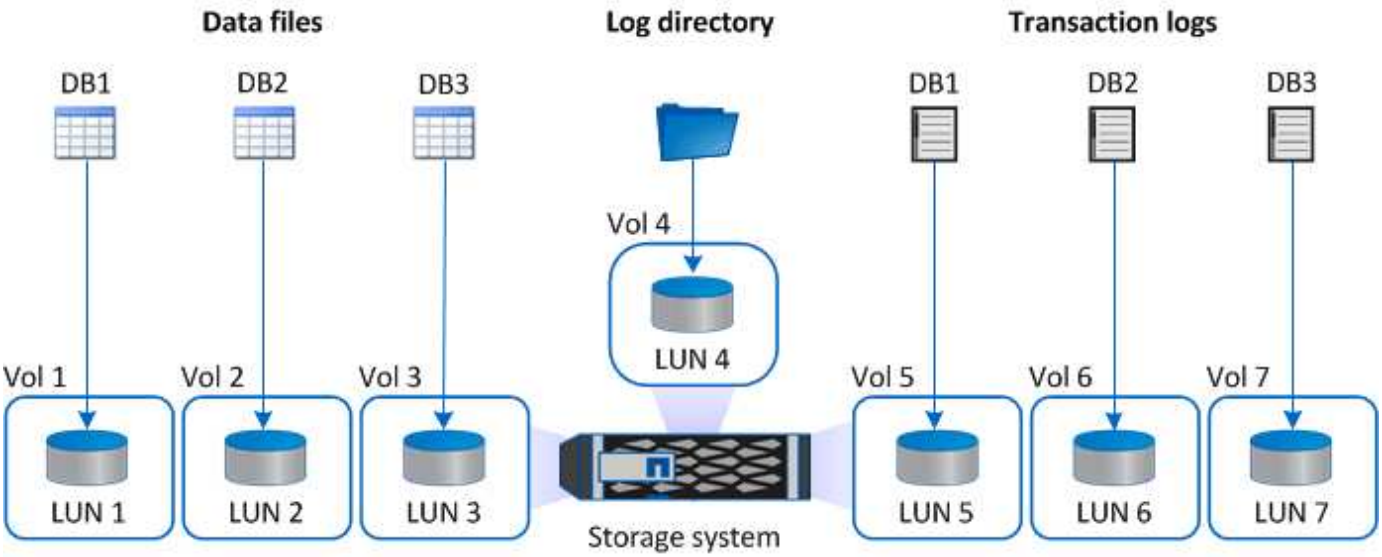
- Directory di log

Per ripristinare database di grandi dimensioni, è consigliabile utilizzare LUN o VMDK dedicati. Il tempo necessario per ripristinare un LUN o un VMDK completo è inferiore al tempo necessario per ripristinare i singoli file memorizzati nel LUN o nel VMDK.

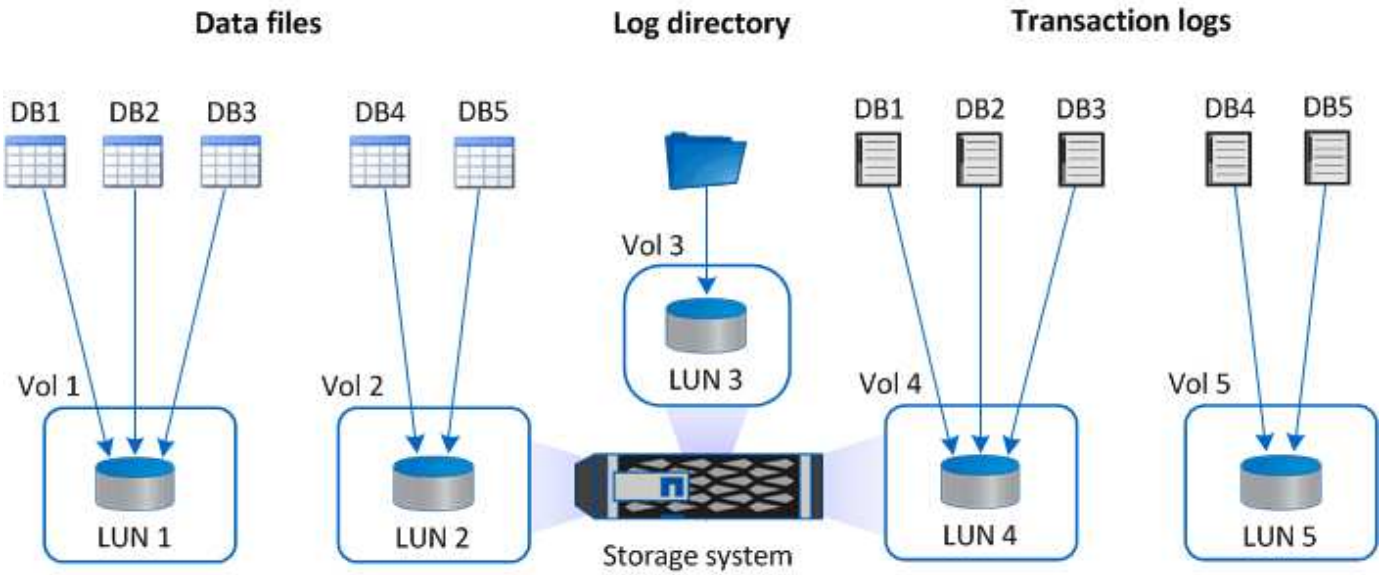
Per la directory di log, è necessario creare un LUN o VMDK separato in modo che vi sia spazio libero sufficiente nei dischi dei file di dati o di log.

Layout di esempio LUN e VMDK

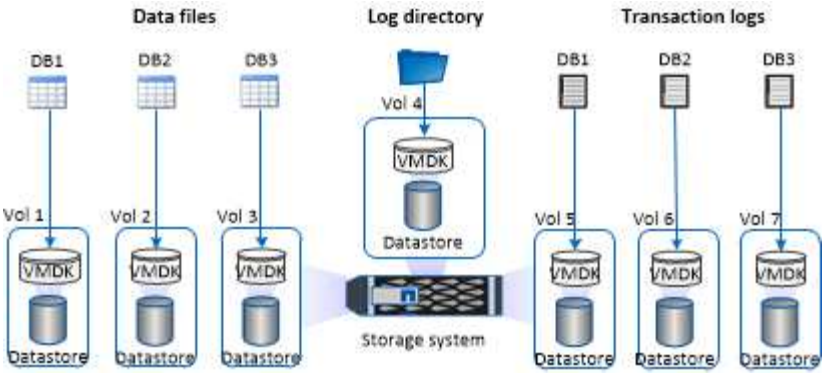
La seguente figura mostra come configurare il layout dello storage per database di grandi dimensioni su LUN:



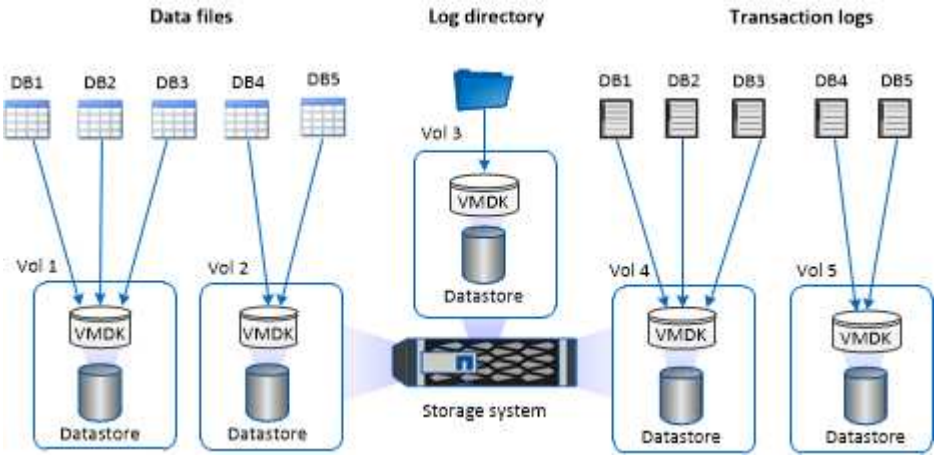
La seguente figura mostra come configurare il layout dello storage per database di medie o piccole dimensioni su LUN:



La seguente figura mostra come configurare il layout dello storage per database di grandi dimensioni su VMDK:



La seguente figura mostra come configurare il layout dello storage per database medi o piccoli su VMDK:



Privilegi minimi di ONTAP richiesti per il plug-in SQL

I privilegi minimi di ONTAP richiesti variano in base ai plug-in di SnapCenter utilizzati per la protezione dei dati.

- All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
  - event generate-autosupport-log
  - mostra la cronologia dei lavori
  - interruzione del lavoro
  - lun
  - lun create (crea lun)
  - lun delete (elimina lun)
  - lun igroup add
  - lun igroup create
  - lun igroup delete (elimina igroup lun)
  - lun igroup rename (rinomina lun igroup)
  - lun igroup show
  - lun mapping add-reporting-node
  - creazione mappatura lun

- eliminazione della mappatura lun
- nodi di remove-reporting-mapping lun
- visualizzazione della mappatura del lun
- modifica del lun
- lun move-in-volume
- lun offline
- lun online
- ridimensionamento del lun
- lun seriale
- lun show
- regola aggiuntiva del criterio snapmirror
- regola-modifica del criterio snapmirror
- regola di rimozione del criterio snapmirror
- policy di snapmirror
- ripristino di snapmirror
- spettacolo di snapmirror
- storia di snapmirror
- aggiornamento di snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione del clone del volume
- visualizzazione del clone del volume
- avvio della divisione del clone del volume
- interruzione della divisione del clone del volume
- creazione del volume
- distruggere il volume
- creazione del clone del file di volume
- file di volume show-disk-usage
- volume offline
- volume online
- modifica del volume
- creazione del qtree del volume
- eliminazione del qtree del volume
- modifica del qtree del volume
- visualizzazione del qtree del volume
- limitazione del volume

- presentazione del volume
- creazione di snapshot di volume
- eliminazione dello snapshot del volume
- modifica dello snapshot del volume
- rinominare lo snapshot del volume
- ripristino dello snapshot del volume
- file di ripristino dello snapshot del volume
- visualizzazione di snapshot di volume
- smontare il volume
- cifs vserver
- creazione condivisione cifs vserver
- eliminazione condivisione cifs vserver
- vserver cifs shadowcopy mostra
- show di condivisione di vserver cifs
- vserver cifs show
- policy di esportazione di vserver
- creazione policy di esportazione vserver
- eliminazione della policy di esportazione di vserver
- creazione della regola dei criteri di esportazione di vserver
- visualizzazione della regola dei criteri di esportazione di vserver
- visualizzazione della policy di esportazione di vserver
- iscsi vserver
- visualizzazione della connessione iscsi del vserver
- show di vserver
- interfaccia di rete
- visualizzazione dell'interfaccia di rete
- server virtuale
- spettacolo di MetroCluster

Preparare i sistemi storage per la replica di SnapMirror e SnapVault per il plug-in per SQL Server

È possibile utilizzare un plug-in SnapCenter con la tecnologia SnapMirror di ONTAP per creare copie mirror dei set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replica del backup disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti di SnapMirror e SnapVault al termine dell'operazione di Snapshot. Gli

aggiornamenti di SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter; non creare una pianificazione ONTAP separata.

Se vieni a SnapCenter da un prodotto NetApp SnapManager e sei soddisfatto delle relazioni di protezione dei dati che hai configurato, puoi saltare questa sezione.

Una relazione di protezione dei dati replica i dati sullo storage primario (il volume di origine) nello storage secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui fa riferimento il volume di origine al volume di destinazione.

SnapCenter non supporta le relazioni a cascata tra SnapMirror e i volumi SnapVault (**primario** > **Mirror** > **Vault**). Si consiglia di utilizzare le relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per ulteriori informazioni sulle relazioni di SnapMirror flessibili per la versione e sulla loro configurazione, vedere la "Documentazione ONTAP".

SnapCenter non supporta la replica **Sync_mirror**.

Strategia di backup per le risorse di SQL Server

Definire una strategia di backup per le risorse di SQL Server

La definizione di una strategia di backup prima di creare i processi di backup consente di garantire la presenza dei backup necessari per ripristinare o clonare correttamente i database. Il Service Level Agreement (SLA), l'RTO (Recovery Time Objective) e l'RPO (Recovery Point Objective) determinano in gran parte la strategia di backup.

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. L'RTO è il momento in cui un processo di business deve essere ripristinato dopo un'interruzione del servizio. Un RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di backup.

Tipo di backup supportati

Il backup dei database di sistema e utente di SQL Server mediante SnapCenter richiede la scelta del tipo di risorsa, ad esempio database, istanze di SQL Server e gruppi di disponibilità (AG). La tecnologia Snapshot viene sfruttata per creare copie online di sola lettura dei volumi in cui risiedono le risorse.

È possibile selezionare l'opzione di sola copia per specificare che SQL Server non tronca i registri delle transazioni. Utilizzare questa opzione anche quando si gestisce SQL Server con altre applicazioni di backup. Mantenendo intatti i log delle transazioni, qualsiasi applicazione di backup può ripristinare i database di sistema. I backup di sola copia sono indipendenti dalla sequenza di backup pianificati e non influiscono sulle procedure di backup e ripristino del database.

Tipo di backup	Descrizione	Opzione di sola copia con tipo di backup
Backup completo e backup dei log	Esegue il backup del database di sistema e tronca i log delle transazioni. SQL Server tronca i registri delle transazioni rimuovendo le voci già assegnate al database. Una volta completato il backup completo, questa opzione crea un log delle transazioni che acquisisce le informazioni sulle transazioni. In genere, scegliere questa opzione. Tuttavia, se il tempo di backup è breve, è possibile scegliere di non eseguire un backup del log delle transazioni con un backup completo. Non è possibile creare un backup del registro per i database master e del sistema msdb. Tuttavia, è possibile creare backup di log per il database del modello di sistema.	Esegue il backup dei file di database di sistema e dei log delle transazioni senza troncare i log. Un backup di sola copia non può fungere da base differenziale o backup differenziale e non influisce sulla base differenziale. Il ripristino di un backup completo di sola copia equivale al ripristino di qualsiasi altro backup completo.
Backup completo del database	Esegue il backup dei file di database di sistema. È possibile creare un backup completo del database per database master, modello e sistema msdb.	Esegue il backup dei file di database di sistema.
Backup del log delle transazioni	Esegue il backup dei log delle transazioni troncate, copiando solo le transazioni effettuate dopo il backup del log delle transazioni più recente. Se si pianificano backup frequenti del log delle transazioni insieme a backup completi del database, è possibile scegliere punti di ripristino granulari.	Esegue il backup dei log delle transazioni senza troncare. Questo tipo di backup non influisce sulla sequenza dei backup regolari dei log. I backup dei log di sola copia sono utili per eseguire operazioni di ripristino online.

Pianificazioni di backup per il plug-in per SQL Server

La frequenza di backup (tipo di pianificazione) viene specificata nei criteri; nella configurazione del gruppo di risorse viene specificata una pianificazione di backup. Il

fattore più critico per determinare una frequenza o una pianificazione di backup è il tasso di cambiamento per la risorsa e l'importanza dei dati. È possibile eseguire il backup di una risorsa utilizzata in modo pesante ogni ora, mentre è possibile eseguire il backup di una risorsa utilizzata raramente una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo Service Level Agreement (SLA) e il tuo Recover Point Objective (RPO).

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. Un RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA e RPO contribuiscono alla strategia di protezione dei dati.

Anche per una risorsa molto utilizzata, non è necessario eseguire un backup completo più di una o due volte al giorno. Ad esempio, i backup regolari del log delle transazioni potrebbero essere sufficienti per garantire la disponibilità dei backup necessari. Più spesso si esegue il backup dei database, minore è il numero di log delle transazioni che SnapCenter deve utilizzare al momento del ripristino, con conseguente accelerazione delle operazioni di ripristino.

Le pianificazioni dei backup sono in due parti, come segue:

- Frequenza di backup

  La frequenza di backup (con quale frequenza devono essere eseguiti i backup), denominata *tipo di pianificazione* per alcuni plug-in, fa parte di una configurazione di policy. È possibile selezionare ogni ora, ogni giorno, ogni settimana o ogni mese come frequenza di backup per la policy. Se non si seleziona una di queste frequenze, la policy creata è solo on-demand. Puoi accedere alle policy facendo clic su **Impostazioni** > **politiche**.

- Pianificazioni di backup

  Le pianificazioni di backup (esattamente quando devono essere eseguiti i backup) fanno parte di una configurazione di gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione per il backup ogni giovedì alle 10:00. È possibile accedere alle pianificazioni dei gruppi di risorse facendo clic su **risorse** > **gruppi di risorse**.

Numero di processi di backup necessari per i database

I fattori che determinano il numero di processi di backup necessari includono la dimensione del database, il numero di volumi utilizzati, la velocità di modifica del database e il contratto SLA (Service Level Agreement).

Per i backup del database, il numero di processi di backup scelto dipende in genere dal numero di volumi da cui sono posizionati i database. Ad esempio, se si posizionano un gruppo di database di piccole dimensioni su un volume e un database di grandi dimensioni su un altro volume, è possibile creare un processo di backup per i database di piccole dimensioni e un processo di backup per il database di grandi dimensioni.

Convenzioni di denominazione del backup per il plug-in per SQL Server

È possibile utilizzare la convenzione di naming predefinita di Snapshot o una convenzione di naming personalizzata. La convenzione di denominazione predefinita dei backup aggiunge un indicatore data e ora ai nomi Snapshot che consente di identificare

quando le copie sono state create.

L'istantanea utilizza la seguente convenzione di denominazione predefinita:

`resourcegroupname_hostname_timestamp`

È necessario assegnare un nome logico ai gruppi di risorse di backup, come nell'esempio seguente:

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

In questo esempio, gli elementi di sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* indica data e ora.

In alternativa, è possibile specificare il formato del nome dell'istantanea mentre si proteggono le risorse o i gruppi di risorse selezionando **Usa il formato del nome personalizzato per la copia dell'istantanea**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso dell'indicatore data e ora viene aggiunto al nome dell'istantanea.

Opzioni di conservazione del backup per il plug-in per SQL Server

È possibile scegliere il numero di giorni per i quali conservare le copie di backup o specificare il numero di copie di backup che si desidera conservare, fino a un massimo di 255 copie ONTAP. Ad esempio, l'organizzazione potrebbe richiedere di conservare 10 giorni di copie di backup o 130 copie di backup.

Durante la creazione di un criterio, è possibile specificare le opzioni di conservazione per il tipo di backup e il tipo di pianificazione.

Se si imposta la replica di SnapMirror, il criterio di conservazione viene mirrorato sul volume di destinazione.

SnapCenter elimina i backup conservati con etichette di conservazione corrispondenti al tipo di pianificazione. Se il tipo di pianificazione è stato modificato per la risorsa o il gruppo di risorse, i backup con la vecchia etichetta del tipo di pianificazione potrebbero rimanere nel sistema.

Per la conservazione a lungo termine delle copie di backup, è necessario utilizzare il backup di SnapVault.

Per quanto tempo conservare i backup del log delle transazioni sul sistema di storage di origine

Il plug-in SnapCenter per Microsoft SQL Server richiede backup del log delle transazioni per eseguire operazioni di ripristino aggiornate al minuto, che ripristinano il database a un intervallo di tempo compreso tra due backup completi.

Ad esempio, se Plug-in per SQL Server ha eseguito un backup completo alle 8:00 e un altro backup completo alle 5:00, potrebbe utilizzare l'ultimo backup del log delle transazioni per ripristinare il database in qualsiasi momento tra le 8:00 e le 5:00 se i log delle transazioni non sono disponibili, il plug-in per SQL Server è in grado di eseguire solo operazioni di ripristino point-in-time che ripristinano un database al momento in cui il

plug-in per SQL Server ha completato un backup completo.

In genere, è necessario eseguire operazioni di ripristino fino al minuto per uno o due giorni. Per impostazione predefinita, SnapCenter conserva un minimo di due giorni.

Database multipli sullo stesso volume

È possibile inserire tutti i database nello stesso volume, poiché il criterio di backup dispone di un'opzione per impostare il numero massimo di database per backup (il valore predefinito è 100).

Ad esempio, se nello stesso volume sono presenti 200 database, vengono creati due snapshot con 100 database in ciascuno dei due snapshot.

Verifica della copia di backup utilizzando il volume di storage primario o secondario per il plug-in per SQL Server

È possibile verificare le copie di backup sul volume di storage primario o sul volume di storage secondario SnapMirror o SnapVault. La verifica mediante un volume di storage secondario riduce il carico sul volume di storage primario.

Quando si verifica un backup che si trova sul volume di storage primario o secondario, tutti gli Snapshot primari e secondari vengono contrassegnati come verificati.

La licenza SnapRestore è necessaria per verificare le copie di backup su SnapMirror e sul volume di storage secondario SnapVault.

Quando pianificare i processi di verifica

Sebbene SnapCenter sia in grado di verificare i backup subito dopo averli creati, ciò può aumentare significativamente il tempo necessario per completare il processo di backup e richiede un uso intensivo di risorse. Quindi, è quasi sempre meglio pianificare la verifica in un lavoro separato per un secondo momento. Ad esempio, se si esegue il backup di un database alle 5:00 di ogni giorno, è possibile pianificare la verifica per un'ora successiva alle 6:00

Per lo stesso motivo, di solito non è necessario eseguire la verifica del backup ogni volta che si esegue un backup. L'esecuzione di verifiche a intervalli regolari ma meno frequenti è in genere sufficiente per garantire l'integrità del backup. Un singolo processo di verifica può verificare più backup contemporaneamente.

Strategia di ripristino per SQL Server

Definire una strategia di ripristino per SQL Server

La definizione di una strategia di ripristino per SQL Server consente di ripristinare correttamente il database.

Origini e destinazioni per un'operazione di ripristino

È possibile ripristinare un database SQL Server da una copia di backup sullo storage primario o secondario. È inoltre possibile ripristinare il database in diverse destinazioni

oltre alla posizione originale, consentendo di scegliere la destinazione che supporta i requisiti.

Origini di un'operazione di ripristino

È possibile ripristinare i database dallo storage primario o secondario.

Destinazioni per un'operazione di ripristino

È possibile ripristinare i database in diverse destinazioni:

Destinazione	Descrizione
La posizione originale	Per impostazione predefinita, SnapCenter ripristina il database nella stessa posizione della stessa istanza di SQL Server.
Una posizione diversa	È possibile ripristinare il database in una posizione diversa su qualsiasi istanza di SQL Server all'interno dello stesso host.
Posizione originale o diversa utilizzando nomi di database diversi	È possibile ripristinare il database con un nome diverso in qualsiasi istanza di SQL Server sullo stesso host in cui è stato creato il backup.

Il ripristino su host alternativo tra server ESX per database SQL su VMDK (datastore NFS e VMFS) non è supportato.

Modelli di ripristino di SQL Server supportati da SnapCenter

Per impostazione predefinita, a ciascun tipo di database vengono assegnati modelli di ripristino specifici. L'amministratore del database di SQL Server può riassegnare ciascun database a un modello di ripristino diverso.

SnapCenter supporta tre tipi di modelli di ripristino di SQL Server:

- Semplice modello di recovery

  Quando si utilizza il modello di ripristino semplice, non è possibile eseguire il backup dei registri delle transazioni.

- Modello di recovery completo

  Quando si utilizza il modello di ripristino completo, è possibile ripristinare un database allo stato precedente dal punto in cui si verifica un errore.

- Modello di recovery registrato in blocco

  Quando si utilizza il modello di recovery registrato in blocco, è necessario eseguire di nuovo manualmente l'operazione registrata in blocco. È necessario eseguire l'operazione di registrazione in blocco se il registro delle transazioni che contiene il record Commit dell'operazione non è stato sottoposto a backup prima del ripristino. Se l'operazione di registrazione in blocco inserisce 10 milioni di righe in un database e il

database non riesce prima di eseguire il backup del log delle transazioni, il database ripristinato non conterrà le righe inserite dall'operazione di registrazione in blocco.

Tipi di operazioni di ripristino

È possibile utilizzare SnapCenter per eseguire diversi tipi di operazioni di ripristino sulle risorse di SQL Server.

- Ripristino up-to-the-minute
- Ripristinare un punto precedente

È possibile eseguire il ripristino fino al minuto o fino a un punto precedente nelle seguenti situazioni:

- Ripristino dallo storage secondario SnapMirror o SnapVault
- Ripristina su percorso alternativo (posizione)

SnapCenter non supporta SnapRestore basato su volume.

Ripristino fino al minuto

In un'operazione di ripristino up-to-the-minute (selezionata per impostazione predefinita), i database vengono ripristinati fino al punto di errore. SnapCenter esegue questa operazione eseguendo la seguente sequenza:

1. Esegue il backup dell'ultimo log delle transazioni attivo prima di ripristinare il database.
2. Ripristina i database dal backup completo del database selezionato.
3. Applica tutti i log delle transazioni che non sono stati impegnati nei database (inclusi i log delle transazioni dei backup dal momento in cui è stato creato il backup fino all'ora più recente).

   I log delle transazioni vengono spostati in avanti e applicati a qualsiasi database selezionato.

Un'operazione di ripristino aggiornata al minuto richiede un set contiguo di log delle transazioni.

Poiché SnapCenter non è in grado di ripristinare i log delle transazioni del database SQL Server dai file di backup per la distribuzione dei log (la distribuzione dei log consente di inviare automaticamente i backup del log delle transazioni da un database primario su un'istanza del server primario a uno o più database secondari su istanze del server secondario separate), non è possibile eseguire un'operazione di ripristino aggiornata al minuto dai backup del log delle transazioni. Per questo motivo, è necessario utilizzare SnapCenter per eseguire il backup dei file di log delle transazioni del database SQL Server.

Se non è necessario mantenere una funzionalità di ripristino aggiornata al minuto per tutti i backup, è possibile configurare la conservazione del backup del log delle transazioni del sistema attraverso le policy di backup.

Esempio di un'operazione di ripristino aggiornata al minuto

Si supponga di eseguire il backup di SQL Server ogni giorno a mezzogiorno e mercoledì alle 4:00 è necessario eseguire il ripristino da un backup. Per qualche motivo, la verifica del backup da mercoledì a mezzogiorno non è riuscita, quindi si decide di eseguire il ripristino dal backup di martedì a mezzogiorno. Successivamente, se il backup viene ripristinato, tutti i log delle transazioni vengono spostati in avanti e applicati ai database ripristinati, a partire da quelli che non sono stati impegnati al momento della creazione del backup di martedì e proseguendo con l'ultimo log delle transazioni scritto mercoledì alle 4:00 (se è stato eseguito il backup dei registri delle transazioni).

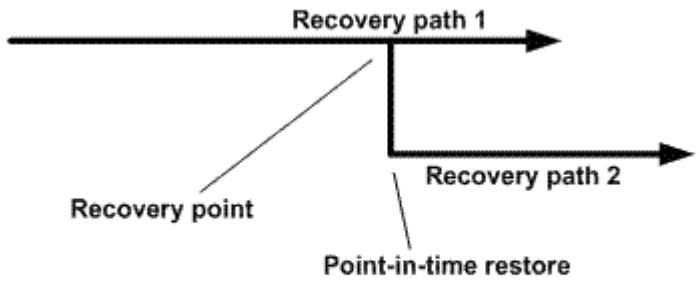
Ripristinare un punto precedente

In un'operazione di ripristino point-in-time, i database vengono ripristinati solo a un'ora specifica rispetto al passato. Un'operazione di ripristino point-in-time si verifica nelle seguenti situazioni di ripristino:

- Il database viene ripristinato a un determinato intervallo di tempo in un log delle transazioni di cui è stato eseguito il backup.
- Il database viene ripristinato e viene applicato solo un sottoinsieme di log delle transazioni di cui è stato eseguito il backup.

Il ripristino di un database a un punto nel tempo determina un nuovo percorso di ripristino.

La seguente immagine illustra i problemi che si verificano quando viene eseguita un'operazione di ripristino point-in-time:



Nell'immagine, il percorso di ripristino 1 è costituito da un backup completo seguito da diversi backup del log delle transazioni. Il database viene ripristinato a un punto temporale. I nuovi backup del log delle transazioni vengono creati dopo l'operazione di ripristino point-in-time, che determina il percorso di ripristino 2. I nuovi backup del log delle transazioni vengono creati senza creare un nuovo backup completo. A causa della corruzione dei dati o di altri problemi, non è possibile ripristinare il database corrente fino a quando non viene creato un nuovo backup completo. Inoltre, non è possibile applicare i log delle transazioni creati nel percorso di ripristino 2 al backup completo appartenente al percorso di ripristino 1.

Se si applicano i backup del log delle transazioni, è anche possibile specificare una data e un'ora particolari in cui si desidera interrompere l'applicazione delle transazioni di cui è stato eseguito il backup. A tale scopo, si specifica una data e un'ora all'interno dell'intervallo disponibile e il SnapCenter rimuove tutte le transazioni che non sono state impegnate prima di quel momento. È possibile utilizzare questo metodo per ripristinare i database a un punto temporale prima che si verificasse un danneggiamento o per eseguire il ripristino da un database accidentale o dall'eliminazione di una tabella.

Esempio di un'operazione di ripristino point-in-time

Si supponga di eseguire backup completi del database una volta a mezzanotte e un backup del log delle transazioni ogni ora. Il database si blocca alle 9:45, ma si continua a eseguire il backup dei registri delle transazioni del database guasto. È possibile scegliere tra i seguenti scenari di ripristino point-in-time:

- Ripristinare il backup completo del database eseguito a mezzanotte e accettare la perdita delle modifiche apportate successivamente. (Opzione: Nessuna)
- Ripristinare il backup completo del database e applicare tutti i backup del log delle transazioni fino alle 9:45 (opzione: Log until)

- Ripristinare il backup completo del database e applicare i backup del log delle transazioni, specificando l'ora in cui si desidera che le transazioni vengano ripristinate dall'ultimo set di backup del log delle transazioni. (Opzione: In base all'ora specifica)

In questo caso, è necessario calcolare la data e l'ora in cui è stato segnalato un determinato errore. Tutte le transazioni che non sono state impegnate prima della data e dell'ora specificate vengono rimosse.

Definire una strategia di cloning per SQL Server

La definizione di una strategia di cloning consente di clonare correttamente il database.

1. Esaminare le limitazioni relative alle operazioni di clonazione.
2. Decidere il tipo di clone desiderato.

Limitazioni delle operazioni di cloni

Prima di clonare i database, è necessario conoscere i limiti delle operazioni di clonazione.

- Se si utilizza una qualsiasi versione di Oracle dalla 11.2.0.4 alla 12.1.0.1, l'operazione di clonazione sarà in stato di sospensione quando si esegue il comando *renamedg*. È possibile applicare la patch Oracle 19544733 per risolvere questo problema.
- Non è supportata la clonazione di database da un LUN direttamente collegato a un host (ad esempio, utilizzando Microsoft iSCSI Initiator su un host Windows) a un LUN VMDK o RDM sullo stesso host Windows o su un altro host Windows o viceversa.
- La directory principale del punto di montaggio del volume non può essere una directory condivisa.
- Se si sposta un LUN che contiene un clone in un nuovo volume, il clone non può essere cancellato.

Tipi di operazioni di cloni

È possibile utilizzare SnapCenter per clonare un backup del database SQL Server o un database di produzione.

- Clonare da un backup del database

  Il database clonato può fungere da base per lo sviluppo di nuove applicazioni e aiutare a isolare gli errori delle applicazioni che si verificano nell'ambiente di produzione. Il database clonato può essere utilizzato anche per il ripristino da errori del database soft.

- Ciclo di vita dei cloni

  È possibile utilizzare SnapCenter per pianificare i lavori ricorrenti di clonazione che si verificheranno quando il database di produzione non è occupato.

Guida rapida all'installazione del plug-in SnapCenter per Microsoft SQL Server

Preparazione per l'installazione del server e del plug-in SnapCenter

Fornisce una serie di istruzioni per la preparazione dell'installazione del server SnapCenter e del plug-in SnapCenter per Microsoft SQL Server.

Requisiti di dominio e gruppo di lavoro

Il server SnapCenter può essere installato su sistemi che si trovano in un dominio o in un gruppo di lavoro.

Se si utilizza un dominio Active Directory, è necessario utilizzare un utente di dominio con diritti di amministratore locale. L'utente di dominio deve essere membro del gruppo Administrator locale sull'host Windows.

Se si utilizzano gruppi di lavoro, è necessario utilizzare un account locale con diritti di amministratore locale.

Requisiti di licenza

Il tipo di licenze installate dipende dall'ambiente in uso.

Licenza	Dove richiesto
Basato su controller standard SnapCenter	Richiesto per i controller di storage FAS o AFF La licenza standard di SnapCenter è una licenza basata su controller ed è inclusa nel pacchetto premium. Se si dispone della licenza della suite SnapManager, si ottiene anche il diritto di licenza standard SnapCenter. Se si desidera installare SnapCenter in prova con lo storage FAS o AFF, è possibile ottenere una licenza di valutazione Premium Bundle contattando il rappresentante commerciale.
SnapCenter basato sulla capacità standard	Richiesto con ONTAP Select e Cloud Volumes ONTAP Se sei un cliente Cloud Volumes ONTAP o ONTAP Select, devi procurarti una licenza per TB basata sulla capacità in base ai dati gestiti da SnapCenter. Per impostazione predefinita, SnapCenter fornisce una licenza di prova integrata per SnapCenter standard da 100 TB, valida 90 giorni. Per ulteriori informazioni, contattare il rappresentante commerciale.
SnapMirror o SnapVault	ONTAP Se la replica è attivata in SnapCenter, è necessario disporre di una licenza SnapMirror o SnapVault.
Licenze aggiuntive (opzionali)	Vedere "Licenze SnapCenter".
Licenze standard SnapCenter (opzionali)	Destinazioni secondarie Si consiglia, ma non è necessario, di aggiungere le licenze standard di SnapCenter alle destinazioni secondarie. Se le licenze standard di SnapCenter non sono abilitate sulle destinazioni secondarie, non è possibile utilizzare SnapCenter per eseguire il backup delle risorse sulla destinazione secondaria dopo aver eseguito un'operazione di failover. Tuttavia, è necessaria una licenza FlexClone sulle destinazioni secondarie per eseguire operazioni di cloning e verifica.

Requisiti di host e porte

Per i requisiti minimi di ONTAP e plug-in delle applicazioni, vedere "Tool di matrice di interoperabilità".

Host	Requisiti minimi
Sistema operativo (64 bit)	Vedere "Tool di matrice di interoperabilità"
CPU	• Host server: 4 core • Host plug-in: 1 core
RAM	• Host server: 8 GB • Host plug-in: 1 GB
Spazio su disco rigido	Host del server: • 4 GB per il software e i registri del server SnapCenter • 6 GB per repository SnapCenter • Ciascun host plug-in: 2 GB per l'installazione del plug-in e i log, necessario solo se il plug-in è installato su un host dedicato.
Librerie di terze parti	Richiesto sull'host del server SnapCenter e sull'host plug-in: • Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva
Browser	Chrome, Internet Explorer e Microsoft Edge

Tipo di porta	Porta predefinita
Porta SnapCenter	8146 (HTTPS), bidirezionale, personalizzabile, come nell'URL *https://server:8146*
Porta di comunicazione SMCore SnapCenter	8145 (HTTPS), bidirezionale, personalizzabile
Database del repository	3306 (HTTPS), bidirezionale
Host plug-in Windows	135, 445 (TCP) Oltre alle porte 135 e 445, dovrebbe essere aperto anche l'intervallo di porte dinamiche specificato da Microsoft. Le operazioni di installazione remota utilizzano il servizio WMI (Windows Management Instrumentation), che ricerca dinamicamente questo intervallo di porte. Per informazioni sull'intervallo di porte dinamiche supportato, vedere "Panoramica del servizio e requisiti della porta di rete per Windows".

Tipo di porta	Porta predefinita
Plug-in SnapCenter per Windows	8145 (HTTPS), bidirezionale, personalizzabile
Porta di comunicazione SVM o cluster ONTAP	443 (HTTPS), bidirezionale; 80 (HTTP), bidirezionale La porta viene utilizzata per la comunicazione tra l'host del server SnapCenter, l'host plug-in e SVM o il cluster ONTAP.

Requisiti del plug-in SnapCenter per Microsoft SQL Server

Si consiglia di disporre di un utente con privilegi di amministratore locale con autorizzazioni di accesso locale sull'host remoto. Se si gestiscono i nodi del cluster, è necessario disporre di un utente con privilegi amministrativi per tutti i nodi del cluster.

Si consiglia di disporre di un utente con autorizzazioni sysadmin su SQL Server. Il plug-in utilizza Microsoft VDI Framework, che richiede l'accesso sysadmin.

Installare il server SnapCenter per Microsoft SQL Server

Fornisce una serie di istruzioni di installazione per l'installazione del server SnapCenter per Microsoft SQL Server.

Fase 1: Scaricare e installare il server SnapCenter

1. Scaricare il pacchetto di installazione del server SnapCenter dal "Sito di supporto NetApp" e fare doppio clic sul file exe.

   Dopo aver avviato l'installazione, vengono eseguiti tutti i controlli preliminari e, se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati. È possibile ignorare i messaggi di avviso e procedere con l'installazione; tuttavia, gli errori dovrebbero essere corretti.

2. Esaminare i valori precompilati richiesti per l'installazione del server SnapCenter e modificarli, se necessario.

   Non è necessario specificare la password per il database del repository MySQL Server. Durante l'installazione del server SnapCenter, la password viene generata automaticamente.

   Il carattere speciale "%" non è supportato nel percorso personalizzato per l'installazione. Se si include "%" nel percorso, l'installazione non riesce.

3. Fare clic su **Installa ora**.

Fase 2: Accedere a SnapCenter

1. Avviare SnapCenter da un collegamento sul desktop host o dall'URL fornito dall'installazione (*https://server:8146* per la porta predefinita 8146 in cui è installato il server SnapCenter).
2. Immettere le credenziali.

   Per un formato nome utente amministratore di dominio incorporato, utilizzare: *NetBIOS/<username>* o *<username>@<domain>* o *<DomainFQDN>/<username>*.

Per un formato nome utente admin locale incorporato, utilizzare *<username>*.

3. Fare clic su **Accedi**.

Fase 3: Aggiunta di una licenza basata su controller standard SnapCenter

1. Accedere al controller utilizzando la riga di comando ONTAP e digitare:

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

2. Verificare la licenza:

```
license show
```

Fase 4: Aggiunta di una licenza SnapCenter basata sulla capacità

1. Nel riquadro sinistro della GUI di SnapCenter, fare clic su **Impostazioni > Software**, quindi nella sezione licenza fare clic su **+**.
2. Selezionare uno dei due metodi per ottenere la licenza:
   - Immettere le credenziali di accesso al NetApp Support Site per importare le licenze.
   - Individuare il percorso del file di licenza NetApp e fare clic su **Open** (Apri).
3. Nella pagina Notifiche della procedura guidata, utilizzare la soglia di capacità predefinita del 90%.
4. Fare clic su **fine**.

Fase 5: Configurare le connessioni del sistema di storage

1. Nel riquadro di sinistra, fare clic su **Storage Systems > New** (sistemi storage > nuovo).
2. Nella pagina Add Storage System (Aggiungi sistema di storage), eseguire le seguenti operazioni:
   a. Inserire il nome o l'indirizzo IP del sistema di storage.
   b. Inserire le credenziali utilizzate per accedere al sistema di storage.
   c. Selezionare le caselle di controllo per attivare il sistema di gestione degli eventi (EMS) e AutoSupport.
3. Fare clic su **altre opzioni** per modificare i valori predefiniti assegnati a piattaforma, protocollo, porta e timeout.
4. Fare clic su **Invia**.

Installare il plug-in SnapCenter per Microsoft SQL Server

Fornisce una serie di istruzioni di installazione per il plug-in SnapCenter per Microsoft SQL Server.

Fase 1: Impostare le credenziali Run as per installare il plug-in per Microsoft SQL Server

1. Nel riquadro di sinistra, fare clic su **Impostazioni > credenziali > nuovo**.
2. Immettere le credenziali.

   Per un formato nome utente amministratore di dominio incorporato, utilizzare: *NetBIOS/<username>* o *<username>@<domain>* o *<DomainFQDN>/<username>*.

Per un formato nome utente admin locale incorporato, utilizzare *<username>*.

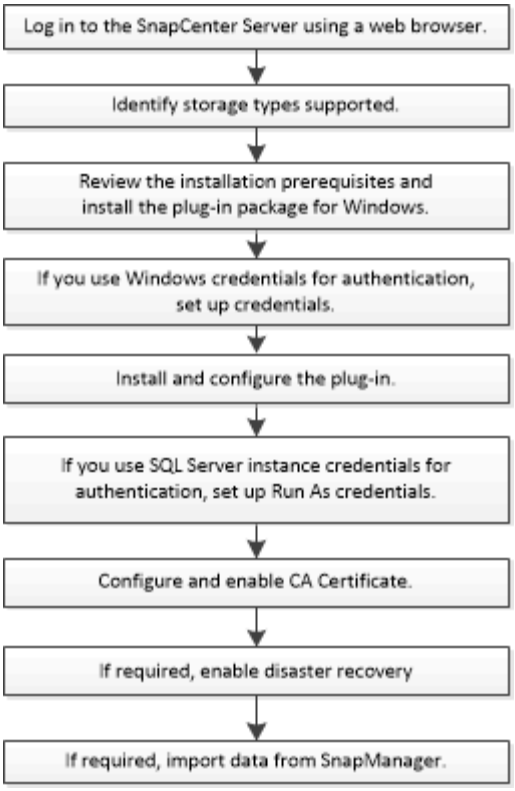
Fase 2: Aggiungere un host e installare il plug-in per Microsoft SQL Server

1. Nel riquadro sinistro della GUI di SnapCenter, fare clic su **host > host gestiti > Aggiungi**.
2. Nella pagina host della procedura guidata, eseguire le seguenti operazioni:
   a. Host Type (tipo host): Selezionare il tipo di host Windows.
   b. Host name (Nome host): Utilizzare l'host SQL o specificare l'FQDN di un host Windows dedicato.
   c. Credenziali: Selezionare il nome della credenziale valido dell'host creato o creare nuove credenziali.
3. Nella sezione Seleziona plug-in da installare, selezionare **Microsoft SQL Server**.
4. Fare clic su **altre opzioni** per specificare i seguenti dettagli:
   a. Port (porta): Mantenere il numero di porta predefinito o specificare il numero di porta.
   b. Installation Path (percorso di installazione): Il percorso predefinito è *C:/Program Files/NetApp/SnapCenter*. È possibile personalizzare il percorso.
   c. Add all hosts in the cluster (Aggiungi tutti gli host nel cluster): Selezionare questa casella di controllo se si utilizza SQL in WSFC.
   d. Ignora controlli di preinstallazione: Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente o non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.
5. Fare clic su **Invia**.

Preparare l'installazione del plug-in SnapCenter per Microsoft SQL Server

Workflow di installazione del plug-in SnapCenter per Microsoft SQL Server

Se si desidera proteggere i database di SnapCenter, è necessario installare e configurare il plug-in di SQL Server.



Prerequisiti per aggiungere host e installare il plug-in SnapCenter per Microsoft SQL Server

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario completare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È necessario disporre di un utente con privilegi di amministratore locale con autorizzazioni di accesso locale sull'host remoto.
- Se si gestiscono i nodi del cluster in SnapCenter, è necessario disporre di un utente con privilegi amministrativi per tutti i nodi del cluster.
- È necessario disporre di un utente con autorizzazioni sysadmin su SQL Server.

  Il plug-in SnapCenter per Microsoft SQL Server utilizza Microsoft VDI Framework, che richiede l'accesso sysadmin.

  "Articolo di supporto Microsoft 2926557: Le operazioni di backup e ripristino VDI di SQL Server richiedono privilegi di amministratore di sistema"

- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.
- Se SnapManager per Microsoft SQL Server è installato, è necessario aver arrestato o disattivato il servizio e le pianificazioni.

  Se si prevede di importare processi di backup o clonazione in SnapCenter, non disinstallare SnapManager per Microsoft SQL Server.

- L'host deve essere risolvibile con il nome di dominio completo (FQDN) dal server.

  Se il file hosts viene modificato in modo da renderlo risolvibile e se nel file hosts sono specificati sia il nome breve che l'FQDN, creare una voce nel file hosts di SnapCenter nel seguente formato: <ip_address> <host_fqdn> <host_name>

Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario conoscere alcuni requisiti di base relativi allo spazio del sistema host e al dimensionamento.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	5 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp". Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet."

Impostare le credenziali per il pacchetto di plug-in SnapCenter per Windows

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per l'esecuzione delle operazioni di protezione dei dati su database o file system Windows.

Prima di iniziare

- Prima di installare i plug-in, è necessario impostare le credenziali di Windows.
- È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.
- Autenticazione SQL su host Windows

  È necessario impostare le credenziali SQL dopo l'installazione dei plug-in.

  Se si implementa il plug-in SnapCenter per Microsoft SQL Server, è necessario impostare le credenziali SQL dopo l'installazione dei plug-in. Impostare una credenziale per un utente con autorizzazioni sysadmin di SQL Server.

  Il metodo di autenticazione SQL esegue l'autenticazione con un'istanza di SQL Server. Ciò significa che un'istanza di SQL Server deve essere rilevata in SnapCenter. Pertanto, prima di aggiungere una credenziale SQL, è necessario aggiungere un host, installare pacchetti plug-in e aggiornare le risorse. È necessaria l'autenticazione di SQL Server per eseguire operazioni come la pianificazione o il rilevamento delle risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.
4. Nella pagina credenziale, specificare le informazioni necessarie per la configurazione delle credenziali:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale	Immettere un nome per la credenziale.

Per questo campo…	Eseguire questa operazione…
Nome utente/Password	Immettere il nome utente e la password da utilizzare per l'autenticazione. • Amministratore di dominio Specificare l'amministratore di dominio sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Amministratore locale (solo per gruppi di lavoro) Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host. Il formato valido per il campo Nome utente è: `UserName` Non utilizzare virgolette doppie (") o backtick (`) nelle password. Non utilizzare il valore inferiore a (<) e il punto esclamativo (!) simboli insieme nelle password. Ad esempio, meno di<!10, meno di 10<!, backtick`12.
Modalità di autenticazione	Selezionare la modalità di autenticazione che si desidera utilizzare. Se si seleziona la modalità di autenticazione SQL, è necessario specificare anche l'istanza di SQL Server e l'host in cui si trova l'istanza SQL.

5. Fare clic su **OK**.

Al termine dell'impostazione delle credenziali, è possibile assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina User and Access (utenti e accesso).

Configurare le credenziali per una singola risorsa SQL Server

È possibile configurare le credenziali per eseguire processi di protezione dei dati su una singola risorsa SQL Server per ciascun utente. Sebbene sia possibile configurare le credenziali a livello globale, è possibile eseguire questa operazione solo per una risorsa specifica.

A proposito di questa attività

- Se si utilizzano credenziali Windows per l'autenticazione, è necessario impostare le credenziali prima di installare i plug-in.

  Tuttavia, se si utilizza un'istanza di SQL Server per l'autenticazione, è necessario aggiungere la credenziale dopo l'installazione dei plug-in.

- Se è stata attivata l'autenticazione SQL durante la configurazione delle credenziali, l'istanza o il database rilevato viene visualizzato con un'icona a forma di lucchetto di colore rosso.

  Se viene visualizzata l'icona del lucchetto, è necessario specificare le credenziali dell'istanza o del database per aggiungere correttamente l'istanza o il database a un gruppo di risorse.

- È necessario assegnare la credenziale a un utente RBAC (role-based access control) senza accesso sysadmin quando vengono soddisfatte le seguenti condizioni:
  - La credenziale viene assegnata a un'istanza SQL.
  - L'istanza o l'host SQL viene assegnato a un utente RBAC.

    L'utente deve disporre sia del gruppo di risorse che dei privilegi di backup.

Fase 1: Aggiungere e configurare le credenziali

1. Nel riquadro di navigazione a sinistra, selezionare **Impostazioni**.
2. Nella pagina Impostazioni, selezionare **credenziale**.
   a. Per aggiungere una nuova credenziale, selezionare **nuovo**.
   b. Nella pagina credenziale, configurare le credenziali:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale	Immettere un nome per le credenziali.
Nome utente	Immettere il nome utente utilizzato per l'autenticazione di SQL Server. • L'amministratore di dominio o qualsiasi membro del gruppo di amministratori specificano l'amministratore di dominio o qualsiasi membro del gruppo di amministratori sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo **Nome utente** sono: ◦ *NetBIOS/nome utente* ◦ *Dominio FQDN/nome utente* • Amministratore locale (solo per i gruppi di lavoro) per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host. Il formato valido per il campo **Nome utente** è: *Nome utente*
Password	Inserire la password utilizzata per l'autenticazione.

Per questo campo…	Eseguire questa operazione…
Modalità di autenticazione	Selezionare la modalità di autenticazione di SQL Server. È inoltre possibile scegliere l'autenticazione di Windows se l'utente Windows dispone dei privilegi di amministratore di sistema sul server SQL.
Host	Selezionare l'host.
Istanza di SQL Server	Selezionare l'istanza di SQL Server.

c. Selezionare **OK** per aggiungere la credenziale.

Fase 2: Configurare le istanze

1. Nel riquadro di navigazione a sinistra, selezionare **risorse**.
2. Nella pagina Resources (risorse), selezionare **Instance** (istanza) dall'elenco **View** (Visualizza).
   a. Selezionare , quindi scegliere il nome host per filtrare le istanze.
   b. Selezionare per chiudere il riquadro del filtro.
3. Nella pagina protezione istanza, proteggere l'istanza e, se necessario, selezionare **Configura credenziali**.

   Se l'utente che ha effettuato l'accesso al server SnapCenter non ha accesso al plug-in SnapCenter per Microsoft SQL Server, l'utente deve configurare le credenziali.

   L'opzione credenziale non si applica ai database e ai gruppi di disponibilità.

4. Selezionare **Aggiorna risorse**.

Configurare gMSA su Windows Server 2012 o versione successiva

Windows Server 2012 o versione successiva consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatica delle password dell'account di servizio da un account di dominio gestito.

Prima di iniziare

- È necessario disporre di un controller di dominio Windows Server 2012 o versione successiva.
- È necessario disporre di un host Windows Server 2012 o versione successiva, membro del dominio.

Fasi

1. Creare una chiave root KDS per generare password univoche per ogni oggetto in gMSA.
2. Per ciascun dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Creare e configurare gMSA:
   a. Creare un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo di utenti appena creato per creare gMSA.
```

Ad esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Eseguire `Get-ADServiceAccount` il comando per verificare
l'account del servizio.
```

4. Configurare gMSA sugli host:

   a. Attivare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

      A tale scopo, eseguire il seguente comando da PowerShell:

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

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


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

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

   a. Riavviare l'host.

   b. Installare gMSA sull'host eseguendo il comando seguente dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

   c. Verificare il proprio account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter.

Il server SnapCenter installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

Installare il plug-in SnapCenter per Microsoft SQL Server

Aggiungere host e installare il pacchetto di plug-in SnapCenter per Windows

Utilizzare la pagina SnapCenter **Aggiungi host** per aggiungere host e installare il pacchetto dei plug-in. I plug-in vengono installati automaticamente sugli host remoti.

Prima di iniziare

- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata, è necessario disattivare il controllo dell'account utente sull'host.
- Assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare account di servizio gestito di gruppo su Windows Server 2012 o versione successiva per SQL"

A proposito di questa attività

Non è possibile aggiungere un server SnapCenter come host plug-in a un altro server SnapCenter.

È possibile aggiungere un host e installare i pacchetti plug-in per un singolo host o per un cluster. Se si installano i plug-in su un cluster o su un cluster di failover di Windows Server (WSFC), i plug-in vengono installati su tutti i nodi del cluster.

Per informazioni sulla gestione degli host, vedere "Gestire gli host".

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata nella parte superiore.
3. Selezionare **Aggiungi**.
4. Nella pagina hosts:

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare Windows come tipo di host. Il server SnapCenter aggiunge l'host, quindi installa il plug-in per Windows se il plug-in non è già installato sull'host. Se si seleziona l'opzione Microsoft SQL Server nella pagina Plug-in, il server SnapCenter installa il plug-in per SQL Server.

Per questo campo…	Eseguire questa operazione…
Nome host	Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. L'indirizzo IP è supportato per gli host di dominio non attendibili solo se viene risolto nell'FQDN. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire l'FQDN. È possibile immettere gli indirizzi IP o il nome FQDN di uno dei seguenti elementi: • Host standalone • WSFC se si aggiunge un host utilizzando SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN.
Credenziali	Selezionare il nome della credenziale creata o creare nuove credenziali. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere le informazioni sulla creazione delle credenziali. È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome specificato. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

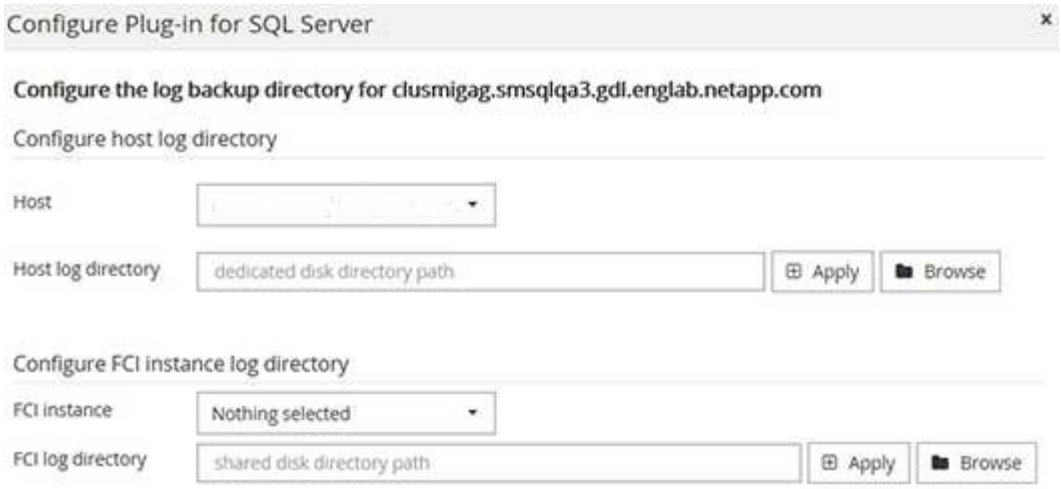
5. Nella sezione **Seleziona plug-in da installare**, selezionare i plug-in da installare.
6. Selezionare **altre opzioni**.

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.

Per questo campo…	Eseguire questa operazione…
Percorso di installazione	Il percorso predefinito è C:/Program Files/NetApp/SnapCenter. È possibile personalizzare il percorso.
Aggiungere tutti gli host nel cluster	Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un WSFC o in un gruppo di disponibilità SQL. Per gestire e identificare più gruppi di disponibilità SQL disponibili all'interno di un cluster, è necessario aggiungere tutti i nodi del cluster selezionando la casella di controllo cluster appropriata nella GUI.
Ignorare i controlli di preinstallazione	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.
Utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in	Selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in. Fornire il nome gMSA nel seguente formato: Nome dominio/nome account. Se l'host viene aggiunto con gMSA e gMSA dispone dei privilegi di login e di amministratore di sistema, gMSA verrà utilizzato per connettersi all'istanza SQL.

7. Selezionare **Invia**.
8. Per il plug-in SQL, selezionare l'host per configurare la directory del registro.
   a. Selezionare **Configure log directory** e nella pagina Configure host log directory, selezionare **Browse** (Sfoglia) e completare la seguente procedura:

      Solo i LUN (dischi) NetApp sono elencati per la selezione. SnapCenter esegue il backup e replica della directory del registro host come parte dell'operazione di backup.



i. Selezionare la lettera dell'unità o il punto di montaggio sull'host in cui verrà memorizzato il log dell'host.

ii. Scegliere una sottodirectory, se necessario.

iii. Selezionare **Salva**.

9. Selezionare **Invia**.

   Se non è stata selezionata la casella di controllo **Ignora controlli preliminari**, l'host viene convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione PowerShell, . La versione NET, la posizione (per i plug-in Windows) e la versione Java (per i plug-in Linux) sono convalidate in base ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati.

   Se l'errore riguarda lo spazio su disco o la RAM, è possibile aggiornare il file web.config che si trova in C: File di programma NetApp SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione ha, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

10. Monitorare l'avanzamento dell'installazione.

Installare il plug-in SnapCenter per Microsoft SQL Server su più host remoti utilizzando i cmdlet

È possibile installare il plug-in SnapCenter per Microsoft SQL Server su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage PowerShell.

Prima di iniziare

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto del plug-in.

Fasi

1. Avviare PowerShell.
2. Sull'host del server SnapCenter, stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in SnapCenter per Microsoft SQL Server su più host remoti utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserire le credenziali per l'installazione remota.

Installare il plug-in SnapCenter per Microsoft SQL Server in modo invisibile dalla riga di comando

Installare il plug-in SnapCenter per Microsoft SQL Server dall'interfaccia utente di SnapCenter. Tuttavia, se per qualche motivo non è possibile eseguire il programma di installazione del plug-in per SQL Server in modalità automatica dalla riga di comando di Windows.

Prima di iniziare

- Prima di eseguire l'installazione, è necessario eliminare la versione precedente del plug-in SnapCenter per Microsoft SQL Server.

  Per ulteriori informazioni, vedere "Come installare un plug-in SnapCenter manualmente e direttamente dall'host del plug-in".

Fasi

1. Verificare se la cartella C:/temp esiste sull'host del plug-in e se l'utente connesso ha accesso completo a tale cartella.
2. Scaricare il plug-in per il software SQL Server da C: ProgramData/NetApp/SnapCenter/Package Repository.

   Questo percorso è accessibile dall'host in cui è installato il server SnapCenter.

3. Copiare il file di installazione nell'host su cui si desidera installare il plug-in.
4. Dal prompt dei comandi di Windows sull'host locale, accedere alla directory in cui sono stati salvati i file di installazione del plug-in.
5. Installare il plug-in per il software SQL Server:

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

   Sostituire i valori segnaposto con i dati

   - Debug_Log_Path è il nome e la posizione del file di log del programma di installazione della suite.
   - Log_Path è la posizione dei log di installazione dei componenti plug-in (SCW, SCSQL e SMCore).
   - Num è la porta su cui SnapCenter comunica con SMCore
   - Install_Directory_Path è la directory di installazione del pacchetto del plug-in host.
   - Dominio/amministratore è il plug-in SnapCenter per l'account del servizio Web Microsoft Windows.

◦ Password è la password dell'account del servizio Web del plug-in SnapCenter per Microsoft Windows.

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

Tutti i parametri passati durante l'installazione del plug-in per SQL Server sono sensibili al maiuscolo/minuscolo.

6. Monitorare il Task Scheduler di Windows, il file di log dell'installazione principale C: Installdebug.log e i file di installazione aggiuntivi in C:
7. Monitorare la directory %temp% per verificare che i programmi di installazione msiexe.exe stiano installando il software senza errori.

L'installazione del plug-in per SQL Server registra il plug-in sull'host e non sul server SnapCenter. È possibile registrare il plug-in sul server SnapCenter aggiungendo l'host utilizzando l'interfaccia grafica di SnapCenter o il cmdlet PowerShell. Una volta aggiunto l'host, il plug-in viene rilevato automaticamente.

Monitorare lo stato di installazione del plug-in per SQL Server

È possibile monitorare lo stato di avanzamento dell'installazione del pacchetto plug-in di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento dell'installazione per determinare quando è completa o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filter** (filtro).
   b. Facoltativo: Specificare la data di inizio e di fine.
   c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).
   d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.

e. Fare clic su **Apply** (Applica).

4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Configurare il certificato CA

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare una CSR, vedere "Come generare il file CSR del certificato CA".

Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Formato del file di importazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
   c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
   d. Copiare i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

      Get-ChildItem -Path Certate: LocalMachine/My

   b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

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

   Ad esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in
   dell'host Windows eseguendo i seguenti comandi:
   ```

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

   Ad esempio:

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

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.

5. Selezionare **attiva convalida certificato**.

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- * * Indica che il certificato CA non è né abilitato né assegnato all'host del plug-in.
- * * Indica che il certificato CA è stato convalidato correttamente.
- * * Indica che il certificato CA non può essere convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Configurare il disaster recovery

Disaster recovery del plug-in SnapCenter per SQL Server

Quando il plug-in SnapCenter per SQL Server non è disponibile, attenersi alla seguente procedura per passare a un host SQL diverso e ripristinare i dati.

Prima di iniziare

- L'host secondario deve avere lo stesso sistema operativo, l'applicazione e il nome host dell'host primario.
- Trasferire il plug-in SnapCenter per SQL Server a un host alternativo utilizzando la pagina **Aggiungi host** o **Modifica host**. Per ulteriori informazioni, vedere "Gestire gli host" .

Fasi

1. Selezionare l'host dalla pagina **hosts** per modificare e installare il plug-in SnapCenter per SQL Server.
2. (Facoltativo) sostituire il plug-in SnapCenter per i file di configurazione di SQL Server dal backup di disaster recovery (DR) al nuovo computer.
3. Importare pianificazioni Windows e SQL dalla cartella del plug-in SnapCenter per SQL Server dal backup DR.

Informazioni correlate

Vedere il "API di disaster recovery" video.

Disaster recovery (DR) dello storage per il plug-in SnapCenter per SQL Server

È possibile ripristinare il plug-in SnapCenter per lo storage SQL Server attivando la modalità DR per lo storage nella pagina Impostazioni globali.

Prima di iniziare

- Assicurarsi che i plug-in siano in modalità di manutenzione.
- Interrompere la relazione SnapMirror/SnapVault. "Interrompere le relazioni con SnapMirror"
- Collegare il LUN da secondario al computer host con la stessa lettera di unità.
- Assicurarsi che tutti i dischi siano collegati utilizzando le stesse lettere di unità utilizzate prima del DR.

- Riavviare il servizio del server MSSQL.
- Assicurarsi che le risorse SQL siano di nuovo in linea.

A proposito di questa attività

Il disaster recovery (DR) non è supportato nelle configurazioni VMDK e RDM.

Fasi

1. Nella pagina Settings (Impostazioni), selezionare **Settings** (Impostazioni) > **Global Settings** (Impostazioni globali) > **Disaster Recovery**.
2. Selezionare **Enable Disaster Recovery** (attiva Disaster Recovery).
3. Fare clic su **Apply** (Applica).
4. Verificare se il processo DR è attivato o meno facendo clic su **Monitor** > **Jobs**.

Al termine

- Se vengono creati nuovi database dopo il failover, i database saranno in modalità non DR.

  I nuovi database continueranno a funzionare come prima del failover.

- I nuovi backup creati in modalità DR saranno elencati in SnapMirror o SnapVault (secondario) nella pagina topologia.

  Accanto ai nuovi backup viene visualizzata l'icona "i" per indicare che questi backup sono stati creati durante la modalità DR.

- È possibile eliminare il plug-in SnapCenter per i backup di SQL Server creato durante il failover utilizzando l'interfaccia utente o il seguente cmdlet: `Remove-SmBackup`
- Dopo il failover, se si desidera che alcune risorse siano in modalità non DR, utilizzare il cmdlet seguente: `Remove-SmResourceDRMode`

  Per ulteriori informazioni, fare riferimento alla "Guida di riferimento al cmdlet del software SnapCenter".

- Il server SnapCenter gestirà le singole risorse di storage (database SQL) in modalità DR o non DR, ma non il gruppo di risorse con risorse di storage in modalità DR o non DR.

Failback dal plug-in SnapCenter per lo storage secondario SQL Server allo storage primario

Una volta che il plug-in SnapCenter per lo storage primario di SQL Server è tornato online, è necessario eseguire il failback allo storage primario.

Prima di iniziare

- Impostare il plug-in SnapCenter per SQL Server in modalità **manutenzione** dalla pagina host gestiti.
- Scollegare lo storage secondario dall'host e connettersi allo storage primario.
- Per eseguire il failback allo storage primario, assicurarsi che la direzione della relazione rimanga la stessa di prima del failover eseguendo l'operazione di risincronizzazione inversa.

  Per mantenere i ruoli dello storage primario e secondario dopo l'operazione di risincronizzazione inversa, eseguire nuovamente l'operazione di risincronizzazione inversa.

  Per ulteriori informazioni, vedere "Risincronizzazione inversa delle relazioni mirror"

- Riavviare il servizio del server MSSQL.
- Assicurarsi che le risorse SQL siano di nuovo in linea.

> Durante il failover o il failback del plug-in, lo stato generale del plug-in non viene aggiornato immediatamente. Lo stato generale dell'host e del plug-in viene aggiornato durante la successiva operazione di refresh dell'host.

Fasi

1. Nella pagina Settings (Impostazioni), selezionare **Settings** (Impostazioni) > **Global Settings** (Impostazioni globali) > **Disaster Recovery**.
2. Deselezionare **Enable Disaster Recovery**.
3. Fare clic su **Apply** (Applica).
4. Verificare se il processo DR è attivato o meno facendo clic su **Monitor** > **Jobs**.

Al termine

È possibile eliminare il plug-in SnapCenter per i backup di SQL Server creato durante il failover utilizzando l'interfaccia utente o il seguente cmdlet: `Remove-SmDRFailoverBackups`

Installare il plug-in SnapCenter per VMware vSphere

Se il database o il file system sono memorizzati su macchine virtuali (VM), o se si desidera proteggere macchine virtuali e datastore, è necessario implementare il plug-in SnapCenter per l'appliance virtuale VMware vSphere.

Per informazioni sulla distribuzione, vedere "Panoramica sull'implementazione".

Implementare il certificato CA

Per configurare il certificato CA con il plug-in SnapCenter per VMware vSphere, vedere "Creare o importare un certificato SSL".

Configurare il file CRL

Il plug-in SnapCenter per VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il plug-in SnapCenter per VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Prepararsi alla protezione dei dati

Prerequisiti per l'utilizzo del plug-in SnapCenter per Microsoft SQL Server

Prima di iniziare a utilizzare il plug-in per SQL Server, l'amministratore di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività dei prerequisiti.

- Installare e configurare il server SnapCenter.
- Accedere a SnapCenter.

- Configurare l'ambiente SnapCenter aggiungendo o assegnando connessioni al sistema di storage e creando credenziali.

  > SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM supportata da SnapCenter deve avere un nome univoco.

- Aggiungere host, installare i plug-in, individuare (aggiornare) le risorse e configurare i plug-in.
- Spostare un database Microsoft SQL Server esistente da un disco locale a un LUN NetApp o viceversa eseguendo Invoke-SmConfigureResources.

  Per informazioni sull'esecuzione del cmdlet, consultare la "Guida di riferimento al cmdlet del software SnapCenter"

- Se si utilizza il server SnapCenter per proteggere i database SQL che risiedono su LUN o VMDM VMware, è necessario implementare il plug-in SnapCenter per VMware vSphere e registrare il plug-in con SnapCenter. Il plug-in SnapCenter per la documentazione di VMware vSphere contiene ulteriori informazioni.

  "Plug-in SnapCenter per la documentazione di VMware vSphere"

- Eseguire il provisioning dello storage sul lato host utilizzando il plug-in SnapCenter per Microsoft Windows.
- Impostare le relazioni di SnapMirror e SnapVault, se si desidera eseguire la replica del backup.

Per ulteriori informazioni, vedere le informazioni sull'installazione di SnapCenter.

Per gli utenti di SnapCenter 4.1.1, la documentazione del plug-in SnapCenter per VMware vSphere 4.1.1 contiene informazioni sulla protezione dei database e dei file system virtualizzati. Per gli utenti di SnapCenter 4.2.x, NetApp Data Broker 1.0 e 1.0.1, la documentazione contiene informazioni sulla protezione dei database virtualizzati e dei file system mediante il plug-in SnapCenter per VMware vSphere fornito dall'appliance virtuale NetApp Data Broker basata su Linux (formato di appliance virtuale aperta). Per gli utenti di SnapCenter 4.3.x, la documentazione relativa al plug-in SnapCenter per VMware vSphere 4.3 contiene informazioni sulla protezione dei database e dei file system virtualizzati mediante il plug-in SnapCenter basato su Linux per l'appliance virtuale VMware vSphere (formato appliance virtuale aperta).

"Plug-in SnapCenter per la documentazione di VMware vSphere"

Utilizzo di risorse, gruppi di risorse e policy per la protezione di SQL Server

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- In genere, le risorse sono database, istanze di database o gruppi di disponibilità di Microsoft SQL Server di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è un insieme di risorse su un host o cluster.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

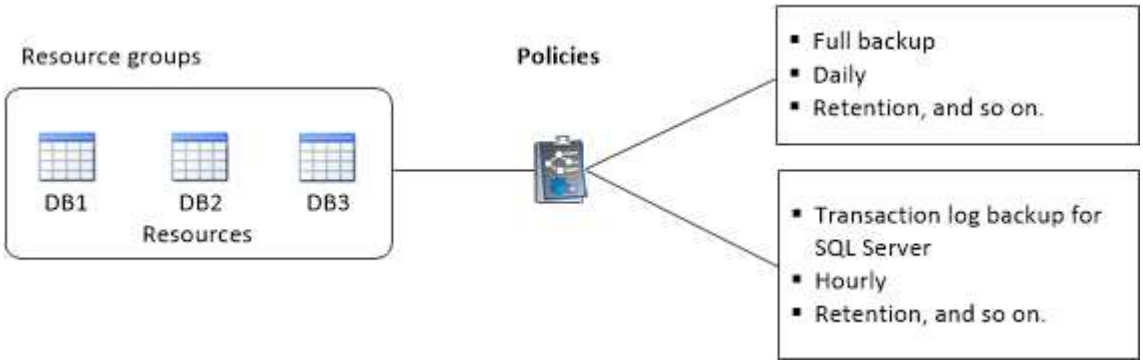
  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È inoltre possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- I criteri specificano la frequenza di backup, la conservazione delle copie, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano uno o più criteri per tale gruppo. È inoltre possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

Un gruppo di risorse definisce *cosa* si desidera proteggere e quando si desidera proteggerlo in termini di giorno e ora. Pensa a una policy come a definire *come* la vuoi proteggere. Ad esempio, se si esegue il backup di tutti i database o di tutti i file system di un host, è possibile creare un gruppo di risorse che includa tutti i database o tutti i file system dell'host. È quindi possibile associare due criteri al gruppo di risorse: Una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si allegano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno e un altro programma che esegua i backup del registro ogni ora.

L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i database:



Eseguire il backup del database, dell'istanza o del gruppo di disponibilità di SQL Server

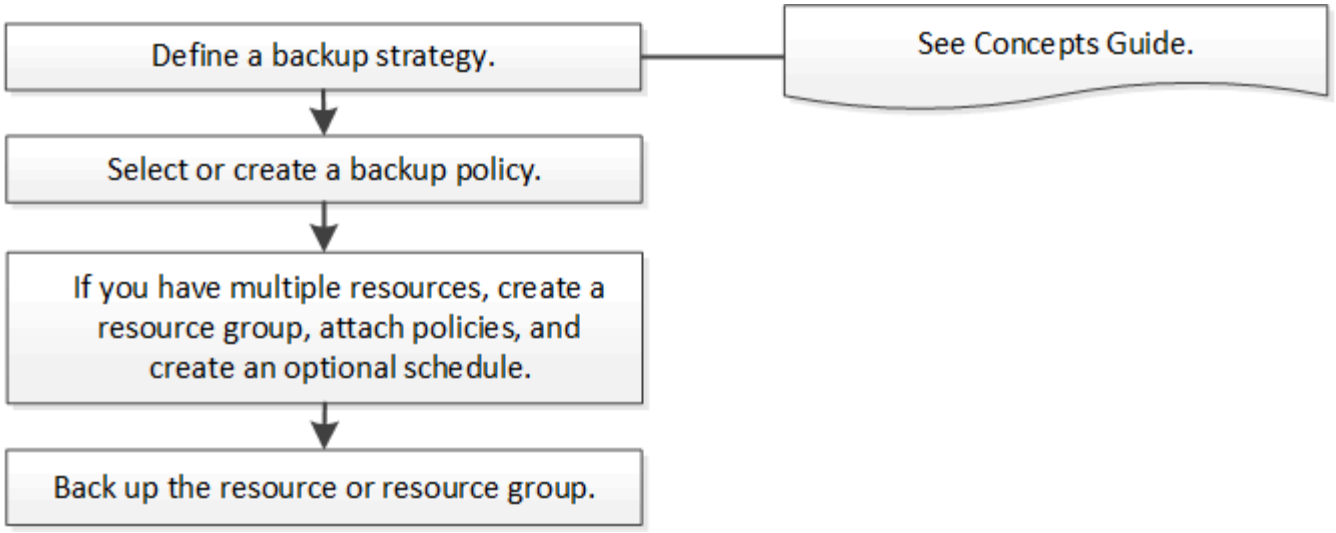
Workflow di backup

Quando si installa il plug-in SnapCenter per Microsoft SQL Server nell'ambiente in uso, è possibile utilizzare SnapCenter per eseguire il backup delle risorse di SQL Server.

È possibile pianificare più backup per l'esecuzione simultanea tra i server.

Le operazioni di backup e ripristino non possono essere eseguite contemporaneamente sulla stessa risorsa.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di backup:



Le opzioni Backup Now (Backup ora), Restore (Ripristina), Manage Backup (Gestisci backup) e Clone (Clona) nella pagina Resources (risorse) sono disattivate se si seleziona un LUN non NetApp, un database danneggiato o un database da ripristinare.

È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino, ripristino, verifica e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida dei cmdlet di SnapCenter o vedere la "Guida di riferimento al cmdlet del software SnapCenter"

Come SnapCenter esegue il backup dei database

SnapCenter utilizza la tecnologia Snapshot per eseguire il backup dei database di SQL Server che risiedono su LUN o VMDK. SnapCenter crea il backup creando istantanee dei database.

Quando si seleziona un database per un backup completo del database dalla pagina risorse, SnapCenter seleziona automaticamente tutti gli altri database che risiedono nello stesso volume di storage. Se il LUN o VMDK memorizza solo un singolo database, è possibile cancellare o riselezionare il database singolarmente. Se il LUN o il VMDK ospita più database, è necessario cancellare o riselezionare i database come gruppo.

Viene eseguito il backup di tutti i database che risiedono su un singolo volume contemporaneamente utilizzando Snapshot. Se il numero massimo di database di backup simultanei è 35 e se più di 35 database risiedono in un volume di archiviazione, il numero totale di snapshot creati corrisponde al numero di database diviso per 35.

È possibile configurare il numero massimo di database per ciascuna istantanea nel criterio di backup.

Quando SnapCenter crea una Snapshot, l'intero volume del sistema storage viene acquisito nella Snapshot. Tuttavia, il backup è valido solo per il server host SQL per il quale è stato creato il backup.

Se i dati di altri server host SQL si trovano sullo stesso volume, non è possibile ripristinarli dalla Snapshot.

Ulteriori informazioni

"Eseguire il backup delle risorse utilizzando i cmdlet PowerShell"

"Le operazioni di quiesce o raggruppamento delle risorse non riescono"

Determinare se le risorse sono disponibili per il backup

Le risorse sono i database, le istanze dell'applicazione, i gruppi di disponibilità e i componenti simili gestiti dai plug-in installati. È possibile aggiungere tali risorse ai gruppi di risorse in modo da poter eseguire lavori di protezione dei dati, ma prima occorre identificare le risorse disponibili. La determinazione delle risorse disponibili verifica inoltre che l'installazione del plug-in sia stata completata correttamente.

Prima di iniziare

- È necessario aver già completato attività come l'installazione del server SnapCenter, l'aggiunta di host, la creazione di connessioni al sistema di storage e l'aggiunta di credenziali.
- Per rilevare i database Microsoft SQL, è necessario soddisfare una delle seguenti condizioni.
  - L'utente utilizzato per aggiungere l'host del plug-in al server SnapCenter deve disporre delle autorizzazioni necessarie (sysadmin).
  - Se la suddetta condizione non viene soddisfatta, nel server SnapCenter è necessario configurare l'utente che dispone delle autorizzazioni necessarie (sysadmin). L'utente deve essere configurato a livello di istanza di Microsoft SQL Server e può essere un utente SQL o Windows.
- Per rilevare i database Microsoft SQL in un cluster Windows, è necessario sbloccare la porta TCP/IP FCI (failover Cluster Instance).
- Se i database risiedono su LUN o VMDK VMware RDM, è necessario implementare il plug-in SnapCenter per VMware vSphere e registrare il plug-in con SnapCenter.

  Per ulteriori informazioni, vedere "Implementare il plug-in SnapCenter per VMware vSphere"
- Se l'host viene aggiunto con gMSA e gMSA dispone dei privilegi di accesso e amministratore di sistema, gMSA verrà utilizzato per connettersi all'istanza SQL.

A proposito di questa attività

Non è possibile eseguire il backup dei database se l'opzione **Stato generale** nella pagina Dettagli è impostata su non disponibile per il backup. L'opzione **Stato generale** è impostata su non disponibile per il backup quando si verifica una delle seguenti condizioni:

- I database non si trovano su un LUN NetApp.
- I database non sono in stato normale.

  I database non sono in stato normale quando sono offline, ripristinati, in sospeso, sospetti e così via.
- I database non dispongono di privilegi sufficienti.

  Ad esempio, se un utente ha solo accesso di visualizzazione al database, i file e le proprietà del database non possono essere identificati e quindi non può essere eseguito il backup.

> SnapCenter può eseguire il backup solo del database primario se si dispone di una configurazione del gruppo di disponibilità nell'edizione standard di SQL Server.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **Database**, **Instance** o **Availability Group** dall'elenco a discesa **View**.

Fare clic su e selezionare il nome host e l'istanza SQL Server per filtrare le risorse. È quindi possibile fare clic su per chiudere il riquadro del filtro.

3. Fare clic su **Aggiorna risorse**.

   Le risorse appena aggiunte, rinominate o eliminate vengono aggiornate nell'inventario del server SnapCenter.

   È necessario aggiornare le risorse se i database vengono rinominati al di fuori di SnapCenter.

   Le risorse vengono visualizzate insieme a informazioni quali tipo di risorsa, nome host o cluster, gruppi di risorse associati, tipo di backup, criteri e stato generale.

   - Se il database si trova su un'unità di archiviazione non NetApp, `Not available for backup` viene visualizzato nella colonna **Stato generale**.

     Non è possibile eseguire operazioni di protezione dei dati su un database su uno storage non NetApp.

   - Se il database si trova su un'unità di archiviazione NetApp e non è protetto, `Not protected` viene visualizzato nella colonna **Stato generale**.
   - Se il database si trova su un sistema di archiviazione NetApp e protetto, l'interfaccia utente visualizza il `Backup not run` messaggio nella colonna **Stato generale**.
   - Se il database si trova su un sistema di archiviazione NetApp e è protetto e se il backup viene attivato per il database, l'interfaccia utente visualizza il `Backup succeeded` messaggio nella colonna **Stato generale**.

   Se è stata attivata un'autenticazione SQL durante la configurazione delle credenziali, l'istanza o il database rilevato viene visualizzato con un'icona a forma di lucchetto rosso. Se viene visualizzata l'icona del lucchetto, è necessario specificare le credenziali dell'istanza o del database per aggiungere correttamente l'istanza o il database a un gruppo di risorse.

1. Dopo che l'amministratore di SnapCenter ha assegnato le risorse a un utente RBAC, l'utente RBAC deve effettuare l'accesso e fare clic su **Aggiorna risorse** per visualizzare l'ultimo **Stato complessivo** delle risorse.

Migrazione delle risorse al sistema storage NetApp

Dopo aver eseguito il provisioning del sistema storage NetApp utilizzando il plug-in SnapCenter per Microsoft Windows, è possibile migrare le risorse al sistema storage NetApp o da un LUN NetApp a un altro LUN NetApp utilizzando l'interfaccia grafica utente (GUI) SnapCenter o i cmdlet PowerShell.

Prima di iniziare

- È necessario aggiungere sistemi storage al server SnapCenter.
- È necessario aggiornare (rilevare) le risorse di SQL Server.

La maggior parte dei campi presenti in queste pagine della procedura guidata sono esplicativi. Le seguenti informazioni descrivono alcuni dei campi per i quali potrebbe essere necessaria una guida.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Instance** dall'elenco a discesa **View** (Visualizza).
3. Selezionare il database o l'istanza dall'elenco e fare clic su **Migra**.
4. Nella pagina risorse, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome database (opzionale)	Se è stata selezionata un'istanza per la migrazione, è necessario selezionare i database di tale istanza dall'elenco a discesa **Database**.
Scegliere le destinazioni	Selezionare la posizione di destinazione per i file di dati e di log. I file di dati e di log vengono spostati rispettivamente nella cartella Data e Log sotto l'unità NetApp selezionata. Se non è presente alcuna cartella nella struttura di cartelle, viene creata una cartella e la risorsa viene migrata.
Mostra dettagli file di database (opzionale)	Selezionare questa opzione se si desidera migrare più file di un singolo database. Questa opzione non viene visualizzata quando si seleziona la risorsa **istanza**.
Opzioni	Selezionare **Delete copy of migrated Database at Original Location** (Elimina copia del database migrato nella posizione originale) per eliminare la copia del database dall'origine. Facoltativo: **ESEGUIRE LE STATISTICHE DI AGGIORNAMENTO sulle tabelle prima di scollegare il database**.

5. Nella pagina di verifica, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Opzioni di verifica della coerenza del database	Selezionare **Esegui prima** per verificare l'integrità del database prima della migrazione. Selezionare **Esegui dopo** per verificare l'integrità del database dopo la migrazione.

Per questo campo…	Eseguire questa operazione…
DBCC CHECKDB options	• Selezionare l'opzione **PHYSICAL_ONLY** per limitare il controllo dell'integrità alla struttura fisica del database e rilevare pagine lacerate, errori di checksum e guasti hardware comuni che influiscono sul database. • Selezionare l'opzione **NO_INFOMSGS** per eliminare tutti i messaggi informativi. • Selezionare l'opzione **ALL_ERRORMSGS** per visualizzare tutti gli errori segnalati per oggetto. • Selezionare l'opzione **NOINDEX** se non si desidera controllare gli indici non in cluster. Il database SQL Server utilizza Microsoft SQL Server Database Consistency Checker (DBCC) per verificare l'integrità fisica e logica degli oggetti nel database. Selezionare questa opzione per ridurre il tempo di esecuzione. • Selezionare l'opzione **TABLOCK** per limitare i controlli e ottenere i blocchi invece di utilizzare un'istantanea del database interna.

6. Esaminare il riepilogo, quindi fare clic su **fine**.

Creare criteri di backup per i database di SQL Server

È possibile creare un criterio di backup per la risorsa o il gruppo di risorse prima di utilizzare SnapCenter per eseguire il backup delle risorse di SQL Server oppure creare un criterio di backup al momento della creazione di un gruppo di risorse o del backup di una singola risorsa.

Prima di iniziare

- Devi aver definito la tua strategia di protezione dei dati.
- Devi essere preparato per la protezione dei dati completando attività come l'installazione di SnapCenter, l'aggiunta di host, l'identificazione delle risorse e la creazione di connessioni al sistema di storage.
- È necessario aver configurato la directory del registro host per il backup del registro.
- È necessario aggiornare (rilevare) le risorse di SQL Server.
- Se si stanno replicando Snapshot in un mirror o un vault, l'amministratore della SnapCenter deve aver assegnato le Storage Virtual Machine (SVM) per entrambi i volumi di origine e di destinazione.

  Per informazioni sulle modalità di assegnazione delle risorse agli utenti da parte degli amministratori, consultare le informazioni di installazione di SnapCenter.

- Se si desidera eseguire gli script PowerShell in prescripts e postscripts, impostare il valore del parametro usePowershellProcessforScripts su true nel file web.config.

Il valore predefinito è false.

- Per SnapMirror Business Continuity (SM-BC), per ulteriori informazioni sui prerequisiti e sulle limitazioni, fare riferimento a "Limiti a oggetti per la business continuity di SnapMirror".

A proposito di questa attività

- Un criterio di backup è un insieme di regole che regolano la gestione e la conservazione dei backup e la frequenza con cui viene eseguito il backup delle risorse o del gruppo di risorse. Inoltre, è possibile specificare le impostazioni di replica e script. La specifica delle opzioni in un criterio consente di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.

  IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

  Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

  È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- SnapLock
  - Se è selezionata l'opzione "conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere minore o uguale ai giorni di conservazione menzionati.

    La specifica di un periodo di blocco snapshot impedisce l'eliminazione delle istantanee fino alla scadenza del periodo di conservazione. Questo potrebbe portare a mantenere un numero di Snapshot maggiore del conteggio specificato nel criterio.

    Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

  Le impostazioni SnapLock primarie vengono gestite nel criterio di backup SnapCenter e le impostazioni SnapLock secondarie vengono gestite da ONTAP.

Fase 1: Creazione del nome della policy

1. Nel riquadro di navigazione a sinistra, selezionare **Impostazioni**.
2. Nella pagina Impostazioni, selezionare **Criteri**.
3. Selezionare **nuovo**.
4. Nella pagina **Nome**, inserire il nome e la descrizione della policy.

Fase 2: Configurare le opzioni di backup

1. Scegliere il tipo di backup

Backup completo e backup dei log

Eseguire il backup dei file di database e dei log delle transazioni e troncare i log delle transazioni.

1. Selezionare **Backup completo e Backup del registro**.
2. Immettere il numero massimo di database di cui eseguire il backup per ciascuna istantanea.

> È necessario aumentare questo valore se si desidera eseguire più operazioni di backup contemporaneamente.

Backup completo

Eseguire il backup dei file di database.

1. Selezionare **Backup completo**.
2. Immettere il numero massimo di database di cui eseguire il backup per ciascuna istantanea. Il valore predefinito è 100

> È necessario aumentare questo valore se si desidera eseguire più operazioni di backup contemporaneamente.

Backup del registro

Eseguire il backup dei registri delle transazioni. . Selezionare **Log backup**.

Backup solo copia

1. Se si esegue il backup delle risorse utilizzando un'altra applicazione di backup, selezionare **Copia solo backup**.

Mantenendo intatti i log delle transazioni, qualsiasi applicazione di backup può ripristinare i database. In genere, l'utente non deve utilizzare l'opzione copia solo in altre circostanze.

> Microsoft SQL non supporta l'opzione **Copia solo backup** insieme all'opzione **Backup completo e Backup del registro** per lo storage secondario.

1. Nella sezione Availability Group Settings (Impostazioni gruppo di disponibilità), eseguire le seguenti operazioni:

   a. Backup solo su replica di backup preferita.

      Selezionare questa opzione per eseguire il backup solo sulla replica di backup preferita. La replica di backup preferita viene stabilita dalle preferenze di backup configurate per AG in SQL Server.

   b. Selezionare le repliche per il backup.

      Scegliere la replica AG primaria o la replica AG secondaria per il backup.

   c. Selezionare la priorità di backup (priorità di backup minima e massima)

      Specificare un numero minimo di priorità di backup e un numero massimo di priorità di backup che decida la replica AG per il backup. Ad esempio, è possibile avere una priorità minima di 10 e una priorità massima di 50. In questo caso, tutte le repliche AG con priorità superiore a 10 e inferiore a 50

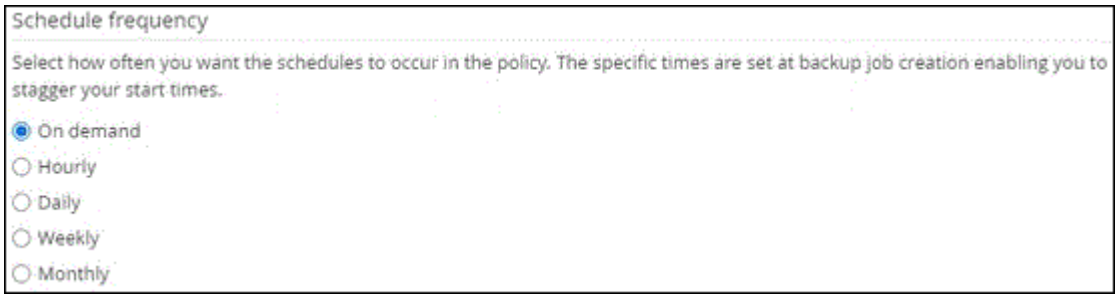
vengono considerate come backup.

Per impostazione predefinita, la priorità minima è 1 e la priorità massima è 100.

Nelle configurazioni del cluster, i backup vengono conservati in ciascun nodo del cluster in base alle impostazioni di conservazione impostate nel criterio. Se il nodo proprietario di AG cambia, i backup vengono eseguiti in base alle impostazioni di conservazione e i backup del nodo proprietario precedente vengono conservati. La conservazione per AG è applicabile solo a livello di nodo.

2. Pianificare la frequenza di backup per questa policy. Specificare il tipo di pianificazione selezionando **on demand**, **Hourly**, **Daily**, **Weekly** o **Monthly**.

   È possibile selezionare un solo tipo di pianificazione per un criterio.



È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e frequenza di backup, ma consente di assegnare diverse pianificazioni di backup a ciascun criterio.

Se sono previste le 2:00, la programmazione non verrà attivata durante l'ora legale (DST).

Fase 3: Configurare le impostazioni di conservazione

Nella pagina di conservazione, a seconda del tipo di backup selezionato nella pagina del tipo di backup, eseguire una o più delle seguenti operazioni:

1. Nella sezione Impostazioni di conservazione per l'operazione di ripristino aggiornata al minuto, eseguire una delle seguenti operazioni:

Numero specifico di copie

Conserva solo un numero specifico di snapshot.

1. Selezionare l'opzione **Mantieni backup registro applicabili agli ultimi giorni <number>** e specificare il numero di giorni da conservare. Se ci si avvicina a questo limite, si consiglia di eliminare le copie meno recenti.

Numero specifico di giorni

Conservare le copie di backup per un numero specifico di giorni.

1. Selezionare l'opzione **Mantieni backup registro applicabili agli ultimi giorni <number> dei backup completi** e specificare il numero di giorni per conservare le copie di backup del registro.

1. Nella sezione **Impostazioni di conservazione backup completo** per le impostazioni di conservazione su richiesta, eseguire le seguenti operazioni:
   a. Specificare il numero totale di istantanee da conservare
      i. Per specificare il numero di istantanee da conservare, selezionare **totale copie snapshot da conservare**.
      ii. Se il numero di istantanee supera il numero specificato, le istantanee vengono eliminate con le copie meno recenti eliminate per prime.

> Per impostazione predefinita, il valore del conteggio di conservazione è impostato su 2. Se si imposta il conteggio della conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è il Snapshot di riferimento per la relazione SnapVault fino a quando una snapshot più recente non viene replicata nella destinazione.

> Il valore massimo di conservazione è 1018 per le risorse su ONTAP 9.4 o versioni successive e 254 per le risorse su ONTAP 9.3 o versioni precedenti. I backup non avranno esito positivo se la conservazione viene impostata su un valore superiore a quello supportato dalla versione di ONTAP sottostante.

1. Tempo necessario per conservare le istantanee
   a. Se si desidera specificare il numero di giorni per i quali si desidera conservare le istantanee prima di eliminarle, selezionare **Mantieni copie snapshot per**.
2. Se si desidera specificare il periodo di blocco dell'istantanea, selezionare **periodo di blocco della copia istantanea** e selezionare giorni, mesi o anni.

   Il periodo di conservazione di SnapLock deve essere inferiore a 100 anni.

3. Nella sezione **Impostazioni di conservazione backup completo** per le impostazioni di conservazione oraria, giornaliera, settimanale e mensile, specificare le impostazioni di conservazione per il tipo di pianificazione selezionato nella pagina tipo di backup.
   a. Specificare il numero totale di istantanee da conservare
      i. Per specificare il numero di istantanee da conservare, selezionare **totale copie snapshot da conservare**. Se il numero di istantanee supera il numero specificato, le istantanee vengono eliminate con le copie meno recenti eliminate per prime.

Se si intende attivare la replica SnapVault, è necessario impostare il numero di conservazione su 2 o superiore. Se si imposta il conteggio della conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è il Snapshot di riferimento per la relazione SnapVault fino a quando una snapshot più recente non viene replicata nella destinazione.

1. Tempo necessario per conservare le istantanee
   a. Per specificare il numero di giorni per i quali si desidera conservare le istantanee prima di eliminarle, selezionare **Mantieni copie snapshot per**.
2. Se si desidera specificare il periodo di blocco dell'istantanea, selezionare **periodo di blocco della copia istantanea** e selezionare giorni, mesi o anni.

   Il periodo di conservazione di SnapLock deve essere inferiore a 100 anni.

   Per impostazione predefinita, la conservazione dell'istantanea del registro è impostata su 7 giorni. Utilizzare il cmdlet Set-SmPolicy per modificare la conservazione dello snapshot di registro.

Questo esempio imposta la conservazione dello snapshot di registro su 2:

Esempio 1. Mostra esempio

```
Set-SmPolicy -policyName 'newpol' -PolicyType 'Backup' -PluginPolicyType 'SCSQL' -sqlbackuptype
'FullBackupAndLogBackup' -RetentionSettings
@{BackupType='DATA';ScheduleType='Hourly';RetentionCount=}@{ScheduleType='Hourly
Count';Retenth2} ScheduleType='Hourly Count';None=Hourly Count'Hourly='2';Conteggio@{}
```

"SnapCenter conserva le copie Snapshot del database"

Fase 4: Configurare le impostazioni di replica

1. Nella pagina Replication (Replica), specificare la replica nel sistema di storage secondario:

Aggiornare SnapMirror

Aggiornare SnapMirror dopo aver creato una copia Snapshot locale.

1. Selezionare questa opzione per creare copie mirror dei set di backup su un altro volume (SnapMirror).

   Questa opzione deve essere abilitata per SnapMirror Business Continuity (SM-BC) o per SnapMirror Sync (SM-S).

   Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante **Aggiorna** nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP.

   Vedere "Visualizzare i backup e i cloni di SQL Server nella pagina topologia".

Aggiornare SnapVault

Aggiornare SnapVault dopo aver creato una copia Snapshot.

1. Selezionare questa opzione per eseguire la replica del backup disk-to-disk.

   Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante **Aggiorna** nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP.

   Quando SnapLock è configurato solo sul secondario da ONTAP noto come vault di SnapLock, facendo clic sul pulsante **Aggiorna** nella pagina topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP.

   Per ulteriori informazioni sul vault di SnapLock, vedere "Assegnare le copie Snapshot a WORM su una destinazione del vault"

   Vedere "Visualizzare i backup e i cloni di SQL Server nella pagina topologia".

Etichetta policy secondaria

1. Selezionare un'etichetta Snapshot.

A seconda dell'etichetta Snapshot selezionata, ONTAP applica la politica di conservazione Snapshot secondaria corrispondente all'etichetta.

> Se è stato selezionato **Update SnapMirror dopo la creazione di una copia Snapshot locale**, è possibile specificare l'etichetta del criterio secondario. Tuttavia, se è stato selezionato **Aggiorna SnapVault dopo la creazione di una copia Snapshot locale**, è necessario specificare l'etichetta del criterio secondario.

Numero tentativi di errore

1. Immettere il numero di tentativi di replica che devono verificarsi prima dell'arresto del processo.

Fase 5: Configurare le impostazioni dello script

1. Nella pagina script, immettere il percorso e gli argomenti del prespt o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di backup.

Ad esempio, è possibile eseguire uno script per aggiornare i trap SNMP, automatizzare gli avvisi e inviare i registri.

Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

È necessario configurare il criterio di conservazione SnapMirror in ONTAP in modo che lo storage secondario non raggiunga il limite massimo di Snapshot.

Fase 6: Configurare le impostazioni di verifica

Nella pagina verifica, attenersi alla seguente procedura:

1. Nella sezione Esegui verifica per le seguenti pianificazioni di backup, selezionare la frequenza di pianificazione.
2. Nella sezione Opzioni di verifica della coerenza del database, eseguire le seguenti operazioni:
   a. Limitare la struttura di integrità alla struttura fisica del database (SOLO_FISICA)
      i. Selezionare **Limit the Integrity Structure to Physical Structure of the database (PHYSICAL_ONLY)** (limita la struttura di integrità alla struttura fisica del database) per limitare il controllo dell'integrità alla struttura fisica del database e rilevare pagine lacerate, errori di checksum e guasti hardware comuni che influiscono sul database.
   b. Elimina tutti i messaggi informativi (NESSUN INFOMSGS)
      i. Selezionare **Sospendi tutti i messaggi informativi (NO_INFOMSGS)** per eliminare tutti i messaggi informativi. Selezionato per impostazione predefinita.
   c. Visualizza tutti i messaggi di errore riportati per oggetto (ALL_ERRORMSGS)
      i. Selezionare **Visualizza tutti i messaggi di errore riportati per oggetto (ALL_ERRORMSGS)** per visualizzare tutti gli errori segnalati per oggetto.
   d. Non controllare gli indici non in cluster (NOINDEX)
      i. Selezionare **non selezionare gli indici non cluster (NOINDEX)** se non si desidera controllare gli indici non cluster. Il database SQL Server utilizza Microsoft SQL Server Database Consistency Checker (DBCC) per verificare l'integrità fisica e logica degli oggetti nel database.
   e. Limitare i controlli e ottenere i blocchi invece di utilizzare un'istantanea del database interna (TABLOCK)
      i. Selezionare **limita i controlli e ottenere i blocchi invece di utilizzare una copia snapshot del database interno (TABLOCK)** per limitare i controlli e ottenere i blocchi invece di utilizzare un'istantanea del database interna.
3. Nella sezione **Log Backup**, selezionare **Verify log backup upon completed** (verifica backup registro al completamento) per verificare il backup del registro al completamento.
4. Nella sezione **Verification script settings** (Impostazioni script di verifica), immettere il percorso e gli argomenti del prescrittt o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di verifica.

Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

Fase 7: Riepilogo

1. Esaminare il riepilogo, quindi selezionare **fine**.

Creare gruppi di risorse e allegare criteri per SQL Server

Un gruppo di risorse è un container al quale si aggiungono risorse che si desidera eseguire insieme per il backup e la protezione. Un gruppo di risorse consente di eseguire contemporaneamente il backup di tutti i dati associati a una determinata applicazione. Per qualsiasi lavoro di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario associare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire.

È possibile proteggere le risorse singolarmente senza creare un nuovo gruppo di risorse. È possibile eseguire backup sulla risorsa protetta.

A proposito di questa attività

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.
- L'aggiunta di nuovi database senza SM-BC a un gruppo di risorse esistente che contiene risorse con SM-BC non è supportata.
- L'aggiunta di nuovi database a un gruppo di risorse esistente in modalità di failover di SM-BC non è supportata. È possibile aggiungere risorse al gruppo di risorse solo in stato normale o di failback.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** dall'elenco **View** (Visualizza).

   Se di recente è stata aggiunta una risorsa a SnapCenter, fare clic su **Aggiorna risorse** per visualizzare la risorsa appena aggiunta.

3. Fare clic su **New Resource Group** (nuovo gruppo di risorse).
4. Nella pagina Name (Nome), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere il nome del gruppo di risorse. Il nome del gruppo di risorse non deve superare i 250 caratteri.
Tag	Inserire una o più etichette per facilitare la ricerca del gruppo di risorse in un secondo momento. Ad esempio, se si aggiunge HR come tag a più gruppi di risorse, è possibile trovare in seguito tutti i gruppi di risorse associati al tag HR.

Per questo campo…	Eseguire questa operazione…
USA il formato nome personalizzato per la copia Snapshot	Opzionale: Immettere un nome e un formato dell'istantanea personalizzato. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

5. Nella pagina risorse, attenersi alla seguente procedura:
   a. Selezionare il nome host, il tipo di risorsa e l'istanza di SQL Server dagli elenchi a discesa per filtrare l'elenco delle risorse.

      Le risorse aggiunte di recente vengono visualizzate nell'elenco delle risorse disponibili solo dopo l'aggiornamento dell'elenco delle risorse.

   b. Per spostare le risorse dalla sezione **risorse disponibili** alla sezione risorse selezionate, eseguire una delle seguenti operazioni:
      - Selezionare **selezione automatica di tutte le risorse sullo stesso volume di storage** per spostare tutte le risorse dello stesso volume nella sezione risorse selezionate.
      - Selezionare le risorse dalla sezione **risorse disponibili**, quindi fare clic sulla freccia destra per spostarle nella sezione **risorse selezionate**.
6. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.

      È anche possibile creare una policy facendo clic su * * .

      Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

   b. Nella sezione Configura pianificazioni per i criteri selezionati, fare clic su * * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare la pianificazione.
   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione specificando la data di inizio, la data di scadenza e la frequenza, quindi fare clic su **OK**.

      È necessario eseguire questa operazione per ciascuna frequenza elencata nella policy. Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate) nella sezione **Configure schedules for selected policy** (Configura pianificazioni per policy selezionate).

   d. Selezionare lo scheduler di Microsoft SQL Server.

      È inoltre necessario selezionare un'istanza di scheduler da associare al criterio di scheduling.

      Se non si seleziona Microsoft SQL Server Scheduler, l'impostazione predefinita è Microsoft Windows Scheduler.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup di SnapCenter. Non modificare le pianificazioni e rinominare il processo di backup creato in

Windows Scheduler o nell'agente SQL Server.

7. Nella pagina verifica, attenersi alla seguente procedura:

   a. Selezionare il server di verifica dall'elenco a discesa **Server di verifica**.

      L'elenco include tutti gli SQL Server aggiunti in SnapCenter. È possibile selezionare più server di verifica (host locale o host remoto).

      La versione del server di verifica deve corrispondere alla versione e all'edizione del server SQL che ospita il database primario.

   a. Fare clic su **Load Locator** (carica locatori) per caricare i volumi SnapMirror e SnapVault per eseguire la verifica sullo storage secondario.

   b. Selezionare il criterio per cui si desidera configurare la pianificazione della verifica, quindi fare clic su * *  .

   c. Nella finestra di dialogo Add Verification Schedules policy_name, eseguire le seguenti operazioni:

Se si desidera…	Eseguire questa operazione…
Eseguire la verifica dopo il backup	Selezionare **Esegui verifica dopo backup**.
Pianifica una verifica	Selezionare **Esegui verifica pianificata**.

   d. Fare clic su **OK**.

      Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

      È possibile rivedere e modificare facendo clic su * *  o eliminare facendo clic su * * .

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report**.

   Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando il comando GUI o PowerShell Set-SmtpServer.

9. Esaminare il riepilogo, quindi fare clic su **fine**.

Informazioni correlate

"Creare criteri di backup per i database di SQL Server"

Requisiti per il backup delle risorse SQL

Prima di eseguire il backup di una risorsa SQL, è necessario assicurarsi che siano soddisfatti diversi requisiti.

- È necessario eseguire la migrazione di una risorsa da un sistema di storage non NetApp a un sistema di

storage NetApp.

- È necessario aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con uno storage secondario, il ruolo ONTAP assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- L'operazione di backup avviata da un utente Active Directory (ad) non riesce se la credenziale dell'istanza SQL non è assegnata all'utente o al gruppo ad. È necessario assegnare la credenziale dell'istanza SQL all'utente o al gruppo ad dalla pagina **Impostazioni** > **accesso utente**.
- È necessario aver creato un gruppo di risorse con un criterio allegato.
- Se un gruppo di risorse dispone di più database provenienti da host diversi, l'operazione di backup su alcuni host potrebbe essere attivata in ritardo a causa di problemi di rete. È necessario configurare il valore di FMaxRetryForUninitializedHosts in web.config utilizzando il cmdlet Set-SmConfigSettings PS.

Eseguire il backup delle risorse SQL

Se una risorsa non fa ancora parte di un gruppo di risorse, è possibile eseguire il backup della risorsa dalla pagina risorse.

A proposito di questa attività

- Per l'autenticazione delle credenziali Windows, è necessario impostare le credenziali prima di installare i plug-in.
- Per l'autenticazione dell'istanza di SQL Server, è necessario aggiungere la credenziale dopo l'installazione dei plug-in.
- Per l'autenticazione gMSA, è necessario configurare gMSA durante la registrazione dell'host con SnapCenter nella pagina **Aggiungi host** o **Modifica host** per abilitare e utilizzare gMSA.
- Se l'host viene aggiunto con gMSA e gMSA dispone dei privilegi di accesso e amministratore di sistema, gMSA verrà utilizzato per connettersi all'istanza SQL.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **Database**, **Instance** o **Availability Group** dall'elenco a discesa **View**.

   a. Selezionare il database, l'istanza o il gruppo di disponibilità di cui si desidera eseguire il backup.

      Quando si esegue un backup di un'istanza, le informazioni sullo stato dell'ultimo backup o sull'indicatore data e ora di tale istanza non saranno disponibili nella pagina delle risorse.

   Nella vista della topologia, non è possibile distinguere se lo stato del backup, la data e l'ora o il backup sono per un'istanza o un database.

3. Nella pagina risorse, selezionare la casella di controllo formato nome personalizzato per copia istantanea*, quindi immettere un formato nome personalizzato che si desidera utilizzare per il nome istantanea.

   Ad esempio, customtext_policy_hostname o resource_hostname. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

4. Nella pagina Criteri, eseguire le seguenti operazioni:

a. Nella sezione Criteri, selezionare uno o più criteri dall'elenco a discesa.

   È possibile creare un criterio selezionando * * per avviare la procedura guidata.

   Nella sezione **Configure schedules for selected policy** (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

b. Selezionare * * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra di dialogo **Aggiungi pianificazioni per criterio** `policy_name` , configurare la pianificazione, quindi selezionare **OK**.

   Ecco `policy_name` il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna **Pianificazioni applicate**.

a. Selezionare **Use Microsoft SQL Server Scheduler**, quindi selezionare l'istanza di scheduler dall'elenco a discesa **Scheduler Instance** associata al criterio di scheduling.

5. Nella pagina verifica, attenersi alla seguente procedura:

   a. Selezionare il server di verifica dall'elenco a discesa **Server di verifica**.

      È possibile selezionare più server di verifica (host locale o host remoto).

      La versione del server di verifica deve essere uguale o superiore alla versione dell'edizione del server SQL che ospita il database primario.

   a. Selezionare **Load secondary locators to verify backups on secondary** (carica locatori secondari) per verificare i backup sul sistema di storage secondario.

   b. Selezionare il criterio per cui si desidera configurare la pianificazione della verifica, quindi selezionare * * .

   c. Nella finestra di dialogo Add Verification Schedules *policy_name*, eseguire le seguenti operazioni:

Se si desidera…	**Eseguire questa operazione…**
Eseguire la verifica dopo il backup	Selezionare **Esegui verifica dopo backup**.
Pianifica una verifica	Selezionare **Esegui verifica pianificata**.

      Se il server di verifica non dispone di una connessione storage, l'operazione di verifica non riesce e viene visualizzato il messaggio di errore: Impossibile montare il disco.

   d. Selezionare **OK**.

      Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

6. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report**.

> Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando il comando GUI o PowerShell Set-SmtpServer.

7. Esaminare il riepilogo, quindi selezionare **fine**.

   Viene visualizzata la pagina della topologia del database.

8. Selezionare **Esegui backup ora**.
9. Nella pagina Backup, attenersi alla seguente procedura:

   a. Se sono stati applicati più criteri alla risorsa, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **verify after backup** (verifica dopo il backup) per verificare il backup.
   c. Selezionare **Backup**.

      > Non rinominare il processo di backup creato in Windows Scheduler o nell'agente SQL Server.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   Viene creato un gruppo di risorse implicito. È possibile visualizzare questa opzione selezionando il rispettivo utente o gruppo dalla pagina User Access (accesso utente). Il tipo di gruppo di risorse implicito è "Resource".

10. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Al termine

- Nelle configurazioni MetroCluster, SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

  "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover di MetroCluster"

- Se si esegue il backup dei dati delle applicazioni su VMDK e la dimensione dell'heap Java per il plug-in SnapCenter per VMware vSphere non è sufficiente, il backup potrebbe non riuscire. Per aumentare la dimensione dell'heap Java, individuare il file script /opt/netapp/init_scripts/scvservice. In tale script, il `do_start method` comando avvia il servizio plug-in VMware di SnapCenter. Aggiornare il comando al seguente indirizzo: `Java -jar -Xmx8192M -Xms4096M`.

Informazioni correlate

"Creare criteri di backup per i database di SQL Server"

"Eseguire il backup delle risorse utilizzando i cmdlet PowerShell"

"Le operazioni di backup non riescono con un errore di connessione MySQL a causa del ritardo nel TCP_TIMEOUT"

"Il backup non riesce e viene visualizzato un errore dello scheduler di Windows"

"Le operazioni di quiesce o raggruppamento delle risorse non riescono"

Eseguire il backup dei gruppi di risorse di SQL Server

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina risorse. Se un gruppo di risorse dispone di un criterio associato e di una pianificazione configurata, i backup vengono eseguiti automaticamente in base alla pianificazione.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).

   È possibile eseguire una ricerca nel gruppo di risorse immettendo il nome del gruppo di risorse nella casella di ricerca oppure selezionando * *, quindi selezionando il tag. È quindi possibile selezionare * * per chiudere il riquadro del filtro.
3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi selezionare **Esegui backup ora**.
4. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se sono stati associati più criteri al gruppo di risorse, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Dopo il backup, selezionare **verify** (verifica) per verificare il backup on-demand.

      L'opzione **verify** del criterio si applica solo ai processi pianificati.

   c. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Informazioni correlate

"Creare criteri di backup per i database di SQL Server"

"Creare gruppi di risorse e allegare criteri per SQL Server"

"Eseguire il backup delle risorse utilizzando i cmdlet PowerShell"

"Le operazioni di backup non riescono con un errore di connessione MySQL a causa del ritardo nel TCP_TIMEOUT"

"Il backup non riesce e viene visualizzato un errore dello scheduler di Windows"

Monitorare le operazioni di backup

Monitorare le operazioni di backup delle risorse SQL nella pagina processi SnapCenter

È possibile monitorare l'avanzamento di diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere necessario controllare i progressi per determinare quando sono stati completati o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Status** (Stato), selezionare lo stato del backup.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene venga visualizzato lo stato del processo di backup , quando si fa clic sui dettagli del processo, è possibile che alcune delle attività secondarie dell'operazione di backup siano ancora in corso o contrassegnate da segnali di avviso.

5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Monitorare le operazioni di protezione dei dati sulle risorse SQL nel riquadro attività

Il riquadro Activity (attività) visualizza le cinque operazioni più recenti eseguite. Il riquadro Activity (attività) visualizza anche il momento in cui l'operazione è stata avviata e lo stato dell'operazione.

Il riquadro Activity (attività) visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Fare clic  sul riquadro attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli commessa**.

Creare una connessione al sistema storage e una credenziale utilizzando i cmdlet PowerShell

È necessario creare una connessione SVM (Storage Virtual Machine) e una credenziale prima di utilizzare i cmdlet PowerShell per eseguire operazioni di protezione dei dati.

Prima di iniziare

- L'ambiente PowerShell dovrebbe essere stato preparato per l'esecuzione dei cmdlet PowerShell.
- Per creare le connessioni storage, è necessario disporre delle autorizzazioni necessarie nel ruolo Infrastructure Admin.
- Assicurarsi che le installazioni dei plug-in non siano in corso.

  Le installazioni dei plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage perché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nella GUI di SnapCenter come "non disponibile per il backup" o "non su storage NetApp".

- I nomi dei sistemi di storage devono essere univoci.

  SnapCenter non supporta più sistemi storage con lo stesso nome su cluster diversi. Ogni sistema storage supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF di gestione univoco.

Fasi

1. Avviare una sessione di connessione PowerShell utilizzando il cmdlet Open-SmConnection.

   Questo esempio apre una sessione PowerShell:

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

2. Creare una nuova connessione al sistema di storage utilizzando il cmdlet Add-SmStorageConnection.

   Questo esempio crea una nuova connessione al sistema di storage:

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

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   In questo esempio viene creata una nuova credenziale denominata FinanceAdmin con credenziali Windows:

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Eseguire il backup delle risorse utilizzando i cmdlet PowerShell

È possibile utilizzare i cmdlet PowerShell per eseguire il backup dei database SQL Server o dei file system Windows. Il backup di un database o di un file system di SQL Server include la connessione con il server SnapCenter, il rilevamento delle istanze o dei file system di SQL Server, l'aggiunta di un criterio, la creazione di un gruppo di risorse di backup, il backup e la verifica del backup.

Prima di iniziare

- È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- È necessario aver aggiunto la connessione al sistema di storage e creato una credenziale.
- È necessario aggiungere host e rilevare risorse.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

   Viene visualizzato il prompt di nome utente e password.

2. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   In questo esempio viene creata una nuova policy di backup con un tipo di backup completo SQL:

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

   Questo esempio crea una nuova policy di backup con un tipo di backup del file system Windows di CrashConsistent:

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

3. Individuare le risorse host utilizzando il cmdlet Get-SmResources.

   In questo esempio vengono illustrate le risorse per il plug-in Microsoft SQL sull'host specificato:

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

   In questo esempio vengono illustrate le risorse per i file system Windows sull'host specificato:

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

4. Aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   Questo esempio crea un nuovo gruppo di risorse di backup del database SQL con i criteri e le risorse specificati:

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

   Questo esempio crea un nuovo gruppo di risorse di backup del file system Windows con i criteri e le risorse specificati:

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

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

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

6. Visualizzare lo stato del processo di backup utilizzando il cmdlet Get-SmBackupReport.

   Questo esempio visualizza un report di riepilogo di tutti i lavori eseguiti alla data specificata:

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Annullare il plug-in SnapCenter per le operazioni di backup di Microsoft SQL Server

È possibile annullare le operazioni di backup in esecuzione, in coda o che non rispondono. Quando si annulla un'operazione di backup, il server SnapCenter interrompe l'operazione e rimuove tutte le istantanee dall'archivio se il backup creato non è registrato con il server SnapCenter. Se il backup è già registrato con il server SnapCenter, non verrà eseguito il rollback dell'istantanea già creata anche dopo l'attivazione dell'annullamento.

Prima di iniziare

- Per annullare le operazioni di ripristino, è necessario accedere come amministratore SnapCenter o come proprietario del processo.
- È possibile annullare solo il log o le operazioni di backup complete in coda o in esecuzione.
- Non è possibile annullare l'operazione dopo l'avvio della verifica.

  Se si annulla l'operazione prima della verifica, l'operazione viene annullata e l'operazione di verifica non viene eseguita.
- È possibile annullare un'operazione di backup dalla pagina Monitor o dal riquadro attività.
- Oltre a utilizzare l'interfaccia grafica di SnapCenter, è possibile utilizzare i cmdlet PowerShell per annullare le operazioni.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di backup in coda degli altri membri durante l'utilizzo di tale ruolo.

Fasi

Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	1. Nel riquadro di spostamento a sinistra, selezionare **Monitor** > **Jobs**. 2. Selezionare il lavoro e selezionare **Annulla lavoro** .

Dal…	Azione
Riquadro delle attività	1. Dopo aver avviato il processo di backup, selezionare nel riquadro attività per visualizzare le cinque operazioni più recenti. 2. Selezionare l'operazione. 3. Nella pagina Dettagli lavoro, selezionare **Annulla lavoro**.

Risultato

L'operazione viene annullata e la risorsa viene riportata allo stato precedente. Se l'operazione annullata non risponde allo stato di annullamento o esecuzione, è necessario eseguire il `Cancel-SmJob -JobID <int> -Force` cmdlet per arrestare forzatamente l'operazione di backup.

Visualizzare i backup e i cloni di SQL Server nella pagina topologia

Quando si prepara il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e cloni sullo storage primario e secondario.

A proposito di questa attività

Nella pagina topologia, è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e selezionarli per eseguire le operazioni di protezione dei dati.

È possibile esaminare le seguenti icone nella vista **Gestisci copie** per determinare se i backup e i cloni sono disponibili sullo storage primario o secondario (copie Mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- Visualizza il numero di backup e cloni su cui viene eseguito il mirroring dello storage secondario utilizzando la tecnologia SnapMirror.
- Visualizza il numero di backup e cloni replicati sullo storage secondario utilizzando la tecnologia SnapVault.
  - Il numero di backup visualizzati include i backup eliminati dallo storage secondario.

    Ad esempio, se sono stati creati 6 backup utilizzando un criterio per conservare solo 4 backup, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror flessibile della versione su un volume di tipo mirror-vault vengono visualizzati nella vista della topologia, ma il numero di backup mirror nella vista della topologia non include il backup flessibile della versione.

Se disponi di una relazione secondaria come SnapMirror Business Continuity (SM-BC), puoi visualizzare le

seguenti icone aggiuntive:

-  implica che il sito di replica è attivo.
-  implica che il sito di replica non è attivo.
-  implica che la relazione del mirror secondario o del vault non è stata ristabilita.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa selezionata è un database clonato, proteggere il database clonato, l'origine del clone viene visualizzata nella pagina topologia. Fare clic su **Dettagli** per visualizzare il backup utilizzato per la clonazione.

   Se la risorsa è protetta, viene visualizzata la pagina topologia della risorsa selezionata.

4. Consulta la scheda Summary per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione **Summary Card** mostra il numero totale di backup e cloni.

   Facendo clic sul pulsante **Refresh** viene avviata una query dello storage per visualizzare un conteggio accurato.

   Se viene eseguito il backup abilitato SnapLock, facendo clic sul pulsante **Aggiorna** si aggiornano i tempi di scadenza SnapLock primari e secondari recuperati da ONTAP. Inoltre, una pianificazione settimanale aggiorna il tempo di scadenza SnapLock primario e secondario recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza del SnapLock per il backup sarà il tempo di scadenza del SnapLock più lungo impostato per una Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Per SnapMirror Business Continuity (SM-BC), facendo clic sul pulsante **Refresh** (Aggiorna) viene aggiornato l'inventario di backup di SnapCenter eseguendo una query su ONTAP per i siti principali e di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti relazioni SM-BC.

   - Per le relazioni SM-BC, Async Mirror, Vault o MirrorVault con la nuova destinazione primaria deve essere configurato manualmente dopo il failover.
   - Dopo il failover, è necessario creare un backup affinché SnapCenter sia consapevole del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista **Gestisci copie**, fare clic su **backup** o **cloni** dallo storage primario o secondario per visualizzare i dettagli di un backup o clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni

di ripristino, clonazione, ridenominazione ed eliminazione.

Non è possibile rinominare o eliminare i backup presenti nello storage secondario.

7. Selezionare un clone dalla tabella e fare clic su **Clone Split**.
8. Se si desidera eliminare un clone, selezionarlo dalla tabella, quindi fare clic su .

Rimuovere i backup utilizzando i cmdlet PowerShell

È possibile utilizzare il cmdlet Remove-SmBackup per eliminare i backup se non sono più necessari per altre operazioni di protezione dei dati.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Eliminare uno o più backup utilizzando il cmdlet Remove-SmBackup.

   Questo esempio elimina due backup utilizzando i relativi ID di backup:

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

Ripulire il numero di backup secondari utilizzando i cmdlet PowerShell

È possibile utilizzare il cmdlet Remove-SmBackup per eliminare il conteggio dei backup per i backup secondari che non dispongono di snapshot. È possibile utilizzare questo cmdlet quando le istantanee totali visualizzate nella topologia Manage Copies (Gestisci copie) non corrispondono all'impostazione di conservazione Snapshot dello storage secondario.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Eliminare il numero di backup secondari utilizzando il parametro -CleanupSecondaryBackups.

   Nell'esempio riportato di seguito viene eliminato il conteggio dei backup per i backup secondari senza istantanee:

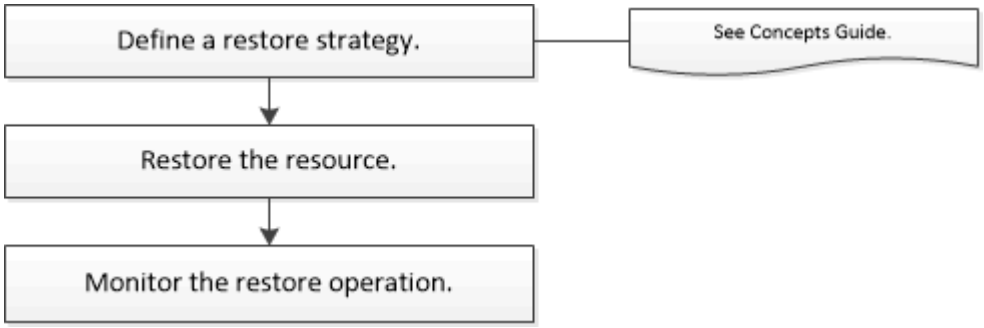
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Ripristinare le risorse di SQL Server

Ripristinare il flusso di lavoro

È possibile utilizzare SnapCenter per ripristinare i database di SQL Server ripristinando i dati da uno o più backup nel file system attivo e ripristinando il database. È inoltre possibile ripristinare i database presenti nei gruppi di disponibilità e aggiungere i database ripristinati al gruppo di disponibilità. Prima di ripristinare un database SQL Server, è necessario eseguire diverse attività preparatorie.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di ripristino del database:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino, ripristino, verifica e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida dei cmdlet di SnapCenter o vedere la "Guida di riferimento al cmdlet del software SnapCenter"

Ulteriori informazioni

"Ripristinare un database SQL Server dallo storage secondario"

"Ripristinare e ripristinare le risorse utilizzando i cmdlet PowerShell"

"L'operazione di ripristino potrebbe non riuscire in Windows 2008 R2"

Requisiti per il ripristino di un database

Prima di ripristinare un database SQL Server da un plug-in SnapCenter per il backup di Microsoft SQL Server, è necessario assicurarsi che siano soddisfatti diversi requisiti.

- L'istanza di SQL Server di destinazione deve essere in linea e in esecuzione prima di poter ripristinare un database.

  Ciò vale sia per le operazioni di ripristino del database utente che per le operazioni di ripristino del database di sistema.

- Le operazioni di SnapCenter pianificate per l'esecuzione sui dati di SQL Server che si stanno ripristinando devono essere disattivate, inclusi i processi pianificati su server di gestione remota o di verifica remota.
- Se i database di sistema non funzionano, è necessario prima ricostruire i database di sistema utilizzando un'utilità SQL Server.
- Se si sta installando il plug-in, assicurarsi di concedere le autorizzazioni per altri ruoli per ripristinare i backup del gruppo di disponibilità (AG).

  Il ripristino di AG non riesce quando viene soddisfatta una delle seguenti condizioni:

  - Se il plug-in viene installato dall'utente RBAC e un amministratore tenta di ripristinare un backup AG
  - Se il plug-in viene installato da un amministratore e un utente RBAC tenta di ripristinare un backup AG
- Se si ripristinano i backup personalizzati della directory di log su un host alternativo, il server SnapCenter e l'host del plug-in devono avere la stessa versione di SnapCenter installata.
- È necessario aver installato la correzione rapida Microsoft KB2887595. Il sito del supporto Microsoft contiene ulteriori informazioni su KB2887595.

  "Articolo di supporto Microsoft 2887595: Rollup degli aggiornamenti di Windows RT 8.1, Windows 8.1 e Windows Server 2012 R2: Novembre 2013"

- È necessario aver eseguito il backup dei gruppi di risorse o del database.
- Se si stanno replicando Snapshot in un mirror o un vault, l'amministratore della SnapCenter deve aver assegnato le Storage Virtual Machine (SVM) per entrambi i volumi di origine e di destinazione.

  Per informazioni sulle modalità di assegnazione delle risorse agli utenti da parte degli amministratori, consultare le informazioni di installazione di SnapCenter.

- Tutti i processi di backup e clonazione devono essere interrotti prima di ripristinare il database.
- L'operazione di ripristino potrebbe andare in timeout se le dimensioni del database sono in terabyte (TB).

  È necessario aumentare il valore del parametro RESTTimeout del server SnapCenter a 20000000 ms eseguendo il seguente comando: Set-SmConfigSettings -Agent -configSettings @{"RESTTimeout" = "20000000"}. In base alle dimensioni del database, è possibile modificare il valore di timeout e impostare un valore massimo di 86400000 ms.

Se si desidera eseguire il ripristino mentre i database sono online, l'opzione di ripristino online deve essere attivata nella pagina Restore.

Ripristinare i backup del database di SQL Server

È possibile utilizzare SnapCenter per ripristinare i database di SQL Server di cui è stato eseguito il backup. Il ripristino del database è un processo multifase che copia tutti i dati e le pagine di registro da un backup di SQL Server specificato in un database specifico.

A proposito di questa attività

- È possibile ripristinare i database di SQL Server di cui è stato eseguito il backup in un'istanza di SQL Server diversa sullo stesso host in cui è stato creato il backup.

  È possibile utilizzare SnapCenter per ripristinare i database di SQL Server di cui è stato eseguito il backup in un percorso alternativo, in modo da non sostituire una versione di produzione.

- SnapCenter può ripristinare i database in un cluster Windows senza disattivare il gruppo di cluster di SQL Server.
- Se si verifica un errore del cluster (operazione di spostamento di un gruppo di cluster) durante un'operazione di ripristino (ad esempio, se il nodo proprietario delle risorse non funziona), è necessario riconnettersi all'istanza di SQL Server e riavviare l'operazione di ripristino.
- Non è possibile ripristinare il database quando gli utenti o i processi di SQL Server Agent accedono al database.
- Non è possibile ripristinare i database di sistema su un percorso alternativo.
- IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

  Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

  È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- La maggior parte dei campi delle pagine della procedura guidata di ripristino sono esplicativi. Le seguenti informazioni descrivono i campi per i quali potrebbe essere necessaria una guida.
- Per l'operazione di ripristino SnapMirror Business Continuity (SM-BC), devi selezionare il backup dalla posizione principale.
- Per i criteri abilitati per SnapLock, per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco Snapshot, i cloni creati dagli Snapshot a prova di manomissione come parte del ripristino ereditano il tempo di scadenza SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

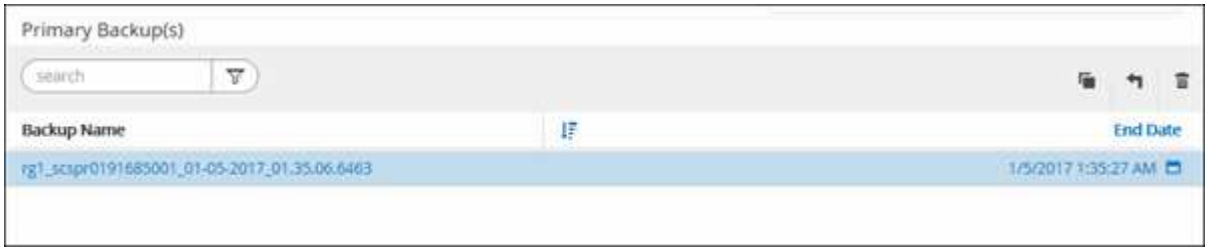
Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina topologia.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dal sistema di storage.

5. Selezionare il backup dalla tabella, quindi fare clic sull' icona.



6. Nella pagina Restore Scope (ambito ripristino), selezionare una delle seguenti opzioni:

Opzione	Descrizione
Ripristinare il database sullo stesso host in cui è stato creato il backup	Selezionare questa opzione se si desidera ripristinare il database sullo stesso server SQL in cui vengono eseguiti i backup.
Ripristinare il database su un host alternativo	Selezionare questa opzione se si desidera ripristinare il database in un server SQL diverso nello stesso host o in un altro host in cui vengono eseguiti i backup. Selezionare un nome host, fornire un nome di database (facoltativo), selezionare un'istanza e specificare i percorsi di ripristino. L'estensione del file fornita nel percorso alternativo deve essere uguale all'estensione del file di database originale. Se l'opzione **Restore the database to an alternate host** (Ripristina database su un host alternativo) non viene visualizzata nella pagina Restore Scope (Ripristina ambito), cancellare la cache del browser.
Ripristinare il database utilizzando i file di database esistenti	Selezionare questa opzione se si desidera ripristinare il database in un SQL Server alternativo nello stesso host o in un host diverso in cui vengono eseguiti i backup. I file di database devono essere già presenti nei percorsi di file esistenti. Selezionare un nome host, fornire un nome di database (facoltativo), selezionare un'istanza e specificare i percorsi di ripristino.

7. Nella pagina Recovery Scope (ambito ripristino), selezionare una delle seguenti opzioni:

Opzione	Descrizione
Nessuno	Selezionare **None** (Nessuno) se si desidera ripristinare solo il backup completo senza alcun registro.
Tutti i backup dei log	Selezionare **All log backups** up-to-the-minute backup restore operation per ripristinare tutti i backup dei log disponibili dopo il backup completo.
In base ai backup dei log fino a.	Selezionare **by log backups** per eseguire un'operazione di ripristino point-in-time, che ripristina il database in base ai log di backup fino al log di backup con la data selezionata.
Per data specifica fino al	Selezionare **per data specifica fino a** per specificare la data e l'ora dopo le quali i registri delle transazioni non vengono applicati al database ripristinato. Questa operazione di ripristino point-in-time interrompe il ripristino delle voci del log delle transazioni registrate dopo la data e l'ora specificate.
Utilizzare una directory di log personalizzata	Se è stato selezionato **All log backups**, **by log backups** o **by specifiche date until** e i log si trovano in una posizione personalizzata, selezionare **Use custom log directory**, quindi specificare la posizione del log. L'opzione **Usa directory log personalizzata** è disponibile solo se è stato selezionato **Ripristina il database su un host alternativo** o **Ripristina il database utilizzando i file di database esistenti**. È anche possibile utilizzare il percorso condiviso, ma assicurarsi che il percorso sia accessibile dall'utente SQL. La directory di log personalizzata non è supportata per il database del gruppo di disponibilità.

8. Nella pagina Pre Ops (operazioni di pre-elaborazione), attenersi alla seguente procedura:
   a. Nella pagina Pre Restore Options (Opzioni di pre-ripristino), selezionare una delle seguenti opzioni:
      - Selezionare **sovrascrivere il database con lo stesso nome durante il ripristino** per ripristinare il database con lo stesso nome.
      - Selezionare **Mantieni impostazioni di replica del database SQL** per ripristinare il database e conservare le impostazioni di replica esistenti.

- Selezionare **Crea backup del log delle transazioni prima del ripristino** per creare un log delle transazioni prima dell'inizio dell'operazione di ripristino.
- Selezionare **Quit restore if Transaction log backup before restore fails** (Esci dal ripristino se il backup del log delle transazioni non riesce) per interrompere l'operazione di ripristino.

b. Specificare gli script opzionali da eseguire prima di eseguire un processo di ripristino.

Ad esempio, è possibile eseguire uno script per aggiornare i trap SNMP, automatizzare gli avvisi, inviare i registri e così via.

Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

9. Nella pagina Post Ops (operazioni successive), attenersi alla seguente procedura:

a. Nella sezione Scegli stato database dopo il completamento del ripristino, selezionare una delle seguenti opzioni:

- Selezionare **operativo, ma non disponibile per il ripristino di log di transazioni aggiuntivi** se si stanno ripristinando tutti i backup necessari.

  Questo è il comportamento predefinito, che lascia il database pronto per l'uso eseguendo il rollback delle transazioni non assegnate. Non è possibile ripristinare ulteriori registri delle transazioni fino a quando non si crea un backup.

- Selezionare **non operativo, ma disponibile per il ripristino di registri transazionali aggiuntivi** per lasciare il database non operativo senza eseguire il rollback delle transazioni non assegnate.

  È possibile ripristinare ulteriori registri delle transazioni. Non è possibile utilizzare il database fino a quando non viene ripristinato.

- Selezionare **Read-only mode, disponibile per il ripristino di registri transazionali aggiuntivi** per lasciare il database in modalità di sola lettura.

  Questa opzione annulla le transazioni non assegnate, ma salva le azioni non riuscite in un file di standby in modo che gli effetti di ripristino possano essere ripristinati.

Se l'opzione Undo directory (Annulla directory) è attivata, vengono ripristinati altri log delle transazioni. Se l'operazione di ripristino del log delle transazioni non riesce, è possibile eseguire il rollback delle modifiche. La documentazione di SQL Server contiene ulteriori informazioni.

b. Specificare gli script opzionali da eseguire dopo l'esecuzione di un processo di ripristino.

Ad esempio, è possibile eseguire uno script per aggiornare i trap SNMP, automatizzare gli avvisi, inviare i registri e così via.

Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

10. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail.

11. Esaminare il riepilogo, quindi fare clic su **fine**.
12. Monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

Informazioni correlate

"Ripristinare e ripristinare le risorse utilizzando i cmdlet PowerShell"

"Ripristinare un database SQL Server dallo storage secondario"

Ripristinare un database SQL Server dallo storage secondario

È possibile ripristinare i database di SQL Server di cui è stato eseguito il backup dalle LUN fisiche (RDM, iSCSI o FCP) su un sistema di storage secondario. La funzionalità di ripristino è un processo multifase che copia tutti i dati e le pagine di registro da un backup SQL Server specificato che risiede nel sistema di storage secondario in un database specifico.

Prima di iniziare

- È necessario aver replicato gli snapshot dal sistema di storage primario a quello secondario.
- È necessario assicurarsi che il server SnapCenter e l'host del plug-in siano in grado di connettersi al sistema di storage secondario.
- La maggior parte dei campi delle pagine della procedura guidata di ripristino viene spiegata nel processo di ripristino di base. Le seguenti informazioni descrivono alcuni dei campi per i quali potrebbe essere necessaria una guida.

A proposito di questa attività

Per i criteri abilitati per SnapLock, per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco Snapshot, i cloni creati dagli Snapshot a prova di manomissione come parte del ripristino ereditano il tempo di scadenza SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare **plug-in SnapCenter per SQL Server** dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco a discesa **View** (Visualizza).
3. Selezionare il database o il gruppo di risorse.

   Viene visualizzata la pagina della topologia del database o del gruppo di risorse.
4. Nella sezione Gestisci copie, selezionare **backup** dal sistema di storage secondario (mirroring o vault).
5. Selezionare il backup dall'elenco, quindi fare clic su  .
6. Nella pagina Location (percorso), scegliere il volume di destinazione per il ripristino della risorsa selezionata.
7. Completare la procedura guidata di ripristino, esaminare il riepilogo, quindi fare clic su **fine**.

Se un database è stato ripristinato su un percorso diverso condiviso da altri database, è necessario eseguire un backup completo e una verifica del backup per verificare che il database ripristinato non sia corrotto a livello fisico.

Eseguire nuovamente il reeed dei database del gruppo di disponibilità

Reseed è un'opzione per ripristinare i database del gruppo di disponibilità (AG). Se un database secondario non viene sincronizzato con il database primario in un AG, è possibile eseguire nuovamente il reeeding del database secondario.

Prima di iniziare

- È necessario aver creato il backup del database AG secondario che si desidera ripristinare.
- Il server SnapCenter e l'host del plug-in devono avere la stessa versione di SnapCenter installata.

A proposito di questa attività

- Non è possibile eseguire l'operazione di riseed sui database primari.
- Non è possibile eseguire un'operazione di riseed se il database di replica viene rimosso dal gruppo di disponibilità. Quando la replica viene rimossa, l'operazione di reeed non riesce.
- Durante l'esecuzione dell'operazione di riseed nel database di SQL Availability Group, non è necessario attivare i backup dei log nei database di replica del database di quel gruppo di disponibilità. Se si attivano i backup dei log durante l'operazione di riseed, l'operazione di riseeding non riesce con il database mirror, "nome_database" non dispone di dati del log delle transazioni sufficienti per conservare la catena di backup dei log del messaggio di errore del database principale.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare **plug-in SnapCenter per SQL Server** dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** dall'elenco **View** (Visualizza).
3. Selezionare il database AG secondario dall'elenco.
4. Fare clic su **reseed**.
5. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Ripristinare le risorse utilizzando i cmdlet PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con il server SnapCenter, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Recuperare le informazioni relative a uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio mostra informazioni su tutti i backup disponibili:

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

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

Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

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

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

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

3. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di ripristino delle risorse SQL

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

gli stati di post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi altra azione di ripristino che è possibile eseguire.

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Ripristina**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato di ripristino.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Annullare le operazioni di ripristino delle risorse SQL

È possibile annullare i processi di ripristino in coda.

Per annullare le operazioni di ripristino, è necessario accedere come amministratore SnapCenter o come proprietario del processo.

A proposito di questa attività

- È possibile annullare un'operazione di ripristino in coda dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione di ripristino in corso.
- È possibile utilizzare l'interfaccia grafica di SnapCenter, i cmdlet PowerShell o i comandi CLI per annullare le operazioni di ripristino in coda.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni di ripristino che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di ripristino in coda degli altri membri durante l'utilizzo di tale ruolo.

Fase

Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. 2. Selezionare il lavoro e fare clic su **Annulla lavoro**.
Riquadro delle attività	1. Dopo aver avviato l'operazione di ripristino, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. 2. Selezionare l'operazione. 3. Nella pagina Dettagli processo, fare clic su **Annulla processo**.

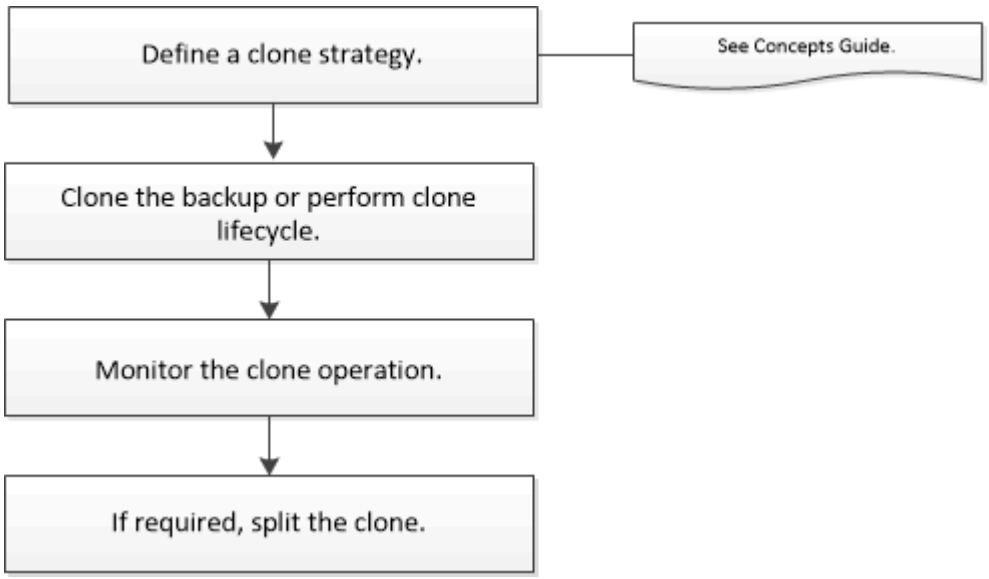
Clonare le risorse di database di SQL Server

Clonare il flusso di lavoro

Prima di clonare le risorse di database da un backup, è necessario eseguire diverse attività utilizzando il server SnapCenter. La clonazione del database è il processo di creazione di una copia point-in-time di un database di produzione o del relativo set di backup. È possibile clonare i database per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto del database corrente durante i cicli di sviluppo delle applicazioni, per utilizzare gli strumenti di estrazione e manipolazione dei dati durante il popolamento dei data warehouse o per ripristinare i dati cancellati o modificati erroneamente.

Un'operazione di clonazione del database genera report basati sugli ID lavoro.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di cloning:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino, ripristino, verifica e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida dei cmdlet di SnapCenter o vedere la "Guida di riferimento al cmdlet del software SnapCenter"

Ulteriori informazioni

"Clonare da un backup di database SQL Server"

"Eseguire il ciclo di vita del clone"

"L'operazione di clonazione potrebbe non riuscire o richiedere più tempo per il completamento con il valore TCP_TIMEOUT predefinito"

Clonare da un backup di database SQL Server

È possibile utilizzare SnapCenter per clonare un backup del database SQL Server. Se si desidera accedere o ripristinare una versione precedente dei dati, è possibile clonare i backup del database su richiesta.

Prima di iniziare

- Dovresti aver preparato per la protezione dei dati completando attività come l'aggiunta di host, l'identificazione delle risorse e la creazione di connessioni al sistema di storage.
- Si dovrebbe aver eseguito il backup di database o gruppi di risorse.
- Il tipo di protezione, ad esempio mirror, vault o mirror-vault per LUN di dati e LUN di log, deve essere lo stesso per rilevare i locatori secondari durante la clonazione a un host alternativo utilizzando i backup di log.
- Se il disco clone montato non viene trovato durante un'operazione di clonazione SnapCenter, modificare il parametro CloneRetryTimeout del server SnapCenter in 300.
- Assicurarsi che gli aggregati che ospitano i volumi siano inclusi nell'elenco degli aggregati assegnati della macchina virtuale di storage (SVM).

A proposito di questa attività

- Durante la clonazione in un'istanza di database standalone, assicurarsi che il percorso del punto di montaggio esista e che si tratti di un disco dedicato.
- Durante la clonazione in un'istanza del cluster di failover (FCI), assicurarsi che i punti di montaggio esistano, che si tratti di un disco condiviso e che il percorso e l'FCI appartengano allo stesso gruppo di risorse SQL.
- Assicurarsi che a ciascun host sia collegato un solo iniziatore VFC o FC. Questo perché SnapCenter supporta un solo iniziatore per host.
- Se il database di origine o l'istanza di destinazione si trova su un volume condiviso del cluster (csv), il database clonato si trova nel file csv.
- IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

  Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

  È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

Per gli ambienti virtuali (VMDK/RDM), assicurarsi che il punto di montaggio sia un disco dedicato.

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare **plug-in SnapCenter per SQL Server** dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).

   La clonazione di un backup di un'istanza non è supportata.

3. Selezionare il database o il gruppo di risorse.
4. Dalla pagina di visualizzazione **Gestisci copie**, selezionare il backup dal sistema di storage primario o secondario (mirrorato o vault).
5. Selezionare il backup, quindi .
6. Nella pagina **Clone Options**, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Server clone	Scegliere un host su cui creare il clone.
Clonare l'istanza	Scegliere un'istanza di clone in cui clonare il backup del database. Questa istanza SQL deve trovarsi nel server clone specificato.
Suffisso clone	Inserire un suffisso che verrà aggiunto al nome del file clone per identificare che il database è un clone. Ad esempio, *db1_clone*. Se si esegue la clonazione nella stessa posizione del database originale, è necessario fornire un suffisso per differenziare il database clonato dal database originale. In caso contrario, l'operazione non riesce.

Per questo campo…	Eseguire questa operazione…
Assegnazione automatica del punto di montaggio o assegnazione automatica del punto di montaggio del volume sotto il percorso	Scegliere se assegnare automaticamente un punto di montaggio o un punto di montaggio del volume sotto un percorso. Auto assign volume mount point under path (assegnazione automatica del punto di montaggio del volume sotto il percorso): Il punto di montaggio sotto un percorso consente di fornire una directory specifica. I punti di montaggio verranno creati all'interno di tale directory. Prima di scegliere questa opzione, assicurarsi che la directory sia vuota. Se nella directory è presente un database, il database si trova in uno stato non valido dopo l'operazione di montaggio.

7. Nella pagina registri, selezionare una delle seguenti opzioni:

Per questo campo…	Eseguire questa operazione…
Nessuno	Scegliere questa opzione se si desidera clonare solo il backup completo senza alcun log.
Tutti i backup dei log	Scegliere questa opzione per clonare tutti i backup del registro disponibili datati dopo il backup completo.
In base ai backup dei log fino a.	Scegliere questa opzione per clonare il database in base ai registri di backup creati fino al log di backup con la data selezionata.
Per data specifica fino al	Specificare la data e l'ora dopo le quali i log delle transazioni non vengono applicati al database clonato. Questo clone point-in-time interrompe il clone delle voci del log delle transazioni registrate dopo la data e l'ora specificate.

8. Nella pagina **script**, immettere il timeout dello script, il percorso e gli argomenti del prescrittt o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di clone.

   Ad esempio, è possibile eseguire uno script per aggiornare i trap SNMP, automatizzare gli avvisi, inviare i registri e così via.

   > Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

   Il timeout predefinito dello script è di 60 secondi.

9. Nella pagina **Notification**, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report**.

   Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

   Per EMS, fare riferimento a. "Gestire la raccolta di dati EMS"

10. Esaminare il riepilogo, quindi selezionare **fine**.
11. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Al termine

Una volta creato il clone, non rinominarlo.

Informazioni correlate

"Eseguire il backup del database, dell'istanza o del gruppo di disponibilità di SQL Server"

"Clonare i backup utilizzando i cmdlet PowerShell"

"L'operazione di clonazione potrebbe non riuscire o richiedere più tempo per il completamento con il valore TCP_TIMEOUT predefinito"

"Il clone del database dell'istanza del cluster di failover non riesce"

Clonare i backup utilizzando i cmdlet PowerShell

Il flusso di lavoro dei cloni include la pianificazione, l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Elencare i backup che possono essere clonati utilizzando il cmdlet Get-SmBackup o Get-SmResourceGroup.

   Questo esempio mostra informazioni su tutti i backup disponibili:

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

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

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

Nell'esempio riportato di seguito vengono visualizzate informazioni su un gruppo di risorse specificato, sulle relative risorse e sui criteri associati:

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

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
```

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

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

3. Avviare un'operazione di clonazione da un backup esistente utilizzando il cmdlet New-SmClone.

   Questo esempio crea un clone da un backup specificato con tutti i log:

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

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

   In questo esempio viene creato un clone per un'istanza specifica di Microsoft SQL Server:

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

4. Visualizzare lo stato del processo clone utilizzando il cmdlet Get-SmCloneReport.

   Questo esempio visualizza un report clone per l'ID lavoro specificato:

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                   Sally_DRAPER}
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Eseguire il ciclo di vita del clone

Utilizzando SnapCenter, è possibile creare cloni da un gruppo di risorse o da un database. È possibile eseguire cloni on-demand o pianificare operazioni ricorrenti di cloni di un gruppo di risorse o di un database. Se si clonano periodicamente un backup, è possibile utilizzare il clone per sviluppare applicazioni, popolare i dati o ripristinare i dati.

SnapCenter consente di pianificare più operazioni di cloni da eseguire contemporaneamente su più server.

Prima di iniziare

- Durante la clonazione in un'istanza di database standalone, assicurarsi che il percorso del punto di montaggio esista e che si tratti di un disco dedicato.
- Durante la clonazione in un'istanza del cluster di failover (FCI), assicurarsi che i punti di montaggio esistano, che si tratti di un disco condiviso e che il percorso e l'FCI appartengano allo stesso gruppo di risorse SQL.
- Se il database di origine o l'istanza di destinazione si trova su un volume condiviso del cluster (csv), il database clonato si trova nel file csv.

Per gli ambienti virtuali (VMDK/RDM), assicurarsi che il punto di montaggio sia un disco dedicato.

A proposito di questa attività

- IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

  Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

  È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- La maggior parte dei campi delle pagine della procedura guidata del ciclo di vita del clone sono esplicativi. Le seguenti informazioni descrivono i campi per i quali potrebbe essere necessaria una guida.
- Per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco Snapshot, i cloni creati dagli Snapshot a prova di manomissione ereditano il tempo di scadenza SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il gruppo di risorse o il database, quindi fare clic su **Clone Lifecycle**.
4. Nella pagina Opzioni, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Clonare il nome del lavoro	Specificare il nome del lavoro del ciclo di vita del clone che consente di monitorare e modificare il lavoro del ciclo di vita del clone.
Server clone	Scegliere l'host su cui posizionare il clone.
Clonare l'istanza	Scegliere l'istanza del clone in cui si desidera clonare il database. Questa istanza SQL deve trovarsi nel server clone specificato.
Suffisso clone	Inserire un suffisso che verrà aggiunto al database dei cloni per identificare che si tratta di un clone. Ogni istanza SQL utilizzata per creare un gruppo di risorse clone deve avere un nome di database univoco. Ad esempio, se il gruppo di risorse clone contiene un database di origine "db1" da un'istanza SQL "inst1" e se "db1" viene clonato in "inst1", il nome del database clone deve essere "db1*clone". "*clone" è un suffisso obbligatorio definito dall'utente in quanto il database viene clonato nella stessa istanza. Se "db1" viene clonato nell'istanza SQL "inst2", il nome del database clone può rimanere "db1" (il suffisso è facoltativo) perché il database viene clonato in un'istanza diversa.

Per questo campo…	Eseguire questa operazione…
Assegnazione automatica del punto di montaggio o assegnazione automatica del punto di montaggio del volume sotto il percorso	Scegliere se assegnare automaticamente un punto di montaggio o un punto di montaggio del volume sotto un percorso. La scelta di assegnare automaticamente un punto di montaggio del volume sotto un percorso consente di fornire una directory specifica. I punti di montaggio verranno creati all'interno di tale directory. Prima di scegliere questa opzione, assicurarsi che la directory sia vuota. Se nella directory è presente un database, il database si trova in uno stato non valido dopo l'operazione di montaggio.

5. Nella pagina Location (posizione), selezionare una posizione di storage per creare un clone.
6. Nella pagina script, immettere il percorso e gli argomenti del prespt o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di clone.

   Ad esempio, è possibile eseguire uno script per aggiornare i trap SNMP, automatizzare gli avvisi, inviare i registri e così via.

   > Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

   Il timeout predefinito dello script è di 60 secondi.

7. Nella pagina Schedule (Pianificazione), eseguire una delle seguenti operazioni:
   - Selezionare **Esegui ora** se si desidera eseguire il processo di clonazione immediatamente.
   - Selezionare **Configure schedule** (Configura pianificazione) per determinare la frequenza con cui deve essere eseguita l'operazione di clonazione, quando deve essere avviata la pianificazione, in quale giorno deve essere eseguita l'operazione di clonazione, quando deve scadere la pianificazione e se i cloni devono essere cancellati dopo la scadenza della pianificazione.
8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report**.

   > Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

   Per EMS, fare riferimento a. "Gestire la raccolta di dati EMS"

9. Esaminare il riepilogo, quindi fare clic su **fine**.

È necessario monitorare il processo di cloning utilizzando la pagina **Monitor** > **Jobs**.

Monitorare le operazioni di clonazione del database SQL

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter

utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Clone**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato del clone.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro clone, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

Annullare le operazioni di clonazione delle risorse SQL

È possibile annullare le operazioni di clonazione inserite nella coda.

Per annullare le operazioni di clonazione, accedere come amministratore SnapCenter o come proprietario del processo.

A proposito di questa attività

- È possibile annullare un'operazione di clonazione in coda dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione clone in esecuzione.
- È possibile utilizzare l'interfaccia grafica di SnapCenter, i cmdlet PowerShell o i comandi CLI per annullare le operazioni di clonazione in coda.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di cloni in coda degli altri membri durante l'utilizzo di tale ruolo.

Fase

Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. 2. Selezionare l'operazione e fare clic su **Annulla lavoro**.
Riquadro delle attività	1. Dopo aver avviato l'operazione di clonazione, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. 2. Selezionare l'operazione. 3. Nella pagina **Dettagli processo**, fare clic su **Annulla processo**.

Separare un clone

È possibile utilizzare SnapCenter per separare una risorsa clonata dalla risorsa principale. Il clone diviso diventa indipendente dalla risorsa padre.

A proposito di questa attività

- Non è possibile eseguire l'operazione di suddivisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato il clone1 da un backup del database, è possibile creare un backup del clone1 e clonare il backup (clone2). Dopo aver creato il clone2, il clone1 è un clone intermedio e non è possibile eseguire l'operazione di suddivisione del clone sul clone1. Tuttavia, è possibile eseguire l'operazione di suddivisione dei cloni sul clone2.

  Dopo aver diviso il clone2, è possibile eseguire l'operazione di divisione del clone sul clone1, poiché il clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i lavori di clonazione del clone vengono eliminati.
- Per informazioni sulle limitazioni delle operazioni di suddivisione clone, vedere "Guida alla gestione dello storage logico di ONTAP 9".
- Assicurarsi che il volume o l'aggregato sul sistema di storage sia online.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **risorse**, selezionare l'opzione appropriata dall'elenco Visualizza:

Opzione	Descrizione
Per applicazioni di database	Selezionare **Database** dall'elenco View (Visualizza).
Per file system	Selezionare **Path** dall'elenco View (Visualizza).

3. Selezionare la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Nella vista **Gestisci copie**, selezionare la risorsa clonata (ad esempio, il database o il LUN), quindi fare clic su * *  .
5. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
6. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

   Se il servizio SMCore viene riavviato, l'operazione di split clone smette di rispondere. Eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione di suddivisione del clone.

   Se si desidera un tempo di polling più lungo o più breve per controllare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo in cui SMCore deve eseguire il polling per lo stato dell'operazione di suddivisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Ad esempio:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   L'operazione di avvio del clone split non riesce se sono in corso operazioni di backup, ripristino o altro clone split. È necessario riavviare l'operazione di suddivisione dei cloni solo al termine delle operazioni in esecuzione.

Informazioni correlate

"Il clone o la verifica di SnapCenter non riesce e l'aggregato non esiste"

Proteggere i database SAP HANA

Plug-in SnapCenter per database SAP HANA

Panoramica del plug-in SnapCenter per il database SAP HANA

Il plug-in SnapCenter per database SAP HANA è un componente lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati applicativa dei database SAP HANA. Il plug-in per il database SAP HANA automatizza il backup, il ripristino e la clonazione dei database SAP HANA nel tuo ambiente SnapCenter.

SnapCenter supporta container singoli e container di database multi-tenant (MDC). È possibile utilizzare il plug-in per il database SAP HANA in ambienti Windows e Linux. Il plug-in non installato sull'host del database HANA è noto come plug-in centralizzato dell'host. Il plug-in dell'host centralizzato può gestire database HANA multipli su host diversi.

Una volta installato il plug-in per il database SAP HANA, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror dei set di backup su un altro volume. È inoltre possibile utilizzare il plug-in con la tecnologia NetApp SnapVault per eseguire la replica del backup disk-to-disk per garantire la conformità agli standard.

Operazioni che è possibile eseguire utilizzando il plug-in SnapCenter per il database SAP HANA

Quando installi il plug-in per il database SAP HANA nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei database SAP HANA e delle relative risorse. È inoltre possibile eseguire attività a supporto di tali operazioni.

- Aggiungere database.
- Creare backup.
- Ripristinare dai backup.
- Clonare i backup.
- Pianificare le operazioni di backup.
- Monitorare le operazioni di backup, ripristino e clonazione.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

Plug-in SnapCenter per le funzionalità del database SAP HANA

SnapCenter si integra con l'applicazione plug-in e con le tecnologie NetApp del sistema storage. Per utilizzare il plug-in per il database SAP HANA, utilizzare l'interfaccia grafica utente di SnapCenter.

- **Interfaccia utente grafica unificata**

  L'interfaccia SnapCenter offre standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia di SnapCenter consente di completare operazioni di backup, ripristino e clonazione coerenti tra i plug-in, utilizzare report centralizzati, utilizzare visualizzazioni dashboard a colpo d'occhio, impostare RBAC (role-

based access control) e monitorare i processi in tutti i plug-in.

- **Amministrazione centrale automatizzata**

  È possibile pianificare le operazioni di backup, configurare la conservazione dei backup basata su policy ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per l'invio di avvisi e-mail.

- **Tecnologia di copia Snapshot NetApp senza interruzioni**

  SnapCenter utilizza la tecnologia Snapshot di NetApp con il plug-in per il database SAP HANA per eseguire il backup delle risorse.

L'utilizzo del plug-in per il database SAP HANA offre anche i seguenti vantaggi:

- Supporto per flussi di lavoro di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È inoltre possibile impostare le credenziali in modo che gli utenti SnapCenter autorizzati dispongano delle autorizzazioni a livello di applicazione.

- Creazione di copie delle risorse efficienti in termini di spazio e point-in-time per il test o l'estrazione dei dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema storage in cui si desidera creare il clone.

- Supporto della funzionalità di snapshot del gruppo di coerenza (CG) di ONTAP durante la creazione dei backup.
- Possibilità di eseguire più backup contemporaneamente su più host di risorse

  In una singola operazione, le Snapshot vengono consolidate quando le risorse di un singolo host condividono lo stesso volume.

- Possibilità di creare snapshot utilizzando comandi esterni.
- Supporto per il backup basato su file.
- Supporto per Linux LVM su file system XFS.

Tipi di storage supportati dal plug-in SnapCenter per database SAP HANA

SnapCenter supporta un'ampia gamma di tipi di storage su macchine fisiche e macchine virtuali (VM). Prima di installare il plug-in SnapCenter per il database SAP HANA, è necessario verificare il supporto per il tipo di storage in uso.

Macchina	Tipo di storage
Server fisici e virtuali	LUN connessi a FC
Server fisico	LUN connessi a iSCSI
Server fisici e virtuali	Volumi connessi a NFS

Privilegi ONTAP minimi richiesti per il plug-in SAP HANA

I privilegi minimi di ONTAP richiesti variano in base ai plug-in di SnapCenter utilizzati per la protezione dei dati.

- All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
  - event generate-autosupport-log
  - mostra la cronologia dei lavori
  - interruzione del lavoro
  - lun
  - lun create (crea lun)
  - lun create (crea lun)
  - lun create (crea lun)
  - lun delete (elimina lun)
  - lun igroup add
  - lun igroup create
  - lun igroup delete (elimina igroup lun)
  - lun igroup rename (rinomina lun igroup)
  - lun igroup rename (rinomina lun igroup)
  - lun igroup show
  - lun mapping add-reporting-node
  - creazione mappatura lun
  - eliminazione della mappatura lun
  - nodi di remove-reporting-mapping lun
  - visualizzazione della mappatura del lun
  - modifica del lun
  - lun move-in-volume
  - lun offline
  - lun online
  - lun persistent-reservation clear
  - ridimensionamento del lun
  - lun seriale
  - lun show
  - regola aggiuntiva del criterio snapmirror
  - regola-modifica del criterio snapmirror
  - regola di rimozione del criterio snapmirror
  - policy di snapmirror
  - ripristino di snapmirror

- spettacolo di snapmirror
- storia di snapmirror
- aggiornamento di snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione del clone del volume
- visualizzazione del clone del volume
- avvio della divisione del clone del volume
- interruzione della divisione del clone del volume
- creazione del volume
- distruggere il volume
- creazione del clone del file di volume
- file di volume show-disk-usage
- volume offline
- volume online
- modifica del volume
- creazione del qtree del volume
- eliminazione del qtree del volume
- modifica del qtree del volume
- visualizzazione del qtree del volume
- limitazione del volume
- presentazione del volume
- creazione di snapshot di volume
- eliminazione dello snapshot del volume
- modifica dello snapshot del volume
- rinominare lo snapshot del volume
- ripristino dello snapshot del volume
- file di ripristino dello snapshot del volume
- visualizzazione di snapshot di volume
- smontare il volume
- cifs vserver
- creazione condivisione cifs vserver
- eliminazione condivisione cifs vserver
- vserver cifs shadowcopy mostra
- show di condivisione di vserver cifs
- vserver cifs show

    - policy di esportazione di vserver
    - creazione policy di esportazione vserver
    - eliminazione della policy di esportazione di vserver
    - creazione della regola dei criteri di esportazione di vserver
    - visualizzazione della regola dei criteri di esportazione di vserver
    - visualizzazione della policy di esportazione di vserver
    - iscsi vserver
    - visualizzazione della connessione iscsi del vserver
    - show di vserver
- Comandi di sola lettura: Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete
    - visualizzazione dell'interfaccia di rete
    - server virtuale

Preparazione dei sistemi storage per la replica di SnapMirror e SnapVault per i database SAP HANA

È possibile utilizzare un plug-in SnapCenter con la tecnologia SnapMirror di ONTAP per creare copie mirror dei set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replica del backup disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti di SnapMirror e SnapVault al termine dell'operazione di Snapshot. Gli aggiornamenti di SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter; non creare una pianificazione ONTAP separata.

Se vieni a SnapCenter da un prodotto NetApp SnapManager e sei soddisfatto delle relazioni di protezione dei dati che hai configurato, puoi saltare questa sezione.

Una relazione di protezione dei dati replica i dati sullo storage primario (il volume di origine) nello storage secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui fa riferimento il volume di origine al volume di destinazione.

SnapCenter non supporta le relazioni a cascata tra SnapMirror e i volumi SnapVault (**primario** > **Mirror** > **Vault**). Si consiglia di utilizzare le relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per ulteriori informazioni sulle relazioni di SnapMirror flessibili per la versione e sulla loro configurazione, vedere la "Documentazione ONTAP".

SnapCenter non supporta la replica **Sync_mirror**.

Strategia di backup per i database SAP HANA

Definire una strategia di backup per i database SAP HANA

La definizione di una strategia di backup prima della creazione dei processi di backup consente di ottenere i backup necessari per ripristinare o clonare correttamente le risorse. Il tuo SLA (Service-Level Agreement), RTO (Recovery Time Objective) e RPO (Recovery Point Objective) determinano in gran parte la tua strategia di backup.

A proposito di questa attività

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. RTO è il momento in cui un processo di business deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

Fasi

1. Stabilire quando eseguire il backup delle risorse.
2. Decidere il numero di processi di backup necessari.
3. Decidere come assegnare un nome ai backup.
4. Decidere se creare un criterio basato su copie Snapshot per eseguire il backup degli Snapshot coerenti con l'applicazione del database.
5. Decidere se verificare l'integrità del database.
6. Decidere se utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.
7. Determina il periodo di conservazione per gli Snapshot sul sistema di storage di origine e sulla destinazione di SnapMirror.
8. Determinare se si desidera eseguire qualsiasi comando prima o dopo l'operazione di backup e fornire una prescrizione o postscript.

Rilevamento automatico delle risorse sull'host Linux

Le risorse sono database SAP HANA e volumi non dati sull'host Linux gestiti da SnapCenter. Dopo aver installato il plug-in SnapCenter per il database SAP HANA, i database SAP HANA su quell'host vengono automaticamente rilevati e visualizzati nella pagina risorse.

Il rilevamento automatico è supportato per le seguenti risorse SAP HANA:

- Contenitori singoli

  Dopo l'installazione o l'aggiornamento del plug-in, le singole risorse container situate in un plug-in host centralizzato continueranno come risorse aggiunte manualmente.

  Dopo aver installato o aggiornato il plug-in, i database SAP HANA vengono rilevati automaticamente solo sugli host SAP HANA Linux, che sono direttamente registrati in SnapCenter.

- Container di database multi-tenant (MDC)

Dopo aver installato o aggiornato il plug-in, le risorse MDC che si trovano in un plug-in host centralizzato continueranno come risorse aggiunte manualmente.

È necessario continuare ad aggiungere manualmente le risorse MDC nel plug-in host centralizzato dopo l'aggiornamento a SnapCenter 4.3.

Per gli host SAP HANA Linux registrati direttamente in SnapCenter, l'installazione o l'aggiornamento del plug-in attiverà un rilevamento automatico delle risorse sull'host. Dopo l'aggiornamento del plug-in, per ogni risorsa MDC che si trovava sull'host del plug-in, un'altra risorsa MDC verrà automaticamente rilevata con un formato GUID diverso e registrata in SnapCenter. La nuova risorsa sarà bloccata.

Ad esempio, in SnapCenter 4.2, se la risorsa MDC E90 era localizzata nell'host del plug-in e registrata manualmente, dopo l'aggiornamento a SnapCenter 4.3, un'altra risorsa MDC E90 con un GUID diverso verrà rilevata e registrata in SnapCenter.

Il rilevamento automatico non è supportato per le seguenti configurazioni:

- Layout RDM e VMDK

  Nel caso in cui vengano rilevate le suddette risorse, le operazioni di protezione dei dati non sono supportate da queste risorse.

- Configurazione di più host HANA
- Istanze multiple sullo stesso host
- Replica del sistema HANA con scalabilità orizzontale multi-Tier
- Ambiente di replica a cascata in modalità di replica del sistema

Tipo di backup supportati

Il tipo di backup specifica il tipo di backup che si desidera creare. SnapCenter supporta i tipi di backup basati su file e snapshot per i database SAP HANA.

Backup basato su file

I backup basati su file verificano l'integrità del database. È possibile pianificare l'esecuzione dell'operazione di backup basata su file a intervalli specifici. Viene eseguito il backup solo dei tenant attivi. Non è possibile ripristinare e clonare i backup basati su file da SnapCenter.

Backup basato su copia Snapshot

I backup basati su copie Snapshot sfruttano la tecnologia NetApp Snapshot per creare copie online di sola lettura dei volumi su cui risiedono i database SAP HANA.

Come il plug-in SnapCenter per database SAP HANA utilizza le Snapshot del gruppo di coerenza

È possibile utilizzare il plug-in per creare istantanee del gruppo di coerenza per i gruppi di risorse. Un gruppo di coerenza è un container che può ospitare più volumi in modo da poterli gestire come un'unica entità. Un gruppo di coerenza è costituito da Snapshot simultanee di più volumi, che forniscono copie coerenti di un gruppo di volumi.

È anche possibile specificare il tempo di attesa per lo storage controller che raggruppa in modo coerente gli

Snapshot. Le opzioni di tempo di attesa disponibili sono **urgente**, **Medio** e **rilassato**. È inoltre possibile attivare o disattivare la sincronizzazione WAFL (Write Anywhere file Layout) durante l'operazione snapshot di gruppo coerente. WAFL Sync migliora le prestazioni di una Snapshot del gruppo di coerenza.

In che modo SnapCenter gestisce l'housekeeping dei backup di log e dati

SnapCenter gestisce la gestione dei backup di log e dati a livello di sistema storage e file system e all'interno del catalogo di backup SAP HANA.

Le Snapshot sullo storage primario o secondario e le relative voci nel catalogo SAP HANA vengono eliminate in base alle impostazioni di conservazione. Le voci del catalogo SAP HANA vengono eliminate anche durante il backup e l'eliminazione del gruppo di risorse.

Considerazioni per la determinazione delle pianificazioni di backup per il database SAP HANA

Il fattore più critico per determinare una pianificazione di backup è il tasso di cambiamento per la risorsa. È possibile eseguire il backup di una risorsa utilizzata in modo pesante ogni ora, mentre è possibile eseguire il backup di una risorsa utilizzata raramente una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo SLA (Service Level Agreement) e l'RPO (Recovery Point Objective).

Le pianificazioni dei backup sono in due parti, come segue:

- Frequenza del backup (frequenza con cui devono essere eseguiti i backup)

  La frequenza di backup, chiamata anche tipo di pianificazione per alcuni plug-in, fa parte di una configurazione di policy. Ad esempio, è possibile configurare la frequenza di backup come oraria, giornaliera, settimanale o mensile.

- Pianificazioni di backup (esattamente quando devono essere eseguiti i backup

  Le pianificazioni dei backup fanno parte di una configurazione di risorse o gruppi di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione per il backup ogni giovedì alle 10:00

Numero di processi di backup necessari per i database SAP HANA

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, il tasso di cambiamento della risorsa e il contratto SLA (Service Level Agreement).

Convenzioni di denominazione del backup per il plug-in per i database SAP HANA

È possibile utilizzare la convenzione di naming predefinita di Snapshot o una convenzione di naming personalizzata. La convenzione di denominazione predefinita dei backup aggiunge un indicatore data e ora ai nomi Snapshot che consente di identificare quando le copie sono state create.

L'istantanea utilizza la seguente convenzione di denominazione predefinita:

`resourcegroupname_hostname_timestamp`

È necessario assegnare un nome logico ai gruppi di risorse di backup, come nell'esempio seguente:

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

In questo esempio, gli elementi di sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* indica data e ora.

In alternativa, è possibile specificare il formato del nome dell'istantanea mentre si proteggono le risorse o i gruppi di risorse selezionando **Usa il formato del nome personalizzato per la copia dell'istantanea**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso dell'indicatore data e ora viene aggiunto al nome dell'istantanea.

Strategia di ripristino e recovery per i database SAP HANA

Definire una strategia di ripristino per le risorse SAP HANA

È necessario definire una strategia prima di ripristinare e ripristinare il database in modo da poter eseguire correttamente le operazioni di ripristino e ripristino.

Fasi

1. Determinare le strategie di ripristino supportate per le risorse SAP HANA aggiunte manualmente
2. Determinare le strategie di ripristino supportate per i database SAP HANA rilevati automaticamente
3. Decidere il tipo di operazioni di ripristino che si desidera eseguire.

Tipi di strategie di ripristino supportate per le risorse SAP HANA aggiunte manualmente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per le risorse SAP HANA aggiunte manualmente. Non è possibile ripristinare le risorse SAP HANA aggiunte manualmente.

Non è possibile ripristinare le risorse SAP HANA aggiunte manualmente.

Ripristino completo delle risorse

- Ripristina tutti i volumi, le qtree e le LUN di una risorsa

Se la risorsa contiene volumi o qtree, gli Snapshot acquisiti dopo la Snapshot selezionata per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata.

Ripristino a livello di file

- Ripristina i file da volumi, qtree o directory
- Ripristina solo i LUN selezionati

Tipi di strategie di ripristino supportate per i database SAP HANA rilevati automaticamente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per i database SAP HANA rilevati automaticamente.

Ripristino completo delle risorse

- Ripristina tutti i volumi, le qtree e le LUN di una risorsa
  - Per ripristinare l'intero volume, selezionare l'opzione **Volume Revert** (Ripristina volume).

> Se la risorsa contiene volumi o qtree, gli Snapshot acquisiti dopo la Snapshot selezionata per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata.

Database tenant

- Ripristina il database tenant

Se l'opzione **Database tenant** è selezionata, per eseguire l'operazione di ripristino è necessario utilizzare gli script di ripristino HANA studio o HANA esterni a SnapCenter.

Tipi di operazioni di ripristino per i database SAP HANA rilevati automaticamente

SnapCenter supporta i tipi di ripristino VBSR (Volume-Based SnapRestore), Single file SnapRestore e Connect-and-copy per i database SAP HANA rilevati automaticamente.

Il volume-based SnapRestore (VBSR) viene eseguito in ambienti NFS per i seguenti scenari:

- Quando il backup selezionato per il ripristino viene eseguito su release precedenti a SnapCenter 4.3 e solo se è selezionata l'opzione **completa risorsa**
- Quando il backup selezionato per il ripristino viene eseguito in SnapCenter 4.3 e se è selezionata l'opzione **Ripristino volume**

Single file SnapRestore viene eseguito negli ambienti NFS per i seguenti scenari:

- Quando il backup selezionato per il ripristino viene eseguito in SnapCenter 4.3 e se è selezionata solo l'opzione **completa risorsa**
- Per i contenitori di database multi-tenant (MDC), quando il backup selezionato per il ripristino viene eseguito su SnapCenter 4.3 e l'opzione **Database tenant** è selezionata
- Quando il backup selezionato proviene da una posizione secondaria SnapMirror o SnapVault e l'opzione **completa risorsa** è selezionata

Single file SnapRestore viene eseguito negli ambienti SAN per i seguenti scenari:

- Quando i backup vengono eseguiti su release precedenti a SnapCenter 4.3 e solo se è selezionata l'opzione **completa risorsa**
- Quando i backup vengono eseguiti in SnapCenter 4.3 e solo se è selezionata l'opzione **completa risorsa**
- Quando si seleziona il backup da una posizione secondaria SnapMirror o SnapVault e si seleziona l'opzione **completa risorsa**

Il ripristino basato su connessione e copia viene eseguito negli ambienti SAN per il seguente scenario:

- Per MDC, quando il backup selezionato per il ripristino viene eseguito in SnapCenter 4.3 e l'opzione **Database tenant** è selezionata

Le opzioni **complete Resource**, **Volume Revert** e **Database tenant** sono disponibili nella pagina Restore Scope.

Tipi di operazioni di recovery supportati per i database SAP HANA

SnapCenter consente di eseguire diversi tipi di operazioni di recovery per i database SAP HANA.

- Ripristinare il database fino allo stato più recente
- Ripristinare il database fino a un momento specifico

  Specificare la data e l'ora per il ripristino.

- Ripristinare il database fino a un backup dei dati specifico

SnapCenter offre anche l'opzione No recovery per i database SAP HANA.

Preparare l'installazione del plug-in SnapCenter per il database SAP HANA

Workflow di installazione del plug-in SnapCenter per database SAP HANA

Se si desidera proteggere i database SnapCenter HANA, è necessario installare e configurare il plug-in SAP per il database SAP HANA.

Prerequisiti per l'aggiunta di host e l'installazione del plug-in SnapCenter per il database SAP HANA

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario completare tutti i requisiti. Il plug-in SnapCenter per database SAP HANA è disponibile sia in ambienti Windows che Linux.

- È necessario aver installato Java a 1.8 64 bit sull'host.

  IBM Java non è supportato.

- È necessario aver installato il terminale interattivo del database SAP HANA (client HDBSQL) sull'host.
- Per Windows, il servizio di creazione del plug-in deve essere eseguito utilizzando l'utente di Windows "LocalSystem", che è il comportamento predefinito quando il plug-in per il database SAP HANA viene installato come amministratore di dominio.
- Per Windows, le chiavi dell'archivio utente devono essere create come utente DI SISTEMA.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host. Il plug-in SnapCenter per Microsoft Windows verrà implementato per impostazione predefinita con il plug-in SAP HANA sugli host Windows.
- Per l'host Linux, le chiavi HDB Secure User Store sono accessibili come utente del sistema operativo HDBSQL.
- Il server SnapCenter deve avere accesso alla porta 8145 o alla porta personalizzata del plug-in per l'host del database SAP HANA.

Host Windows

- È necessario disporre di un utente di dominio con privilegi di amministratore locale con autorizzazioni di accesso locale sull'host remoto.
- Durante l'installazione del plug-in per database SAP HANA su un host Windows, il plug-in SnapCenter per Microsoft Windows viene installato automaticamente.
- È necessario aver attivato la connessione SSH basata su password per l'utente root o non root.
- È necessario aver installato Java a 1.8 64 bit sull'host Windows.

  "Download Java per tutti i sistemi operativi"

  "Tool di matrice di interoperabilità NetApp"

Host Linux

- È necessario aver attivato la connessione SSH basata su password per l'utente root o non root.
- È necessario aver installato Java a 1.8 64 bit sull'host Linux.

  "Download Java per tutti i sistemi operativi"

  "Tool di matrice di interoperabilità NetApp"

- Per i database SAP HANA in esecuzione su un host Linux, durante l'installazione del plug-in per il database SAP HANA, il plug-in SnapCenter per UNIX viene installato automaticamente.
- Si dovrebbe avere **bash** come shell predefinita per l'installazione del plug-in.

Comandi supplementari

Per eseguire un comando supplementare sul plug-in SnapCenter per SAP HANA, è necessario includerlo nel `allowed_commands.config` file.

`allowed_commands.config` Il file si trova nella sottodirectory "etc" della directory SnapCenter Plug-in for SAP HANA.

Host Windows

Predefinito: `C:\Program Files\NetApp\SnapCenter\HANA\etc\allowed_commands.config`

Percorso personalizzato:
`<Custome_Directory>\NetApp\SnapCenter\HANA\etc\allowed_commands.config` Host Windows:

Host Linux

Predefinito: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`

Percorso personalizzato:
`<Custome_Directory>/NetApp/snapcenter/scc/etc/allowed_commands.config`

Per consentire comandi supplementari sull'host del plug-in, aprire `allowed_commands.config` il file in un editor. Immettere ciascun comando su una riga separata. Non rileva la distinzione tra maiuscole e minuscole. Ad esempio,

comando: mount

comando: umount

Assicurarsi di specificare il nome del percorso completo. Racchiudere il percorso tra virgolette (") se contiene spazi. Ad esempio,

Comando: "C:\Program Files\NetApp\SnapCreator Commands\sdcli.exe"

comando: myscript.bat

Se il `allowed_commands.config` file non è presente, i comandi o l'esecuzione dello script vengono bloccati e il flusso di lavoro non riesce e viene visualizzato il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizzare aggiungendo il comando nel file %s sull'host del plugin."

Se il comando o lo script non è presente in `allowed_commands.config`, l'esecuzione del comando o dello script viene bloccata e il flusso di lavoro non riesce con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizzare aggiungendo il comando nel file %s sull'host del plugin."

Non utilizzare un carattere jolly (*) per consentire tutti i comandi.

Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario conoscere alcuni requisiti di base relativi allo spazio del sistema host e al dimensionamento.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Elemento	Requisiti
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	5 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp". Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet."

Requisiti dell'host per l'installazione del pacchetto di plug-in SnapCenter per Linux

Prima di installare il pacchetto di plug-in SnapCenter per Linux, è necessario conoscere alcuni requisiti di spazio e dimensionamento di base del sistema host.

Elemento	Requisiti
Sistemi operativi	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".
RAM minima per il plug-in SnapCenter sull'host	1 GB

Elemento	Requisiti
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	Java 1,8.x (64 bit) Oracle Java e OpenJDK Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto. Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Impostare le credenziali per il plug-in SnapCenter per il database SAP HANA

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per l'esecuzione delle operazioni di protezione dei dati su database o file system Windows.

A proposito di questa attività

- Host Linux

  È necessario impostare le credenziali per l'installazione dei plug-in sugli host Linux.

  Per installare e avviare il processo di plug-in, è necessario impostare le credenziali per l'utente root o per un utente non root che dispone dei privilegi di sudo.

  Best practice: sebbene sia consentito creare credenziali per Linux dopo l'implementazione degli host e l'installazione dei plug-in, la Best practice consiste nel creare credenziali dopo l'aggiunta di SVM, prima di distribuire host e installare plug-in.

- Host Windows

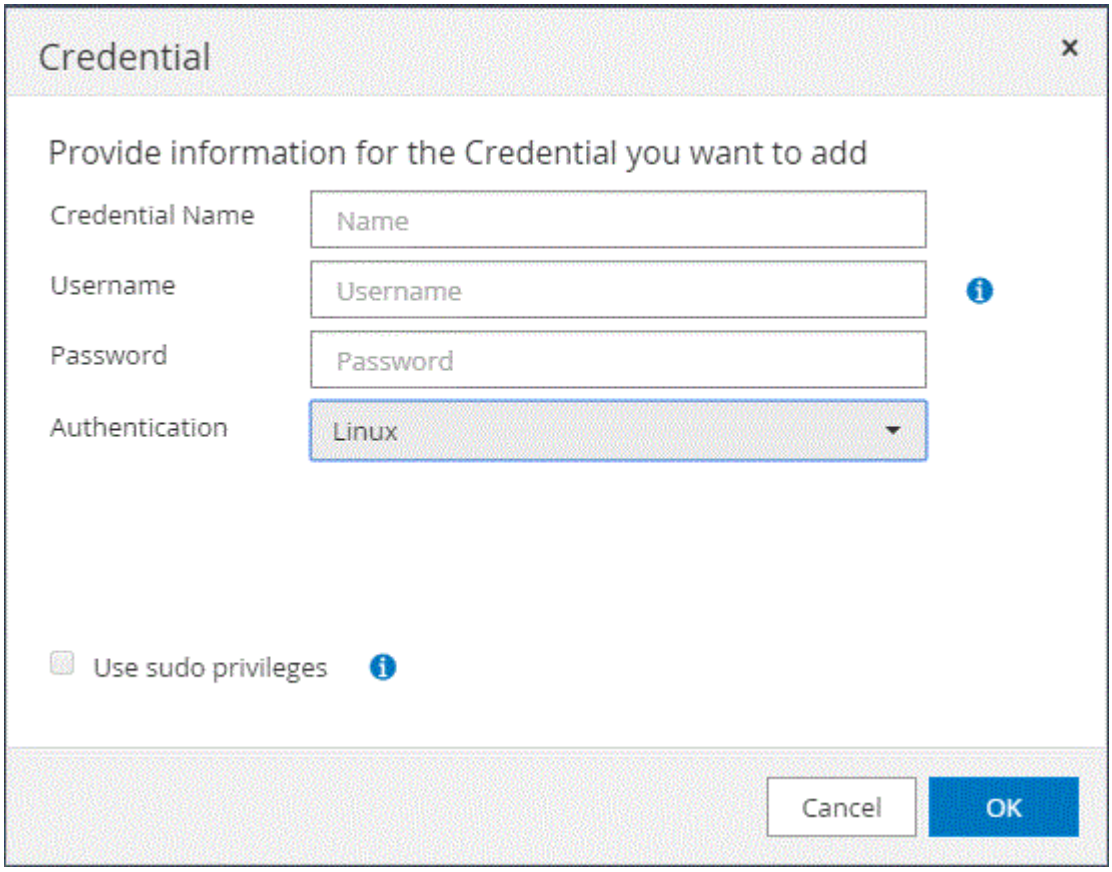
  Prima di installare i plug-in, è necessario impostare le credenziali di Windows.

  È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup al nome utente.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.



4. Nella pagina credenziale, specificare le informazioni necessarie per la configurazione delle credenziali:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale	Immettere un nome per le credenziali.

Per questo campo…	Eseguire questa operazione…
Nome utente	Immettere il nome utente e la password da utilizzare per l'autenticazione. • Amministratore di dominio o qualsiasi membro del gruppo di amministratori Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono: ◦ *NetBIOS/nome utente* ◦ *Dominio FQDN/nome utente* • Amministratore locale (solo per gruppi di lavoro) Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host. Il formato valido per il campo Nome utente è: *Nome utente* Non utilizzare virgolette doppie (") o backtick (`) nelle password. Non utilizzare il valore inferiore a (<) e il punto esclamativo (!) simboli insieme nelle password. Ad esempio, meno di<!10, meno di 10<!, backtick`12.
Password	Inserire la password utilizzata per l'autenticazione.
Modalità di autenticazione	Selezionare la modalità di autenticazione che si desidera utilizzare.
Utilizzare i privilegi sudo	Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root. Applicabile solo agli utenti Linux.

5. Fare clic su **OK**.

Al termine dell'impostazione delle credenziali, è possibile assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina User and Access (utenti e accesso).

Configurare gMSA su Windows Server 2012 o versione successiva

Windows Server 2012 o versione successiva consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatica delle password dell'account di servizio da un account di dominio gestito.

Prima di iniziare

- È necessario disporre di un controller di dominio Windows Server 2012 o versione successiva.
- È necessario disporre di un host Windows Server 2012 o versione successiva, membro del dominio.

Fasi

1. Creare una chiave root KDS per generare password univoche per ogni oggetto in gMSA.
2. Per ciascun dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Creare e configurare gMSA:
   a. Creare un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo di utenti appena creato per creare gMSA.
```

   Ad esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Eseguire `Get-ADServiceAccount` il comando per verificare
l'account del servizio.
```

4. Configurare gMSA sugli host:
   a. Attivare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

   A tale scopo, eseguire il seguente comando da PowerShell:

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

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


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

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Riavviare l'host.

b. Installare gMSA sull'host eseguendo il comando seguente dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verificare il proprio account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter.

   Il server SnapCenter installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

Installare il plug-in SnapCenter per i database SAP HANA

Aggiungere host e installare pacchetti plug-in su host remoti

Utilizzare la pagina Aggiungi host di SnapCenter per aggiungere host e installare i pacchetti dei plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster.

Prima di iniziare

- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.
- Assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.

- La documentazione di amministrazione contiene informazioni sulla gestione degli host.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare account di servizio gestito di gruppo su Windows Server 2012 o versione successiva per SAP HANA"

A proposito di questa attività

- Non è possibile aggiungere un server SnapCenter come host plug-in a un altro server SnapCenter.
- Per consentire a SAP HANA System Replication di rilevare le risorse sui sistemi primario e secondario, si consiglia di aggiungere sia il sistema primario che quello secondario utilizzando l'utente root o sudo.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata nella parte superiore.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare il tipo di host: • Windows • Linux Il plug-in per SAP HANA viene installato sull'host client HDBSQL e questo host può essere installato su un sistema Windows o Linux.
Nome host	Inserire il nome host della comunicazione. Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire l'FQDN. È necessario configurare il client HDBSQL e HDBUserStore su questo host.

Per questo campo…	Eseguire questa operazione…
Credenziali	Selezionare il nome della credenziale creata o creare nuove credenziali. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere le informazioni sulla creazione delle credenziali. È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome fornito. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare i plug-in da installare.
6. (Facoltativo) fare clic su **altre opzioni**.

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.
Percorso di installazione	Il plug-in per SAP HANA viene installato sull'host client HDBSQL e questo host può essere installato su un sistema Windows o Linux. • Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C: In alternativa, è possibile personalizzare il percorso. • Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è /opt/NetApp/snapcenter. In alternativa, è possibile personalizzare il percorso.
Ignorare i controlli di preinstallazione	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

Per questo campo…	Eseguire questa operazione…
Utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in	Per l'host Windows, selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in. Fornire il nome gMSA nel seguente formato: Nome dominio/nome account. GMSA verrà utilizzato come account del servizio di accesso solo per il servizio del plug-in SnapCenter per Windows.

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo Ignora controlli preliminari, l'host viene convalidato per verificare se l'host soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione PowerShell, . La versione NET, la posizione (per i plug-in Windows) e la versione Java (per i plug-in Linux) sono convalidate in base ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati.

   Se l'errore riguarda lo spazio su disco o la RAM, è possibile aggiornare il file web.config che si trova in C: File di programma NetApp SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione ha, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi fare clic su **Confirm and Submit** (Conferma e invia).

   In una configurazione del cluster, verificare l'impronta digitale di ciascuno dei nodi del cluster.

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

   I file di log specifici dell'installazione si trovano in /custom_location/snapcenter/logs.

Installare i pacchetti plug-in SnapCenter per Linux o Windows su più host remoti utilizzando i cmdlet

È possibile installare i pacchetti plug-in SnapCenter per Linux o Windows su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage PowerShell.

Prima di iniziare

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto del plug-in.

Fasi

1. Avviare PowerShell.
2. Sull'host del server SnapCenter, stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in su più host utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

   È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserire le credenziali per l'installazione remota.

Installare il plug-in SnapCenter per il database SAP HANA su host Linux utilizzando l'interfaccia della riga di comando

Installare il plug-in SnapCenter per il database SAP HANA utilizzando l'interfaccia utente (UI) di SnapCenter. Se l'ambiente in uso non consente l'installazione remota del plug-in dall'interfaccia utente di SnapCenter, è possibile installare il plug-in per il database SAP HANA in modalità console o silent utilizzando l'interfaccia a riga di comando (CLI).

Prima di iniziare

- Installare il plug-in per il database SAP HANA su ciascun host Linux in cui risiede il client HDBSQL.
- L'host Linux su cui si installa il plug-in SnapCenter per il database SAP HANA deve soddisfare i requisiti di software, database e sistema operativo dipendenti.

  Lo strumento matrice di interoperabilità (IMT) contiene le informazioni più recenti sulle configurazioni supportate.

  "Tool di matrice di interoperabilità NetApp"

- Il plug-in SnapCenter per il database SAP HANA fa parte del pacchetto di plug-in SnapCenter per Linux. Prima di installare il pacchetto di plug-in SnapCenter per Linux, è necessario aver già installato SnapCenter su un host Windows.

Fasi

1. Copiare il file di installazione del pacchetto plug-in SnapCenter per Linux (Snapcenter_linux_host_plugin.bin) da C: ProgramData/NetApp SnapCenter/Package Repository all'host in cui si desidera installare il plug-in per il database SAP HANA.

   È possibile accedere a questo percorso dall'host in cui è installato il server SnapCenter.

2. Dal prompt dei comandi, accedere alla directory in cui è stato copiato il file di installazione.
3. Installare il plug-in: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

   - -DPORT specifica la porta di comunicazione HTTPS SMCore.
   - -DSERVER_IP specifica l'indirizzo IP del server SnapCenter.

- -DSERVER_HTTPS_PORT specifica la porta HTTPS del server SnapCenter.
- -DUSER_INSTALL_DIR specifica la directory in cui si desidera installare il pacchetto di plug-in SnapCenter per Linux.
- DINSTALL_LOG_NAME specifica il nome del file di log.

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

4. Modificare il file /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, quindi aggiungere IL parametro PLUGINS_ENABLED = hana:3.0.
5. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare lo stato dell'installazione del plug-in per SAP HANA

È possibile monitorare lo stato di avanzamento dell'installazione del pacchetto plug-in di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento dell'installazione per determinare quando è completa o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filter** (filtro).
   b. Facoltativo: Specificare la data di inizio e di fine.
   c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).

d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.

e. Fare clic su **Apply** (Applica).

4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Configurare il certificato CA

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare una CSR, vedere "Come generare il file CSR del certificato CA".

Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato del file di importazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
   c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
   d. Copiare i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

      Get-ChildItem -Path Certate: LocalMachine/My

   b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

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

   Ad esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in
   dell'host Windows eseguendo i seguenti comandi:
   ```

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

   Ad esempio:

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

Configurare il certificato CA per il servizio plug-in SAP HANA di SnapCenter sull'host Linux

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file 'keystore.jks', che si trova in */opt/NetApp/snapcenter/scc/etc* sia come Trust-store che come keystore.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Modificare la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle chiavi private nel
keystore con la stessa password utilizzata per il keystore:
```

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

Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.

La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato: /Opt/NetApp/snapcenter/scc/ecc.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

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

4. Aggiungere un certificato root o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Riavviare il servizio dopo aver configurato i certificati root o
intermedi in un archivio di trust plug-in personalizzato.
```

Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato /opt/NetApp/snapcenter/scc/ecc.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

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

4. Aggiungere il certificato CA con chiave pubblica e privata.

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

5. Elencare i certificati aggiunti nel keystore.

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

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file agent.properties.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias con un nome
semplice:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurare il nome alias del certificato CA nel file
agent.properties.
```

   Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è ' opt/NetApp/snapcenter/scc/etc/crl'.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

   È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Configurare il certificato CA per il servizio plug-in SAP HANA di SnapCenter sull'host Windows

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file *keystore.jks*, che si trova in _C: File di programma NetApp, SnapCenter, Snapcenter Plug-in Creator, ecc., sia come archivio di fiducia che come archivio chiavi.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Modificare la password del keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se il comando "keytool" non viene riconosciuto dal prompt dei comandi di Windows, sostituire il comando keytool con il relativo percorso completo.

   C: File di programma Java <jdk_version> keytool.exe" -storepasswd -keystore keystore.jks

3. Modificare la password per tutti gli alias delle chiavi private nel keystore con la stessa password utilizzata per il keystore:

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

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.

   > La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato _C: File di programma/NetApp/SnapCenter/Snapcenter Plug-in Creator
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

keytool -list -v -keystore keystore.jks

4. Aggiungere un certificato root o intermedio:

   Keytool -import -trustcaacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Riavviare il servizio dopo aver configurato i certificati root o intermedi in un archivio di trust plug-in personalizzato.

   Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato _C: File di programma/NetApp/SnapCenter/Snapcenter Plug-in Creator
2. Individuare il file *keystore.jks*.
3. Elencare i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungere il certificato CA con chiave pubblica e privata.

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

5. Elencare i certificati aggiunti nel keystore.

   keytool -list -v -keystore keystore.jks

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file agent.properties.

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

8. Configurare il nome alias del certificato CA nel file *agent.properties*.

   Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- Per scaricare il file CRL più recente per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoca dei certificati nel certificato CA di SnapCenter".
- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.

- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è _'C: File di programma, NetApp, SnapCenter, SnapCenter Plug-in Creator, ecc.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave CRL_PATH.
2. È possibile inserire più file CRL in questa directory.

   I certificati in entrata verranno verificati per ciascun CRL.

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.
5. Selezionare **attiva convalida certificato**.

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- * * Indica che il certificato CA non è né abilitato né assegnato all'host del plug-in.
- * * Indica che il certificato CA è stato convalidato correttamente.
- * * Indica che il certificato CA non può essere convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Installare il plug-in SnapCenter per VMware vSphere

Se il database o il file system sono memorizzati su macchine virtuali (VM), o se si

desidera proteggere macchine virtuali e datastore, è necessario implementare il plug-in SnapCenter per l'appliance virtuale VMware vSphere.

Per informazioni sulla distribuzione, vedere "Panoramica sull'implementazione".

Implementare il certificato CA

Per configurare il certificato CA con il plug-in SnapCenter per VMware vSphere, vedere "Creare o importare un certificato SSL".

Configurare il file CRL

Il plug-in SnapCenter per VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il plug-in SnapCenter per VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Prepararsi alla protezione dei dati

Prerequisiti per l'utilizzo del plug-in SnapCenter per il database SAP HANA

Prima di utilizzare il plug-in SnapCenter per il database SAP HANA, l'amministratore di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività necessarie.

- Installare e configurare il server SnapCenter.
- Accedere al server SnapCenter.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di storage e creando credenziali, se applicabili.
- Installare Java 1.7 o Java 1.8 sull'host Linux o Windows.

  È necessario impostare il percorso Java nella variabile di percorso ambientale del computer host.

- Impostare SnapMirror e SnapVault, se si desidera eseguire la replica del backup.
- Installare il client HDBSQL sull'host in cui verrà installato il plug-in per il database SAP HANA.

  Configurare le chiavi dell'archivio utente per i nodi SAP HANA che verranno gestiti tramite questo host.

- Per il database SAP HANA 2.0SPS05, se si utilizza un account utente del database SAP HANA, assicurarsi di disporre delle seguenti autorizzazioni per eseguire operazioni di backup, ripristino e clonazione nel server SnapCenter:
  - Amministratore del backup
  - Catalogo letto
  - Amministratore del backup del database
  - Operatore di ripristino del database

Utilizzo di risorse, gruppi di risorse e policy per la protezione dei database SAP HANA

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- In genere, le risorse sono database SAP HANA di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è un insieme di risorse su un host.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È inoltre possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- I criteri specificano la frequenza di backup, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano uno o più criteri per tale gruppo. È inoltre possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

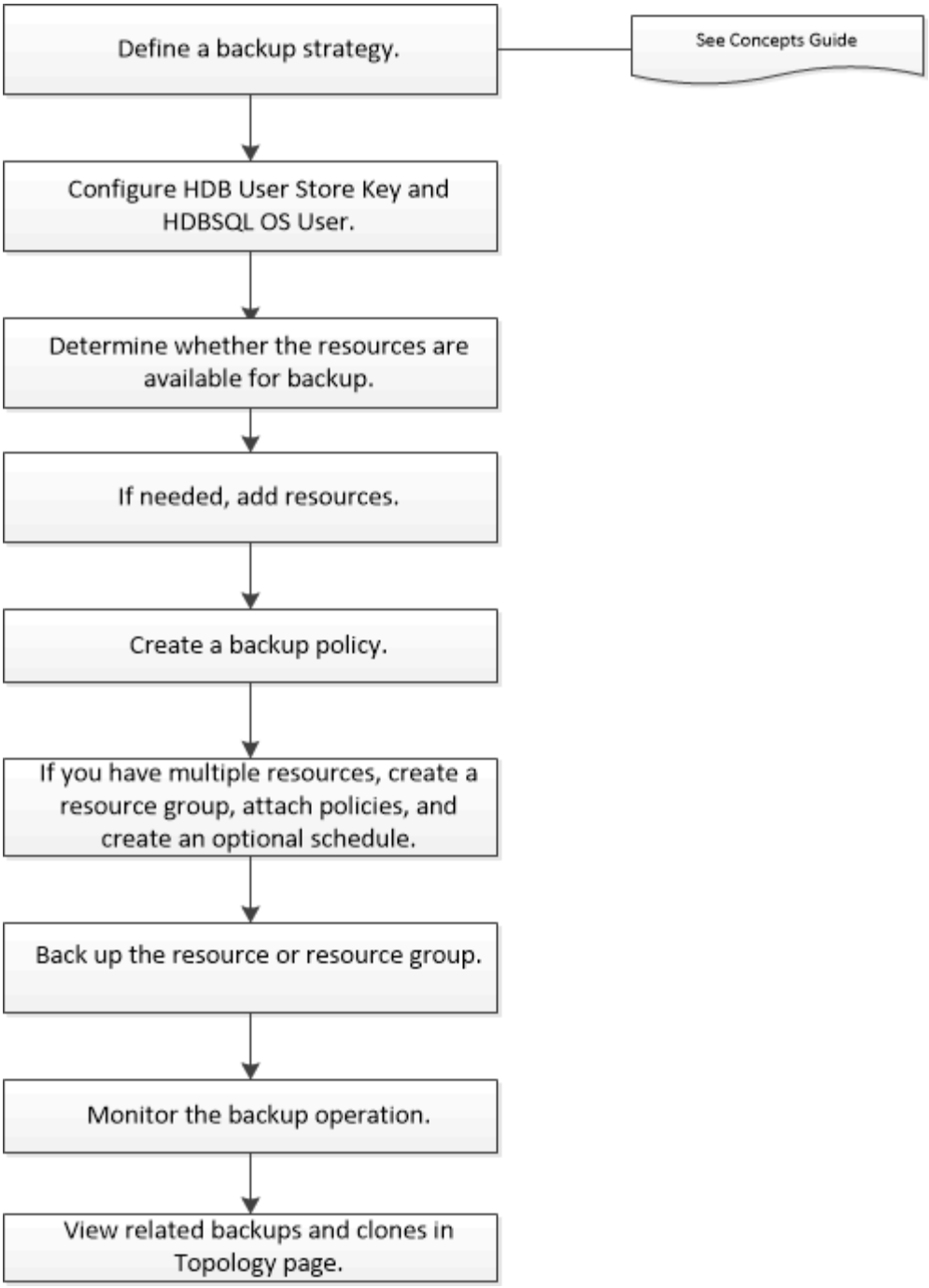
Un gruppo di risorse definisce ciò che si desidera proteggere e quando si desidera proteggerlo in termini di giorno e ora. Pensa a una policy come a come vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i database, è possibile creare un gruppo di risorse che includa tutti i database dell'host. È quindi possibile associare due criteri al gruppo di risorse: Una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si allegano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno.

Eseguire il backup delle risorse SAP HANA

Eseguire il backup delle risorse SAP HANA

È possibile creare un backup di una risorsa (database) o di un gruppo di risorse. Il workflow di backup include la pianificazione, l'identificazione dei database per il backup, la gestione delle policy di backup, la creazione di gruppi di risorse e l'aggiunta di policy, la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida in linea del cmdlet di SnapCenter e le informazioni di riferimento del cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell. "Guida di riferimento al cmdlet del software SnapCenter".

Configurare HDB User Store Key e HDBSQL OS User per il database SAP HANA

È necessario configurare HDB User Store Key e HDBSQL OS User per eseguire operazioni di protezione dei dati sui database SAP HANA.

Prima di iniziare

- Se il database SAP HANA non dispone della chiave HDB Secure User Store e dell'utente HDB SQL OS, viene visualizzata un'icona a forma di lucchetto rosso solo per le risorse rilevate automaticamente. Se

durante un'operazione di rilevamento successiva, la chiave di memorizzazione utente sicura HDB configurata non è corretta o non ha consentito l'accesso al database stesso, viene visualizzata nuovamente l'icona del lucchetto rosso.

- È necessario configurare la chiave di archiviazione utente sicura HDB e l'utente SQL OS HDB per proteggere il database o aggiungerlo a un gruppo di risorse per eseguire operazioni di protezione dei dati.
- È necessario configurare HDB SQL OS User per accedere al database di sistema. Se HDB SQL OS User è configurato per accedere solo al database tenant, l'operazione di rilevamento non riesce.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in SnapCenter per il database SAP HANA dall'elenco.
2. Nella pagina risorse, selezionare il tipo di risorsa dall'elenco **Visualizza**.
3. (Facoltativo) fare clic su e selezionare il nome host.

   È quindi possibile fare clic su per chiudere il riquadro del filtro.
4. Selezionare il database, quindi fare clic su **Configura database**.
5. Nella sezione Configure database settings (Configura impostazioni database), immettere HDB Secure User Store Key (chiave archivio utente sicura HDB).

   Viene visualizzato il nome host del plug-in e l'utente SQL del sistema operativo HDB viene automaticamente inserito nel campo <sid>.
6. Fare clic su **OK**.

È possibile modificare la configurazione del database dalla pagina topologia.

Scopri le risorse e prepara i container di database multi-tenant per la protezione dei dati

Rilevare automaticamente i database

Le risorse sono database SAP HANA e volumi non dati sull'host Linux gestiti da SnapCenter. È possibile aggiungere queste risorse ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database SAP HANA disponibili.

Prima di iniziare

- È necessario aver già completato attività come l'installazione del server SnapCenter, l'aggiunta della chiave di archiviazione utente HDB, l'aggiunta di host e la configurazione delle connessioni del sistema di storage.
- È necessario aver configurato la chiave di archiviazione utente sicura HDB e l'utente del sistema operativo SQL HDB sull'host Linux.
  - È necessario configurare la chiave di memorizzazione utente HDB con l'utente SID adm. Ad esempio, per il sistema HANA con A22 come SID, la chiave di memorizzazione utente HDB deve essere configurata con a22adm.
- Il plug-in SnapCenter per database SAP HANA non supporta il rilevamento automatico delle risorse che risiedono negli ambienti virtuali RDM/VMDK. Durante l'aggiunta manuale dei database, è necessario fornire le informazioni di storage per gli ambienti virtuali.

A proposito di questa attività

Dopo aver installato il plug-in, tutte le risorse su quell'host Linux vengono automaticamente rilevate e visualizzate nella pagina risorse.

Le risorse rilevate automaticamente non possono essere modificate o eliminate.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Resources**, quindi selezionare il plug-in per il database SAP HANA dall'elenco.
2. Nella pagina risorse, selezionare il tipo di risorsa dall'elenco Visualizza.
3. (Facoltativo) fare clic su  , quindi selezionare il nome host.

   È quindi possibile fare clic su  per chiudere il riquadro del filtro.
4. Fare clic su **Refresh Resources** (Aggiorna risorse) per scoprire le risorse disponibili sull'host.

   Le risorse vengono visualizzate insieme a informazioni quali tipo di risorsa, nome host, gruppi di risorse associati, tipo di backup, criteri e stato generale.

   - Se il database si trova su uno storage NetApp e non è protetto, nella colonna Stato generale viene visualizzato non protetto.
   - Se il database si trova su un sistema storage NetApp e viene protetto e non viene eseguita alcuna operazione di backup, nella colonna Stato generale viene visualizzato Backup Not run (Backup non eseguito). In caso contrario, lo stato cambia in Backup failed (Backup non riuscito) o Backup successed (Backup riuscito) in base allo stato dell'ultimo backup.

> Se il database SAP HANA non dispone di una chiave di memorizzazione utente sicura HDB configurata, accanto alla risorsa viene visualizzata un'icona a forma di lucchetto rosso. Se durante un'operazione di rilevamento successiva, la chiave di memorizzazione utente sicura HDB configurata non è corretta o non ha consentito l'accesso al database stesso, viene visualizzata nuovamente l'icona del lucchetto rosso.

> È necessario aggiornare le risorse se i database vengono rinominati al di fuori di SnapCenter.

Al termine

È necessario configurare la chiave di archiviazione utente sicura HDB e l'utente del sistema operativo HDBSQL per proteggere il database o aggiungerlo al gruppo di risorse per eseguire operazioni di protezione dei dati.

"Configurare HDB User Store Key e HDBSQL OS User per il database SAP HANA"

Preparare container di database multi-tenant per la protezione dei dati

Per gli host SAP HANA registrati direttamente in SnapCenter, l'installazione o l'aggiornamento del plug-in SnapCenter per il database SAP HANA attiverà un rilevamento automatico delle risorse sull'host. Dopo l'installazione o l'aggiornamento del plug-in, per ogni risorsa MDC (Multitenant Database Container) che si trovava sull'host del plug-in, un'altra risorsa MDC verrà rilevata automaticamente con un formato GUID diverso e registrata in SnapCenter. La nuova risorsa sarà in stato "Locked".

A proposito di questa attività

Ad esempio, in SnapCenter 4.2, se la risorsa MDC E90 era localizzata nell'host del plug-in e registrata manualmente, dopo l'aggiornamento a SnapCenter 4.3, un'altra risorsa MDC E90 con un GUID diverso verrà rilevata e registrata in SnapCenter.

> I backup associati alla risorsa di SnapCenter 4.2 e versioni precedenti devono essere conservati fino alla scadenza del periodo di conservazione. Una volta scaduto il periodo di conservazione, è possibile eliminare la vecchia risorsa MDC e continuare a gestire la nuova risorsa MDC rilevata automaticamente.

`Old MDC resource` È la risorsa MDC per un host plug-in aggiunto manualmente in SnapCenter 4,2 o versioni precedenti.

Attenersi alla seguente procedura per iniziare a utilizzare la nuova risorsa scoperta in SnapCenter 4.3 per le operazioni di protezione dei dati:

Fasi

1. Nella pagina risorse, selezionare la vecchia risorsa MDC con i backup aggiunti alla release precedente di SnapCenter e posizionarla in "maintage mode" dalla pagina topologia.

   Se la risorsa fa parte di un gruppo di risorse, posizionare il gruppo di risorse in "maintance mode".

2. Configurare la nuova risorsa MDC rilevata dopo l'aggiornamento a SnapCenter 4.3 selezionando la nuova risorsa dalla pagina risorse.

   "Nuova risorsa MDC" è la risorsa MDC scoperta di recente e scoperta dopo l'aggiornamento del server SnapCenter e dell'host plug-in alla versione 4.3. La nuova risorsa MDC può essere identificata come risorsa con lo stesso SID della vecchia risorsa MDC, per un determinato host e con un'icona a forma di lucchetto rosso accanto alla risorsa nella pagina risorse.

3. Proteggere la nuova risorsa MDC rilevata dopo l'aggiornamento a SnapCenter 4.3 selezionando criteri di protezione, pianificazioni e impostazioni di notifica.
4. Eliminare i backup eseguiti in SnapCenter 4.2 o versioni precedenti in base alle impostazioni di conservazione.
5. Eliminare il gruppo di risorse dalla pagina topologia.
6. Eliminare la vecchia risorsa MDC dalla pagina Resources (risorse).

   Ad esempio, se il periodo di conservazione degli Snapshot primari è di 7 giorni e la conservazione degli Snapshot secondari è di 45 giorni, dopo il completamento di 45 giorni e dopo l'eliminazione di tutti i backup, è necessario eliminare il gruppo di risorse e la vecchia risorsa MDC.

Informazioni correlate

"Configurare HDB User Store Key e HDBSQL OS User per il database SAP HANA"

"Visualizzare i backup e i cloni del database SAP HANA nella pagina topologia"

Aggiungere le risorse manualmente all'host del plug-in

Il rilevamento automatico non è supportato per alcune istanze di HANA. È necessario aggiungere queste risorse manualmente.

Prima di iniziare

- È necessario completare attività come l'installazione del server SnapCenter, l'aggiunta di host, la configurazione delle connessioni del sistema di storage e l'aggiunta della chiave di archiviazione utente HDB.
- Per la replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema HANA in un unico gruppo di risorse e di eseguire il backup di un gruppo di risorse. Ciò garantisce un backup perfetto durante la modalità takeover-failback.

"Creare gruppi di risorse e allegare policy".

A proposito di questa attività

Il rilevamento automatico non è supportato per le seguenti configurazioni:

- Layout RDM e VMDK

> Nel caso in cui vengano rilevate le suddette risorse, le operazioni di protezione dei dati non sono supportate da queste risorse.

- Configurazione di più host HANA
- Istanze multiple sullo stesso host
- Replica del sistema HANA con scalabilità orizzontale multi-Tier
- Ambiente di replica a cascata in modalità di replica del sistema

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare il plug-in SnapCenter per il database SAP HANA dall'elenco a discesa, quindi fare clic su **risorse**.
2. Nella pagina Resources (risorse), fare clic su **Add SAP HANA Database** (Aggiungi database SAP HANA).
3. Nella pagina fornire dettagli sulle risorse, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di risorsa	Inserire il tipo di risorsa. I tipi di risorse sono container singolo, container database multi-tenant (MDC) e Volume non dati.
Nome sistema HANA	Inserire il nome descrittivo del sistema SAP HANA. Questa opzione è disponibile solo se sono stati selezionati i tipi di risorse Single Container o MDC.
SID	Inserire l'ID di sistema (SID). Il sistema SAP HANA installato viene identificato da un singolo SID.
Host plug-in	Selezionare l'host del plug-in.

Per questo campo…	Eseguire questa operazione…
Chiavi di memorizzazione utente sicure HDB	Inserire la chiave per connettersi al sistema SAP HANA. La chiave contiene le informazioni di accesso per la connessione al database. Per SAP HANA System Replication, la chiave utente secondaria non viene convalidata. Questo verrà utilizzato durante il takeover.
Utente del sistema operativo HDBSQL	Immettere il nome utente per il quale è configurata la chiave di memorizzazione utente sicura HDB. Per Windows, è obbligatorio che l'utente del sistema operativo HDBSQL sia l'utente DEL SISTEMA. Pertanto, è necessario configurare la chiave di memorizzazione utente sicura HDB per l'utente DI SISTEMA.

4. Nella pagina fornire footprint dello storage, selezionare un sistema storage e scegliere uno o più volumi, LUN e qtree, quindi fare clic su **Salva**.

   Opzionale: Puoi fare clic sull'icona * * per aggiungere ulteriori volumi, LUN e qtree da altri sistemi storage.

5. Esaminare il riepilogo, quindi fare clic su **fine**.

   I database vengono visualizzati insieme a informazioni quali SID, host plug-in, policy e gruppi di risorse associati e stato generale

Se si desidera fornire agli utenti l'accesso alle risorse, è necessario assegnarle agli utenti. In questo modo, gli utenti possono eseguire le azioni per le quali dispongono delle autorizzazioni per le risorse ad essi assegnate.

"Aggiungere un utente o un gruppo e assegnare ruolo e risorse"

Dopo aver aggiunto i database, è possibile modificare i dettagli del database SAP HANA.

Non è possibile modificare quanto segue se sono presenti backup associati alla risorsa SAP HANA:

- Contenitori di database multitenant (MDC): SID o host client HDBSQL (plug-in)
- Container singolo: Host client (plug-in) SID o HDBSQL
- Volume non dati: Nome della risorsa, SID associato o host plug-in

Creare policy di backup per i database SAP HANA

Prima di utilizzare SnapCenter per eseguire il backup delle risorse di database SAP HANA, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Un criterio di backup è un insieme di regole che regolano la gestione, la pianificazione e la conservazione dei backup.

Prima di iniziare

- È necessario aver definito la strategia di backup.

  Per ulteriori informazioni, consulta le informazioni sulla definizione di una strategia di protezione dei dati per i database SAP HANA.

- Devi essere preparato per la protezione dei dati completando attività come l'installazione di SnapCenter, l'aggiunta di host, la configurazione delle connessioni del sistema di storage e l'aggiunta di risorse.
- L'amministratore di SnapCenter deve aver assegnato le SVM per i volumi di origine e destinazione se si stanno replicando Snapshot in un mirror o un vault.

  Inoltre, è possibile specificare le impostazioni di replica, script e applicazione nel criterio. Queste opzioni consentono di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.

A proposito di questa attività

- Replica di sistema SAP HANA
  - È possibile proteggere il sistema SAP HANA primario ed eseguire tutte le operazioni di protezione dei dati.
  - È possibile proteggere il sistema SAP HANA secondario, ma i backup non possono essere creati.

    Dopo il failover, tutte le operazioni di protezione dei dati possono essere eseguite quando il sistema SAP HANA secondario diventa il sistema SAP HANA primario.

  Non è possibile creare un backup per il volume di dati SAP HANA, ma SnapCenter continua a proteggere i volumi non dati (NDV).

- SnapLock
  - Se è selezionata l'opzione "conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere minore o uguale ai giorni di conservazione menzionati.
  - La specifica di un periodo di blocco snapshot impedisce l'eliminazione delle istantanee fino alla scadenza del periodo di conservazione. Questo potrebbe portare a mantenere un numero di Snapshot maggiore del conteggio specificato nel criterio.
  - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Le impostazioni SnapLock primarie vengono gestite nel criterio di backup SnapCenter e le impostazioni SnapLock secondarie vengono gestite da ONTAP.

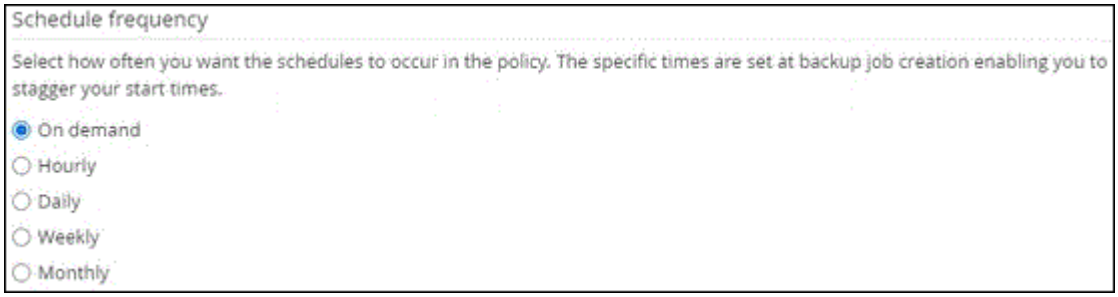
Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **nuovo**.
4. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
5. Nella pagina Impostazioni, attenersi alla seguente procedura:
   - Scegliere il tipo di backup:

Se si desidera…	Eseguire questa operazione…
Eseguire un controllo dell'integrità del database	Selezionare **Backup basato su file**. Viene eseguito il backup solo dei tenant attivi.
Crea un backup utilizzando la tecnologia Snapshot	Selezionare **basato su snapshot**.

- Specificare il tipo di pianificazione selezionando **on demand**, **Hourly**, **Daily**, **Weekly** o **Monthly**.

> ⓘ È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e frequenza di backup, ma consente anche di assegnare diverse pianificazioni di backup a ogni policy.



> ⓘ Se sono previste le 2:00, la programmazione non verrà attivata durante l'ora legale (DST).

- Nella sezione **Impostazioni di backup personalizzate**, specificare le impostazioni di backup specifiche da passare al plug-in in formato key-value.

  È possibile fornire più valori chiave da passare al plug-in.

6. Nella pagina conservazione, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina tipo di backup:

Se si desidera…	Quindi…
Mantenere un certo numero di istantanee	Selezionare **totale copie snapshot da conservare**, quindi specificare il numero di istantanee che si desidera conservare. Se il numero di istantanee supera il numero specificato, le istantanee vengono eliminate con le copie meno recenti eliminate per prime. Il valore massimo di conservazione è 1018 per le risorse su ONTAP 9.4 o versioni successive e 254 per le risorse su ONTAP 9.3 o versioni precedenti. I backup non avranno esito positivo se la conservazione viene impostata su un valore superiore a quello supportato dalla versione di ONTAP sottostante. Per i backup basati su copia Snapshot, è necessario impostare il numero di conservazione su 2 o superiore se si intende attivare la replica SnapVault. Se si imposta il conteggio della conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è il Snapshot di riferimento per la relazione SnapVault fino a quando una snapshot più recente non viene replicata nella destinazione. Per la replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un unico gruppo di risorse. In questo modo si garantisce il corretto numero di backup.

Se si desidera…	Quindi…
Conservare le istantanee per un determinato numero di giorni	Selezionare **Mantieni copie snapshot per**, quindi specificare il numero di giorni per i quali si desidera conservare le istantanee prima di eliminarle.
Periodo di blocco della copia snapshot	Selezionare periodo di blocco della copia Snapshot e selezionare giorni, mesi o anni. Il periodo di conservazione di SnapLock deve essere inferiore a 100 anni.

Replication Primary e SAP HANA System Replication Secondary.
Occorrono massimo 7 snapshot alla

7. Per i backup basati su copia Snapshot, specificare le impostazioni di replica nella pagina Replication:

Per questo campo…	Eseguire questa operazione…
Aggiornare SnapMirror dopo aver creato una copia Snapshot locale	Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror). Se la relazione di protezione in ONTAP è di tipo Mirror e Vault e se si seleziona solo questa opzione, l'istantanea creata sul primario non verrà trasferita alla destinazione, ma sarà elencata nella destinazione. Se si seleziona questa istantanea dalla destinazione per eseguire un'operazione di ripristino, viene visualizzato il messaggio di errore posizione secondaria non disponibile per il backup a vault/mirror selezionato. Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante **Aggiorna** nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP. Vedere "Visualizzare i backup e i cloni del database SAP HANA nella pagina topologia".

Per questo campo…	Eseguire questa operazione…
Aggiornare SnapVault dopo aver creato una copia Snapshot locale	Selezionare questa opzione per eseguire la replica del backup disk-to-disk (backup SnapVault). Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante **Aggiorna** nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP. Quando SnapLock è configurato solo sul secondario da ONTAP noto come vault di SnapLock, facendo clic sul pulsante **Aggiorna** nella pagina topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP. Per ulteriori informazioni sul vault di SnapLock, vedere "Assegnare le copie Snapshot a WORM su una destinazione del vault" Vedere "Visualizzare i backup e i cloni del database SAP HANA nella pagina topologia".
Etichetta del criterio secondario	Selezionare un'etichetta Snapshot. A seconda dell'etichetta Snapshot selezionata, ONTAP applica la politica di conservazione Snapshot secondaria corrispondente all'etichetta. Se è stato selezionato **Update SnapMirror dopo la creazione di una copia Snapshot locale**, è possibile specificare l'etichetta del criterio secondario. Tuttavia, se è stato selezionato **Aggiorna SnapVault dopo la creazione di una copia Snapshot locale**, è necessario specificare l'etichetta del criterio secondario.
Numero tentativi di errore	Immettere il numero massimo di tentativi di replica consentiti prima dell'interruzione dell'operazione.

È necessario configurare il criterio di conservazione SnapMirror in ONTAP per lo storage secondario, in modo da evitare di raggiungere il limite massimo di Snapshot sullo storage secondario.

8. Esaminare il riepilogo, quindi fare clic su **fine**.

Creare gruppi di risorse e allegare policy

Un gruppo di risorse è il container al quale è necessario aggiungere risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire contemporaneamente il backup di tutti i dati associati a una determinata applicazione. Per qualsiasi lavoro di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario associare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire.

A proposito di questa attività

- Per creare backup di replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un unico gruppo di risorse. Ciò garantisce un backup perfetto durante la modalità takeover-failback.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), fare clic su **New Resource Group** (nuovo gruppo di risorse).
3. Nella pagina Name (Nome), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere un nome per il gruppo di risorse. Il nome del gruppo di risorse non deve superare i 250 caratteri.
Tag	Inserire una o più etichette per facilitare la ricerca del gruppo di risorse in un secondo momento. Ad esempio, se si aggiunge HR come tag a più gruppi di risorse, è possibile trovare in seguito tutti i gruppi di risorse associati al tag HR.
USA il formato nome personalizzato per la copia Snapshot	Selezionare questa casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea. Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

4. Nella pagina risorse, selezionare un nome host dall'elenco a discesa **host** e il tipo di risorsa dall'elenco a discesa **tipo di risorsa**.

In questo modo è possibile filtrare le informazioni sullo schermo.

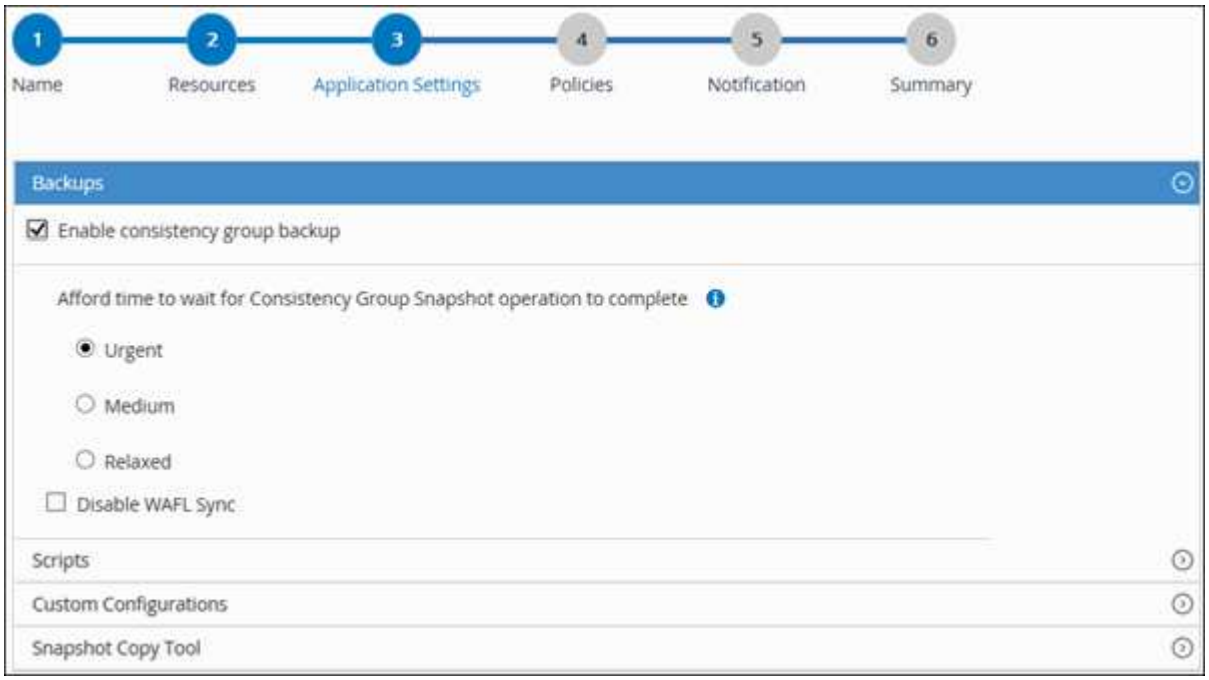
5. Selezionare le risorse dalla sezione **risorse disponibili**, quindi fare clic sulla freccia destra per spostarle nella sezione **risorse selezionate**.
6. Nella pagina Impostazioni applicazione, effettuare le seguenti operazioni:

   a. Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

      Abilitare il backup dei gruppi di coerenza ed eseguire le seguenti attività:

Per questo campo…	Eseguire questa operazione…
Tempo di attesa per il completamento dell'operazione Consistency Group Snapshot	Selezionare **urgente**, **Medio** o **rilassato** per specificare il tempo di attesa per il completamento dell'operazione istantanea. Urgente = 5 secondi, Medio = 7 secondi e rilassato = 20 secondi.
Disattiva sincronizzazione WAFL	Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL.

+



   a. Fare clic sulla freccia **Scripts** e immettere i comandi pre e post per le operazioni quiescenza, istantanea e inquiescenza. In caso di errore, è anche possibile inserire i pre-comandi da eseguire prima di uscire.

   b. Fare clic sulla freccia **Custom Configurations** (configurazioni personalizzate) e immettere le coppie chiave-valore personalizzate richieste per tutte le operazioni di protezione dei dati che utilizzano questa risorsa.

Parametro	Impostazione	Descrizione
ARCHIVE_LOG_ENABLE	(S/N)	Consente alla gestione del log di archiviazione di eliminare i log di archiviazione.
ARCHIVE_LOG_RETENTION	numero_di_giorni	Specifica il numero di giorni in cui i registri di archiviazione vengono conservati. Questa impostazione deve essere uguale o superiore a NTAP_SNAPSHOT_ RETENTIONS.
ARCHIVE_LOG_DIR	change_info_directory/logs	Specifica il percorso della directory che contiene i log di archiviazione.
ARCHIVE_LOG_EXT	estensione_file	Specifica la lunghezza dell'estensione del file di log dell'archivio. Ad esempio, se il log di archiviazione è log_backup_0_0_0_0.16151855 1942 9 e il valore di estensione_file è 5, l'estensione del log conserverà 5 cifre, ossia 16151.
ARCHIVE_LOG_RECURSIVE_ SE ARCH	(S/N)	Attiva la gestione dei log di archiviazione all'interno delle sottodirectory. Utilizzare questo parametro se i log di archiviazione si trovano nelle sottodirectory.

Le coppie chiave-valore personalizzate sono supportate per i sistemi plug-in SAP HANA Linux e non per il database SAP HANA registrato come plug-in Windows centralizzato.

c. Fare clic sulla freccia **Snapshot Copy Tool** per selezionare lo strumento per creare le istantanee:

Se vuoi…	Quindi…
SnapCenter deve utilizzare il plug-in per Windows e mettere il file system in uno stato coerente prima di creare una Snapshot. Per le risorse Linux, questa opzione non è applicabile.	Selezionare **SnapCenter with file system Consistency**. Questa opzione non è applicabile al plug-in SnapCenter per database SAP HANA.

Se vuoi…	Quindi…
SnapCenter per creare una istantanea a livello di storage	Selezionare **SnapCenter senza coerenza del file system**.
Per inserire il comando da eseguire sull'host per creare copie Snapshot.	Selezionare **Altro**, quindi immettere il comando da eseguire sull'host per creare un'istantanea.

7. Nella pagina Criteri, attenersi alla seguente procedura:

   a. Selezionare uno o più criteri dall'elenco a discesa.

      È anche possibile creare una policy facendo clic su * * .

      I criteri sono elencati nella sezione Configura pianificazioni per i criteri selezionati.

   b. Nella colonna Configura pianificazioni, fare clic su * * per il criterio che si desidera configurare.

   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.

      Dove, policy_name è il nome del criterio selezionato.

      Le pianificazioni configurate sono elencate nella colonna **Pianificazioni applicate**.

   Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup di SnapCenter.

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Il server SMTP deve essere configurato in **Impostazioni** > **Impostazioni globali**.

9. Esaminare il riepilogo, quindi fare clic su **fine**.

Eseguire il backup dei database SAP HANA

Se una risorsa non fa ancora parte di un gruppo di risorse, è possibile eseguire il backup della risorsa dalla pagina risorse.

Prima di iniziare

- È necessario aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con uno storage secondario, il ruolo ONTAP assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Per le operazioni di backup basate su copie Snapshot, assicurarsi che tutti i database tenant siano validi e attivi.
- Per creare backup di replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un unico gruppo di risorse. Ciò garantisce un backup perfetto durante la modalità takeover-

failback.

"Creare gruppi di risorse e allegare policy".

"Eseguire il backup dei gruppi di risorse"

- Se si desidera creare un backup basato su file quando uno o più database tenant non sono attivi, impostare il parametro ALLOW_FILE_BASED_BACKUP_IFINATTIVO_INQUILINI_PRESENT su **YES** nel file di proprietà HANA utilizzando il `Set-SmConfigSettings` cmdlet.

  Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, fare riferimento anche alla "Guida di riferimento al cmdlet del software SnapCenter"

- Per i comandi pre e post per le operazioni quiescenza, Snapshot e Unquiesce, è necessario controllare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\programmi\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_Commands.config*
  - Posizione predefinita sull'host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

  Se i comandi non sono presenti nell'elenco dei comandi, l'operazione avrà esito negativo.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resource, filtrare le risorse dall'elenco a discesa **View** in base al tipo di risorsa.

   Selezionare *, quindi selezionare il nome host e il tipo di risorsa per filtrare le risorse. È quindi possibile scegliere di chiudere il riquadro del filtro.
3. Selezionare la risorsa di cui si desidera eseguire il backup.
4. Nella pagina risorsa, selezionare **Usa formato nome personalizzato per copia istantanea**, quindi immettere un formato nome personalizzato che si desidera utilizzare per il nome istantanea.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.
5. Nella pagina Impostazioni applicazione, effettuare le seguenti operazioni:
   - Selezionare la freccia **Backup** per impostare opzioni di backup aggiuntive:

     Attivare il backup dei gruppi di coerenza, se necessario, ed eseguire le seguenti attività:

Per questo campo…	Eseguire questa operazione…
Attendere il completamento dell'operazione "Consistency Group Snapshot"	Selezionare **urgente**, **Medio** o **rilassato** per specificare il tempo di attesa per il completamento dell'operazione istantanea. Urgente = 5 secondi, Medio = 7 secondi e rilassato = 20 secondi.

Per questo campo…	Eseguire questa operazione…
Disattiva sincronizzazione WAFL	Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL.

- Selezionare la freccia **Scripts** per eseguire i comandi pre e post per le operazioni quiescenza, istantanea e inquiescenza.

  È inoltre possibile eseguire i comandi preliminari prima di uscire dall'operazione di backup. Le prescrizioni e i postscript vengono eseguiti nel server SnapCenter.

- Selezionare la freccia **configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i lavori che utilizzano questa risorsa.
- Selezionare la freccia **Snapshot Copy Tool** (strumento di copia istantanea) per selezionare lo strumento per creare le istantanee:

Se vuoi…	Quindi…
SnapCenter per creare una Snapshot a livello di storage	Selezionare **SnapCenter senza coerenza del file system**.
SnapCenter utilizzare il plug-in per Windows per impostare lo stato coerente del file system e quindi creare una Snapshot	Selezionare **SnapCenter with file system Consistency**.
Per immettere il comando per creare un'istantanea	Selezionare **Altro**, quindi immettere il comando per creare un'istantanea.

6. Nella pagina Criteri, attenersi alla seguente procedura:

   a. Selezionare uno o più criteri dall'elenco a discesa.

È anche possibile creare una policy facendo clic su * * .

Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

b. Selezionare * * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi selezionare **OK**.

policy_name è il nome del criterio selezionato.

Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

7. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. SMTP deve essere configurato anche in **Impostazioni** > **Impostazioni globali**.

8. Esaminare il riepilogo, quindi selezionare **fine**.

   Viene visualizzata la pagina della topologia delle risorse.

9. Selezionare **Esegui backup ora**.
10. Nella pagina Backup, attenersi alla seguente procedura:
    a. Se sono stati applicati più criteri alla risorsa, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

       Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Selezionare **Backup**.
11. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

- Nelle configurazioni MetroCluster, SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

  Per informazioni, vedere: "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover di MetroCluster"

- Se si esegue il backup dei dati delle applicazioni su VMDK e la dimensione dell'heap Java per il plug-in SnapCenter per VMware vSphere non è sufficiente, il backup potrebbe non riuscire.

  Per aumentare la dimensione dell'heap Java, individuare il file script */opt/netapp/init_scripts/scvservice*. In questo script, il comando *do_start method* avvia il servizio plug-in VMware di SnapCenter. Aggiornare il comando al seguente: *Java -jar -Xmx8192M -Xms4096M*

Eseguire il backup dei gruppi di risorse

Un gruppo di risorse è un insieme di risorse su un host. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

Prima di iniziare

- È necessario aver creato un gruppo di risorse con un criterio allegato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con uno storage secondario, il ruolo ONTAP assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

A proposito di questa attività

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina risorse. Se un gruppo di risorse dispone di un criterio associato e di una pianificazione configurata, i backup vengono eseguiti automaticamente in base alla pianificazione.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).

   È possibile eseguire una ricerca nel gruppo di risorse immettendo il nome del gruppo di risorse nella casella di ricerca oppure selezionando , quindi selezionando il tag. È quindi possibile scegliere di chiudere il riquadro del filtro.

3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi selezionare **Esegui backup ora**.
4. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se sono stati associati più criteri al gruppo di risorse, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Creare una connessione al sistema storage e una credenziale utilizzando i cmdlet PowerShell per il database SAP HANA

È necessario creare una connessione SVM (Storage Virtual Machine) e una credenziale prima di utilizzare i cmdlet PowerShell per eseguire il backup, il ripristino o la clonazione dei database SAP HANA.

Prima di iniziare

- L'ambiente PowerShell dovrebbe essere stato preparato per l'esecuzione dei cmdlet PowerShell.
- Per creare le connessioni storage, è necessario disporre delle autorizzazioni necessarie nel ruolo Infrastructure Admin.

- Assicurarsi che le installazioni dei plug-in non siano in corso.

  Le installazioni dei plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage perché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nella GUI di SnapCenter come "non disponibile per il backup" o "non su storage NetApp".

- I nomi dei sistemi di storage devono essere univoci.

  SnapCenter non supporta più sistemi storage con lo stesso nome su cluster diversi. Ogni sistema storage supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dei dati univoco.

Fasi

1. Avviare una sessione di connessione PowerShell utilizzando il cmdlet Open-SmConnection.

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

2. Creare una nuova connessione al sistema di storage utilizzando il cmdlet Add-SmStorageConnection.

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

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   Questo esempio mostra come creare una nuova credenziale denominata FinanceAdmin con credenziali Windows:

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

4. Aggiungere l'host di comunicazione SAP HANA al server SnapCenter.

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

5. Installare il pacchetto e il plug-in SnapCenter per il database SAP HANA sull'host.

   Per Linux:

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

   Per Windows:

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

6. Impostare il percorso del client HDBSQL.

   Per Windows:

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

   Per Linux:

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Eseguire il backup dei database utilizzando i cmdlet PowerShell

Il backup di un database include la connessione con il server SnapCenter, l'aggiunta di risorse, l'aggiunta di un criterio, la creazione di un gruppo di risorse di backup e il backup.

Prima di iniziare

- È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- È necessario aver aggiunto la connessione al sistema di storage e creato una credenziale.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

   Viene visualizzato il prompt di nome utente e password.

2. Aggiungere risorse utilizzando il cmdlet Add-SmResources.

   Questo esempio mostra come aggiungere un database SAP HANA di tipo SingleContainer:

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

Questo esempio mostra come aggiungere un database SAP HANA di tipo MultipleContainers:

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

Questo esempio mostra come creare una risorsa di volume non dati:

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

3. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   Questo esempio crea una policy di backup per un backup basato su copia Snapshot:

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

   Questo esempio crea un criterio di backup per un backup basato su file:

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

4. Proteggere la risorsa o aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   Questo esempio protegge una singola risorsa di container:

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

Questo esempio protegge una risorsa di container multipli:

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

In questo esempio viene creato un nuovo gruppo di risorse con le risorse e i criteri specificati:

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

In questo esempio viene creato un gruppo di risorse di volumi non dati:

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

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

   Questo esempio mostra come eseguire il backup di un gruppo di risorse:

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

   Questo esempio esegue il backup di una risorsa protetta:

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

6. Monitorare lo stato del processo (in esecuzione, completato o non riuscito) utilizzando il cmdlet Get-smJobSummaryReport.

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

7. Monitorare i dettagli del processo di backup, come ID di backup, nome del backup per eseguire operazioni di ripristino o clonazione, utilizzando il cmdlet Get-SmBackupReport.

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di backup

Monitorare le operazioni di backup dei database SAP HANA

È possibile monitorare l'avanzamento di diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere necessario controllare i progressi per determinare quando sono stati completati o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Status** (Stato), selezionare lo stato del backup.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene venga visualizzato lo stato del processo di backup , quando si fa clic sui dettagli del processo, è possibile che alcune delle attività secondarie dell'operazione di backup siano ancora in corso o contrassegnate da segnali di avviso.

5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Monitorate le operazioni di protezione dei dati sui database SAP HANA nel riquadro attività

Il riquadro Activity (attività) visualizza le cinque operazioni più recenti eseguite. Il riquadro Activity (attività) visualizza anche il momento in cui l'operazione è stata avviata e lo stato dell'operazione.

Il riquadro Activity (attività) visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli commessa**.

Annulla le operazioni di backup per SAP HANA

È possibile annullare le operazioni di backup inserite nella coda.

Cosa ti serve

- Per annullare le operazioni, è necessario accedere come amministratore SnapCenter o come proprietario del processo.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- Per annullare le operazioni di backup, è possibile utilizzare l'interfaccia grafica utente di SnapCenter, i cmdlet PowerShell o i comandi CLI.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di backup in coda degli altri membri durante l'utilizzo di tale ruolo.

Fasi

1. Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	a. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**.
Riquadro delle attività	a. Dopo aver avviato l'operazione di backup, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. b. Selezionare l'operazione. c. Nella pagina Dettagli processo, fare clic su **Annulla processo**.

L'operazione viene annullata e la risorsa viene riportata allo stato precedente.

Visualizzare i backup e i cloni del database SAP HANA nella pagina topologia

Quando si prepara il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e cloni sullo storage primario e secondario.

A proposito di questa attività

È possibile esaminare le seguenti icone nella vista Manage Copies (Gestisci copie) per determinare se i backup e i cloni sono disponibili sullo storage primario o secondario (copie Mirror o copie Vault).

-  visualizza il numero di backup e cloni disponibili sullo storage primario.
-  Visualizza il numero di backup e cloni su cui viene eseguito il mirroring dello storage secondario utilizzando la tecnologia SnapMirror.
-  Visualizza il numero di backup e cloni replicati sullo storage secondario utilizzando la tecnologia SnapVault.

  Il numero di backup visualizzati include i backup eliminati dallo storage secondario. Ad esempio, se sono stati creati 6 backup utilizzando un criterio per conservare solo 4 backup, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror flessibile della versione su un volume di tipo mirror-vault vengono visualizzati nella vista della topologia, ma il numero di backup mirror nella vista della topologia non include il backup flessibile della versione.

Per le risorse primarie di replica del sistema SAP HANA, sono supportate le operazioni di ripristino ed eliminazione, mentre per le risorse secondarie è supportata l'operazione di clonazione.

Nella pagina topologia, è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e selezionarli per eseguire le operazioni di protezione dei dati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Consultare la scheda **Summary** per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione **scheda di riepilogo** visualizza il numero totale di backup basati su file, backup basati su copia

Snapshot e cloni.

Facendo clic sul pulsante **Refresh** viene avviata una query dello storage per visualizzare un conteggio accurato.

Se viene eseguito il backup abilitato SnapLock, facendo clic sul pulsante **Aggiorna** si aggiornano i tempi di scadenza SnapLock primari e secondari recuperati da ONTAP. Inoltre, una pianificazione settimanale aggiorna il tempo di scadenza SnapLock primario e secondario recuperato da ONTAP.

Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza del SnapLock per il backup sarà il tempo di scadenza del SnapLock più lungo impostato per una Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

Dopo il backup su richiesta, facendo clic sul pulsante **Refresh** (Aggiorna) vengono aggiornati i dettagli del backup o della clonazione.

5. Nella vista Gestisci copie, fare clic su **backup** o **cloni** dallo storage primario o secondario per visualizzare i dettagli di un backup o clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nello storage secondario.

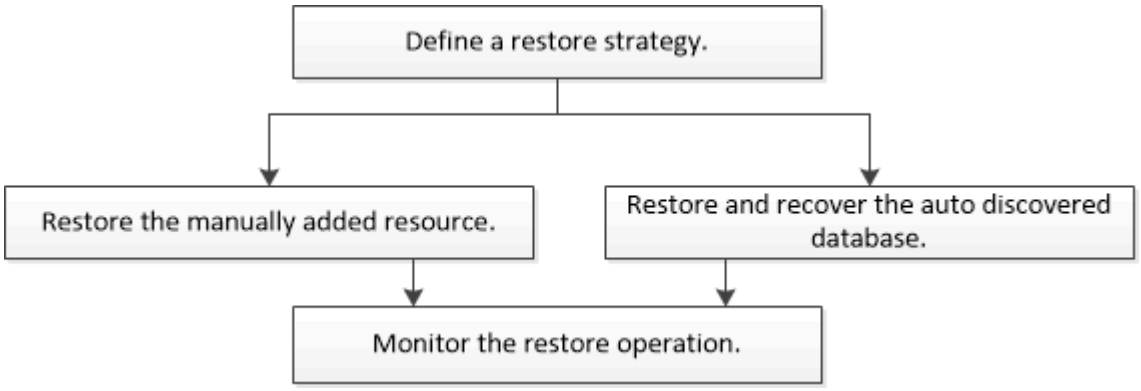
7. Se si desidera eliminare un clone, selezionarlo dalla tabella, quindi fare clic su .
8. Se si desidera dividere un clone, selezionarlo dalla tabella e fare clic su .

Ripristinare i database SAP HANA

Ripristinare il flusso di lavoro

Il flusso di lavoro di ripristino e ripristino include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di ripristino:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida in linea del cmdlet di SnapCenter e le informazioni di riferimento del cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

"Guida di riferimento al cmdlet del software SnapCenter".

Ripristinare e ripristinare un backup delle risorse aggiunto manualmente

È possibile utilizzare SnapCenter per ripristinare e ripristinare i dati da uno o più backup.

Prima di iniziare

- È necessario aver eseguito il backup delle risorse o dei gruppi di risorse.
- È necessario annullare qualsiasi operazione di backup attualmente in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi di pre-restore, post-restore, mount e unmount, controllare se i comandi esistono nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\programmi\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_Commands.config*
  - Posizione predefinita sull'host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

  Se i comandi non sono presenti nell'elenco dei comandi, l'operazione avrà esito negativo.

A proposito di questa attività

- Le copie di backup basate su file non possono essere ripristinate da SnapCenter.
- Dopo l'aggiornamento a SnapCenter 4.3, i backup eseguiti in SnapCenter 4.2 possono essere ripristinati ma non ripristinati. Per ripristinare i backup eseguiti in SnapCenter 4.2, è necessario utilizzare script di ripristino HANA Studio o HANA esterni a SnapCenter.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, filtrare le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

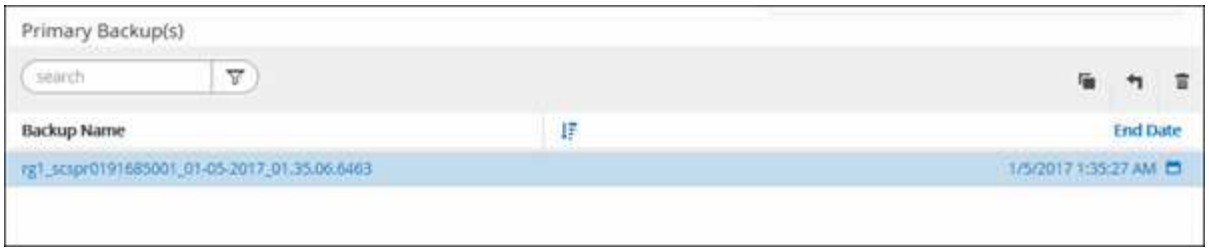
   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse e ai criteri associati e allo stato.

   Anche se un backup potrebbe essere per un gruppo di risorse, quando si esegue il ripristino, è necessario selezionare le singole risorse da ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "NOT Protected". Ciò può significare che la risorsa non è protetta o che il backup della risorsa è stato eseguito da un altro utente.
3. Selezionare la risorsa o un gruppo di risorse, quindi selezionare una risorsa in tale gruppo.

   Viene visualizzata la pagina della topologia delle risorse.
4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primario o secondario (mirrorati o vault).
5. Nella tabella Backup primari, selezionare il backup da cui si desidera eseguire il ripristino, quindi fare clic

su * * .



6. Nella pagina Restore Scope (ambito ripristino), selezionare **complete Resource** (completa risorsa) o **file Level** (livello file).

   a. Se si seleziona **complete Resource** (completa risorsa), vengono ripristinati tutti i volumi di dati configurati del database SAP HANA.

      Se la risorsa contiene volumi o qtree, gli Snapshot acquisiti dopo la Snapshot selezionata per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata.

   b. Se si seleziona **file Level**, è possibile selezionare **All** o selezionare i volumi o le qtree specifici, quindi immettere il percorso relativo a tali volumi o qtree, separati da virgole

      - È possibile selezionare più volumi e qtree.
      - Se il tipo di risorsa è LUN, viene ripristinato l'intero LUN.

        È possibile selezionare più LUN.

   Se si seleziona **tutto**, vengono ripristinati tutti i file presenti nei volumi, nei qtree o nei LUN.

7. Nella pagina Pre Ops (operazioni preliminari), immettere i comandi di pre-ripristino e disinstallazione da eseguire prima di eseguire un processo di ripristino.

   I comandi di disinstallazione non sono disponibili per le risorse rilevate automaticamente.

8. Nella pagina Post Ops (operazioni post), immettere i comandi di montaggio e post ripristino da eseguire dopo l'esecuzione di un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

9. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

10. Esaminare il riepilogo, quindi fare clic su **fine**.
11. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Ripristinare e ripristinare un backup del database rilevato automaticamente

È possibile utilizzare SnapCenter per ripristinare e ripristinare i dati da uno o più backup.

Prima di iniziare

- È necessario aver eseguito il backup delle risorse o dei gruppi di risorse.
- È necessario annullare qualsiasi operazione di backup attualmente in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi di pre-restore, post-restore, mount e unmount, controllare se i comandi esistono nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\programmi\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_Commands.config*
  - Posizione predefinita sull'host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

> Se i comandi non sono presenti nell'elenco dei comandi, l'operazione avrà esito negativo.

A proposito di questa attività

- Le copie di backup basate su file non possono essere ripristinate da SnapCenter.
- Dopo l'aggiornamento a SnapCenter 4.3, i backup eseguiti in SnapCenter 4.2 possono essere ripristinati ma non ripristinati. Per ripristinare i backup eseguiti in SnapCenter 4.2, è necessario utilizzare script di ripristino HANA Studio o HANA esterni a SnapCenter.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, filtrare le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse e ai criteri associati e allo stato.

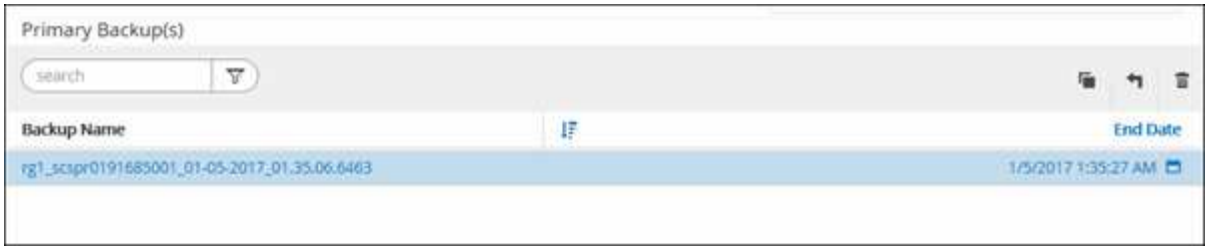
   > Anche se un backup potrebbe essere per un gruppo di risorse, quando si esegue il ripristino, è necessario selezionare le singole risorse da ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "NOT Protected". Ciò può significare che la risorsa non è protetta o che il backup della risorsa è stato eseguito da un altro utente.

3. Selezionare la risorsa o un gruppo di risorse, quindi selezionare una risorsa in tale gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primario o secondario (mirrorati o vault).
5. Nella tabella Backup primari, selezionare il backup da cui si desidera eseguire il ripristino, quindi fare clic su * *  .



6. Nella pagina Restore Scope (ambito ripristino), selezionare **complete Resource** (completa risorsa) per ripristinare i volumi di dati configurati del database SAP HANA.

   È possibile selezionare **complete Resource** (con o senza **Volume Revert**) o **Tenant Database**.

   L'operazione di recovery non è supportata dal server SnapCenter per più tenant quando l'utente seleziona l'opzione **Database tenant** o **Ripristino completo**. Per eseguire l'operazione di ripristino, è necessario utilizzare lo script HANA studio o HANA python.

   a. Selezionare **Volume Revert** (Ripristina volume) per ripristinare l'intero volume.

      Questa opzione è disponibile per i backup eseguiti in SnapCenter 4.3 in ambienti NFS.

      Se la risorsa contiene volumi o qtree, gli Snapshot acquisiti dopo la Snapshot selezionata per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata. Questa opzione è applicabile quando l'opzione **completa risorsa** con **Ripristino volume** è selezionata per il ripristino.

   b. Selezionare **Database tenant**.

      Questa opzione è disponibile solo per le risorse MDC.

      Assicurarsi di arrestare il database tenant prima di eseguire l'operazione di ripristino.

   Se si seleziona l'opzione **Database tenant**, è necessario utilizzare HANA studio o gli script di ripristino HANA esterni a SnapCenter per eseguire l'operazione di ripristino.

7. Nella pagina Recovery Scope (ambito ripristino), selezionare una delle seguenti opzioni:

Se…	Eseguire questa operazione…
Desidera ripristinare il più vicino possibile all'ora corrente	Selezionare **Ripristina allo stato più recente**. Per le risorse container singole, specificare una o più posizioni di backup del registro e del catalogo. Per le risorse MDC (Multitenant Database Container), specificare una o più posizioni di backup dei log e la posizione del catalogo di backup. Per le risorse MDC, il percorso deve contenere sia i log del database del sistema che quelli del tenant.

Se…	Eseguire questa operazione…
Si desidera ripristinare al punto di tempo specificato	Selezionare **Recover to point in time** (Ripristina al punto nel tempo). a. Selezionare il fuso orario. Il fuso orario del browser viene popolato per impostazione predefinita. Il fuso orario selezionato e l'ora di immissione vengono convertiti in GMT assoluto. b. Inserire data e ora. Ad esempio, l'host HANA Linux si trova a Sunnyvale, CA e l'utente di Raleigh, NC, sta recuperando i log in a SnapCenter. La differenza di tempo tra queste due posizioni è di 3 ore e, poiché l'utente ha effettuato l'accesso da Raleigh, NC, il fuso orario predefinito del browser che verrà selezionato nella GUI è GMT-04:00. Se l'utente desidera eseguire un ripristino a 5.sunnyvale, CA, l'utente deve impostare il fuso orario del browser sul fuso orario dell'host HANA Linux, GMT-07:00, specificando data e ora alle 5:00 Per le risorse container singole, specificare una o più posizioni di backup del registro e del catalogo. Per le risorse MDC, specificare una o più posizioni di backup del registro e la posizione del catalogo di backup. Per le risorse MDC, il percorso deve contenere sia i log del database del sistema che quelli del tenant.
Ripristinare un backup dei dati specifico	Selezionare **Recover to specified data backup** (Ripristina backup dati specificati).
Non si desidera eseguire il ripristino	Selezionare **Nessun ripristino**. È necessario eseguire manualmente l'operazione di ripristino da HANA Studio.

È possibile ripristinare solo i backup eseguiti dopo l'aggiornamento a SnapCenter 4.3, a condizione che l'host e il plug-in siano aggiornati a SnapCenter 4.3 e che i backup selezionati per il ripristino vengano eseguiti dopo la conversione o il rilevamento automatico della risorsa.

8. Nella pagina Pre Ops (operazioni preliminari), immettere i comandi di pre-ripristino e disinstallazione da eseguire prima di eseguire un processo di ripristino.

   I comandi di disinstallazione non sono disponibili per le risorse rilevate automaticamente.

9. Nella pagina Post Ops (operazioni post), immettere i comandi di montaggio e post ripristino da eseguire dopo l'esecuzione di un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

10. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

    È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

11. Esaminare il riepilogo, quindi fare clic su **fine**.
12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Ripristinare il database SAP HANA utilizzando i cmdlet PowerShell

Il ripristino di un backup del database SAP HANA include l'avvio di una sessione di connessione con il server SnapCenter, l'elenco dei backup e il recupero delle informazioni di backup e il ripristino di un backup.

Prima di iniziare

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Identificare il backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio mostra che sono disponibili due backup per il ripristino:

```
 PS C:\> Get-SmBackup

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

Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

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

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

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

3. Avviare il processo di ripristino in HANA Studio.

   Il database viene chiuso.

4. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

   AppObjectId è "host/Plugin/UID", dove UID = SID è per la risorsa di tipo container singolo e UID = MDC/SID è per la risorsa di container multipli. È possibile ottenere ResourceID dal cmdlet Get-smResources.

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

Questo esempio mostra come ripristinare il database dallo storage primario:

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

Questo esempio mostra come ripristinare il database dallo storage secondario:

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

I backup saranno disponibili in HANA Studio per il recovery.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Ripristinare le risorse utilizzando i cmdlet PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con il server SnapCenter, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Recuperare le informazioni relative a uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio mostra informazioni su tutti i backup disponibili:

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

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

Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

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

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

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

3. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di ripristino dei database SAP HANA

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

gli stati di post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi altra azione di ripristino che è possibile eseguire.

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Ripristina**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato di ripristino.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Clonare i backup delle risorse SAP HANA

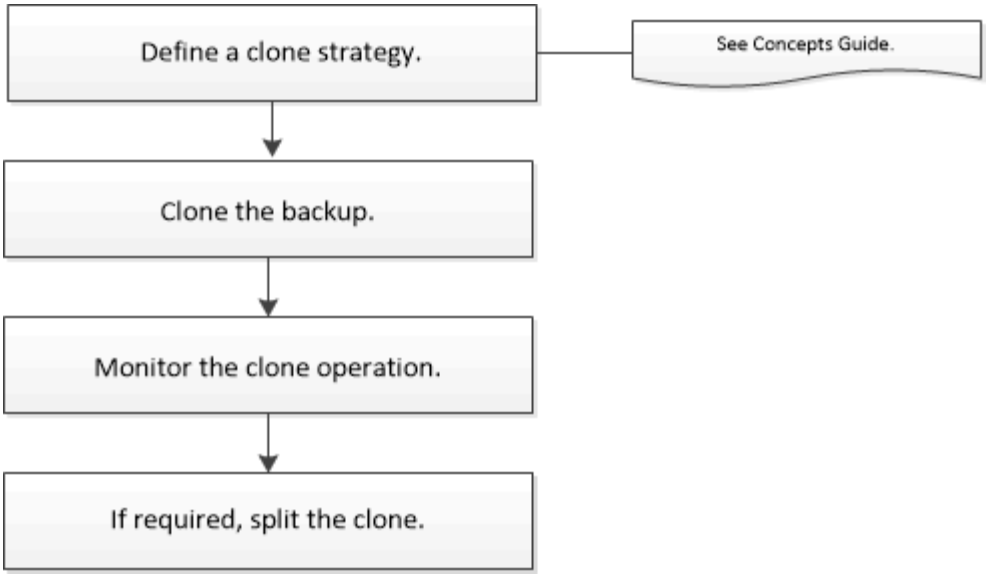
Clonare il flusso di lavoro

Il flusso di lavoro dei cloni include l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

A proposito di questa attività

- È possibile clonare sul server SAP HANA di origine.
- È possibile clonare i backup delle risorse per i seguenti motivi:
  - Per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo delle applicazioni
  - Per l'estrazione e la manipolazione dei dati durante il popolamento dei data warehouse
  - Per ripristinare i dati cancellati o modificati per errore

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di clonazione:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida in linea del cmdlet di SnapCenter e le informazioni di riferimento del cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

Clonare un backup del database SAP HANA

È possibile utilizzare SnapCenter per clonare un backup. È possibile clonare dal backup primario o secondario.

Prima di iniziare

- È necessario aver eseguito il backup delle risorse o del gruppo di risorse.
- Assicurarsi che gli aggregati che ospitano i volumi siano inclusi nell'elenco degli aggregati assegnati della macchina virtuale di storage (SVM).
- Non è possibile clonare backup basati su file.
- Il server clone di destinazione deve avere lo stesso SID dell'istanza SAP HANA fornito nel campo SID clone di destinazione.
- Per i comandi pre-clone o post-clone, controllare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\programmi\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_Commands.config*
  - Posizione predefinita sull'host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

> Se i comandi non sono presenti nell'elenco dei comandi, l'operazione avrà esito negativo.

A proposito di questa attività

- Per informazioni sulle limitazioni delle operazioni di suddivisione clone, vedere "Guida alla gestione dello storage logico di ONTAP 9".
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, filtrare le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme a informazioni quali tipo, host, gruppi di risorse e criteri associati e stato.

3. Selezionare la risorsa o il gruppo di risorse.

   Selezionare una risorsa se si seleziona un gruppo di risorse.

   Viene visualizzata la pagina della topologia di risorse o gruppi di risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primario o secondario (mirrorati o vault).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su  .
6. Nella pagina Location (posizione), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Host plug-in	Selezionare l'host su cui montare il clone e installare il plug-in.
SID clone di destinazione	Inserire l'ID dell'istanza SAP HANA da clonare dai backup esistenti.
NFS Export IP Address (Indirizzo IP esportazione NFS)	Inserire gli indirizzi IP o i nomi host su cui esportare i volumi clonati.
ISCSI Initiator	Inserire il nome iSCSI Initiator dell'host in cui vengono esportati i LUN. Questa opzione è disponibile solo se è stato selezionato il tipo di risorsa LUN.
Protocollo	Inserire il protocollo LUN. Questa opzione è disponibile solo se è stato selezionato il tipo di risorsa LUN.

   Se la risorsa selezionata è un LUN e si sta clonando da un backup secondario, vengono elencati i volumi di destinazione. Una singola origine può avere più volumi di destinazione.

   Prima di eseguire la clonazione, è necessario assicurarsi che l'iniziatore iSCSI o il pannello FCP sia presente e che siano configurati e collegati a host alternativi.

7. Nella pagina script, attenersi alla seguente procedura:

   Gli script vengono eseguiti sull'host del plug-in.

a. Immettere i comandi per pre-clone o post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clone.
   - Comando pre-clone: Elimina i database esistenti con lo stesso nome
   - Comando post clone: Verifica di un database o avvia un database.

b. Immettere il comando mount per montare un file system su un host.

   Comando mount per un volume o qtree su una macchina Linux:

Esempio per NFS: Montare VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail.

9. Esaminare il riepilogo, quindi fare clic su **fine**.
10. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Clonare i backup del database SAP HANA utilizzando i cmdlet PowerShell

Il flusso di lavoro dei cloni include la pianificazione, l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Recuperare i backup per eseguire l'operazione di clonazione utilizzando il cmdlet Get-SmBackup.

   Questo esempio mostra che sono disponibili due backup per la clonazione:

```
 C:\PS> Get-SmBackup

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

3. Avviare un'operazione di clonazione da un backup esistente e specificare gli indirizzi IP di esportazione NFS su cui esportare i volumi clonati.

   Questo esempio mostra che il backup da clonare ha un indirizzo NFSExportIPs 10.232.206.169:

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-2017_02.54.29.3817
-Resources @{"Host"="scsccore1.sccore.test.com";"Uid"="H73"}
-CloneToInstance shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands
'/home/scripts/scpre_clone.sh' -postclonecreatecommands
'/home/scripts/scpost_clone.sh'
```

   Se NFSExportIP non viene specificato, il valore predefinito viene esportato nell'host di destinazione del clone.

4. Verificare che i backup siano stati clonati correttamente utilizzando il cmdlet Get-SmCloneReport per visualizzare i dettagli del processo clone.

   È possibile visualizzare dettagli quali ID clone, data e ora di inizio, data e ora di fine.

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

Monitorare le operazioni di clonazione del database SAP HANA

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.

3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Clone**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato del clone.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro clone, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

Separare un clone

È possibile utilizzare SnapCenter per separare una risorsa clonata dalla risorsa principale. Il clone diviso diventa indipendente dalla risorsa padre.

A proposito di questa attività

- Non è possibile eseguire l'operazione di suddivisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato il clone1 da un backup del database, è possibile creare un backup del clone1 e clonare il backup (clone2). Dopo aver creato il clone2, il clone1 è un clone intermedio e non è possibile eseguire l'operazione di suddivisione del clone sul clone1. Tuttavia, è possibile eseguire l'operazione di suddivisione dei cloni sul clone2.

  Dopo aver diviso il clone2, è possibile eseguire l'operazione di divisione del clone sul clone1, poiché il clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i lavori di clonazione del clone vengono eliminati.
- Per informazioni sulle limitazioni delle operazioni di suddivisione clone, vedere "Guida alla gestione dello storage logico di ONTAP 9".
- Assicurarsi che il volume o l'aggregato sul sistema di storage sia online.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **risorse**, selezionare l'opzione appropriata dall'elenco Visualizza:

Opzione	Descrizione
Per applicazioni di database	Selezionare **Database** dall'elenco View (Visualizza).
Per file system	Selezionare **Path** dall'elenco View (Visualizza).

3. Selezionare la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Nella vista **Gestisci copie**, selezionare la risorsa clonata (ad esempio, il database o il LUN), quindi fare clic su * * .

5. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
6. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

   Se il servizio SMCore viene riavviato, l'operazione di split clone smette di rispondere. Eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione di suddivisione del clone.

   Se si desidera un tempo di polling più lungo o più breve per controllare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo in cui SMCore deve eseguire il polling per lo stato dell'operazione di suddivisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Ad esempio:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   L'operazione di avvio del clone split non riesce se sono in corso operazioni di backup, ripristino o altro clone split. È necessario riavviare l'operazione di suddivisione dei cloni solo al termine delle operazioni in esecuzione.

Informazioni correlate

"Il clone o la verifica di SnapCenter non riesce e l'aggregato non esiste"

Eliminare o separare i cloni del database SAP HANA dopo l'aggiornamento di SnapCenter

Dopo l'aggiornamento a SnapCenter 4.3, i cloni non verranno più visualizzati. È possibile eliminare il clone o suddividere i cloni dalla pagina topologia della risorsa da cui sono stati creati i cloni.

A proposito di questa attività

Se si desidera individuare l'ingombro dello storage dei cloni nascosti, eseguire il seguente comando: `Get-SmClone -ListStorageFootprint`

Fasi

1. Eliminare i backup delle risorse clonate utilizzando il cmdlet remove-smbackup.
2. Eliminare il gruppo di risorse delle risorse clonate utilizzando il cmdlet remove-sresourcegroup.
3. Rimuovere la protezione della risorsa clonata utilizzando il cmdlet remove-smprotectresource.
4. Selezionare la risorsa principale dalla pagina risorse.

   Viene visualizzata la pagina della topologia delle risorse.

5. Dalla vista Manage Copies (Gestisci copie), selezionare i cloni dai sistemi di storage primario o secondario (mirrorati o replicati).
6. Selezionare i cloni, quindi fare clic per eliminare i cloni o fare clic per suddividere i cloni.
7. Fare clic su **OK**.

Proteggere i database Oracle

Panoramica del plug-in SnapCenter per database Oracle

Cosa puoi fare con il plug-in per database Oracle

Il plug-in SnapCenter per database Oracle è un componente sul lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati applicativa dei database Oracle.

Il plug-in per database Oracle automatizza il backup, la catalogazione e la decatalogazione con Oracle Recovery Manager (RMAN), la verifica, il montaggio, lo smontaggio, il ripristino, Recovery e cloning di database Oracle nel tuo ambiente SnapCenter. Il plug-in per database Oracle installa il plug-in SnapCenter per UNIX per eseguire tutte le operazioni di protezione dei dati.

È possibile utilizzare il plug-in per database Oracle per gestire i backup dei database Oracle che eseguono applicazioni SAP. Tuttavia, l'integrazione SAP BR*Tools non è supportata.

- Eseguire il backup di file di dati, file di controllo e file di log di archiviazione.

  Il backup è supportato solo a livello di database container (CDB).

- Ripristino e ripristino di database, CDBS e database collegabili (PDB).

  Il ripristino incompleto dei PDB non è supportato.

- Crea cloni di database di produzione fino a un punto in tempo.

  La clonazione è supportata solo a livello di CDB.

- Verificare immediatamente i backup.
- Montare e smontare i backup dei dati e dei log per l'operazione di recovery.
- Pianifica le operazioni di backup e verifica.
- Monitorare tutte le operazioni.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

Funzionalità del plug-in per database Oracle

Il plug-in per database Oracle si integra con il database Oracle sull'host Linux o AIX e con le tecnologie NetApp sul sistema storage.

- Interfaccia grafica utente unificata

  L'interfaccia SnapCenter offre standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia di SnapCenter consente di completare operazioni di backup, ripristino, ripristino e clonazione coerenti tra i plug-in, utilizzare report centralizzati, utilizzare visualizzazioni dashboard a colpo d'occhio, impostare RBAC (role-based access control) e monitorare i processi in tutti i plug-in.

- Amministrazione centrale automatizzata

È possibile pianificare operazioni di backup e clonazione, configurare la conservazione dei backup basata su policy ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per l'invio di avvisi e-mail.

- Tecnologia Snapshot di NetApp senza interruzioni

  Per eseguire il backup dei database, SnapCenter utilizza la tecnologia Snapshot di NetApp con il plug-in per database e plug-in per UNIX. Le snapshot consumano una quantità minima di spazio storage.

Il plug-in per Oracle Database offre inoltre i seguenti vantaggi:

- Supporto per backup, ripristino, clonare, montare, smontare, e workflow di verifica
- Rilevamento automatico dei database Oracle configurati sull'host
- Supporto per la catalogazione e la decatalogazione con Oracle Recovery Manager (RMAN)
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È inoltre possibile impostare le credenziali in modo che gli utenti SnapCenter autorizzati dispongano delle autorizzazioni a livello di applicazione.

- Supporto di Archive Log Management (ALM) per operazioni di ripristino e clonazione
- Creazione di copie di database di produzione efficienti in termini di spazio e point-in-time per il test o l'estrazione dei dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema storage in cui si desidera creare il clone.

- Supporto della funzionalità CG (Consistency Group) di ONTAP come parte della creazione di backup in ambienti SAN e ASM
- Verifica del backup automatica e senza interruzioni
- Possibilità di eseguire più backup contemporaneamente su più host di database

  In una singola operazione, le Snapshot vengono consolidate quando i database di un singolo host condividono lo stesso volume.

- Supporto per infrastrutture fisiche e virtualizzate
- Supporto per NFS, iSCSI, Fibre Channel (FC), RDM, VMDK su NFS e VMFS e ASM su NFS, SAN, RDM e VMDK
- Supporto per la funzione mappa LUN selettiva (SLM) di ONTAP

  Attivata per impostazione predefinita, la funzione SLM rileva periodicamente le LUN che non dispongono di percorsi ottimizzati e le corregge. È possibile configurare SLM modificando i parametri nel file scu.properties che si trova in /var/opt/snapcenter/scu/ecc.

  - È possibile disattivare questa funzione impostando il valore del parametro ENABLE_LUNPATH_MONITORING su false.
  - È possibile specificare la frequenza con cui i percorsi LUN verranno fissati automaticamente assegnando il valore (in ore) al parametro LUNPATH_MONITORING_INTERVAL. Per informazioni su SLM, vedere "Guida all'amministrazione DI ONTAP 9 SAN".

- Supporto per NVMe (non-volatile Memory Express) su Linux
  - NVMe util deve essere installato sull'host.

È necessario installare NVMe util per clonare o montare su un host alternativo.

- Backup, ripristino, clonare, montare, smontare, le operazioni di catalogo, decatalogo e verifica sono supportate sull'hardware NVMe ad eccezione degli ambienti virtualizzati come VMDK e RDM.

  Le operazioni sopra descritte sono supportate su dispositivi senza partizioni o con singola partizione.

È possibile configurare la soluzione multipathing per i dispositivi NVMe impostando l'opzione multipathing nativa nel kernel. Multipathing DM (Device Mapper) non supportato.

- Supporta qualsiasi utente non predefinito invece di oracle e Grid.

  Per supportare gli utenti non predefiniti, è necessario impostare gli utenti non predefiniti modificando i valori dei parametri nel file **sco.properties** che si trova in *file /var/opt/snapcenter/sco/etc/*.

  I valori predefiniti dei parametri vengono impostati come oracle e Grid.

  - DB_USER=oracle
  - DB_GROUP=oinstall
  - Gi_USER=grid
  - Gi_GROUP=oinstall

Tipi di storage supportati dal plug-in per database Oracle

SnapCenter supporta un'ampia gamma di tipi di storage su macchine fisiche e virtuali. Prima di installare il pacchetto plug-in SnapCenter per Linux o il pacchetto plug-in SnapCenter per AIX, è necessario verificare il supporto per il tipo di storage.

SnapCenter non supporta il provisioning dello storage per Linux e AIX.

Tipi di storage supportati su Linux

La tabella seguente elenca i tipi di storage supportati su Linux.

Macchina	Tipo di storage
Server fisico	• LUN connessi a FC • LUN connessi a iSCSI • Volumi connessi a NFS

Macchina	Tipo di storage
VMware ESXi	• Il completamento delle LUN RDM collegate da un HBASCAN ESXi FC o iSCSI degli HBA (host bus adapter) potrebbe richiedere molto tempo, in quanto SnapCenter esegue la scansione di tutti gli adattatori bus host presenti nell'host. È possibile modificare il file **LinuxConfig.pm** situato in */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* per impostare il valore del parametro **SCSI_HOSTS_OPTIMIZED_RESCAN** su 1 per ripetere la scansione solo degli HBA elencati in HBA_DRIVER_NAMES. • LUN iSCSI collegati direttamente al sistema guest dall'iniziatore iSCSI • VMDK su datastore VMFS o NFS • Volumi NFS collegati direttamente al sistema guest

Tipi di storage supportati su AIX

La tabella seguente elenca i tipi di storage supportati su AIX.

Macchina	Tipo di storage
Server fisico	• LUN connessi a FC e iSCSI. In un ambiente SAN, sono supportati i file system ASM, LVM e SAN. NFS su AIX e il filesystem non sono supportati. • JFS2 (Enhanced Journaled file System) Supporta la registrazione inline su file system SAN e layout LVM.

```
https://imt.netapp.com/matrix/imt.jsp?components=117016;&solution=1259&isHWU&src=IMT["Tool di matrice di interoperabilità NetApp"]Contiene le informazioni più recenti sulle versioni supportate.
```

Preparazione dei sistemi storage per la replica di SnapMirror e SnapVault per il plug-in per Oracle

È possibile utilizzare un plug-in SnapCenter con la tecnologia SnapMirror di ONTAP per creare copie mirror dei set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replica del backup disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti di SnapMirror e SnapVault al termine dell'operazione di Snapshot. Gli aggiornamenti di SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter; non creare una pianificazione ONTAP separata.

Se vieni a SnapCenter da un prodotto NetApp SnapManager e sei soddisfatto delle relazioni di protezione dei dati che hai configurato, puoi saltare questa sezione.

Una relazione di protezione dei dati replica i dati sullo storage primario (il volume di origine) nello storage secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui fa riferimento il volume di origine al volume di destinazione.

SnapCenter non supporta le relazioni a cascata tra SnapMirror e i volumi SnapVault (**primario** > **Mirror** > **Vault**). Si consiglia di utilizzare le relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per ulteriori informazioni sulle relazioni di SnapMirror flessibili per la versione e sulla loro configurazione, vedere la "Documentazione ONTAP".

SnapCenter non supporta la replica **Sync_mirror**.

Privilegi ONTAP minimi richiesti per il plug-in per Oracle

I privilegi minimi di ONTAP richiesti variano in base ai plug-in di SnapCenter utilizzati per la protezione dei dati.

- All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
  - event generate-autosupport-log
  - mostra la cronologia dei lavori
  - interruzione del lavoro
  - lun
  - visualizzazione dell'attributo lun
  - lun create (crea lun)
  - lun delete (elimina lun)
  - geometria del lun
  - lun igroup add
  - lun igroup create

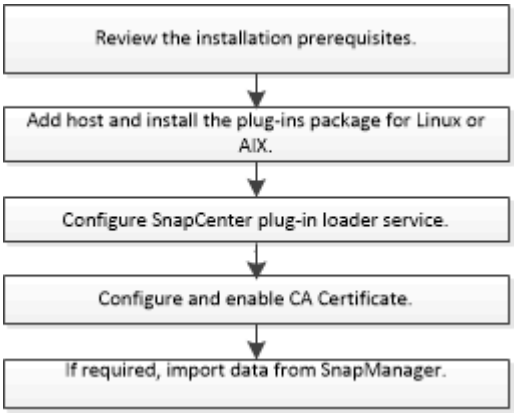
- lun igroup delete (elimina igroup lun)
- lun igroup rename (rinomina lun igroup)
- lun igroup show
- lun mapping add-reporting-node
- creazione mappatura lun
- eliminazione della mappatura lun
- nodi di remove-reporting-mapping lun
- visualizzazione della mappatura del lun
- modifica del lun
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- ridimensionamento del lun
- lun seriale
- lun show
- regola aggiuntiva del criterio snapmirror
- regola-modifica del criterio snapmirror
- regola di rimozione del criterio snapmirror
- policy di snapmirror
- ripristino di snapmirror
- spettacolo di snapmirror
- storia di snapmirror
- aggiornamento di snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione del clone del volume
- visualizzazione del clone del volume
- avvio della divisione del clone del volume
- interruzione della divisione del clone del volume
- creazione del volume
- distruggere il volume
- creazione del clone del file di volume
- file di volume show-disk-usage
- volume offline
- volume online

- modifica del volume
- creazione del qtree del volume
- eliminazione del qtree del volume
- modifica del qtree del volume
- visualizzazione del qtree del volume
- limitazione del volume
- presentazione del volume
- creazione di snapshot di volume
- eliminazione dello snapshot del volume
- modifica dello snapshot del volume
- rinominare lo snapshot del volume
- ripristino dello snapshot del volume
- file di ripristino dello snapshot del volume
- visualizzazione di snapshot di volume
- smontare il volume
- server virtuale
- cifs vserver
- vserver cifs shadowcopy mostra
- show di vserver
- interfaccia di rete
- visualizzazione dell'interfaccia di rete
- spettacolo di MetroCluster

Installare il plug-in SnapCenter per database Oracle

Workflow di installazione del plug-in SnapCenter per database Oracle

Se si desidera proteggere i database SnapCenter, è necessario installare e configurare il plug-in Oracle per il database Oracle.



Prerequisiti per l'aggiunta di host e l'installazione di Plug-ins Package per Linux o AIX

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario completare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È necessario aver attivato la connessione SSH basata su password per l'utente root o non root.

  Il plug-in SnapCenter per database Oracle può essere installato da un utente non root. Tuttavia, è necessario configurare i privilegi sudo per l'utente non root per installare e avviare il processo di plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utenti non root.

- Se si installa il pacchetto di plug-in SnapCenter per AIX su host AIX, i collegamenti simbolici a livello di directory dovrebbero essere stati risolti manualmente.

  Il pacchetto di plug-in SnapCenter per AIX risolve automaticamente il collegamento simbolico a livello di file, ma non i collegamenti simbolici a livello di directory per ottenere il percorso ASSOLUTO JAVA_HOME.

- Creare le credenziali con la modalità di autenticazione come Linux o AIX per l'utente di installazione.
- È necessario aver installato Java 1.8.x o Java 11 a 64 bit sull'host Linux o AIX.

  Assicurarsi di aver installato solo L'edizione certificata DI JAVA 11 sull'host Linux.

  Per informazioni su come scaricare JAVA, consulta:

  - "Download Java per tutti i sistemi operativi"
  - "IBM Java per AIX"
- Per i database Oracle in esecuzione su un host Linux o AIX, è necessario installare sia il plug-in SnapCenter per il database Oracle che il plug-in SnapCenter per UNIX.

  È possibile utilizzare il plug-in per Oracle Database per gestire anche i database Oracle per SAP. Tuttavia, l'integrazione SAP BR*Tools non è supportata.

- Se si utilizza Oracle database 11.2.0.3 o versione successiva, è necessario installare la patch Oracle 13366202.

La mappatura UUID nel file /etc/fstab non è supportata da SnapCenter.

- Si dovrebbe avere **bash** come shell predefinita per l'installazione del plug-in.

Requisiti degli host Linux

Assicurarsi che l'host soddisfi i requisiti prima di installare il pacchetto di plug-in SnapCenter per Linux.

Elemento	Requisiti
Sistemi operativi	• Red Hat Enterprise Linux • Oracle Linux Se si utilizza un database Oracle su LVM nei sistemi operativi Oracle Linux o Red Hat Enterprise Linux 6.6 o 7.0, è necessario installare la versione più recente di Logical Volume Manager (LVM). • SUSE Linux Enterprise Server (SLES)
RAM minima per il plug-in SnapCenter sull'host	2 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	• Java 1,8.x (64 bit) Oracle Java e OpenJDK • Java 11 (64 bit) Oracle Java e OpenJDK Assicurarsi di aver installato solo L'edizione certificata DI JAVA 11 sull'host Linux. Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.

Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Configurare i privilegi sudo per gli utenti non root per l'host Linux

SnapCenter 2.0 e versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per Linux e avviare il processo di plug-in. I processi di plug-in verranno eseguiti come utenti non root. È necessario configurare i privilegi sudo per l'utente non root per fornire l'accesso a diversi percorsi.

Cosa ti serve

- Sudo versione 1.8.7 o successiva.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione del messaggio: Mac hmac-sha2-256 e Mac hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

A proposito di questa attività

È necessario configurare i privilegi sudo per l'utente non root per fornire l'accesso ai seguenti percorsi:

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl

Fasi

1. Accedere all'host Linux su cui si desidera installare il pacchetto di plug-in SnapCenter per Linux.
2. Aggiungere le seguenti righe al file /etc/sudoers usando l'utility visudo Linux.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

LINUX_USER è il nome dell'utente non root creato.

È possibile ottenere il *checksum_value* dal file **oracle_checksum.txt**, che si trova in *C:/ProgramData/NetApp/SnapCenter/Package Repository*.

Se è stata specificata una posizione personalizzata, la posizione sarà *custom_path/NetApp/SnapCenter/Package Repository*.

L'esempio deve essere utilizzato solo come riferimento per la creazione di dati personali.

Requisiti dell'host AIX

Assicurarsi che l'host soddisfi i requisiti prima di installare il pacchetto di plug-in SnapCenter per AIX.

Il plug-in SnapCenter per UNIX, che fa parte del pacchetto plug-in SnapCenter per AIX, non supporta gruppi di volumi simultanei.

Elemento	Requisiti
Sistemi operativi	AIX 7,1 o versione successiva
RAM minima per il plug-in SnapCenter sull'host	4 GB

Elemento	Requisiti
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	• Java 1.8.x (64 bit) IBM Java • Java 11 (64 bit) IBM Java Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.

Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Configurare i privilegi sudo per gli utenti non root per l'host AIX

SnapCenter 4.4 e versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per AIX e di avviare il processo di plug-in. I processi di plug-in verranno eseguiti come utenti non root. È necessario configurare i privilegi sudo per l'utente non root per fornire l'accesso a diversi percorsi.

Cosa ti serve

- Sudo versione 1.8.7 o successiva.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione del messaggio: Mac hmac-sha2-256 e Mac hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

A proposito di questa attività

È necessario configurare i privilegi sudo per l'utente non root per fornire l'accesso ai seguenti percorsi:

- /Home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl

Fasi

1. Accedere all'host AIX su cui si desidera installare il pacchetto plug-in SnapCenter per AIX.
2. Aggiungere le seguenti righe al file /etc/sudoers usando l'utility visudo Linux.

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

AIX_USER è il nome dell'utente non root creato.

È possibile ottenere il *checksum_value* dal file **oracle_checksum.txt**, che si trova in *C:/ProgramData/NetApp/SnapCenter/Package Repository*.

Se è stata specificata una posizione personalizzata, la posizione sarà *custom_path/NetApp/SnapCenter/Package Repository*.

L'esempio deve essere utilizzato solo come riferimento per la creazione di dati personali.

Impostare le credenziali

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. Creare le credenziali per l'installazione del pacchetto plug-in su host Linux o AIX.

A proposito di questa attività

Le credenziali vengono create per l'utente root o per un utente non root che dispone dei privilegi di sudo per installare e avviare il processo di plug-in.

Per informazioni, vedere: Configurare i privilegi sudo per gli utenti non root per l'host Linux O. Configurare i privilegi sudo per gli utenti non root per l'host AIX

Best practice: sebbene sia consentito creare credenziali dopo la distribuzione degli host e l'installazione dei plug-in, la Best practice consiste nel creare credenziali dopo l'aggiunta di SVM, prima di distribuire gli host e installare i plug-in.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.
4. Nella pagina credenziale, immettere le informazioni sulle credenziali:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale	Immettere un nome per le credenziali.

Per questo campo…	Eseguire questa operazione…
Nome utente/Password	Immettere il nome utente e la password da utilizzare per l'autenticazione. • Amministratore di dominio Specificare l'amministratore di dominio sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono: ◦ *NetBIOS/nome utente* ◦ *Dominio FQDN/nome utente* • Amministratore locale (solo per gruppi di lavoro) Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host. Il formato valido per il campo Nome utente è: *Nome utente*
Modalità di autenticazione	Selezionare la modalità di autenticazione che si desidera utilizzare. A seconda del sistema operativo dell'host plug-in, selezionare Linux o AIX.
Utilizzare i privilegi sudo	Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root.

5. Fare clic su **OK**.

Al termine dell'impostazione delle credenziali, è possibile assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina **utente e accesso**.

Configurare le credenziali per un database Oracle

È necessario configurare le credenziali utilizzate per eseguire operazioni di protezione dei dati sui database Oracle.

A proposito di questa attività

È necessario esaminare i diversi metodi di autenticazione supportati per il database Oracle. Per informazioni, vedere "Metodi di autenticazione per le credenziali".

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, il nome utente deve avere almeno privilegi di gruppo di risorse e di backup.

Se è stata attivata l'autenticazione del database Oracle, nella vista delle risorse viene visualizzata un'icona a forma di lucchetto rosso. È necessario configurare le credenziali del database per proteggere il database o aggiungerlo al gruppo di risorse per eseguire le operazioni di protezione dei dati.

Se si specificano dettagli errati durante la creazione di una credenziale, viene visualizzato un messaggio di errore. Fare clic su **Annulla**, quindi riprovare.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** dall'elenco **View** (Visualizza).
3. Fare clic su , quindi selezionare il nome host e il tipo di database per filtrare le risorse.

   È quindi possibile fare clic su per chiudere il riquadro del filtro.
4. Selezionare il database, quindi fare clic su **Impostazioni database** > **Configura database**.
5. Nella sezione Configure database settings (Configura impostazioni database), dall'elenco a discesa **Use Existing Credential** (Usa credenziale esistente), selezionare la credenziale da utilizzare per eseguire i processi di protezione dei dati nel database Oracle.

   L'utente Oracle deve disporre dei privilegi sysdba.

   È anche possibile creare una credenziale facendo clic su .
6. Nella sezione Configure ASM settings (Configura impostazioni ASM), dall'elenco a discesa **Use Existing Credential** (Usa credenziale esistente), selezionare la credenziale da utilizzare per eseguire i processi di protezione dei dati sull'istanza di ASM.

   L'utente ASM deve disporre del privilegio sysasm.

   È anche possibile creare una credenziale facendo clic su .
7. Nella sezione Configure RMAN catalog settings (Configura impostazioni catalogo RMAN), dall'elenco a discesa **Use existing credential** (Usa credenziale esistente), selezionare la credenziale da utilizzare per eseguire i processi di protezione dei dati nel database del catalogo di Oracle Recovery Manager (RMAN).

   È anche possibile creare una credenziale facendo clic su .

   Nel campo **TNSName**, immettere il nome del file TNS (transparent Network substrate) che verrà utilizzato dal server SnapCenter per comunicare con il database.
8. Nel campo **Preferred RAC Nodes** (nodi RAC preferiti), specificare i nodi RAC (Real Application Cluster) preferiti per il backup.

   I nodi preferiti possono essere uno o tutti i nodi del cluster in cui sono presenti le istanze del database RAC. L'operazione di backup viene attivata solo su questi nodi preferiti in ordine di preferenza.

   In RAC One Node, nei nodi preferiti è elencato solo un nodo, che è il nodo in cui è attualmente ospitato il

database.

Dopo il failover o il trasferimento del database RAC a un nodo, l'aggiornamento delle risorse nella pagina risorse SnapCenter rimuoverà l'host dall'elenco **Preferred RAC Node** (nodi RAC preferiti) in cui il database era stato ospitato in precedenza. Il nodo RAC in cui viene ricollocato il database viene elencato in **nodi RAC** e deve essere configurato manualmente come nodo RAC preferito.

Per ulteriori informazioni, vedere "Nodi preferiti nella configurazione RAC".

9. Fare clic su **OK**.

Aggiungere host e installare Plug-ins Package per Linux o AIX utilizzando la GUI

È possibile utilizzare la pagina Aggiungi host per aggiungere host, quindi installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX. I plug-in vengono installati automaticamente sugli host remoti.

A proposito di questa attività

È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster. Se si installa il plug-in su un cluster (Oracle RAC), il plug-in viene installato su tutti i nodi del cluster. Per Oracle RAC One Node, è necessario installare il plug-in su entrambi i nodi attivi e passivi.

È necessario assegnare un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.

Non è possibile aggiungere un server SnapCenter come host plug-in a un altro server SnapCenter.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata nella parte superiore.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare **Linux** o **AIX** come tipo di host. Il server SnapCenter aggiunge l'host, quindi installa il plug-in per il database Oracle e il plug-in per UNIX se i plug-in non sono già installati sull'host.

Per questo campo…	Eseguire questa operazione…
Nome host	Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire l'FQDN. È possibile immettere gli indirizzi IP o il nome FQDN di uno dei seguenti elementi: • Host standalone • Qualsiasi nodo nell'ambiente Oracle Real Application Clusters (RAC) Il nodo VIP o l'IP di scansione non sono supportati Se si aggiunge un host utilizzando SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN.
Credenziali	Selezionare il nome della credenziale creata o creare nuove credenziali. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere le informazioni sulla creazione delle credenziali. È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome specificato. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare i plug-in da installare.
6. (Facoltativo) fare clic su **altre opzioni**.

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.
Percorso di installazione	Il percorso predefinito è */OPT/NetApp/Snapcenter*. È possibile personalizzare il percorso.
Aggiungere tutti gli host in Oracle RAC	Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un RAC Oracle. In una configurazione di Flex ASM, verranno aggiunti tutti i nodi indipendentemente dal fatto che si tratti di un nodo Hub o Leaf.
Ignorare i controlli opzionali di preinstallazione	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo Ignora precheck, l'host viene validato per verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

   Lo script di precheck non convalida lo stato del firewall della porta plug-in se specificato nelle regole di rifiuto del firewall.

   Se non vengono soddisfatti i requisiti minimi, vengono visualizzati messaggi di errore o di avviso appropriati. Se l'errore riguarda lo spazio su disco o la RAM, è possibile aggiornare il file web.config che si trova in *C: File di programma NetApp SnapCenter WebApp* per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione ha, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Verificare l'impronta digitale, quindi fare clic su **Confirm and Submit** (Conferma e invia).

   In una configurazione del cluster, verificare l'impronta digitale di ciascuno dei nodi del cluster.

SnapCenter non supporta l'algoritmo ECDSA.

La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

   I file di log specifici dell'installazione si trovano in */custom_location/snapcenter/logs*.

Risultato

Tutti i database dell'host vengono automaticamente rilevati e visualizzati nella pagina risorse. Se non viene visualizzato alcun messaggio, fare clic su **Refresh Resources** (Aggiorna risorse).

Monitorare lo stato dell'installazione

È possibile monitorare lo stato di avanzamento dell'installazione del pacchetto plug-in di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento dell'installazione per determinare quando è completa o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filter** (filtro).
   b. Facoltativo: Specificare la data di inizio e di fine.
   c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).
   d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.
   e. Fare clic su **Apply** (Applica).
4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Metodi alternativi per installare Plug-ins Package per Linux o AIX

È inoltre possibile installare manualmente il pacchetto di plug-in per Linux o AIX utilizzando i cmdlet o le CLI.

Prima di installare il plug-in manualmente, è necessario convalidare la firma del pacchetto binario utilizzando le chiavi **snapcenter_public_key.pub** e **snapcenter_linux_host_plugin.bin.sig** situate in *C:<ProgramData/NetApp/SnapCenter/Package Repository*.

Assicurarsi che **OpenSSL 1.0.2g** sia installato sull'host in cui si desidera installare il plug-in.

Convalidare la firma del pacchetto binario eseguendo il comando:

- Per host Linux: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- Per l'host AIX: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

Installazione su più host remoti utilizzando cmdlet

Utilizzare il cmdlet *Install-SmHostPackage* PowerShell per installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su più host.

Cosa ti serve

È necessario accedere a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto di plug-in.

Fasi

1. Avviare PowerShell.
2. Sull'host del server SnapCenter, stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
3. Installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX utilizzando il cmdlet *Install-SmHostPackage* e i parametri richiesti.

   È possibile utilizzare l'opzione *-skipprecheck* quando i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

   Lo script di precheck non convalida lo stato del firewall della porta plug-in se specificato nelle regole di rifiuto del firewall.

4. Inserire le credenziali per l'installazione remota.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Installare sull'host del cluster

Installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su entrambi i nodi dell'host del cluster.

Ciascuno dei nodi dell'host del cluster dispone di due IP. Uno degli IP sarà l'IP pubblico dei rispettivi nodi e il secondo IP sarà l'IP del cluster condiviso tra entrambi i nodi.

Fasi

1. Installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su entrambi i nodi dell'host del cluster.
2. Verificare che i valori corretti per i parametri SNAPCENTER_SERVER_HOST, SPL_PORT, SNAPCENTER_SERVER_PORT e SPL_ENABLED_PLUGINS siano specificati nel file spl.properties situato in */var/opt/snapcenter/spl/etc/*.

   Se SPL_ENABLED_PLUGINS non è specificato in spl.properties, è possibile aggiungerlo e assegnare il valore SCO,SCU.

3. Sull'host del server SnapCenter, stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
4. In ciascuno dei nodi, impostare gli IP preferiti del nodo utilizzando il comando *set-PreferredHostIPsInStorageExportPolicy* sccli e i parametri richiesti.
5. Nell'host del server SnapCenter, aggiungere una voce per l'IP del cluster e il nome DNS corrispondente in _C:
6. Aggiungere il nodo al server SnapCenter utilizzando il cmdlet *Add-SmHost* specificando l'IP del cluster per il nome host.

Rilevare il database Oracle sul nodo 1 (supponendo che l'IP del cluster sia ospitato sul nodo 1) e creare un backup del database. In caso di failover, è possibile utilizzare il backup creato sul nodo 1 per ripristinare il database sul nodo 2. È anche possibile utilizzare il backup creato sul nodo 1 per creare un clone sul nodo 2.

Se si verifica il failover mentre sono in esecuzione altre operazioni SnapCenter, saranno presenti volumi, directory e file di blocco obsoleti.

Installare il pacchetto plug-in per Linux in modalità silenziosa

È possibile installare il pacchetto di plug-in SnapCenter per Linux in modalità silenziosa utilizzando l'interfaccia a riga di comando (CLI).

Cosa ti serve

- Esaminare i prerequisiti per l'installazione del pacchetto di plug-in.
- Assicurarsi che la variabile di ambiente DI VISUALIZZAZIONE non sia impostata.

  Se la variabile di ambiente DI VISUALIZZAZIONE è impostata, eseguire unset DISPLAY, quindi provare a installare manualmente il plug-in.

A proposito di questa attività

Durante l'installazione in modalità console, è necessario fornire le informazioni di installazione necessarie, mentre durante l'installazione in modalità silenziosa non è necessario fornire alcuna informazione di installazione.

Fasi

1. Scaricare il pacchetto di plug-in SnapCenter per Linux dal percorso di installazione del server SnapCenter.

Il percorso di installazione predefinito è *C:/ProgramData/NetApp/SnapCenter/PackageRepository*. Questo percorso è accessibile dall'host in cui è installato il server SnapCenter.

2. Dal prompt dei comandi, accedere alla directory in cui è stato scaricato il file di installazione.
3. Eseguire

```
./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR==/opt/custom_path
```

4. Modificare il file spl.properties che si trova in */var/opt/snapcenter/spl/etc/* per aggiungere SPL_ENABLED_PLUGINS=SCO,SCU, quindi riavviare il servizio caricatore plug-in di SnapCenter.

> L'installazione del pacchetto di plug-in registra i plug-in sull'host e non sul server SnapCenter. È necessario registrare i plug-in sul server SnapCenter aggiungendo l'host utilizzando l'interfaccia grafica di SnapCenter o il cmdlet PowerShell. Durante l'aggiunta dell'host, selezionare "Nessuno" come credenziale. Una volta aggiunto l'host, i plug-in installati vengono rilevati automaticamente.

Installare il pacchetto plug-in per AIX in modalità silenziosa

È possibile installare il pacchetto plug-in SnapCenter per AIX in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

Cosa ti serve

- Esaminare i prerequisiti per l'installazione del pacchetto di plug-in.
- Assicurarsi che la variabile di ambiente DI VISUALIZZAZIONE non sia impostata.

  Se la variabile di ambiente DI VISUALIZZAZIONE è impostata, eseguire unset DISPLAY, quindi provare a installare manualmente il plug-in.

Fasi

1. Scaricare il pacchetto di plug-in SnapCenter per AIX dal percorso di installazione del server SnapCenter.

   Il percorso di installazione predefinito è *C:/ProgramData/NetApp/SnapCenter/PackageRepository*. Questo percorso è accessibile dall'host in cui è installato il server SnapCenter.

2. Dal prompt dei comandi, accedere alla directory in cui è stato scaricato il file di installazione.
3. Eseguire

```
./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR==/opt/custom_path-
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
```

4. Modificare il file spl.properties che si trova in */var/opt/snapcenter/spl/etc/* per aggiungere SPL_ENABLED_PLUGINS=SCO,SCU, quindi riavviare il servizio caricatore plug-in di SnapCenter.

L'installazione del pacchetto di plug-in registra i plug-in sull'host e non sul server SnapCenter. È necessario registrare i plug-in sul server SnapCenter aggiungendo l'host utilizzando l'interfaccia grafica di SnapCenter o il cmdlet PowerShell. Durante l'aggiunta dell'host, selezionare "Nessuno" come credenziale. Una volta aggiunto l'host, i plug-in installati vengono rilevati automaticamente.

Configurare il servizio caricatore plug-in di SnapCenter

Il servizio caricatore plug-in SnapCenter carica il pacchetto plug-in per Linux o AIX per interagire con il server SnapCenter. Il servizio caricatore plug-in SnapCenter viene installato quando si installa il pacchetto plug-in SnapCenter per Linux o il pacchetto plug-in SnapCenter per AIX.

A proposito di questa attività

Dopo aver installato il pacchetto plug-in SnapCenter per Linux o il pacchetto plug-in SnapCenter per AIX, il servizio caricatore plug-in SnapCenter si avvia automaticamente. Se il servizio caricatore plug-in di SnapCenter non si avvia automaticamente, è necessario:

- Assicurarsi che la directory in cui opera il plug-in non venga eliminata
- Aumentare lo spazio di memoria assegnato alla Java Virtual Machine

Il file spl.properties, che si trova in */custom_location/NetApp/snapcenter/spl/etc/*, contiene i seguenti parametri. A questi parametri vengono assegnati valori predefiniti.

Nome del parametro	Descrizione
LOG_LEVEL	Visualizza i livelli di registro supportati. I valori possibili sono TRACE, DEBUG, INFO, WARN, ERROR, E FATALE.
PROTOCOLLO_SPL	Visualizza il protocollo supportato dal caricatore plug-in SnapCenter. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.
PROTOCOLLO_SERVER_SNAPCENTER	Visualizza il protocollo supportato dal server SnapCenter. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.
SKIP_JAVAHOME_UPDATE	Per impostazione predefinita, il servizio SPL rileva il percorso java e aggiorna IL parametro JAVA_HOME. Pertanto, il valore predefinito è IMPOSTATO SU FALSE. È possibile impostare SU TRUE se si desidera disattivare il comportamento predefinito e correggere manualmente il percorso java.

Nome del parametro	Descrizione
SPL_KEYSTORE_PASS	Visualizza la password del file keystore. È possibile modificare questo valore solo se si modifica la password o si crea un nuovo file keystore.
SPL_PORT	Visualizza il numero di porta su cui è in esecuzione il servizio caricatore plug-in di SnapCenter. È possibile aggiungere il valore se manca il valore predefinito. Non modificare il valore dopo l'installazione dei plug-in.
SNAPCENTER_SERVER_HOST	Visualizza l'indirizzo IP o il nome host del server SnapCenter.
SPL_KEYSTORE_PATH	Visualizza il percorso assoluto del file keystore.
PORTA_SERVER_SNAPCENTER	Visualizza il numero di porta su cui è in esecuzione il server SnapCenter.
LOG_MAX_COUNT	Visualizza il numero di file di log del caricatore plug-in SnapCenter conservati nella cartella */custom_location/snapcenter/spl/logs*. Il valore predefinito è 5000. Se il conteggio supera il valore specificato, vengono conservati gli ultimi 5000 file modificati. Il controllo del numero di file viene eseguito automaticamente ogni 24 ore dall'avvio del servizio caricatore plug-in di SnapCenter. Se si elimina manualmente il file spl.properties, il numero di file da conservare viene impostato su 9999.
JAVA_HOME	Visualizza il percorso assoluto della directory DI JAVA_HOME che viene utilizzato per avviare il servizio SPL. Questo percorso viene determinato durante l'installazione e come parte dell'avvio di SPL.

Nome del parametro	Descrizione
LOG_MAX_SIZE	Visualizza la dimensione massima del file di log del lavoro. Una volta raggiunta la dimensione massima, il file di registro viene compresso e i registri vengono scritti nel nuovo file del lavoro.
RETAIN_LOGS_OF_LAST_DAYS	Visualizza il numero di giorni in cui i registri vengono conservati.
ENABLE_CERTIFICATE_VALIDATION	Viene visualizzato true quando la convalida del certificato CA è attivata per l'host. È possibile attivare o disattivare questo parametro modificando il file spl.properties o utilizzando l'interfaccia grafica o il cmdlet di SnapCenter.

Se uno di questi parametri non è assegnato al valore predefinito o se si desidera assegnare o modificare il valore, è possibile modificare il file spl.properties. È inoltre possibile verificare il file spl.properties e modificarlo per risolvere eventuali problemi relativi ai valori assegnati ai parametri. Dopo aver modificato il file spl.properties, riavviare il servizio caricatore plug-in di SnapCenter.

Fasi

1. Eseguire una delle seguenti operazioni, secondo necessità:
   - Avviare il servizio caricatore plug-in SnapCenter:
     - Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Arrestare il servizio caricatore plug-in di SnapCenter:
     - Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     È possibile utilizzare l'opzione -force con il comando stop per arrestare con forza il servizio caricatore plug-in di SnapCenter. Tuttavia, prima di eseguire questa operazione, è necessario prestare attenzione, in quanto termina anche le operazioni esistenti.

   - Riavviare il servizio caricatore plug-in di SnapCenter:
     - Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - Individuare lo stato del servizio caricatore plug-in di SnapCenter:

- Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
- Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ Individuare la modifica nel servizio caricatore plug-in di SnapCenter:

- Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurare il certificato CA con il servizio caricatore plug-in (SPL) di SnapCenter sull'host Linux

È necessario gestire la password del keystore SPL e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio di trust SPL e configurare la coppia di chiavi firmate CA per l'archivio di trust SPL con il servizio caricatore plug-in SnapCenter per attivare il certificato digitale installato.

SPL utilizza il file 'keystore.jks', che si trova in '/var/opt/snapcenter/spl/etc' sia come Trust-store che come keystore.

Gestire la password per l'archivio chiavi SPL e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore SPL dal file di proprietà SPL.

   È il valore corrispondente alla chiave 'SOL_KEYSTORE_PASS'.

2. Modificare la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle chiavi private nel
keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

   Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS nel file spl.properties.

3. Riavviare il servizio dopo aver modificato la password.

La password per l'archivio chiavi SPL e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust SPL

È necessario configurare i certificati root o intermedi senza la chiave privata in SPL trust-store.

Fasi

1. Accedere alla cartella contenente il keystore SPL: */var/opt/snapcenter/spl/etc*.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungere un certificato root o intermedio:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Riavviare il servizio dopo aver configurato i certificati root o
intermedi in SPL trust-store.
```

Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi con firma CA nell'archivio di trust SPL

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di fiducia SPL.

Fasi

1. Accedere alla cartella contenente il keystore /var/opt/snapcenter/spl/ecc. della SPL
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungere il certificato CA con chiave pubblica e privata.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Elencare i certificati aggiunti nel keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verificare che il keystore contenga l'alias corrispondente al nuovo
certificato CA aggiunto al keystore.
. Modificare la password della chiave privata aggiunta per il
certificato CA in password archivio chiavi.
```

Default SPL keystore password è il valore della chiave SPL_KEYSTORE_PASS nel file spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias con un nome
semplice:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configurare il nome alias dal keystore che si trova nel file
spl.properties.
```

Aggiornare questo valore con la chiave SPL_CERTIFICATE_ALIAS.

4. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA in SPL trust-store.

Configurare l'elenco CRL (Certificate Revocation List) per SPL

Configurare il CRL per SPL

A proposito di questa attività

- SPL ricerca i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per SPL è */var/opt/snapcenter/spl/etc/crl*.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file spl.properties in base alla chiave SPL_CRL_PATH.
2. È possibile inserire più file CRL in questa directory.

   I certificati in entrata verranno verificati per ciascun CRL.

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.
5. Selezionare **attiva convalida certificato**.

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- * * Indica che il certificato CA non è né abilitato né assegnato all'host del plug-in.
- * * Indica che il certificato CA è stato convalidato correttamente.
- * * Indica che il certificato CA non può essere convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Importa i dati da SnapManager per Oracle e SnapManager per SAP a SnapCenter

L'importazione dei dati da SnapManager per Oracle e SnapManager per SAP a SnapCenter consente di continuare a utilizzare i dati delle versioni precedenti.

È possibile importare i dati da SnapManager per Oracle e SnapManager per SAP a SnapCenter eseguendo lo strumento di importazione dall'interfaccia della riga di comando (CLI host Linux).

Lo strumento di importazione crea policy e gruppi di risorse in SnapCenter. I criteri e i gruppi di risorse creati in SnapCenter corrispondono ai profili e alle operazioni eseguite utilizzando tali profili in SnapManager per Oracle e SnapManager per SAP. Lo strumento di importazione SnapCenter interagisce con i database dei repository SnapManager per Oracle e SnapManager per SAP e con il database che si desidera importare.

- Recupera tutti i profili, le pianificazioni e le operazioni eseguite utilizzando i profili.
- Crea una policy di backup SnapCenter per ogni operazione univoca e ogni pianificazione allegata a un profilo.
- Crea un gruppo di risorse per ogni database di destinazione.

È possibile eseguire lo strumento di importazione eseguendo lo script sc-migra situato in */opt/NetApp/snapcenter/spl/bin*. Quando si installa il pacchetto di plug-in SnapCenter per Linux sull'host di database che si desidera importare, lo script di migrazione sc viene copiato in */opt/NetApp/snapcenter/spl/bin*.

L'importazione dei dati non è supportata dall'interfaccia grafica utente (GUI) di SnapCenter.

SnapCenter non supporta Data ONTAP in 7-Mode. È possibile utilizzare lo strumento di transizione 7-Mode per migrare i dati e le configurazioni memorizzati in un sistema che esegue Data ONTAP in 7-Mode a un sistema ONTAP.

Configurazioni supportate per l'importazione dei dati

Prima di importare i dati da SnapManager 3.4.x per Oracle e SnapManager 3.4.x per SAP a SnapCenter, è necessario conoscere le configurazioni supportate dal plug-in SnapCenter per database Oracle.

Le configurazioni supportate dal plug-in SnapCenter per database Oracle sono elencate nella "Tool di matrice di interoperabilità NetApp".

Cosa viene importato in SnapCenter

È possibile importare profili, pianificazioni e operazioni eseguite utilizzando i profili.

Da SnapManager per Oracle e SnapManager per SAP	A SnapCenter
Profili senza operazioni e pianificazioni	Viene creato un criterio con il tipo di backup predefinito online e l'ambito di backup completo.
Profili con una o più operazioni	Vengono create più policy in base a una combinazione univoca di un profilo e delle operazioni eseguite utilizzando tale profilo. I criteri creati in SnapCenter contengono l'eliminazione del log di archiviazione e i dettagli di conservazione recuperati dal profilo e dalle operazioni corrispondenti.
Profili con configurazione di Oracle Recovery Manager (RMAN)	Le policy vengono create con l'opzione **Catalog backup with Oracle Recovery Manager** attivata. Se è stata utilizzata la catalogazione RMAN esterna in SnapManager, è necessario configurare le impostazioni del catalogo RMAN in SnapCenter. È possibile selezionare la credenziale esistente o crearne una nuova. Se RMAN è stato configurato tramite il file di controllo in SnapManager, non è necessario configurare RMAN in SnapCenter.
Programma allegato a un profilo	Viene creata una policy solo per la pianificazione.

Da SnapManager per Oracle e SnapManager per SAP	A SnapCenter
Database	Viene creato un gruppo di risorse per ogni database importato. In un'installazione di Real Application Clusters (RAC), il nodo su cui viene eseguito lo strumento di importazione diventa il nodo preferito dopo l'importazione e il gruppo di risorse viene creato per quel nodo.

Quando viene importato un profilo, viene creato un criterio di verifica insieme al criterio di backup.

Quando i profili, le pianificazioni e le operazioni eseguite con i profili SnapManager for Oracle e SnapManager for SAP vengono importati in SnapCenter, vengono importati anche i diversi valori dei parametri.

Parametri e valori di SnapManager per Oracle e SnapManager per SAP	Parametri e valori SnapCenter	Note
Ambito del backup • Completo • Dati • Log (Registro)	Ambito del backup • Completo • Dati • Log (Registro)	
Modalità di backup • Automatico • Online • Offline	Tipo di backup • Online • Spegnimento offline	Se la modalità di backup è Auto, lo strumento di importazione controlla lo stato del database al momento dell'esecuzione dell'operazione e imposta correttamente il tipo di backup come Online o Offline Shutdown.
Conservazione • Giorni • Conta	Conservazione • Giorni • Conta	SnapManager per Oracle e SnapManager per SAP utilizzano giorni e conteggi per impostare la conservazione. In SnapCenter, sono disponibili i conteggi dei giorni o dei giorni. Pertanto, la conservazione viene stabilita rispetto ai giorni in cui i giorni ottengono la preferenza rispetto ai conteggi in SnapManager per Oracle e SnapManager per SAP.

Parametri e valori di SnapManager per Oracle e SnapManager per SAP	Parametri e valori SnapCenter	Note
Eliminazione delle pianificazioni • Tutto • Numero di cambio di sistema (SCN) • Data • Registri creati prima di ore, giorni, settimane e mesi specificati	Eliminazione delle pianificazioni • Tutto • Registri creati prima di ore e giorni specificati	SnapCenter non supporta la potatura in base a SCN, Data, settimane e mesi.
Notifica • E-mail inviate solo per operazioni riuscite • E-mail inviate solo per operazioni non riuscite • E-mail inviate per operazioni riuscite e non riuscite	Notifica • Sempre • In caso di guasto • Attenzione • Errore	Le notifiche e-mail vengono importate. Tuttavia, è necessario aggiornare manualmente il server SMTP utilizzando l'interfaccia grafica di SnapCenter. L'oggetto del messaggio di posta elettronica viene lasciato vuoto per la configurazione.

Cosa non viene importato in SnapCenter

Lo strumento di importazione non importa tutto in SnapCenter.

Non è possibile importare quanto segue in SnapCenter:

- Metadati di backup
- Backup parziali
- Backup RDM (Raw Device mapping) e VSC (Virtual Storage Console) correlati
- Ruoli o credenziali disponibili nel repository SnapManager per Oracle e SnapManager per SAP
- Dati relativi alle operazioni di verifica, ripristino e clonazione
- Eliminazione delle operazioni
- Dettagli di replica specificati nel profilo SnapManager per Oracle e SnapManager per SAP

  Dopo l'importazione, è necessario modificare manualmente il criterio corrispondente creato in SnapCenter per includere i dettagli della replica.

- Informazioni di backup catalogate

Prepararsi all'importazione dei dati

Prima di importare i dati in SnapCenter, è necessario eseguire alcune operazioni per eseguire correttamente l'operazione di importazione.

Fasi

1. Identificare il database che si desidera importare.
2. Utilizzando SnapCenter, aggiungere l'host del database e installare il pacchetto di plug-in SnapCenter per Linux.
3. Utilizzando SnapCenter, impostare le connessioni per le macchine virtuali di storage (SVM) utilizzate dai database sull'host.
4. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
5. Nella pagina Resources (risorse), verificare che il database da importare venga rilevato e visualizzato.

   Se si desidera eseguire lo strumento di importazione, il database deve essere accessibile, altrimenti la creazione del gruppo di risorse non riesce.

   Se nel database sono configurate le credenziali, è necessario creare una credenziale corrispondente in SnapCenter, assegnarla al database ed eseguire di nuovo il rilevamento del database. Se il database risiede in Automatic Storage Management (ASM), è necessario creare le credenziali per l'istanza ASM e assegnarle al database.

6. Assicurarsi che l'utente che esegue lo strumento di importazione disponga di privilegi sufficienti per eseguire i comandi CLI di SnapManager per Oracle o SnapManager per SAP (ad esempio il comando per sospendere le pianificazioni) da SnapManager per Oracle o SnapManager per host SAP.
7. Eseguire i seguenti comandi sull'host SnapManager per Oracle o SnapManager per SAP per sospendere le pianificazioni:

   a. Se si desidera sospendere le pianificazioni sull'host SnapManager per Oracle, eseguire:

      - `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smo credential set -profile -name profile_name`

        È necessario eseguire il comando smo credential set per ciascun profilo sull'host.

   b. Se si desidera sospendere le pianificazioni sull'host SnapManager per SAP, eseguire:

      - `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smsap credential set -profile -name profile_name`

   È necessario eseguire il comando sspap credential set per ogni profilo sull'host.

8. Assicurarsi che FQDN (Fully Qualified Domain Name) dell'host di database sia visualizzato quando si

esegue hostname -F.

Se FQDN non viene visualizzato, è necessario modificare /etc/hosts per specificare l'FQDN dell'host.

Importare i dati

È possibile importare i dati eseguendo lo strumento di importazione dall'host del database.

A proposito di questa attività

I criteri di backup di SnapCenter creati dopo l'importazione hanno diversi formati di denominazione:

- Le policy create per i profili senza operazioni e pianificazioni hanno il formato SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED.

  Quando non viene eseguita alcuna operazione utilizzando un profilo, il criterio corrispondente viene creato con il tipo di backup predefinito online e l'ambito di backup completo.

- I criteri creati per i profili con una o più operazioni hanno il formato SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.
- I criteri creati per le pianificazioni associate ai profili hanno il formato SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.

Fasi

1. Accedere all'host di database che si desidera importare.
2. Eseguire lo strumento di importazione eseguendo lo script sc-migra situato in */opt/NetApp/Snapcenter/spl/bin*.
3. Immettere il nome utente e la password del server SnapCenter.

   Una volta convalidate le credenziali, viene stabilita una connessione con SnapCenter.

4. Immettere i dettagli del database del repository SnapManager per Oracle o SnapManager per SAP.

   Il database del repository elenca i database disponibili sull'host.

5. Inserire i dettagli del database di destinazione.

   Se si desidera importare tutti i database sull'host, immettere all (tutti).

6. Se si desidera generare un log di sistema o inviare messaggi ASUP per operazioni non riuscite, è necessario attivarli eseguendo il comando *Add-SmStorageConnection* o *set-SmStorageConnection*.

> Se si desidera annullare un'operazione di importazione, durante l'esecuzione dello strumento di importazione o dopo l'importazione, è necessario eliminare manualmente i criteri, le credenziali e i gruppi di risorse di SnapCenter creati durante l'operazione di importazione.

Risultati

I criteri di backup di SnapCenter vengono creati per i profili, le pianificazioni e le operazioni eseguite utilizzando i profili. Vengono inoltre creati gruppi di risorse per ogni database di destinazione.

Una volta importati correttamente i dati, le pianificazioni associate al database importato vengono sospese in SnapManager per Oracle e SnapManager per SAP.

> Dopo l'importazione, è necessario gestire il database o il file system importato utilizzando SnapCenter.

I log per ogni esecuzione del tool di importazione sono memorizzati nella directory */var/opt/snapcenter/spl/logs* con il nome spl_Migration_timestamp.log. È possibile fare riferimento a questo registro per esaminare gli errori di importazione e risolverli.

Installare il plug-in SnapCenter per VMware vSphere

Se il database o il file system sono memorizzati su macchine virtuali (VM), o se si desidera proteggere macchine virtuali e datastore, è necessario implementare il plug-in SnapCenter per l'appliance virtuale VMware vSphere.

Per informazioni sulla distribuzione, vedere "Panoramica sull'implementazione".

Implementare il certificato CA

Per configurare il certificato CA con il plug-in SnapCenter per VMware vSphere, vedere "Creare o importare un certificato SSL".

Configurare il file CRL

Il plug-in SnapCenter per VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il plug-in SnapCenter per VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Prepararsi alla protezione dei database Oracle

Prima di eseguire qualsiasi operazione di protezione dei dati, ad esempio operazioni di backup, clonazione o ripristino, è necessario definire la strategia e impostare l'ambiente. È inoltre possibile configurare il server SnapCenter in modo che utilizzi le tecnologie SnapMirror e SnapVault.

Per sfruttare i vantaggi delle tecnologie SnapVault e SnapMirror, è necessario configurare e inizializzare una relazione di protezione dei dati tra i volumi di origine e di destinazione sul dispositivo di storage. È possibile utilizzare NetAppSystem Manager oppure la riga di comando della console di storage per eseguire queste attività.

Prima di utilizzare il plug-in per database Oracle, l'amministratore di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività richieste.

- Installare e configurare il server SnapCenter. "Scopri di più"
- Configurare l'ambiente SnapCenter aggiungendo le connessioni del sistema storage. "Scopri di più"

SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM registrato con SnapCenter utilizzando la registrazione SVM o la registrazione del cluster deve essere univoco.

- Creare credenziali con la modalità di autenticazione come Linux o AIX per l'utente di installazione. "Scopri di più"
- Aggiungi host, installa i plug-in e scopri le risorse.
- Se si utilizza il server SnapCenter per proteggere i database Oracle che risiedono su LUN o VMDM VMware, è necessario implementare il plug-in SnapCenter per VMware vSphere e registrare il plug-in con SnapCenter.
- Installare Java sull'host Linux o AIX.

  Per ulteriori informazioni, vedere "Requisiti degli host Linux" o. "Requisiti degli host AIX"

- Impostare il valore di timeout del firewall dell'applicazione su almeno 3 ore.
- Se si dispone di database Oracle in ambienti NFS, è necessario aver configurato almeno una LIF dati NFS per lo storage primario o secondario per eseguire operazioni di montaggio, clonazione, verifica e ripristino.
- Se si dispone di più percorsi dati (LIF) o di una configurazione DNFS, è possibile eseguire le seguenti operazioni utilizzando l'interfaccia utente di SnapCenter sull'host del database:
  - Per impostazione predefinita, tutti gli indirizzi IP dell'host del database vengono aggiunti alla policy di esportazione dello storage NFS in SVM (Storage Virtual Machine) per i volumi clonati. Se si desidera avere un indirizzo IP specifico o limitare un sottoinsieme di indirizzi IP, eseguire la CLI Set-PreferredHostIPsInStorageExportPolicy.
  - Se si dispone di più percorsi di dati (LIF) in SVM, SnapCenter sceglie il percorso di dati appropriato per il montaggio del volume clonato NFS. Tuttavia, se si desidera specificare un percorso dati specifico (LIF), è necessario eseguire la CLI Set-SvmPreferredDataPath. La guida di riferimento ai comandi contiene ulteriori informazioni.
- Se si dispone di database Oracle su ambienti SAN, assicurarsi che l'ambiente SAN sia configurato in base ai consigli indicati nelle seguenti guide:
  - "Impostazioni host consigliate per le utility host unificate Linux"
  - "Utilizzo di host Linux con storage ONTAP"
  - "Impostazioni host interessate dalle utility host AIX"
- Se si dispone di database Oracle su LVM nei sistemi operativi Oracle Linux o RHEL, installare la versione più recente di Logical Volume Management (LVM).
- Se si utilizza SnapManager per Oracle e si desidera migrare al plug-in SnapCenter per database Oracle, è possibile migrare i profili in policy e gruppi di risorse di SnapCenter utilizzando il comando sccli sc-migra.
- Configurare SnapMirror e SnapVault su ONTAP, se si desidera eseguire la replica del backup

Per gli utenti di SnapCenter 4.1.1, la documentazione del plug-in SnapCenter per VMware vSphere 4.1.1 contiene informazioni sulla protezione dei database e dei file system virtualizzati. Per gli utenti di SnapCenter 4.2.x, NetApp Data Broker 1.0 e 1.0.1, la documentazione contiene informazioni sulla protezione dei database virtualizzati e dei file system mediante il plug-in SnapCenter per VMware vSphere fornito dall'appliance virtuale NetApp Data Broker basata su Linux (formato di appliance virtuale aperta). Per gli utenti di SnapCenter 4.3.x, la documentazione relativa al plug-in SnapCenter per VMware vSphere 4.3 contiene informazioni sulla protezione dei database e dei file system virtualizzati mediante il plug-in SnapCenter basato su Linux per l'appliance virtuale VMware vSphere (formato appliance virtuale aperta).

Ulteriori informazioni

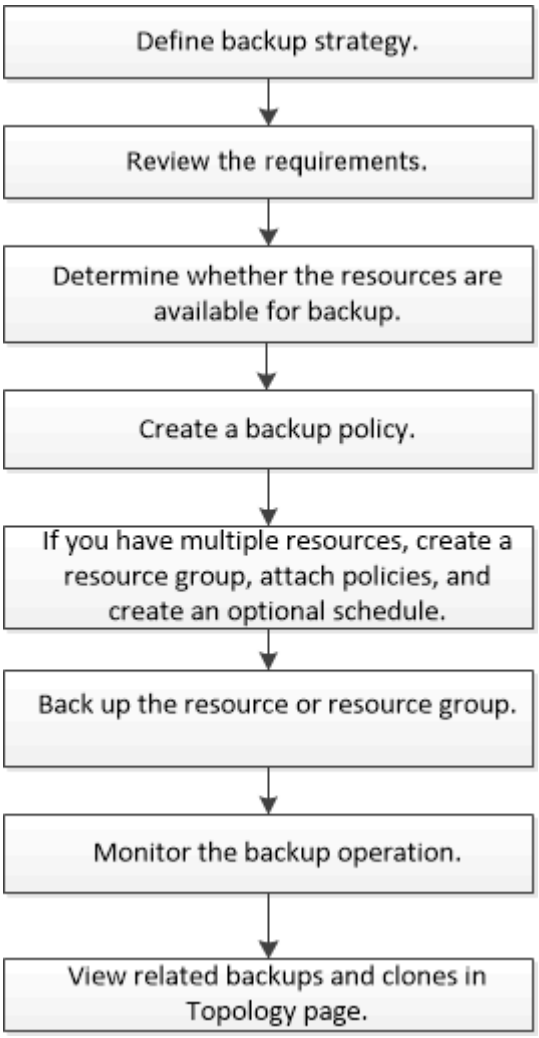
- "Tool di matrice di interoperabilità"
- "Plug-in SnapCenter per la documentazione di VMware vSphere"
- "L'operazione di protezione dei dati non riesce in un ambiente non multipath in RHEL 7 e versioni successive"

Eseguire il backup dei database Oracle

Panoramica della procedura di backup

È possibile creare un backup di una risorsa (database) o di un gruppo di risorse. La procedura di backup include la pianificazione, l'identificazione delle risorse per il backup, la creazione di policy di backup, la creazione di gruppi di risorse e l'aggiunta di policy, la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:



Durante la creazione di un backup per i database Oracle, viene creato un file di blocco operativo (*.SM_lock_dbsid*) sull'host del database Oracle nella directory */var/opt/snapcenter/sco/lock* per evitare l'esecuzione di più operazioni sul database. Una volta eseguito il backup del database, il file di blocco operativo viene rimosso automaticamente.

Tuttavia, se il backup precedente è stato completato con un avviso, il file di blocco operativo potrebbe non essere cancellato e l'operazione di backup successiva viene inserita nella coda di attesa. Potrebbe essere annullato se il file **.SM_lock_dbsid** non viene cancellato. In questo scenario, è necessario eliminare manualmente il file di blocco operativo eseguendo le seguenti operazioni:

1. Dal prompt dei comandi, selezionare */var/opt/snapcenter/sco/lock*.
2. Eliminare il blocco operativo:`rm -rf .sm_lock_dbsid.`

Informazioni sulla configurazione del backup

Configurazioni di database Oracle supportate per i backup

SnapCenter supporta il backup di diverse configurazioni di database Oracle.

- Oracle Standalone
- Oracle Real Application Clusters (RAC)
- Oracle Standalone Legacy
- Database Oracle Standalone Container (CDB)
- Oracle Data Guard in standby

  È possibile creare solo backup offline dei database di standby di Data Guard. Backup offline-shutdown, backup solo log di archiviazione e backup completo non sono supportati.

- Oracle Active Data Guard in standby

  È possibile creare solo backup online dei database di standby di Active Data Guard. Il backup solo del registro di archiviazione e il backup completo non sono supportati.

  Prima di creare un backup del database di standby Data Guard o Active Data Guard, il processo di ripristino gestito (MRP) viene interrotto e, una volta creato, viene avviato MRP.

- Gestione automatica dello storage (ASM)
  - ASM standalone e ASM RAC su Virtual Machine Disk (VMDK)

    Tra tutti i metodi di ripristino supportati per i database Oracle, è possibile eseguire solo il ripristino Connect-and-copy dei database RAC ASM su VMDK.

  - ASM standalone e ASM RAC on Raw Device Mapping (RDM) + è possibile eseguire operazioni di backup, ripristino e clonazione sui database Oracle su ASM, con o senza ASMLib.
  - Oracle ASM Filter driver (ASMFD)

    Le operazioni di migrazione PDB e clonazione PDB non sono supportate.

  - Oracle Flex ASM

Per informazioni aggiornate sulle versioni Oracle supportate, vedere "Tool di matrice di interoperabilità NetApp".

Tipi di backup supportati per i database Oracle

Il tipo di backup specifica il tipo di backup che si desidera creare. SnapCenter supporta i

tipi di backup online e offline per i database Oracle.

Backup online

Un backup creato quando il database si trova nello stato online viene chiamato backup online. Un backup online, chiamato anche backup a caldo, consente di creare un backup del database senza spegnerlo.

Come parte del backup online, è possibile creare un backup dei seguenti file:

- Solo file di dati e file di controllo
- Solo file di log di archiviazione (il database non viene portato in modalità di backup in questo scenario)
- Database completo che include file di dati, file di controllo e file di log di archiviazione

Backup offline

Un backup creato quando il database si trova in uno stato di installazione o di arresto viene definito backup offline. Un backup offline è anche chiamato cold backup. È possibile includere solo file di dati e file di controllo nei backup offline. È possibile creare un backup offline mount o offline shutdown.

- Quando si crea un backup di montaggio offline, è necessario assicurarsi che il database si trovi in uno stato montato.

  Se il database si trova in qualsiasi altro stato, l'operazione di backup non riesce.

- Quando si crea un backup di shutdown offline, il database può trovarsi in qualsiasi stato.

  Lo stato del database viene modificato nello stato richiesto per creare un backup. Dopo aver creato il backup, lo stato del database viene reimpostato sullo stato originale.

In che modo SnapCenter rileva i database Oracle

Le risorse sono database Oracle sull'host gestiti da SnapCenter. È possibile aggiungere questi database ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database disponibili.

Nelle sezioni seguenti viene descritto il processo utilizzato da SnapCenter per rilevare diversi tipi e versioni di database Oracle.

Per le versioni Oracle da 11*g* a 12*c*R1

Database RAC

I database RAC vengono rilevati solo sulla base di /etc/oratab`entry. Le voci del database dovrebbero essere presenti nel file /etc/oratab.

Standalone

I database standalone vengono rilevati solo in base alle voci /etc/oratab.

ASM

La voce dell'istanza di ASM dovrebbe essere disponibile nel file /etc/oratab.

RAC un nodo

I database RAC One Node vengono rilevati solo in base alle voci /etc/oratab. I database devono essere in

stato nomount, mount o open. Le voci del database dovrebbero essere presenti nel file /etc/oratab.

Lo stato del database RAC One Node viene contrassegnato come rinominato o cancellato se il database è già stato rilevato e i backup sono associati al database.

Se il database viene trasferito, attenersi alla seguente procedura:

1. Aggiungere manualmente la voce del database ricollocata nel file /etc/oratab sul nodo RAC failed-over.
2. Aggiornare manualmente le risorse.
3. Selezionare il database RAC One Node dalla pagina delle risorse, quindi fare clic su Database Settings (Impostazioni database).
4. Configurare il database per impostare i nodi del cluster preferiti sul nodo RAC che ospita il database.
5. Eseguire le operazioni SnapCenter.
6. Se si è trasferito un database da un nodo a un altro e la voce di oratab nel nodo precedente non viene eliminata, eliminare manualmente la voce di oratab per evitare che lo stesso database venga visualizzato due volte.

Per le versioni Oracle da 12cR2 a 18c

Database RAC

I database RAC vengono rilevati utilizzando il comando srvctl config. Le voci del database dovrebbero essere presenti nel file /etc/oratab.

Standalone

I database standalone vengono rilevati in base alle voci nel file /etc/oratab e all'output del comando srvctl config.

ASM

La voce dell'istanza ASM non deve essere nel file /etc/oratab.

RAC un nodo

I database RAC One Node vengono rilevati solo utilizzando il comando srvctl config. I database devono essere in stato nomount, mount o open. Lo stato del database RAC One Node viene contrassegnato come rinominato o cancellato se il database è già stato rilevato e i backup sono associati al database.

Se il database viene trasferito, attenersi alla seguente procedura: . Aggiornare manualmente le risorse. . Selezionare il database RAC One Node dalla pagina delle risorse, quindi fare clic su Database Settings (Impostazioni database). . Configurare il database per impostare i nodi del cluster preferiti sul nodo RAC che ospita il database. . Eseguire le operazioni SnapCenter.

> Se sono presenti voci di database Oracle 12*c*R2 e 18*c* nel file /etc/oratab e lo stesso database viene registrato con il comando srvctl config, SnapCenter eliminerà le voci di database duplicate. Se sono presenti voci di database obsolete, il database viene rilevato ma il database non sarà raggiungibile e lo stato sarà offline.

Nodi preferiti nella configurazione RAC

Nella configurazione di Oracle Real Application Clusters (RAC), è possibile specificare i nodi preferiti utilizzati da SnapCenter per eseguire l'operazione di backup. Se non si specifica il nodo preferito, SnapCenter assegna automaticamente un nodo come nodo

preferito e viene creato il backup su tale nodo.

I nodi preferiti possono essere uno o tutti i nodi del cluster in cui sono presenti le istanze del database RAC. L'operazione di backup viene attivata solo su questi nodi preferiti nell'ordine delle preferenze.

Esempio

Il database RAC cdbrac ha tre istanze: Cdbrac1 su node1, cdbrac2 su node2 e cdbrac3 su node3.

Le istanze node1 e node2 sono configurate per essere i nodi preferiti, con node2 come prima preferenza e node1 come seconda preferenza. Quando si esegue un'operazione di backup, l'operazione viene prima tentata sul nodo 2 perché si tratta del primo nodo preferito.

Se node2 non si trova nello stato di backup, il che potrebbe essere dovuto a diversi motivi, come ad esempio l'agente plug-in non è in esecuzione sull'host, l'istanza del database sull'host non si trova nello stato richiesto per il tipo di backup specificato, Oppure l'istanza del database sul nodo 2 in una configurazione FlexASM non viene servita dall'istanza ASM locale; quindi l'operazione verrà tentata sul nodo 1.

Il node3 non verrà utilizzato per il backup perché non è presente nell'elenco dei nodi preferiti.

Configurazione di Flex ASM

In una configurazione di Flex ASM, i nodi Leaf non vengono elencati come nodi preferiti se la cardinalità è inferiore al numero di nodi nel cluster RAC. In caso di modifiche nei ruoli dei nodi del cluster Flex ASM, è necessario eseguire manualmente la ricerca in modo da aggiornare i nodi preferiti.

Stato del database richiesto

Le istanze del database RAC sui nodi preferiti devono trovarsi nello stato richiesto per il completamento del backup:

- Una delle istanze di database RAC nei nodi preferiti configurati deve essere in stato aperto per creare un backup online.
- Una delle istanze del database RAC nei nodi preferiti configurati deve essere in stato di montaggio e tutte le altre istanze, compresi gli altri nodi preferiti, devono essere in stato di montaggio o inferiori per creare un backup di montaggio offline.
- Le istanze del database RAC possono essere in qualsiasi stato, ma è necessario specificare i nodi preferiti per creare un backup di shutdown offline.

Come catalogare i backup con Oracle Recovery Manager

È possibile catalogare i backup dei database Oracle utilizzando Oracle Recovery Manager (RMAN) per memorizzare le informazioni di backup nel repository Oracle RMAN.

I backup catalogati possono essere utilizzati in seguito per operazioni di ripristino a livello di blocco o tablespace point-in-time. Se non sono necessari backup catalogati, è possibile rimuovere le informazioni del catalogo.

Il database deve essere in stato montato o superiore per la catalogazione. È possibile eseguire la catalogazione dei backup dei dati, dei backup dei log di archiviazione e dei backup completi. Se la catalogazione è abilitata per un backup di un gruppo di risorse che ha più database, viene eseguita la catalogazione per ogni database. Per i database Oracle RAC, la catalogazione verrà eseguita sul nodo preferito in cui il database si trova almeno nello stato montato.

Se si desidera catalogare i backup di un database RAC, assicurarsi che non siano in esecuzione altri processi per tale database. Se è in esecuzione un altro processo, l'operazione di catalogazione non riesce invece di essere messa in coda.

Database del catalogo esterno

Per impostazione predefinita, il file di controllo del database di destinazione viene utilizzato per la catalogazione. Se si desidera aggiungere un database del catalogo esterno, è possibile configurarlo specificando la credenziale e il nome del substrato di rete trasparente (TNS) del catalogo esterno utilizzando la procedura guidata Impostazioni database dall'interfaccia grafica utente (GUI) di SnapCenter. È inoltre possibile configurare il database del catalogo esterno dalla CLI eseguendo il comando Configure-SmOracleDatabase con le opzioni -OracleRmanCatalogCredentialName e -OracleRmanCatalogTnsName.

Comando RMAN

Se è stata attivata l'opzione di catalogazione durante la creazione di un criterio di backup Oracle dall'interfaccia grafica di SnapCenter, i backup vengono catalogati utilizzando Oracle RMAN come parte dell'operazione di backup. È inoltre possibile eseguire la catalogazione differita dei backup eseguendo il `Catalog-SmBackupWithOracleRMAN` comando.

Dopo aver catalogato i backup, è possibile eseguire il `Get-SmBackupDetails` comando per ottenere le informazioni di backup catalogate, come il tag per i file di dati catalogati, il percorso del catalogo dei file di controllo e le posizioni dei log di archivio catalogati.

Formato di naming

Se il nome del gruppo di dischi ASM è maggiore o uguale a 16 caratteri, da SnapCenter 3.0, il formato di denominazione utilizzato per il backup è SC_HASHCODEODISKGROUP_DBSID_BACKUPID. Tuttavia, se il nome del gruppo di dischi è inferiore a 16 caratteri, il formato di denominazione utilizzato per il backup è DISKGROUPNAME_DBSID_BACKUPID, che è lo stesso formato utilizzato in SnapCenter 2.0.

HASHCODEofDISKGROUP è un numero generato automaticamente (da 2 a 10 cifre) univoco per ciascun gruppo di dischi ASM.

Operazioni di crosscheck

È possibile eseguire controlli incrociati per aggiornare le informazioni obsolete del repository RMAN sui backup i cui record del repository non corrispondono al loro stato fisico. Ad esempio, se un utente rimuove i log archiviati dal disco con un comando del sistema operativo, il file di controllo indica ancora che i log sono su disco, mentre di fatto non lo sono.

L'operazione di crosscheck consente di aggiornare il file di controllo con le informazioni. È possibile attivare il crosscheck eseguendo il comando set-SmConfigSettings e assegnando il valore TRUE al parametro ENABLE_CROSSCHECK. Il valore predefinito è FALSE.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Rimuovere le informazioni sul catalogo

È possibile rimuovere le informazioni del catalogo eseguendo il comando Uncatalog-SmBackupWithOracleRMAN. Non è possibile rimuovere le informazioni del catalogo utilizzando l'interfaccia grafica di SnapCenter. Tuttavia, le informazioni di un backup catalogato vengono rimosse durante l'eliminazione del backup o durante l'eliminazione della conservazione e del gruppo di risorse associati a tale backup catalogato.

Quando si forza l'eliminazione dell'host SnapCenter, le informazioni dei backup catalogati associati a tale host non vengono rimosse. È necessario rimuovere le informazioni di tutti i backup catalogati per l'host prima di forzare l'eliminazione dell'host.

Se la catalogazione e la decatalogazione non riescono perché il tempo dell'operazione ha superato il valore di timeout specificato per IL parametro ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT, modificare il valore del parametro eseguendo il seguente comando:

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType
Plugin -PluginCode SCO-ConfigSettings
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Dopo aver modificato il valore del parametro, riavviare il servizio caricatore plug-in (SPL) di SnapCenter eseguendo il seguente comando:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help command_name. In alternativa, fare riferimento a "Guida di riferimento al comando software SnapCenter".

Variabili d'ambiente predefinite per Prespt e postscript specifici per il backup

SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono Prespt e postscript durante la creazione di criteri di backup. Questa funzionalità è supportata per tutte le configurazioni Oracle, ad eccezione di VMDK.

SnapCenter predefinisce i valori dei parametri che saranno direttamente accessibili nell'ambiente in cui vengono eseguiti gli script della shell. Non è necessario specificare manualmente i valori di questi parametri durante l'esecuzione degli script.

Variabili di ambiente predefinite supportate per la creazione di policy di backup

- **SC_JOB_ID** specifica l'ID lavoro dell'operazione.

  Esempio: 256

- **SC_ORACLE_SID** specifica l'identificatore di sistema del database.

  Se l'operazione coinvolge più database, il parametro conterrà nomi di database separati da pipe.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: NFSB32|NFSB31

- **SC_HOST** specifica il nome host del database.

  Per RAC, il nome host sarà il nome dell'host su cui viene eseguito il backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** specifica il proprietario del sistema operativo del database.

I dati verranno formattati come <db1>@<osuser1>|<db2>@<osuser2>.

Esempio: NFSB31@oracle|NFSB32@oracle

- **SC_OS_GROUP** specifica il gruppo del sistema operativo del database.

  I dati verranno formattati come <db1>@<osgroup1>|<db2>@<osgroup2>.

  Esempio: NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE**" specifica il tipo di backup (online completo, dati online, log online, shutdown offline, montaggio offline)

  Esempi:

  - Per il backup completo: ONLINEFULL
  - Backup solo dati: ONLINEDATA
  - Per backup solo log: ONLINELOG

- **SC_BACKUP_NAME** specifica il nome del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1|AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267

- **SC_BACKUP_ID** specifica l'ID del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  ESEMPIO: DATA@203|LOG@205|AV@207

- **SC_ORACLE_HOME** specifica il percorso della home directory Oracle.

  Esempio: NFSB32@/ora01/app/oracle/product/18.1.0/db_1|NFSB31@/ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_RETENTION** specifica il periodo di conservazione definito nel criterio.

  Esempi:

  - Per il backup completo: Hourly|DATA@DAYS:3|LOG@COUNT:4
  - Backup solo per dati on-demand: OnDemand|DATA@COUNT:2
  - Per backup on-demand solo log: OnDemand|LOG@COUNT:2

- **Nome_GRUPPO_RISORSA_SC** specifica il nome del gruppo di risorse.

  Esempio: RG1

- **SC_BACKUP_POLICY_NAME** specifica il nome del criterio di backup.

  Esempio: Backup_policy

- **SC_AV_NAME** specifica i nomi dei volumi dell'applicazione.

Esempio: AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** specifica il mapping dello storage di SVM al volume per la directory dei file di dati. Sarà il nome del volume padre per lun e qtree.

  I dati verranno formattati come <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2>.

  Esempi:

  - Per 2 database nello stesso gruppo di risorse: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
  - Per database singolo con file di dati distribuiti su più volumi: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS
- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** specifica la mappatura dello storage di SVM nel volume per la directory dei file di log. Sarà il nome del volume padre per lun e qtree.

  Esempi:

  - Per una singola istanza di database: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
  - Per più istanze di database: NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO
- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** specifica l'elenco di snapshot contenenti il nome del sistema di storage e il nome del volume.

  Esempi:

  - Per una singola istanza di database: buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr24178002_07_21-2021_02.28.26.3973__
  - Per più istanze di database: NFSB32@@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21_2021_21_02.28.26.3973_07_SCS24831_SCS24831_07_2021_02.28.26.3973_SCS24831_SCS242192_02.28.26.3973_SCS24831_21_S24831_SCS242192_2021_SCS24831_2021_SCS24831_SCS24831_SCS24831_S242*SCS24831_SCS24831_21_S24831_SCS24831_SCS24831_S24831_SCS24831_S241*SCS24831_S24831_SCS24831_SCS24831___SCS24831_SCS24831_S24831_07 02.28.26.3973_
- **SC_PRIMARY_SNAPSHOT_NAMES** specifica i nomi delle snapshot primarie create durante il backup.

  Esempi:

  - Per una singola istanza di database: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
  - Per più istanze di database: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
  - Per le istantanee del gruppo di coerenza che coinvolgono 2 volumi: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350

- **SC_PRIMARY_MOUNT_POINTS** specifica i dettagli del punto di montaggio che fanno parte del backup.

  I dettagli includono la directory in cui vengono montati i volumi e non l'origine immediata del file sottoposto a backup. Per una configurazione ASM, si tratta del nome del gruppo di dischi.

  I dati verranno formattati come <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2>.

  Esempi:

  - Per una singola istanza di database: /Mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
  - Per più istanze di database: NFSB31@/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1
  - PER ASM: +DATA2DG,+LOG2DG
- **SC_PRIMARY_SNAPSHOT_AND_MOUNT_POINTS** specifica i nomi degli snapshot creati durante il backup di ciascuno dei punti di montaggio.

  Esempi:

  - Per singola istanza di database: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log
  - Per più istanze di database: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb31_data,RG2_scspr2417819002_07-21-2021_mnt_02.28.26.3973/nt_flog:/nt_nt2/ntm_1
- **SC_ARCHIVELOGS_LOCATIONS** specifica la posizione della directory dei registri di archiviazione.

  I nomi delle directory saranno l'origine immediata dei file di log dell'archivio. Se i registri di archiviazione sono posizionati in più posizioni, tutte le posizioni verranno acquisite. Ciò include anche gli scenari fra. Se vengono utilizzati i softlink per la directory, verranno inseriti gli stessi campi.

  Esempi:

  - Per database singolo su NFS: /Mnt/nfsdb2_log
  - Per più database su NFS e per i log di archiviazione del database NFSB31 che si trovano in due diverse posizioni: NFSB31@/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
  - PER ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15
- **SC_REDO_LOGS_LOCATIONS** specifica la posizione della directory redo logs.

  I nomi delle directory saranno l'origine immediata dei file di log di ripristino. Se vengono utilizzati i softlink per la directory, verranno inseriti gli stessi campi.

  Esempi:

  - Per database singolo su NFS: /Mnt/nfsdb2_data/newdb1
  - Per database multipli su NFS: NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
  - PER ASM: +LOG2DG/ASMDB2/ONLINELOG

- **SC_CONTROL_FILES_LOCATIONS** specifica la posizione della directory dei file di controllo.

  I nomi delle directory saranno l'origine immediata dei file di controllo. Se vengono utilizzati i softlink per la directory, verranno inseriti gli stessi campi.

  Esempi:

  - Per database singolo su NFS: /Mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
  - Per database multipli su NFS: NFSB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_data/newdb32
  - PER ASM: +LOG2DG/ASMDB2/CONTROLFILE
- **SC_DATA_FILES_LOCATIONS**" specifica la posizione della directory dei file di dati.

  I nomi delle directory saranno l'origine immediata dei file di dati. Se vengono utilizzati i softlink per la directory, verranno inseriti gli stessi campi.

  Esempi:

  - Per database singolo su NFS: /Mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/datafile
  - Per database multipli su NFS: NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile
  - PER ASM: +DATA2DG/ASMDB2/DATAFILE,+DATA2DG/ASMDB2/TEMPFILE
- **SC_SNAPSHOT_LABEL** specifica il nome delle etichette secondarie.

  Esempi: Etichetta oraria, giornaliera, settimanale, mensile o personalizzata.

Delimitatori supportati

- **:** viene utilizzato per separare il nome SVM e il nome del volume

  Esempio: buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07 02.28.26.3973-21-2021

- **@** viene utilizzato per separare i dati dal nome del database e per separare il valore dalla chiave.

  Esempi:

  - NFSB1732@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819G2_07_21_SC248B_07_2021_@_SC24831_SC831_SC202_02.28.26.3973_S24831_S24831_S248B_02.28.26.3973_21_S248B_2021_S248B_2021_S248B_07 02.28.26.3973_S248B_21_S248B_S248B_S248B *S248B_S248B*VLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
  - NFSB31@oracle|NFSB32@oracle
- **|** viene utilizzato per separare i dati tra due database diversi e per separare i dati tra due entità diverse per i parametri SC_BACKUP_ID, SC_BACKUP_RETENTION e SC_BACKUP_NAME.

  Esempi:

- DATA@203|LOG@205
- ORARIO|DATA@DAYS:3|LOG@COUNT:4
- DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- **/** viene utilizzato per separare il nome del volume da Snapshot per i parametri SC_PRIMARY_SNAPSHOT_NAMES e SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG.

  Esempio: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2407-21_2021_02.28.26.3973-

- **,** viene utilizzato per separare un insieme di variabili per lo stesso DB.

  Esempio: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21_2021_02.28.26.3973_0,buck:/vol/scspr2417831_NFS_07_21_S24831_07_S24831_S24831_2021 21 07
  02.28.26.3973_S24831_S24831_S2192_S2192_S221_S4021_S4022_02.28.26.3973_S4021_S4021_@_S4021_S4021_S4021_S4021_S402102.28.26.3973
  *2021_S4021_S4021_S4021_S4021_S4021*S4021_S4021_S4021_S4021_S4021*2021 21_S4021_S4021*S

Opzioni di conservazione del backup

È possibile scegliere il numero di giorni per i quali conservare le copie di backup o specificare il numero di copie di backup che si desidera conservare, fino a un massimo di 255 copie ONTAP. Ad esempio, l'organizzazione potrebbe richiedere di conservare 10 giorni di copie di backup o 130 copie di backup.

Durante la creazione di un criterio, è possibile specificare le opzioni di conservazione per il tipo di backup e il tipo di pianificazione.

Se si imposta la replica di SnapMirror, il criterio di conservazione viene mirrorato sul volume di destinazione.

SnapCenter elimina i backup conservati con etichette di conservazione corrispondenti al tipo di pianificazione. Se il tipo di pianificazione è stato modificato per la risorsa o il gruppo di risorse, i backup con la vecchia etichetta del tipo di pianificazione potrebbero rimanere nel sistema.

Per la conservazione a lungo termine delle copie di backup, è necessario utilizzare il backup di SnapVault.

Pianificazioni di backup

La frequenza di backup (tipo di pianificazione) viene specificata nei criteri; nella configurazione del gruppo di risorse viene specificata una pianificazione di backup. Il fattore più critico per determinare una frequenza o una pianificazione di backup è il tasso di cambiamento per la risorsa e l'importanza dei dati. È possibile eseguire il backup di una risorsa utilizzata in modo pesante ogni ora, mentre è possibile eseguire il backup di una risorsa utilizzata raramente una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo Service Level Agreement (SLA) e il tuo Recover Point Objective (RPO).

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. Un RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA e RPO contribuiscono alla strategia di protezione dei dati.

Anche per una risorsa molto utilizzata, non è necessario eseguire un backup completo più di una o due volte al giorno. Ad esempio, i backup regolari del log delle transazioni potrebbero essere sufficienti per garantire la disponibilità dei backup necessari. Più spesso si esegue il backup dei database, minore è il numero di log delle transazioni che SnapCenter deve utilizzare al momento del ripristino, con conseguente accelerazione delle operazioni di ripristino.

Le pianificazioni dei backup sono in due parti, come segue:

- Frequenza di backup

  La frequenza di backup (con quale frequenza devono essere eseguiti i backup), denominata *tipo di pianificazione* per alcuni plug-in, fa parte di una configurazione di policy. È possibile selezionare ogni ora, ogni giorno, ogni settimana o ogni mese come frequenza di backup per la policy. Se non si seleziona una di queste frequenze, la policy creata è solo on-demand. Puoi accedere alle policy facendo clic su **Impostazioni** > **politiche**.

- Pianificazioni di backup

  Le pianificazioni di backup (esattamente quando devono essere eseguiti i backup) fanno parte di una configurazione di gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione per il backup ogni giovedì alle 10:00. È possibile accedere alle pianificazioni dei gruppi di risorse facendo clic su **risorse** > **gruppi di risorse**.

Convenzioni di denominazione del backup

È possibile utilizzare la convenzione di naming predefinita di Snapshot o una convenzione di naming personalizzata. La convenzione di denominazione predefinita dei backup aggiunge un indicatore data e ora ai nomi Snapshot che consente di identificare quando le copie sono state create.

L'istantanea utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

È necessario assegnare un nome logico ai gruppi di risorse di backup, come nell'esempio seguente:

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

In questo esempio, gli elementi di sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* indica data e ora.

In alternativa, è possibile specificare il formato del nome dell'istantanea mentre si proteggono le risorse o i

gruppi di risorse selezionando **Usa il formato del nome personalizzato per la copia dell'istantanea**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso dell'indicatore data e ora viene aggiunto al nome dell'istantanea.

Requisiti per il backup di un database Oracle

Prima di eseguire il backup di un database Oracle, assicurarsi che i prerequisiti siano stati completati.

- È necessario aver creato un gruppo di risorse con un criterio allegato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con uno storage secondario, il ruolo ONTAP assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- È necessario assegnare l'aggregato utilizzato dall'operazione di backup alla SVM (Storage Virtual Machine) utilizzata dal database.
- È necessario verificare che tutti i volumi di dati e i volumi di log di archiviazione appartenenti al database siano protetti se è attivata la protezione secondaria per tale database.
- È necessario verificare che il database che contiene file nei gruppi di dischi ASM sia nello stato "MOUNT" o "OPEN" per verificarne i backup utilizzando l'utility Oracle DBVERIFY.
- È necessario verificare che la lunghezza del punto di montaggio del volume non superi i 240 caratteri.
- Se il database di cui viene eseguito il backup è di grandi dimensioni (dimensioni in TB), è necessario aumentare il valore di RESTTimeout a 86400000 ms nel file *C: File di programma/SMCore/SMCoreServiceHost.exe.config* dell'host server SnapCenter.

  Durante la modifica dei valori, assicurarsi che non vi siano processi in esecuzione e riavviare il servizio SMCore di SnapCenter dopo aver aumentato il valore.

Scopri i database Oracle disponibili per il backup

Le risorse sono database Oracle sull'host gestiti da SnapCenter. È possibile aggiungere questi database ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database disponibili.

Cosa ti serve

- È necessario completare attività come l'installazione del server SnapCenter, l'aggiunta di host, la creazione di connessioni al sistema di storage e l'aggiunta di credenziali.
- Se i database risiedono su un disco macchina virtuale (VMDK) o su un RDM (raw device mapping), è necessario implementare il plug-in SnapCenter per VMware vSphere e registrare il plug-in con SnapCenter.

  Per ulteriori informazioni, vedere "Implementare il plug-in SnapCenter per VMware vSphere".
- Se i database risiedono su un file system VMDK, è necessario aver effettuato l'accesso a vCenter e aver effettuato la navigazione in **Opzioni VM** > **Avanzate** > **Modifica configurazione** per impostare il valore di *disk.enableUUID* su true per la macchina virtuale.
- È necessario aver esaminato il processo seguito da SnapCenter per individuare diversi tipi e versioni di database Oracle.

Fase 1: Impedire a SnapCenter di rilevare voci non del database

È possibile impedire a SnapCenter di rilevare voci non di database aggiunte nel file oratab.

Fasi

1. Dopo aver installato il plug-in per Oracle, l'utente root deve creare il file **sc_oratab.config** nella directory */var/opt/snapcenter/sco/etc/*.

   Concedere l'autorizzazione di scrittura al proprietario e al gruppo binario Oracle in modo che il file possa essere mantenuto in futuro.

2. L'amministratore del database deve aggiungere le voci non di database nel file **sc_oratab.config**.

   Si consiglia di mantenere lo stesso formato definito per le voci non di database nel file */etc/oratab*, altrimenti l'utente può semplicemente aggiungere la stringa di entità non di database.

   La stringa fa distinzione tra maiuscole e minuscole. Qualsiasi testo con il numero all'inizio viene trattato come commento. Il commento può essere aggiunto dopo il nome non del database.

   ```
   For example:
   ----------------------------------------------
   # Sample entries
   # Each line can have only one non-database name
   # These are non-database name
   oratar  # Added by the admin group -1
   #Added by the script team
   NEWSPT
   DBAGNT:/ora01/app/oracle/product/agent:N
   ----------------------------------------------
   ```

3. Scopri le risorse.

   Le voci non di database aggiunte in **sc_oratab.config** non verranno elencate nella pagina risorse.

Si consiglia sempre di eseguire un backup del file sc_oratab.config prima di aggiornare il plug-in SnapCenter.

Fase 2: Individuare le risorse

Dopo aver installato il plug-in, tutti i database su quell'host vengono automaticamente rilevati e visualizzati nella pagina risorse.

I database devono trovarsi almeno nello stato montato o superiore per consentire il rilevamento dei database. In un ambiente Oracle Real Application Clusters (RAC), l'istanza del database RAC nell'host in cui viene eseguito il rilevamento deve trovarsi almeno nello stato montato o superiore per consentire il rilevamento dell'istanza del database. È possibile aggiungere ai gruppi di risorse solo i database rilevati correttamente.

Se è stato eliminato un database Oracle sull'host, il server SnapCenter non sarà a conoscenza e elenterà il

database cancellato. È necessario aggiornare manualmente le risorse per aggiornare l'elenco delle risorse SnapCenter.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** dall'elenco **View** (Visualizza).

   Fare clic su  , quindi selezionare il nome host e il tipo di database per filtrare le risorse. È quindi possibile fare clic sull'  icona per chiudere il riquadro dei filtri.
3. Fare clic su **Aggiorna risorse**.

   In uno scenario RAC One Node, il database viene rilevato come database RAC sul nodo in cui è attualmente ospitato.

Risultati

I database vengono visualizzati insieme a informazioni quali tipo di database, nome host o cluster, criteri e gruppi di risorse associati e stato.

È necessario aggiornare le risorse se i database vengono rinominati al di fuori di SnapCenter.

- Se il database si trova su un sistema di storage non NetApp, l'interfaccia utente visualizza un messaggio non disponibile per il backup nella colonna Stato generale.

  Non è possibile eseguire operazioni di protezione dei dati sul database su un sistema di storage non NetApp.
- Se il database si trova su un sistema storage NetApp e non è protetto, l'interfaccia utente visualizza un messaggio non protetto nella colonna Stato generale.
- Se il database si trova su un sistema storage NetApp e viene protetto, l'interfaccia utente visualizza un messaggio Available for backup (disponibile per il backup) nella colonna Overall Status (Stato generale).

Se è stata attivata l'autenticazione di un database Oracle, nella vista delle risorse viene visualizzata un'icona a forma di lucchetto rosso. È necessario configurare le credenziali del database per proteggere il database o aggiungerlo al gruppo di risorse per eseguire le operazioni di protezione dei dati.

Creare policy di backup per i database Oracle

Prima di utilizzare SnapCenter per eseguire il backup delle risorse di database Oracle, è necessario creare un criterio di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Un criterio di backup è un insieme di regole che regolano la gestione, la pianificazione e la conservazione dei backup. È inoltre possibile specificare le impostazioni di replica, script e tipo di backup. La creazione di una policy consente di risparmiare tempo quando si desidera riutilizzare la policy su un'altra risorsa o gruppo di risorse.

Prima di iniziare

- È necessario aver definito la strategia di backup.
- Devi essere preparato per la protezione dei dati completando attività come l'installazione di SnapCenter, l'aggiunta di host, il rilevamento di database e la creazione di connessioni al sistema di storage.
- Se si stanno replicando Snapshot in uno storage secondario mirror o vault, l'amministratore di SnapCenter deve aver assegnato le SVM per i volumi di origine e di destinazione.
- Se il plug-in è stato installato come utente non root, è necessario assegnare manualmente le autorizzazioni di esecuzione alle directory prescrittt e postscript.
- Per i prerequisiti e le limitazioni di SnapMirror Business Continuity (SM-BC), fare riferimento a "Limiti a oggetti per la business continuity di SnapMirror".

A proposito di questa attività

- SnapLock
  - Se è selezionata l'opzione "conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere minore o uguale ai giorni di conservazione menzionati.

    La specifica di un periodo di blocco snapshot impedisce l'eliminazione delle istantanee fino alla scadenza del periodo di conservazione. Questo potrebbe portare a mantenere un numero di Snapshot maggiore del conteggio specificato nel criterio.

    Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

    Le impostazioni SnapLock primarie vengono gestite nel criterio di backup SnapCenter e le impostazioni SnapLock secondarie vengono gestite da ONTAP.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare **Oracle Database** dall'elenco a discesa.
4. Fare clic su **nuovo**.
5. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
6. Nella pagina Backup Type (tipo di backup), attenersi alla seguente procedura:
   - Se si desidera **creare un backup online**, selezionare **Backup online**.

     È necessario specificare se si desidera eseguire il backup di tutti i file di dati, di controllo e di log dell'archivio, solo dei file di dati e di controllo o solo dei file di log dell'archivio.
   - Se si desidera **creare un backup offline**, selezionare **Backup offline**, quindi selezionare una delle seguenti opzioni:
     - Se si desidera creare un backup offline quando il database è in stato di montaggio, selezionare **Mount**.
     - Se si desidera creare un backup di shutdown offline cambiando lo stato di shutdown del database, selezionare **Shutdown**.

       Se si dispone di database collegabili (PDB) e si desidera salvare lo stato dei PDB prima di creare il

backup, selezionare **Save state of PDBs** (Salva stato dei PDB). In questo modo è possibile portare i PDB allo stato originale dopo la creazione del backup.

- Specificare la frequenza del programma selezionando **on demand**, **Hourly**, **Daily**, **Weekly** o **Monthly**.

  È possibile specificare la pianificazione (data di inizio e data di fine) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e frequenza di backup, ma consente di assegnare diverse pianificazioni di backup a ciascun criterio.

  Se sono previste le 2:00, la programmazione non verrà attivata durante l'ora legale (DST).

- Se si desidera catalogare il backup utilizzando Oracle Recovery Manager (RMAN), selezionare **Catalog backup with Oracle Recovery Manager (RMAN)**.

  È possibile eseguire la catalogazione posticipata per un backup alla volta utilizzando l'interfaccia grafica o il comando CLI di SnapCenter Catalog-SmBackupWithOracleRMAN.

  Se si desidera catalogare i backup di un database RAC, assicurarsi che non siano in esecuzione altri processi per tale database. Se è in esecuzione un altro processo, l'operazione di catalogazione non riesce invece di essere messa in coda.

- Se si desidera ridurre i registri di archiviazione dopo il backup, selezionare **Prune archive logs after backup** (Sintonizzare i registri di archiviazione dopo il backup).

  L'eliminazione dei registri di archiviazione dalla destinazione del registro di archiviazione non configurata nel database viene ignorata.

  Se si utilizza Oracle Standard Edition, è possibile utilizzare I parametri LOG_ARCHIVE_DEST e LOG_ARCHIVE_DUPLEX_DEST durante l'esecuzione del backup del registro di archiviazione.

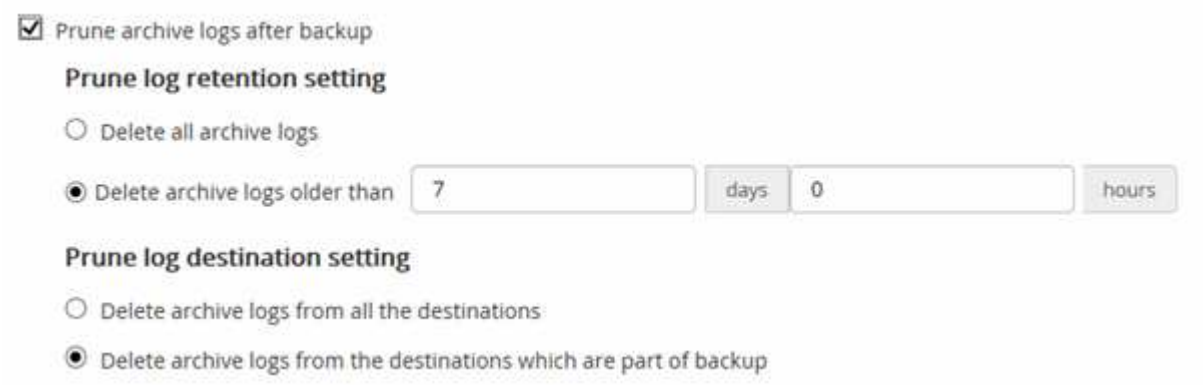
- È possibile eliminare i log di archiviazione solo se sono stati selezionati i file di log di archiviazione come parte del backup.

  Affinché l'operazione di eliminazione abbia esito positivo, è necessario assicurarsi che tutti i nodi in un ambiente RAC possano accedere a tutte le posizioni del registro di archiviazione.

Se si desidera…	**Quindi…**
Eliminare tutti i log di archiviazione	Selezionare **Elimina tutti i log di archiviazione**.
Eliminare i log di archiviazione meno recenti	Selezionare **Delete archive logs older than** (Elimina log di archiviazione precedenti a*), quindi specificare l'età dei log di archiviazione che devono essere cancellati in giorni e ore.

Se si desidera…	Quindi…
Eliminare i log di archiviazione da tutte le destinazioni	Selezionare **Delete archive logs from all the destinations**.
Eliminare i registri di archiviazione dalle destinazioni del registro che fanno parte del backup	Selezionare **Delete archive logs from the destinations welling are of backup**.

+



7. Nella pagina conservazione, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina tipo di backup:

Se si desidera…	Quindi…

Mantenere un certo numero di istantanee	Selezionare **totale copie snapshot da conservare**, quindi specificare il numero di istantanee che si desidera conservare. Se il numero di istantanee supera il numero specificato, le istantanee vengono eliminate con le copie meno recenti eliminate per prime. Il valore massimo di conservazione è 1018 per le risorse su ONTAP 9.4 o versioni successive e 254 per le risorse su ONTAP 9.3 o versioni precedenti. I backup non avranno esito positivo se la conservazione viene impostata su un valore superiore a quello supportato dalla versione di ONTAP sottostante. Se si intende attivare la replica SnapVault, è necessario impostare il numero di conservazione su 2 o superiore. Se si imposta il conteggio della conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è il Snapshot di riferimento per la relazione SnapVault fino a quando una snapshot più recente non viene replicata nella destinazione.
Conservare le istantanee per un determinato numero di giorni	Selezionare **Mantieni copie snapshot per**, quindi specificare il numero di giorni per i quali si desidera conservare le istantanee prima di eliminarle.
Periodo di blocco delle istantanee	Selezionare periodo di blocco della copia Snapshot e selezionare giorni, mesi o anni. Il periodo di conservazione di SnapLock deve essere inferiore a 100 anni.

È possibile conservare i backup dei log di archiviazione solo se sono stati selezionati i file di log di archiviazione come parte del backup.

8. Nella pagina Replication, specificare le impostazioni di replica:

Per questo campo…	Eseguire questa operazione…
Update SnapMirror dopo la creazione di una snapshot locale	Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror). Questa opzione deve essere abilitata per SnapMirror Business Continuity (SM-BC). Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante **Aggiorna** nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP.
Aggiornare SnapVault dopo aver creato un'istantanea locale	Selezionare questa opzione per eseguire la replica del backup disk-to-disk (backup SnapVault). Quando SnapLock è configurato solo sul secondario da ONTAP noto come vault di SnapLock, facendo clic sul pulsante **Aggiorna** nella pagina topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP. Per ulteriori informazioni sul vault di SnapLock, vedere "Assegnare le copie Snapshot a WORM su una destinazione del vault" Vedere "Visualizzare i backup e i cloni dei database Oracle nella pagina topologia".
Etichetta del criterio secondario	Selezionare un'etichetta Snapshot. A seconda dell'etichetta Snapshot selezionata, ONTAP applica la politica di conservazione Snapshot secondaria corrispondente all'etichetta. Se è stato selezionato **Update SnapMirror dopo la creazione di una copia Snapshot locale**, è possibile specificare l'etichetta del criterio secondario. Tuttavia, se è stato selezionato **Aggiorna SnapVault dopo la creazione di una copia Snapshot locale**, è necessario specificare l'etichetta del criterio secondario.

Per questo campo…	Eseguire questa operazione…
Numero tentativi di errore	Immettere il numero massimo di tentativi di replica consentiti prima dell'interruzione dell'operazione.

È necessario configurare il criterio di conservazione SnapMirror in ONTAP per lo storage secondario, in modo da evitare di raggiungere il limite massimo di Snapshot sullo storage secondario.

9. Nella pagina script, immettere il percorso e gli argomenti del prespt o del postscript che si desidera eseguire rispettivamente prima o dopo l'operazione di backup.

   È necessario memorizzare le prescrizioni e i postscript in */var/opt/snapcenter/spl/scripts* o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso */var/opt/snapcenter/spl/scripts* viene compilato. Se sono state create cartelle all'interno di questo percorso per memorizzare gli script, è necessario specificare tali cartelle nel percorso.

   È inoltre possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

   SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono il prescrittivo e postscript. "Scopri di più"

10. Nella pagina verifica, attenersi alla seguente procedura:

    a. Selezionare la pianificazione di backup per la quale si desidera eseguire l'operazione di verifica.
    b. Nella sezione Verification script Commands (comandi script di verifica), immettere il percorso e gli argomenti del prescrittt o del postscript che si desidera eseguire rispettivamente prima o dopo l'operazione di verifica.

       È necessario memorizzare le prescrizioni e i postscript in */var/opt/snapcenter/spl/scripts* o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso */var/opt/snapcenter/spl/scripts* viene compilato. Se sono state create cartelle all'interno di questo percorso per memorizzare gli script, è necessario specificare tali cartelle nel percorso.

    È inoltre possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

11. Esaminare il riepilogo, quindi fare clic su **fine**.

Crea gruppi di risorse e allega policy per database Oracle

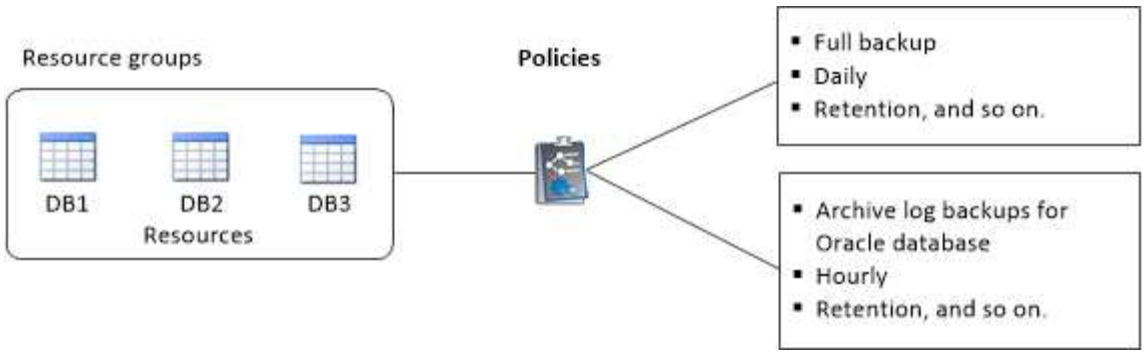
Un gruppo di risorse è un container in cui vengono aggiunte le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire contemporaneamente il backup di tutti i dati associati a una determinata applicazione.

A proposito di questa attività

- Un database con file in gruppi di dischi ASM deve essere in stato "MOUNT" o "OPEN" per verificare i propri backup utilizzando l'utility Oracle DBVERIFY.

  Collegare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire.

  L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i database:



- Per i criteri abilitati per SnapLock, per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco Snapshot, i cloni creati dagli Snapshot a prova di manomissione come parte del ripristino ereditano il tempo di scadenza SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.
- L'aggiunta di nuovi database senza SM-BC a un gruppo di risorse esistente che contiene risorse con SM-BC non è supportata.
- L'aggiunta di nuovi database a un gruppo di risorse esistente in modalità di failover di SM-BC non è supportata. È possibile aggiungere risorse al gruppo di risorse solo in stato normale o di failback.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), fare clic su **New Resource Group** (nuovo gruppo di risorse).
3. Nella pagina Name (Nome), eseguire le seguenti operazioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserire una o più etichette nel campo Tag per facilitare la ricerca del gruppo di risorse in un secondo momento.

      Ad esempio, se si aggiunge HR come tag a più gruppi di risorse, è possibile trovare in seguito tutti i gruppi di risorse associati al tag HR.

   c. Selezionare questa casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea.

      Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

   d. Specificare le destinazioni dei file di log dell'archivio di cui non si desidera eseguire il backup.

      Se necessario, è necessario utilizzare la stessa destinazione impostata in Oracle, compreso il prefisso.

4. Nella pagina Resources (risorse), selezionare un nome host di database Oracle dall'elenco a discesa **host** (host*).

   Le risorse vengono elencate nella sezione risorse disponibili solo se la risorsa viene rilevata correttamente. Le risorse aggiunte di recente vengono visualizzate nell'elenco delle risorse disponibili solo dopo l'aggiornamento dell'elenco delle risorse.

5. Selezionare le risorse dalla sezione risorse disponibili e spostarle nella sezione risorse selezionate.

   È possibile aggiungere database da host Linux e AIX in un singolo gruppo di risorse.

6. Nella pagina Criteri, attenersi alla seguente procedura:

   a. Selezionare uno o più criteri dall'elenco a discesa.

      È inoltre possibile creare un criterio facendo clic su + .

      Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

   b. Fare clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.

      Dove *policy_name* è il nome del criterio selezionato.

      Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

   Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup di SnapCenter.

7. Nella pagina verifica, attenersi alla seguente procedura:

   a. Fare clic su **Load Locators** (carica locatori) per caricare i volumi SnapMirror o SnapVault per eseguire la verifica sullo storage secondario.

   b. Fare clic su + nella colonna Configure Schedules (Configura pianificazioni) per configurare la pianificazione della verifica per tutti i tipi di pianificazione del criterio.

   c. Nella finestra di dialogo Add Verification Schedules policy_name, eseguire le seguenti operazioni:

Se si desidera…	**Eseguire questa operazione…**
Eseguire la verifica dopo il backup	Selezionare **Esegui verifica dopo backup**.
Pianifica una verifica	Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa.

   d. Selezionare **verify on secondary location** (verifica su posizione secondaria) per verificare i backup sul sistema di storage secondario.

   e. Fare clic su **OK**.

      Le pianificazioni di verifica configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in

cui si desidera inviare i messaggi e-mail.

È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report**.

Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

9. Esaminare il riepilogo, quindi fare clic su **fine**.

Backup delle risorse Oracle

Se una risorsa non fa parte di un gruppo di risorse, è possibile eseguarne il backup dalla pagina risorse.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** dall'elenco View (Visualizza).
3. Fare clic su , quindi selezionare il nome host e il tipo di database per filtrare le risorse.

   È quindi possibile fare clic su per chiudere il riquadro del filtro.
4. Selezionare il database di cui si desidera eseguire il backup.

   Viene visualizzata la pagina protezione database.
5. Nella pagina Resources (risorse), è possibile effettuare le seguenti operazioni:
   a. Selezionare la casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea.

      Ad esempio, `customtext_policy_hostname` o `resource_hostname`. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

   b. Specificare le destinazioni dei file di log dell'archivio di cui non si desidera eseguire il backup.
6. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.

      È possibile creare un criterio facendo clic su .

      Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

   b. Fare clic su nella colonna Configura pianificazioni per configurare una pianificazione per il criterio desiderato.
   c. Nella finestra Aggiungi pianificazioni per policy *nome_policy* , configurare la pianificazione, quindi selezionare `OK`.

      policy_name è il nome del criterio selezionato.

Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

7. Nella pagina verifica, attenersi alla seguente procedura:
   a. Fare clic su **Load Locators** (carica locatori) per caricare i volumi SnapMirror o SnapVault e verificare lo storage secondario.
   b. Fare clic su + nella colonna Configure Schedules (Configura pianificazioni) per configurare la pianificazione della verifica per tutti i tipi di pianificazione del criterio. + nella finestra di dialogo Add Verification Schedules *policy_name*, è possibile effettuare le seguenti operazioni:
   c. Selezionare **Esegui verifica dopo backup**.
   d. Selezionare **Esegui verifica pianificata** e selezionare il tipo di pianificazione dall'elenco a discesa.

      In una configurazione di Flex ASM, non è possibile eseguire l'operazione di verifica sui nodi Leaf se la cardinalità è inferiore al numero di nodi nel cluster RAC.

   e. Selezionare **verify on secondary location** (verifica su posizione secondaria) per verificare i backup sullo storage secondario.
   f. Fare clic su **OK**.

      Le pianificazioni di verifica configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

8. Nella pagina Notification (notifica), selezionare gli scenari in cui si desidera inviare i messaggi di posta elettronica dall'elenco a discesa **Email preference** (Preferenze email).

   Specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto del messaggio. Se si desidera allegare il report dell'operazione di backup eseguita sulla risorsa, selezionare **Attach Job Report**.

   Per la notifica e-mail, è necessario specificare i dettagli del server SMTP utilizzando il comando GUI o PowerShell `Set-SmSmtpServer`.

9. Esaminare il riepilogo, quindi fare clic su **fine**.

   Viene visualizzata la pagina della topologia del database.

10. Fare clic su **Esegui backup ora**.
11. Nella pagina Backup, attenersi alla seguente procedura:
    a. Se sono stati applicati più criteri alla risorsa, dall'elenco a discesa Policy (criterio), selezionare il criterio da utilizzare per il backup.

       Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Fare clic su **Backup**.
12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Al termine

- Nell'installazione di AIX, è possibile utilizzare il `lkdev` comando per bloccare e il `rendev` comando per rinominare i dischi su cui risiede il database di cui è stato eseguito il backup.

Il blocco o la ridenominazione dei dispositivi non influisce sull'operazione di ripristino quando si esegue il ripristino utilizzando tale backup.

- Se l'operazione di backup non riesce perché il tempo di esecuzione della query del database ha superato il valore di timeout, è necessario modificare il valore dei parametri ORACLE_SQL_QUERY_TIMEOUT e ORACLE_PLUGIN_SQL_QUERY_TIMEOUT eseguendo il `Set-SmConfigSettings` cmdlet:

  Dopo aver modificato il valore dei parametri, riavviare il servizio SnapCenter Plug-in Loader (SPL) eseguendo il comando seguente `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Se il file non è accessibile e il punto di montaggio non è disponibile durante il processo di verifica, l'operazione potrebbe non riuscire e il file specificato con il codice di errore DBV-00100. Modificare i valori dei parametri VERIFY_DELAY e VERIFY_RETRY_COUNT in sco.properties.

  Dopo aver modificato il valore dei parametri, riavviare il servizio SnapCenter Plug-in Loader (SPL) eseguendo il comando seguente `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Nelle configurazioni MetroCluster, SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.
- Se si esegue il backup dei dati delle applicazioni su VMDK e la dimensione dell'heap Java per il plug-in SnapCenter per VMware vSphere non è sufficiente, il backup potrebbe non riuscire.

  Per aumentare la dimensione dell'heap Java, individuare il file script */opt/netapp/init_scripts/scvservice*. In tale script, il `do_start method` comando avvia il servizio plug-in VMware di SnapCenter. Aggiornare il comando al seguente indirizzo: `Java -jar -Xmx8192M -Xms4096M`.

Trova ulteriori informazioni

- "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover di MetroCluster"
- "Il database Oracle RAC One Node viene ignorato per l'esecuzione delle operazioni SnapCenter"
- "Impossibile modificare lo stato di un database ASM Oracle 12c"
- "Parametri personalizzabili per operazioni di backup, ripristino e clonazione su sistemi AIX" (Richiede l'accesso)

Eseguire il backup dei gruppi di risorse del database Oracle

Un gruppo di risorse è un insieme di risorse su un host o cluster. L'operazione di backup viene eseguita su tutte le risorse definite nel gruppo di risorse.

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina risorse. Se un gruppo di risorse dispone di un criterio allegato e di una pianificazione configurata, i backup vengono creati in base alla pianificazione.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).
3. Immettere il nome del gruppo di risorse nella casella di ricerca o fare clic su , quindi selezionare il tag.

   Fare clic su per chiudere il riquadro del filtro.

4. Nella pagina Resource Group (Gruppo di risorse), selezionare il gruppo di risorse di cui eseguire il backup.

   Se si dispone di un gruppo di risorse federated con due database e uno con dati su storage non NetApp, l'operazione di backup viene interrotta anche se l'altro database si trova sullo storage NetApp.

5. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se al gruppo di risorse sono associati più criteri, selezionare il criterio di backup che si desidera utilizzare dall'elenco a discesa **Policy**.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **Backup**.
6. Monitorare l'avanzamento selezionando **Monitor > processi**.

Al termine

- Nell'installazione di AIX, è possibile utilizzare il `lkdev` comando per bloccare e il `rendev` comando per rinominare i dischi su cui risiede il database di cui è stato eseguito il backup.

  Il blocco o la ridenominazione dei dispositivi non influisce sull'operazione di ripristino quando si esegue il ripristino utilizzando tale backup.

- Se l'operazione di backup non riesce perché il tempo di esecuzione della query del database ha superato il valore di timeout, è necessario modificare il valore dei parametri ORACLE_SQL_QUERY_TIMEOUT e ORACLE_PLUGIN_SQL_QUERY_TIMEOUT eseguendo il `Set-SmConfigSettings` cmdlet:

  Dopo aver modificato il valore dei parametri, riavviare il servizio SnapCenter Plug-in Loader (SPL) eseguendo il comando seguente `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Se il file non è accessibile e il punto di montaggio non è disponibile durante il processo di verifica, l'operazione potrebbe non riuscire e il file specificato con il codice di errore DBV-00100. È necessario modificare i valori dei parametri VERIFY_DELAY_ e VERIFY_RETRY_COUNT in sco.properties.

  Dopo aver modificato il valore dei parametri, riavviare il servizio SnapCenter Plug-in Loader (SPL) eseguendo il comando seguente `/opt/NetApp/snapcenter/spl/bin/spl restart`

Monitorare il backup del database Oracle

Scopri come monitorare l'avanzamento delle operazioni di backup e protezione dei dati.

Monitorare le operazioni di backup del database Oracle

È possibile monitorare l'avanzamento di diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere necessario controllare i progressi per determinare quando sono stati completati o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Status** (Stato), selezionare lo stato del backup.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene venga visualizzato lo stato del processo di backup , quando si fa clic sui dettagli del processo, è possibile che alcune delle attività secondarie dell'operazione di backup siano ancora in corso o contrassegnate da segnali di avviso.

5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Monitorare le operazioni di protezione dei dati nel riquadro attività

Il riquadro Activity (attività) visualizza le cinque operazioni più recenti eseguite. Il riquadro Activity (attività) visualizza anche il momento in cui l'operazione è stata avviata e lo stato dell'operazione.

Il riquadro Activity (attività) visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli commessa**.

Altre operazioni di backup

Eseguire il backup dei database Oracle utilizzando i comandi UNIX

Il workflow di backup include la pianificazione, l'identificazione delle risorse per il backup, la creazione di policy di backup, la creazione di gruppi di risorse e l'aggiunta di policy, la creazione di backup e il monitoraggio delle operazioni.

Cosa ti serve

- È necessario aggiungere le connessioni del sistema di storage e creare la credenziale utilizzando i comandi *Add-SmStorageConnection* e *Add-SmCredential*.
- La sessione di connessione con il server SnapCenter dovrebbe essere stata stabilita utilizzando il comando *Apri-connessione_automatica*.

  È possibile avere una sola sessione di accesso all'account SnapCenter e il token viene memorizzato nella home directory dell'utente.

  La sessione di connessione è valida solo per 24 ore. Tuttavia, è possibile creare un token con l'opzione TokenNeverExpires per creare un token che non scade mai e la sessione sarà sempre valida.

A proposito di questa attività

Eseguire i seguenti comandi per stabilire la connessione con il server SnapCenter, individuare le istanze del database Oracle, aggiungere criteri e gruppi di risorse, eseguire il backup e verificare il backup.

Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al comando software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico: *Open-SmConnection*
2. Eseguire l'operazione di rilevamento delle risorse host: *Get-SmResources*
3. Configurare le credenziali del database Oracle e i nodi preferiti per le operazioni di backup di un database Real Application Cluster (RAC): *Configure-SmOracleDatabase*
4. Creare una policy di backup: *Add-SmPolicy*
5. Recuperare le informazioni relative alla posizione dello storage secondario (SnapVault o SnapMirror): *Get-SmSecondaryDettagli*

   Questo comando recupera i dettagli di mappatura dello storage primario-secondario di una risorsa specificata. È possibile utilizzare i dettagli della mappatura per configurare le impostazioni di verifica secondarie durante la creazione di un gruppo di risorse di backup.

6. Aggiungere un gruppo di risorse a SnapCenter: *Add-SmResourceGroup*
7. Creare un backup: *New-SmBackup*

   È possibile eseguire il polling del processo utilizzando l'opzione WaitForCompletion. Se viene specificata questa opzione, il comando continua a eseguire il polling del server fino al completamento del processo di

backup.

8. Recuperare i log da SnapCenter: *Get-SmLogs*

Annullare le operazioni di backup dei database Oracle

È possibile annullare le operazioni di backup in esecuzione, in coda o che non rispondono.

Per annullare le operazioni di backup, è necessario accedere come amministratore SnapCenter o come proprietario del processo.

A proposito di questa attività

Quando si annulla un'operazione di backup, il server SnapCenter interrompe l'operazione e rimuove tutte le istantanee dall'archivio se il backup creato non è registrato con il server SnapCenter. Se il backup è già registrato con il server SnapCenter, non verrà eseguito il rollback dell'istantanea già creata anche dopo l'attivazione dell'annullamento.

- È possibile annullare solo il log o l'operazione di backup completo in coda o in esecuzione.
- Non è possibile annullare l'operazione dopo l'avvio della verifica.

  Se si annulla l'operazione prima della verifica, l'operazione viene annullata e l'operazione di verifica non viene eseguita.

- Non è possibile annullare l'operazione di backup dopo l'avvio delle operazioni del catalogo.
- È possibile annullare un'operazione di backup dalla pagina Monitor o dal riquadro attività.
- Oltre a utilizzare la GUI di SnapCenter, è possibile utilizzare i comandi CLI per annullare le operazioni.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di backup in coda degli altri membri durante l'utilizzo di tale ruolo.

Passo

Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. 2. Selezionare l'operazione e fare clic su **Annulla lavoro**.
Riquadro delle attività	1. Dopo aver avviato il processo di backup, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. 2. Selezionare l'operazione. 3. Nella pagina Dettagli processo, fare clic su **Annulla processo**.

Risultati

L'operazione viene annullata e la risorsa viene riportata allo stato originale.

Se l'operazione annullata non risponde nello stato di annullamento o esecuzione, eseguire Annulla-SmJob -JobID <int> -Force per interrompere forzatamente l'operazione di backup.

Visualizzare i backup e i cloni dei database Oracle nella pagina topologia

Quando si prepara il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e cloni sullo storage primario e secondario.

A proposito di questa attività

Nella pagina topologia, è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e selezionarli per eseguire le operazioni di protezione dei dati.

È possibile esaminare le seguenti icone nella vista Manage Copies (Gestisci copie) per determinare se i backup e i cloni sono disponibili sullo storage primario o secondario (copie Mirror o copie Vault).

-  visualizza il numero di backup e cloni disponibili sullo storage primario.
-  Visualizza il numero di backup e cloni su cui viene eseguito il mirroring dello storage secondario utilizzando la tecnologia SnapMirror.
-  Visualizza il numero di backup e cloni replicati sullo storage secondario utilizzando la tecnologia SnapVault.

  Il numero di backup visualizzati include i backup eliminati dallo storage secondario. Ad esempio, se sono stati creati 6 backup utilizzando un criterio per conservare solo 4 backup, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror flessibile della versione su un volume di tipo mirror-vault vengono visualizzati nella vista della topologia, ma il numero di backup mirror nella vista della topologia non include il backup flessibile della versione.

Se disponi di una relazione secondaria come SnapMirror Business Continuity (SM-BC), puoi visualizzare le seguenti icone aggiuntive:

-  implica che il sito di replica è attivo.
-  implica che il sito di replica non è attivo.
-  implica che la relazione del mirror secondario o del vault non è stata ristabilita.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina topologia della risorsa selezionata.

4. Consulta la scheda Summary per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione Summary Card (scheda di riepilogo) visualizza il numero totale di backup e cloni e il numero totale di backup dei log.

   Facendo clic sul pulsante **Refresh** viene avviata una query dello storage per visualizzare un conteggio accurato.

   Se viene eseguito il backup abilitato SnapLock, facendo clic sul pulsante **Aggiorna** si aggiornano i tempi di scadenza SnapLock primari e secondari recuperati da ONTAP. Inoltre, una pianificazione settimanale aggiorna il tempo di scadenza SnapLock primario e secondario recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza del SnapLock per il backup sarà il tempo di scadenza del SnapLock più lungo impostato per una Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Per SnapMirror Business Continuity (SM-BC), facendo clic sul pulsante **Refresh** (Aggiorna) viene aggiornato l'inventario di backup di SnapCenter eseguendo una query su ONTAP per i siti principali e di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti relazioni SM-BC.

   - Per le relazioni SM-BC, Async Mirror, Vault o MirrorVault con la nuova destinazione primaria deve essere configurato manualmente dopo il failover.
   - Dopo il failover, è necessario creare un backup affinché SnapCenter sia consapevole del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista Gestisci copie, fare clic su **backup** o **cloni** dallo storage primario o secondario per visualizzare i dettagli di un backup o clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire il ripristino, clonare, montare, smontare, rinominare, operazioni di catalogo, decatalogo ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nello storage secondario.

   - Se è stato selezionato un backup del registro, è possibile eseguire solo ridenominazione, montaggio, disinstallazione, catalogo, annullamento della catalogatura, ed eliminare le operazioni.
   - Se il backup è stato catalogato utilizzando Oracle Recovery Manager (RMAN), non è possibile rinominare i backup catalogati.

7. Se si desidera eliminare un clone, selezionarlo dalla tabella, quindi fare clic su .

Se il valore assegnato a SnapmirrorStatusUpdateWaitTime è inferiore, le copie di backup Mirror e Vault non

vengono elencate nella pagina della topologia anche se i volumi di dati e log sono protetti correttamente. È necessario aumentare il valore assegnato a SnapmirrorStatusUpdateWaitTime utilizzando il cmdlet *set-SmConfigSettings* PowerShell.

Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*.

In alternativa, è possibile fare riferimento anche a "Guida di riferimento al comando software SnapCenter" o "Guida di riferimento al cmdlet del software SnapCenter".

Montare e smontare i backup del database

Se si desidera accedere ai file del backup, è possibile montare uno o più backup di dati e solo log. È possibile montare il backup sullo stesso host in cui è stato creato il backup o su un host remoto con lo stesso tipo di configurazioni Oracle e host. Se i backup sono stati montati manualmente, è necessario disinstallarli manualmente dopo aver completato l'operazione. In qualsiasi istanza, è possibile montare un backup di un database su qualsiasi host. Durante l'esecuzione di un'operazione, è possibile montare solo un backup singolo.

In una configurazione di Flex ASM, non è possibile eseguire l'operazione di montaggio sui nodi Leaf se la cardinalità è inferiore al numero di nodi nel cluster RAC.

Montare un backup del database

Se si desidera accedere ai file del backup, è necessario montare manualmente un backup del database.

Cosa ti serve

- Se si dispone di un'istanza di database ASM (Automatic Storage Management) in un ambiente NFS e si desidera montare i backup ASM, è necessario aggiungere il percorso del disco ASM */var/opt/snapcenter/sco/backup*/*/*/*/_** al percorso esistente definito nel parametro asm_diskstring.
- Se si dispone di un'istanza di database ASM in un ambiente NFS e si desidera montare i backup del log ASM come parte di un'operazione di recovery, è necessario aggiungere il percorso del disco ASM */var/opt/snapcenter/scu/cloni/*/*_* al percorso esistente definito nel parametro asm_diskstring.
- Nel parametro asm_diskstring, configurare *AFD:** se si utilizza ASMFD o configurare *ORCL:** se si utilizza ASMLIB.

Per informazioni su come modificare il parametro asm_diskstring, vedere "Come aggiungere i percorsi dei dischi ad asm_diskstring".

- È necessario configurare le credenziali ASM e la porta ASM se differisce da quella dell'host del database di origine durante il montaggio del backup.
- Se si desidera eseguire il montaggio su un host alternativo, verificare che l'host alternativo soddisfi i seguenti requisiti:
  - Stessi UID e GID dell'host originale
  - Stessa versione di Oracle dell'host originale
  - Stessa distribuzione e versione del sistema operativo dell'host originale

◦ Per NVMe, è necessario installare NVMe util

- Assicurarsi che il LUN non sia mappato all'host AIX utilizzando iGroup costituito da protocolli misti iSCSI e FC. Per ulteriori informazioni, vedere "Operazione non riuscita con errore Impossibile rilevare il dispositivo per il LUN".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.
4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dal sistema di storage primario o secondario (mirrorato o replicato).
5. Selezionare il backup dalla tabella, quindi fare clic su  .
6. Nella pagina Mount backups (Installa backup), selezionare l'host su cui si desidera montare il backup dall'elenco a discesa **Choose the host to mount the backup** (Scegli l'host su cui montare il backup*).

   Viene visualizzato il percorso di montaggio */var/opt/snapcenter/sco/backup_mount/backup_name/database_name*.

   Se si sta montando il backup di un database ASM, viene visualizzato il percorso di montaggio +diskgroupname_SID_backupid.
7. Fare clic su **Mount**.

Al termine

- È possibile eseguire il seguente comando per recuperare le informazioni relative al backup montato:

  ```
  ./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
  ```

- Se è stato montato un database ASM, è possibile eseguire il seguente comando per recuperare le informazioni relative al backup montato:

  ```
  ./sccli Get-Smbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
  ```

- Per recuperare l'ID di backup, eseguire il seguente comando:

  ```
  ./sccli Get-Smbackup-BackupNamebackup_name
  ```

  Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al comando software SnapCenter".

Smontare un backup del database

È possibile smontare manualmente un backup del database montato quando non si desidera più accedere ai file sul backup.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

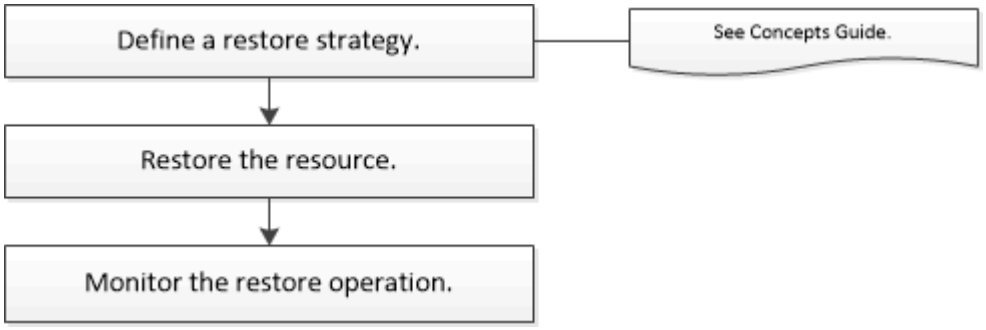
4. Selezionare il backup montato, quindi fare clic su .
5. Fare clic su **OK**.

Ripristinare e ripristinare i database Oracle

Ripristinare il flusso di lavoro

Il flusso di lavoro di ripristino include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di ripristino:



Definire una strategia di ripristino per i database Oracle

È necessario definire una strategia prima di ripristinare e ripristinare il database in modo da poter eseguire correttamente le operazioni di ripristino e ripristino.

Tipi di backup supportati per le operazioni di ripristino e ripristino

SnapCenter supporta il ripristino e il ripristino di diversi tipi di backup dei database Oracle.

- Backup dei dati online
- Backup dei dati di shutdown offline
- Backup dei dati di montaggio offline

Se si sta ripristinando un shutdown offline o un backup dei dati di montaggio offline, SnapCenter lascia il database in stato offline. È necessario ripristinare manualmente il database e i registri.

- Backup completo
- Backup offline dei database di standby di Data Guard
- Backup online solo dati dei database di standby di Active Data Guard

> Non è possibile eseguire il ripristino dei database di standby di Active Data Guard.

- Backup dei dati online, backup completi online, backup di montaggio offline e backup di arresto offline in una configurazione RAC (Real Application Clusters)
- Backup dei dati online, backup completi online, backup di montaggio offline e backup di arresto offline in una configurazione di Automatic Storage Management (ASM)

Tipi di metodi di ripristino supportati per i database Oracle

SnapCenter supporta il ripristino Connect-and-copy o in-place per i database Oracle. Durante un'operazione di ripristino, SnapCenter determina il metodo di ripristino appropriato per il file system da utilizzare per il ripristino senza alcuna perdita di dati.

> SnapCenter non supporta SnapRestore basato su volume.

Ripristino connessione e copia

Se il layout del database differisce dal backup o se sono presenti nuovi file dopo la creazione del backup, viene eseguito il ripristino della connessione e della copia. Nel metodo di ripristino Connect-and-copy, vengono eseguite le seguenti attività:

Fasi

1. Il volume viene clonato dalla Snapshot e lo stack del file system viene creato sull'host utilizzando i LUN o i volumi clonati.
2. I file vengono copiati dai file system clonati ai file system originali.
3. I file system clonati vengono quindi smontati dall'host e i volumi clonati vengono cancellati da ONTAP.

> Per una configurazione di Flex ASM (dove la cardinalità è inferiore al numero di nodi nel cluster RAC) o per i database ASM RAC su VMDK o RDM, è supportato solo il metodo di ripristino Connect-and-copy.

Anche se il ripristino in-place è stato attivato forzatamente, SnapCenter esegue il ripristino della connessione e della copia nei seguenti scenari:

- Eseguire il ripristino dal sistema di storage secondario e se Data ONTAP è precedente alla 8.3
- Ripristino di gruppi di dischi ASM presenti sui nodi di un'installazione Oracle RAC su cui l'istanza di database non è configurata
- Nell'installazione di Oracle RAC, su uno qualsiasi dei nodi peer se l'istanza ASM o l'istanza del cluster non è in esecuzione o se il nodo peer non è attivo
- Ripristino solo dei file di controllo
- Ripristinare un sottoinsieme di tablespace che risiedono su un gruppo di dischi ASM
- Il gruppo di dischi è condiviso tra file di dati, file sp e file di password
- Il servizio caricatore plug-in (SPL) di SnapCenter non è installato o non è in esecuzione sul nodo remoto in

un ambiente RAC

- Vengono aggiunti nuovi nodi al RAC Oracle e il server SnapCenter non è a conoscenza dei nuovi nodi aggiunti

Ripristino in-place

Se il layout del database è simile al backup e non ha subito modifiche di configurazione nello stack di storage e database, viene eseguito il ripristino in-place, in cui il ripristino del file o del LUN viene eseguito su ONTAP. SnapCenter supporta solo SFSR (Single file SnapRestore) come parte del metodo di ripristino in-place.

Data ONTAP 8.3 o versione successiva supporta il ripristino in-place da una posizione secondaria.

Se si desidera eseguire il ripristino in-place sul database, assicurarsi di avere solo i file di dati nel gruppo di dischi ASM. È necessario creare un backup dopo aver apportato modifiche al gruppo di dischi ASM o alla struttura fisica del database. Dopo aver eseguito il ripristino in-place, il gruppo di dischi conterrà lo stesso numero di file di dati al momento del backup.

Il ripristino in-place viene applicato automaticamente quando il gruppo di dischi o il punto di montaggio soddisfano i seguenti criteri:

- Non vengono aggiunti nuovi file dati dopo il backup (controllo dei file esterni)
- Nessuna aggiunta, eliminazione o ricreazione del disco ASM o del LUN dopo il backup (controllo delle modifiche strutturali del gruppo di dischi ASM)
- Nessuna aggiunta, eliminazione o ricreazione di LUN al gruppo di dischi LVM (controllo delle modifiche strutturali del gruppo di dischi LVM)

È inoltre possibile attivare il ripristino in-place forzatamente utilizzando GUI, CLI SnapCenter o cmdlet PowerShell per eseguire l'override del controllo dei file esterni e del controllo delle modifiche strutturali del gruppo di dischi LVM.

Esecuzione del ripristino in-place su ASM RAC

In SnapCenter, il nodo su cui si esegue il ripristino viene definito nodo primario e tutti gli altri nodi del RAC su cui risiede il gruppo di dischi ASM sono denominati nodi peer. SnapCenter modifica lo stato del gruppo di dischi ASM in modo che venga dismontato su tutti i nodi in cui il gruppo di dischi ASM si trova in stato di montaggio prima di eseguire l'operazione di ripristino dello storage. Una volta completato il ripristino dello storage, SnapCenter modifica lo stato del gruppo di dischi ASM come prima dell'operazione di ripristino.

Negli ambienti SAN, SnapCenter rimuove i dispositivi da tutti i nodi peer ed esegue l'operazione LUN unmap prima dell'operazione di ripristino dello storage. Dopo l'operazione di ripristino dello storage, SnapCenter esegue l'operazione di mappatura LUN e costruisce i dispositivi su tutti i nodi peer. In un ambiente SAN, se il layout ASM del RAC si trova su LUN, durante il ripristino di SnapCenter vengono eseguite le operazioni di annullamento mappatura LUN, ripristino LUN e mappatura LUN su tutti i nodi del cluster RAC in cui risiede il gruppo di dischi ASM. Prima di eseguire il ripristino, anche se tutti gli iniziatori dei nodi RAC non sono stati utilizzati per le LUN, dopo il ripristino SnapCenter crea un nuovo iGroup con tutti gli iniziatori di tutti i nodi RAC.

- In caso di errore durante l'attività di pre-ripristino sui nodi peer, SnapCenter ripristina automaticamente lo stato del gruppo di dischi ASM così com'era prima di eseguire il ripristino sui nodi peer su cui l'operazione di pre-ripristino ha avuto esito positivo. Il rollback non è supportato per il nodo primario e il nodo peer in cui l'operazione non è riuscita. Prima di tentare un altro ripristino, è necessario risolvere manualmente il problema sul nodo peer e riportare il gruppo di dischi ASM sul nodo primario allo stato di montaggio.

- Se si verifica un errore durante l'attività di ripristino, l'operazione di ripristino non riesce e non viene eseguito il rollback. Prima di tentare un altro ripristino, è necessario risolvere manualmente il problema di ripristino dello storage e riportare il gruppo di dischi ASM sul nodo primario allo stato di montaggio.
- In caso di errore durante l'attività di postripristino su uno dei nodi peer, SnapCenter continua con l'operazione di ripristino sugli altri nodi peer. È necessario risolvere manualmente il problema di post-ripristino sul nodo peer.

Tipi di operazioni di ripristino supportate per i database Oracle

SnapCenter consente di eseguire diversi tipi di operazioni di ripristino per i database Oracle.

Prima di ripristinare il database, i backup vengono validati per identificare se mancano file rispetto ai file di database effettivi.

Ripristino completo

- Ripristina solo i file di dati
- Ripristina solo i file di controllo
- Ripristina i file di dati e di controllo
- Ripristina i file di dati, i file di controllo e i file di log di ripristino nei database di standby Data Guard e Active Data Guard

Ripristino parziale

- Ripristina solo gli spazi delle tabelle selezionati
- Ripristina solo i database collegabili (PDB) selezionati
- Ripristina solo gli spazi delle tabelle selezionate di una PDB

Tipi di operazioni di recovery supportati per i database Oracle

SnapCenter consente di eseguire diversi tipi di operazioni di recovery per i database Oracle.

- Il database fino all'ultima transazione (tutti i log)
- Il database fino a un numero SCN (System Change Number) specifico
- Il database fino a una data e un'ora specifiche

  È necessario specificare la data e l'ora del ripristino in base al fuso orario dell'host del database.

  SnapCenter offre anche l'opzione No recovery per i database Oracle.

> Il plug-in per il database Oracle non supporta il ripristino se è stato ripristinato utilizzando un backup creato con il ruolo di standby del database. È sempre necessario eseguire un ripristino manuale per i database fisici di standby.

Limitazioni relative al ripristino e al ripristino dei database Oracle

Prima di eseguire le operazioni di ripristino, è necessario essere consapevoli delle limitazioni.

Se si utilizza una qualsiasi versione di Oracle dalla 11.2.0.4 alla 12.1.0.1, l'operazione di ripristino sarà in stato di sospensione quando si esegue il comando *renamedg*. È possibile applicare la patch Oracle 19544733 per

risolvere questo problema.

Le seguenti operazioni di ripristino non sono supportate:

- Ripristino e ripristino degli spazi delle tabelle del database dei container root (CDB)
- Ripristino di tablespace temporanei e tablespace temporanei associati ai PDB
- Ripristino e ripristino di tablespace da più PDB contemporaneamente
- Ripristino dei backup dei log
- Ripristino dei backup in una posizione diversa
- Ripristino dei file di log di ripristino in qualsiasi configurazione diversa dai database di standby Data Guard o Active Data Guard
- Ripristino del file SPFILE e Password
- Quando si esegue un'operazione di ripristino su un database ricreato utilizzando il nome del database preesistente sullo stesso host, gestito da SnapCenter e con backup validi, l'operazione di ripristino sovrascrive i file di database appena creati anche se i DBID sono diversi.

  È possibile evitare questo problema eseguendo una delle seguenti operazioni:

  - Individuare le risorse SnapCenter dopo la creazione del database
  - Creare un backup del database ricreato

Limitazioni relative al ripristino point-in-time degli spazi delle tabelle

- Il PITR (Point-in-Time Recovery) di SISTEMA, SYSAUX e TABLESPACE DI ANNULLAMENTO non è supportato
- Non è possibile eseguire PITR di tablespace insieme ad altri tipi di ripristino
- Se un tablespace viene rinominato e si desidera ripristinarlo fino a un punto prima che sia stato rinominato, specificare il nome precedente del tablespace
- Se i vincoli per le tabelle in uno spazio tabella sono contenuti in un altro spazio tabella, è necessario ripristinare entrambi gli spazi tabella
- Se una tabella e i relativi indici sono memorizzati in spazi tabella diversi, gli indici devono essere ignorati prima di eseguire PITR
- Non è possibile utilizzare PITR per ripristinare lo spazio tabella predefinito corrente
- Non è possibile utilizzare PITR per ripristinare gli spazi delle tabelle contenenti uno dei seguenti oggetti:
  - Oggetti con oggetti sottostanti (ad esempio viste materializzate) o oggetti contenuti (ad esempio tabelle partizionate), a meno che tutti gli oggetti sottostanti o contenuti non si trovino nel set di ripristino

    Inoltre, se le partizioni di una tabella partizionata sono memorizzate in spazi tabella diversi, è necessario rilasciare la tabella prima di eseguire PITR o spostare tutte le partizioni nello stesso spazio tabella prima di eseguire PITR.

  - Disfare o eseguire il rollback dei segmenti
  - Code avanzate compatibili con Oracle 8 con più destinatari
  - Oggetti di proprietà dell'utente SYS

    Esempi di questi tipi di oggetti sono PL/SQL, classi Java, programmi di richiamo, viste, sinonimi, utenti, privilegi, dimensioni, directory e sequenze.

Origini e destinazioni per il ripristino dei database Oracle

È possibile ripristinare un database Oracle da una copia di backup sullo storage primario o secondario. È possibile ripristinare i database solo nella stessa posizione della stessa istanza di database. Tuttavia, nella configurazione di Real Application Cluster (RAC), è possibile ripristinare i database in altri nodi.

Fonti per le operazioni di ripristino

È possibile ripristinare i database da un backup sullo storage primario o secondario. Se si desidera eseguire il ripristino da un backup sullo storage secondario in una configurazione con mirroring multiplo, è possibile selezionare il mirror dello storage secondario come origine.

Destinazioni per le operazioni di ripristino

È possibile ripristinare i database solo nella stessa posizione della stessa istanza di database.

In una configurazione RAC, è possibile ripristinare i database RAC da qualsiasi nodo del cluster.

Variabili di ambiente predefinite per il ripristino di specifiche prescrittt e postscript

SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prespt e postscript durante il ripristino di un database.

Variabili di ambiente predefinite supportate per il ripristino di un database

- **SC_JOB_ID** specifica l'ID lavoro dell'operazione.

  Esempio: 257

- **SC_ORACLE_SID** specifica l'identificatore di sistema del database.

  Se l'operazione coinvolge più database, questo conterrà nomi di database separati da pipe.

  Esempio: NFSB31

- **SC_HOST** specifica il nome host del database.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** specifica il proprietario del sistema operativo del database.

  Esempio: oracle

- **SC_OS_GROUP** specifica il gruppo del sistema operativo del database.

  Esempio: Oinstall

- **SC_BACKUP_NAME** specifica il nome del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempi:

    - Se il database non è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
    - Se il database è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1,RG2_scspr2417819002_07-21-2021_12.16.48.9267_1,RG2_scspr2417819002_07-22-2021_12.16.48.9267_1
- **SC_BACKUP_ID** specifica l'ID del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempi:

    - Se il database non è in esecuzione in modalità ARCHIVELOG: DATA@203|LOG@205
    - Se il database è in esecuzione in modalità ARCHIVELOG: DATA@203|LOG@205,206,207
- **Nome_GRUPPO_RISORSA_SC** specifica il nome del gruppo di risorse.

  Esempio: RG1
- **SC_ORACLE_HOME** specifica il percorso della home directory Oracle.

  Esempio: /Ora01/app/oracle/product/18.1.0/db_1
- **SC_RECOVERY_TYPE** specifica i file ripristinati e l'ambito del ripristino.

  Esempio: RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false.

Per informazioni sui delimitatori, vedere "Delimitatori supportati".

Requisiti per il ripristino di un database Oracle

Prima di ripristinare un database Oracle, assicurarsi che i prerequisiti siano stati completati.

- La strategia di ripristino e ripristino dovrebbe essere stata definita.
- L'amministratore di SnapCenter deve aver assegnato le Storage Virtual Machine (SVM) sia per i volumi di origine che per i volumi di destinazione, se si replicano Snapshot in un mirror o un vault.
- Se i log di archiviazione vengono annullati come parte del backup, è necessario montare manualmente i backup del log di archiviazione richiesti.
- Se si desidera ripristinare i database Oracle che risiedono su un Virtual Machine Disk (VMDK), assicurarsi che la macchina guest disponga del numero richiesto di slot liberi per allocare i VMDK clonati.
- È necessario garantire che tutti i volumi di dati e i volumi di log di archiviazione appartenenti al database siano protetti se è attivata la protezione secondaria per tale database.
- Assicurarsi che il database RAC One Node sia in stato "nomount" per eseguire il ripristino completo del file di controllo o del database.
- Se si dispone di un'istanza di database ASM in ambiente NFS, aggiungere il percorso del disco ASM */var/opt/snapcenter/scu/cloni/*/** al percorso esistente definito nel parametro asm_diskstring per montare correttamente i backup del registro ASM come parte dell'operazione di recovery.

- Nel parametro asm_diskstring, configurare *AFD:** se si utilizza ASMFD o configurare *ORCL:** se si utilizza ASMLIB.

  Per informazioni su come modificare il parametro asm_diskstring, vedere "Come aggiungere i percorsi dei dischi ad asm_diskstring"

- È necessario configurare il listener statico nel file **listener.ora** disponibile all'indirizzo _ Oracle_HOME/network/admin_ per i database non ASM e _ Grid_HOME/network/admin_ per i database ASM se l'autenticazione del sistema operativo è stata disattivata e l'autenticazione del database Oracle è stata abilitata per un database Oracle e si desidera ripristinare i file di dati e di controllo di tale database.
- Se le dimensioni del database sono in terabyte (TB), aumentare il valore del parametro SCORestoreTimeout eseguendo il comando Set- SmConfigSettings.
- Assicurarsi che tutte le licenze richieste per vCenter siano installate e aggiornate.

  Se le licenze non sono installate o aggiornate, viene visualizzato un messaggio di avviso. Se si ignora l'avviso e si procede, il ripristino da RDM non riesce.

- Assicurarsi che il LUN non sia mappato all'host AIX utilizzando iGroup costituito da protocolli misti iSCSI e FC. Per ulteriori informazioni, vedere "Operazione non riuscita con errore Impossibile rilevare il dispositivo per il LUN".

Ripristinare e ripristinare il database Oracle

In caso di perdita di dati, è possibile utilizzare SnapCenter per ripristinare i dati da uno o più backup nel file system attivo e quindi ripristinare il database.

Prima di iniziare

Se il plug-in è stato installato come utente non root, è necessario assegnare manualmente le autorizzazioni di esecuzione alle directory prescrittt e postscript.

A proposito di questa attività

- Il ripristino viene eseguito utilizzando i registri di archiviazione disponibili nella posizione del registro di archiviazione configurata. Se il database viene eseguito in modalità ARCHIVELOG, il database Oracle salva i gruppi pieni di file di log di ripristino in una o più destinazioni offline, denominate collettivamente log di ripristino archiviato. SnapCenter identifica e monta il numero ottimale di backup dei log in base all'opzione SCN specificata, data e ora selezionate o tutti i log. Se i log di archivio richiesti per il ripristino non sono disponibili nella posizione configurata, è necessario montare l'istantanea contenente i log e specificare il percorso come log di archivio esterni.

  Se si esegue la migrazione del database ASM da ASMLIB ad ASMFD, i backup creati con ASMLIB non possono essere utilizzati per ripristinare il database. È necessario creare backup nella configurazione ASMFD e utilizzarli per il ripristino. Analogamente, se il database ASM viene migrato da ASMFD ad ASMLIB, è necessario creare i backup nella configurazione ASMLIB per il ripristino.

  Quando si ripristina un database, viene creato un file di blocco operativo (.SM_lock_dbsid) sull'host del database Oracle nella directory */var/opt/snapcenter/sco/lock* per evitare l'esecuzione di più operazioni sul database. Una volta ripristinato il database, il file di blocco operativo viene automaticamente rimosso.

  Il ripristino del file SPFILE e Password non è supportato.

- Per i criteri abilitati per SnapLock, per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco Snapshot, i cloni creati dagli Snapshot a prova di manomissione come parte del ripristino ereditano il tempo di scadenza SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.
4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dal sistema di storage primario o secondario (mirrorato o replicato).
5. Selezionare il backup dalla tabella, quindi fare clic su * *  .
6. Nella pagina Restore Scope (ambito ripristino), eseguire le seguenti operazioni:

   a. Se è stato selezionato un backup di un database in un ambiente RAC (Real Application Clusters), selezionare il nodo RAC.

   b. Quando si selezionano dati mirrorati o del vault:

      - se non è presente alcun backup del log nel mirror o nel vault, non viene selezionato nulla e i locatori sono vuoti.
      - se i backup del log esistono nel mirror o nel vault, viene selezionato l'ultimo backup del log e viene visualizzato il localizzatore corrispondente.

      Se il backup del log selezionato esiste sia nella posizione del mirror che nel vault, vengono visualizzati entrambi i locator.

   c. Eseguire le seguenti operazioni:

Se si desidera ripristinare…	Eseguire questa operazione…
Tutti i file di dati del database	Selezionare **tutti i file dati**. Vengono ripristinati solo i file di dati del database. I file di controllo, i log di archiviazione o i file di log di ripristino non vengono ripristinati.
Tablespace	Selezionare **tablespace**. È possibile specificare gli spazi delle tabelle che si desidera ripristinare.

Se si desidera ripristinare…	Eseguire questa operazione…
File di controllo	Selezionare **file di controllo**. Durante il ripristino dei file di controllo, assicurarsi che la struttura della directory esista o debba essere creata con le proprietà corrette di utenti e gruppi, se presenti, per consentire la copia dei file nella posizione di destinazione mediante il processo di ripristino. Se la directory non esiste, il processo di ripristino avrà esito negativo.
Ripristinare i file di log	Selezionare **Ripeti file di log**. Questa opzione è disponibile solo per i database di standby Data Guard o Active Data Guard. Il backup dei file di log di ripristino non viene eseguito per i database non Data Guard. Per i database non Data Guard, il ripristino viene eseguito utilizzando i registri di archiviazione.
Database collegabili (PDB)	Selezionare **Database inseribili**, quindi specificare i PDB che si desidera ripristinare.
Tablespace dei database collegabili (PDB)	Selezionare **tablespace del database Pluggable (PDB)**, quindi specificare il PDB e gli spazi delle tabelle del PDB che si desidera ripristinare. Questa opzione è disponibile solo se è stato selezionato un PDB per il ripristino.

d. Selezionare **Cambia stato del database se necessario per il ripristino e il ripristino** per impostare lo stato del database sullo stato richiesto per eseguire le operazioni di ripristino e ripristino.

   I vari stati di un database, da quelli superiori a quelli inferiori, sono aperti, montati, avviati e arrestati. Selezionare questa casella di controllo se il database si trova in uno stato superiore ma lo stato deve essere modificato in uno stato inferiore per eseguire un'operazione di ripristino. Se il database si trova in uno stato inferiore ma lo stato deve essere modificato in uno stato superiore per eseguire l'operazione di ripristino, lo stato del database viene modificato automaticamente anche se non si seleziona la casella di controllo.

Se un database si trova in stato aperto e per il ripristino il database deve essere in stato montato, lo stato del database viene modificato solo se si seleziona questa casella di controllo.

a. Selezionare **Imponi ripristino** se si desidera eseguire il ripristino in-place negli scenari in cui vengono aggiunti nuovi file di dati dopo il backup o quando i LUN vengono aggiunti, cancellati o ricreati in un gruppo di dischi LVM.

7. Nella pagina Recovery Scope (ambito ripristino), eseguire le seguenti operazioni:

Se…	Eseguire questa operazione…
Ripristinare l'ultima transazione	Selezionare **tutti i registri**.
Ripristinare un numero SCN (System Change Number) specifico	Selezionare **fino a quando SCN (System Change Number)**.
Desidera ripristinare dati e tempi specifici	Selezionare **Data e ora**. Specificare la data e l'ora del fuso orario dell'host del database.
Non si desidera eseguire il ripristino	Selezionare **Nessun ripristino**.
Specificare le posizioni dei registri di archiviazione esterni	Se il database viene eseguito in modalità ARCHIVELOG, SnapCenter identifica e monta il numero ottimale di backup dei log in base all'opzione SCN specificata, data e ora selezionate o tutti i log. Se si desidera comunque specificare la posizione dei file di log dell'archivio esterno, selezionare **specifica le posizioni esterne del log dell'archivio**. Se i log di archiviazione vengono annullati come parte del backup e sono stati montati manualmente i backup del log di archiviazione richiesti, è necessario specificare il percorso di backup montato come posizione del log di archiviazione esterno per il ripristino. Verificare il percorso e il contenuto del percorso di montaggio prima di inserirlo come percorso di log esterno. • "Data Protection di Oracle con ONTAP" • "Operazione non riuscita con errore ora-00308"

Non è possibile eseguire il ripristino con il ripristino da backup secondari se i volumi di log dell'archivio non sono protetti ma i volumi di dati sono protetti. È possibile eseguire il ripristino solo selezionando **No recovery**.

Se si sta ripristinando un database RAC con l'opzione di database aperto selezionata, solo l'istanza RAC in cui è stata avviata l'operazione di ripristino viene riportata allo stato aperto.

Il ripristino non è supportato per i database di standby Data Guard e Active Data Guard.

8. Nella pagina PreOps, immettere il percorso e gli argomenti della prescrizione che si desidera eseguire prima dell'operazione di ripristino.

   È necessario memorizzare le prescrizioni nel percorso */var/opt/snapcenter/spl/scripts* o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso */var/opt/snapcenter/spl/scripts* viene compilato. Se sono state create cartelle all'interno di questo percorso per memorizzare gli script, è necessario specificare tali cartelle nel percorso.

   È inoltre possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

   SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono il prescrittivo e postscript. "Scopri di più"

9. Nella pagina PostOps, attenersi alla seguente procedura:

   a. Immettere il percorso e gli argomenti del postscript che si desidera eseguire dopo l'operazione di ripristino.

      È necessario memorizzare i postscript in */var/opt/snapcenter/spl/scripts* o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso */var/opt/snapcenter/spl/scripts* viene compilato. Se sono state create cartelle all'interno di questo percorso per memorizzare gli script, è necessario specificare tali cartelle nel percorso.

      Se l'operazione di ripristino non riesce, i postscript non vengono eseguiti e le attività di pulizia vengono attivate direttamente.

   b. Selezionare questa casella di controllo se si desidera aprire il database dopo il ripristino.

      Dopo il ripristino di un database container (CDB) con o senza file di controllo, o dopo il ripristino solo dei file di controllo CDB, se si specifica di aprire il database dopo il ripristino, viene aperto solo il CDB e non i database collegabili (PDB) in quel CDB.

      In un'installazione RAC, dopo il ripristino viene aperta solo l'istanza RAC utilizzata per il ripristino.

      Dopo aver ripristinato uno spazio tabella utente con file di controllo, uno spazio tabella di sistema con o senza file di controllo o un PDB con o senza file di controllo, solo lo stato del PDB correlato all'operazione di ripristino viene modificato nello stato originale. Lo stato degli altri PDB non utilizzati per il ripristino non viene modificato nello stato originale perché lo stato di tali PDB non è stato salvato. È necessario modificare manualmente lo stato dei PDB non utilizzati per il ripristino.

10. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare le notifiche email.

    È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di ripristino eseguita, selezionare **Allega report**.

    Per la notifica via email, è necessario specificare i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

11. Esaminare il riepilogo, quindi fare clic su **fine**.

12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Per ulteriori informazioni

- "Il database Oracle RAC One Node viene ignorato per l'esecuzione delle operazioni SnapCenter"
- "Impossibile eseguire il ripristino da una posizione SnapMirror o SnapVault secondaria"
- "Impossibile eseguire il ripristino da un backup di un'incarnazione orfana"
- "Parametri personalizzabili per operazioni di backup, ripristino e clonazione su sistemi AIX"

Ripristinare e ripristinare gli spazi delle tabelle utilizzando il ripristino point-in-time

È possibile ripristinare un sottoinsieme di tablespace corrotti o interrotti senza influire sugli altri tablespace del database. SnapCenter utilizza RMAN per eseguire il recovery point-in-time (PITR) dei tablespace.

Prima di iniziare

- I backup necessari per eseguire il PITR delle tablespace devono essere catalogati e montati.
- Se il plug-in è stato installato come utente non root, è necessario assegnare manualmente le autorizzazioni di esecuzione alle directory prescrittt e postscript.

A proposito di questa attività

Durante l'operazione PITR, RMAN crea un'istanza ausiliaria nella destinazione ausiliaria specificata. La destinazione ausiliaria potrebbe essere un punto di montaggio o un gruppo di dischi ASM. Se lo spazio disponibile nella posizione di montaggio è sufficiente, è possibile riutilizzare una delle posizioni di montaggio invece di un punto di montaggio dedicato.

Specificare la data e l'ora o SCN e lo spazio delle tabelle viene ripristinato nel database di origine.

È possibile selezionare e ripristinare più tablespace che risiedono in ambienti ASM, NFS e SAN. Ad esempio, se gli spazi delle tabelle TS2 e TS3 risiedono su NFS e TS4 risiedono SU SAN, è possibile eseguire una singola operazione PITR per ripristinare tutti gli spazi delle tabelle.

In una configurazione RAC, è possibile eseguire PITR di tablespace da qualsiasi nodo del RAC.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database di tipo istanza singola (multi-tenant) dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dal sistema di storage primario o secondario (mirrorato o replicato).

   Se il backup non è catalogato, selezionare il backup e fare clic su **Catalog** (Catalogo).

5. Selezionare il backup catalogato, quindi fare clic su * *  .
6. Nella pagina Restore Scope (ambito ripristino), eseguire le seguenti operazioni:
   a. Se è stato selezionato un backup di un database in un ambiente RAC (Real Application Clusters), selezionare il nodo RAC.
   b. Selezionare **tablespace**, quindi specificare gli spazi delle tabelle da ripristinare.

      Non è possibile eseguire PITR su SYSAUX, SYSTEM e UNDO tablespace.

   c. Selezionare **Cambia stato del database se necessario per il ripristino e il ripristino** per impostare lo stato del database sullo stato richiesto per eseguire le operazioni di ripristino e ripristino.
7. Nella pagina Recovery Scope (ambito ripristino), eseguire una delle seguenti operazioni:
   - Se si desidera ripristinare un numero SCN (System Change Number) specifico, selezionare **fino a SCN** e specificare il numero SCN e la destinazione ausiliaria.
   - Se si desidera ripristinare una data e un'ora specifiche, selezionare **Data e ora** e specificare la data e l'ora e la destinazione ausiliaria.

     SnapCenter identifica e quindi monta e cataloga il numero ottimale di backup dei dati e dei log necessari per eseguire il PITR in base alla data e all'ora specificate.
8. Nella pagina PreOps, immettere il percorso e gli argomenti della prescrizione che si desidera eseguire prima dell'operazione di ripristino.

   Le prescrizioni devono essere memorizzate nel percorso /var/opt/snapcenter/spl/scripts o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso /var/opt/snapcenter/spl/scripts viene compilato. Se sono state create cartelle all'interno di questo percorso per memorizzare gli script, è necessario specificare tali cartelle nel percorso.

   È inoltre possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

   SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono il prescrittivo e postscript. "Scopri di più"
9. Nella pagina PostOps, attenersi alla seguente procedura:
   a. Immettere il percorso e gli argomenti del postscript che si desidera eseguire dopo l'operazione di ripristino.

      Se l'operazione di ripristino non riesce, i postscript non vengono eseguiti e le attività di pulizia vengono attivate direttamente.

   b. Selezionare questa casella di controllo se si desidera aprire il database dopo il ripristino.
10. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare le notifiche email.
11. Esaminare il riepilogo, quindi fare clic su **fine**.
12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Ripristino e ripristino di database collegabili mediante ripristino point-in-time

È possibile ripristinare e ripristinare un database collegabile (PDB) che è stato

danneggiato o interrotto senza influire sulle altre PDB nel database container (CDB). SnapCenter utilizza RMAN per eseguire il recovery point-in-time (PITR) del PDB.

Prima di iniziare

- I backup necessari per eseguire il PITR di una PDB devono essere catalogati e montati.

  In una configurazione RAC, chiudere manualmente la PDB (cambiando lo stato in MONTATO) su tutti i nodi della configurazione RAC.

- Se il plug-in è stato installato come utente non root, è necessario assegnare manualmente le autorizzazioni di esecuzione alle directory prescrittt e postscript.

A proposito di questa attività

Durante l'operazione PITR, RMAN crea un'istanza ausiliaria nella destinazione ausiliaria specificata. La destinazione ausiliaria potrebbe essere un punto di montaggio o un gruppo di dischi ASM. Se lo spazio disponibile nella posizione di montaggio è sufficiente, è possibile riutilizzare una delle posizioni di montaggio invece di un punto di montaggio dedicato.

Specificare la data e l'ora o l'SCN per eseguire il PITR del PDB. RMAN è in grado di ripristinare PDB IN LETTURA/SCRITTURA, IN SOLA LETTURA o eliminati, inclusi i file di dati.

È possibile ripristinare e ripristinare solo:

- Un PDB alla volta
- Un tablespace in una PDB
- Tablespace multipli dello stesso PDB

In una configurazione RAC, è possibile eseguire PITR di tablespace da qualsiasi nodo del RAC.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database di tipo istanza singola (multi-tenant) dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dal sistema di storage primario o secondario (mirrorato o replicato).

   Se il backup non è catalogato, selezionare il backup e fare clic su **Catalog** (Catalogo).

5. Selezionare il backup catalogato, quindi fare clic su * *  .
6. Nella pagina Restore Scope (ambito ripristino), eseguire le seguenti operazioni:
   a. Se è stato selezionato un backup di un database in un ambiente RAC (Real Application Clusters), selezionare il nodo RAC.

b. A seconda che si desideri ripristinare la PDB o gli spazi delle tabelle in una PDB, eseguire una delle seguenti operazioni:

Se si desidera…	Fasi…
Ripristinare un PDB	i. Selezionare **Pluggable Databases (PDB)**. ii. Specificare il PDB che si desidera ripristinare. Non è possibile eseguire PITR sul database DI INIZIALIZZAZIONE PDB.
Ripristinare gli spazi delle tabelle in una PDB	i. Selezionare **tablespace Pluggable database (PDB)**. ii. Specificare l'PDB. iii. Specificare un singolo tablespace o più tablespace da ripristinare. Non è possibile eseguire PITR su SYSAUX, SYSTEM e UNDO tablespace.

c. Selezionare **Cambia stato del database se necessario per il ripristino e il ripristino** per impostare lo stato del database sullo stato richiesto per eseguire le operazioni di ripristino e ripristino.

7. Nella pagina Recovery Scope (ambito ripristino), eseguire una delle seguenti operazioni:
   - Se si desidera ripristinare un numero SCN (System Change Number) specifico, selezionare **fino a SCN** e specificare il numero SCN e la destinazione ausiliaria.
   - Se si desidera ripristinare una data e un'ora specifiche, selezionare **Data e ora** e specificare la data e l'ora e la destinazione ausiliaria.

     SnapCenter identifica e quindi monta e cataloga il numero ottimale di backup dei dati e dei log necessari per eseguire il PITR in base alla data e all'ora specificate.

8. Nella pagina PreOps, immettere il percorso e gli argomenti della prescrizione che si desidera eseguire prima dell'operazione di ripristino.

   Le prescrizioni devono essere memorizzate nel percorso /var/opt/snapcenter/spl/scripts o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso /var/opt/snapcenter/spl/scripts viene compilato. Se sono state create cartelle all'interno di questo percorso per memorizzare gli script, è necessario specificare tali cartelle nel percorso.

   È inoltre possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

   SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono il prescrittivo e postscript. "Scopri di più"

9. Nella pagina PostOps, attenersi alla seguente procedura:
   a. Immettere il percorso e gli argomenti del postscript che si desidera eseguire dopo l'operazione di

ripristino.

> Se l'operazione di ripristino non riesce, i postscript non vengono eseguiti e le attività di pulizia vengono attivate direttamente.

b. Selezionare questa casella di controllo se si desidera aprire il database dopo il ripristino.

   In una configurazione RAC, la PDB viene aperta solo sul nodo in cui è stato ripristinato il database. Aprire manualmente la PDB recuperata su tutti gli altri nodi della configurazione RAC.

10. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare le notifiche email.
11. Esaminare il riepilogo, quindi fare clic su **fine**.
12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Ripristinare e ripristinare i database Oracle utilizzando i comandi UNIX

Il flusso di lavoro di ripristino e ripristino include la pianificazione, l'esecuzione delle operazioni di ripristino e ripristino e il monitoraggio delle operazioni.

A proposito di questa attività

- Eseguire i seguenti comandi per stabilire la connessione con il server SnapCenter, elencare i backup, recuperare le informazioni e ripristinare il backup.

  Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al comando software SnapCenter".

- Per l'operazione di ripristino SnapMirror Business Continuity (SM-BC), devi selezionare il backup dalla posizione principale.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico: *Open-SmConnection*
2. Recuperare le informazioni sui backup che si desidera ripristinare: *Get-SmBackup*
3. Recuperare le informazioni dettagliate sul backup specificato: *Get-SmBackupDetails*

   Questo comando recupera le informazioni dettagliate sul backup di una risorsa specificata con un ID di backup specificato. Le informazioni includono nome del database, versione, home, SCN iniziale e finale, tablespace, database collegabili e relativi spazi tabella.

4. Ripristinare i dati dal backup: *Restore-SmBackup*

Monitorare le operazioni di ripristino del database Oracle

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

gli stati di post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi altra azione di ripristino che è possibile eseguire.

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Ripristina**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato di ripristino.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Annullare le operazioni di ripristino del database Oracle

È possibile annullare i processi di ripristino in coda.

Per annullare le operazioni di ripristino, è necessario accedere come amministratore SnapCenter o come proprietario del processo.

A proposito di questa attività

- È possibile annullare un'operazione di ripristino in coda dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione di ripristino in corso.
- È possibile utilizzare l'interfaccia grafica di SnapCenter, i cmdlet PowerShell o i comandi CLI per annullare le operazioni di ripristino in coda.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni di ripristino che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di ripristino in coda degli altri membri durante l'utilizzo di tale ruolo.

Fase

Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. 2. Selezionare il lavoro e fare clic su **Annulla lavoro**.
Riquadro delle attività	1. Dopo aver avviato l'operazione di ripristino, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. 2. Selezionare l'operazione. 3. Nella pagina Dettagli processo, fare clic su **Annulla processo**.

Clonare il database Oracle

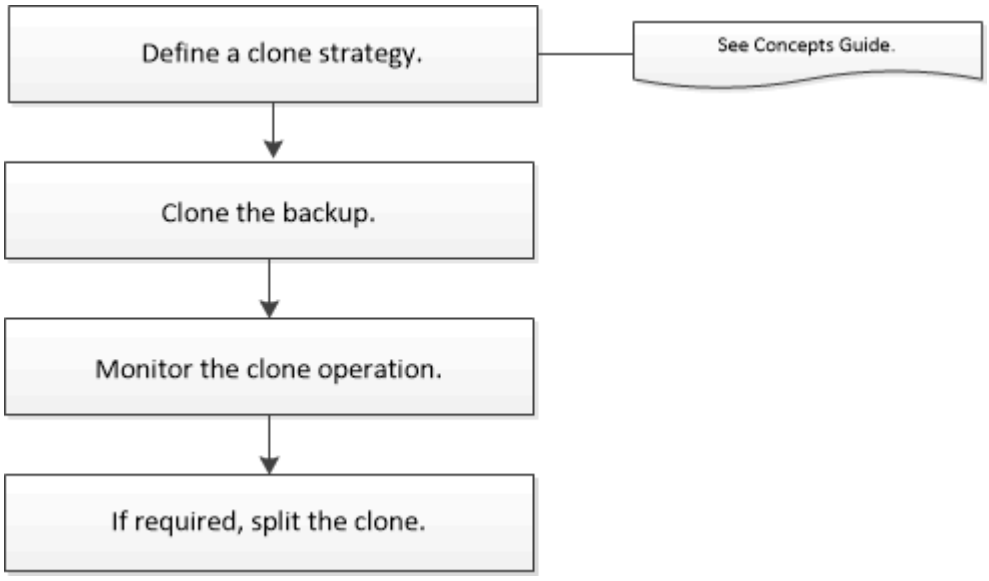
Clonare il flusso di lavoro

Il flusso di lavoro dei cloni include la pianificazione, l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

È possibile clonare i database per i seguenti motivi:

- Per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto del database corrente durante i cicli di sviluppo delle applicazioni.
- Popolare i data warehouse utilizzando strumenti di estrazione e manipolazione dei dati.
- Per ripristinare i dati cancellati o modificati per errore.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di clonazione:



Definire una strategia di clonazione per i database Oracle

La definizione di una strategia prima della clonazione del database garantisce il successo dell'operazione di clonazione.

Tipi di backup supportati per la clonazione

SnapCenter supporta la clonazione di diversi tipi di backup dei database Oracle.

- Backup dei dati online
- Backup completo online
- Backup di montaggio offline
- Backup shutdown offline
- Backup dei database di standby di Data Guard e dei database di standby di Active Data Guard
- Backup dei dati online, backup completi online, backup di montaggio offline e backup di arresto offline in una configurazione RAC (Real Application Clusters)
- Backup dei dati online, backup completi online, backup di montaggio offline e backup di arresto offline in una configurazione di Automatic Storage Management (ASM)

> Le configurazioni SAN non sono supportate se l'opzione user_friendly_names nel file di configurazione multipath è impostata su yes.

> La clonazione dei backup del registro di archiviazione non è supportata.

Tipi di cloning supportati per i database Oracle

In un ambiente di database Oracle, SnapCenter supporta la clonazione di un backup di database. È possibile clonare il backup dai sistemi di storage primario e secondario.

Il server SnapCenter utilizza la tecnologia FlexClone di NetApp per clonare i backup.

È possibile aggiornare un clone eseguendo il comando "Refresh-SmClone". Questo comando crea un backup del database, elimina il clone esistente e crea un clone con lo stesso nome.

> L'operazione di refresh dei cloni può essere eseguita solo utilizzando i comandi UNIX.

Convenzioni di denominazione dei cloni per i database Oracle

A partire da SnapCenter 3.0, la convenzione di naming utilizzata per i cloni dei file system è diversa dai cloni dei gruppi di dischi ASM.

- La convenzione di naming per i file system SAN o NFS è FileSystemNameofsourcedatabase_CLONESID.
- La convenzione di naming per i gruppi di dischi ASM è SC_HASHCODEofDISKGROUP_CLONESID.

  HASHCODEofDISKGROUP è un numero generato automaticamente (da 2 a 10 cifre) univoco per ciascun gruppo di dischi ASM.

Limitazioni della clonazione dei database Oracle

Prima di clonare i database, è necessario conoscere i limiti delle operazioni di clonazione.

- Se si utilizza una qualsiasi versione di Oracle dalla 11.2.0.4 alla 12.1.0.1, l'operazione di clonazione sarà in stato di sospensione quando si esegue il comando *renamedg*. È possibile applicare la patch Oracle 19544733 per risolvere questo problema.
- Non è supportata la clonazione di database da un LUN direttamente collegato a un host (ad esempio, utilizzando Microsoft iSCSI Initiator su un host Windows) a un LUN VMDK o RDM sullo stesso host Windows o su un altro host Windows o viceversa.
- La directory principale del punto di montaggio del volume non può essere una directory condivisa.
- Se si sposta un LUN che contiene un clone in un nuovo volume, il clone non può essere cancellato.

Variabili di ambiente predefinite per il clone specifico prespt e postscript

SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prespt e postscript durante la clonazione di un database.

Variabili di ambiente predefinite supportate per la clonazione di un database

- **SC_ORIGINAL_SID** specifica il SID del database di origine.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: NFSB32

- **SC_ORIGINAL_HOST** specifica il nome dell'host di origine.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: asmrac1.gdl.englab.netapp.com

- **SC_ORACLE_HOME** specifica il percorso della home directory Oracle del database di destinazione.

  Esempio: /Ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_NAME**" specifica il nome del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempi:

  - Se il database non è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Se il database è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG:RG2_scspr2417819002_07-20-2021_12.16.48.9267_1,RG2_scspr2417819002_07-21-2021_12.16.48.9267_1,RG2_scspr2417819002_07-22-2021_12.16.48.9267_1

- **SC_AV_NAME** specifica i nomi dei volumi dell'applicazione.

  Esempio: AV1|AV2

- **SC_ORIGINAL_OS_USER** specifica il proprietario del sistema operativo del database di origine.

  Esempio: oracle

- **SC_ORIGINAL_OS_GROUP** specifica il gruppo di sistemi operativi del database di origine.

  Esempio: Oinstall

- **SC_TARGET_SID**" specifica il SID del database clonato.

  Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: Clonedb

- **SC_TARGET_HOST** specifica il nome dell'host in cui verrà clonato il database.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: asmrac1.gdl.englab.netapp.com

- **SC_TARGET_OS_USER** specifica il proprietario del sistema operativo del database clonato.

  Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito.

  Esempio: oracle

- **SC_TARGET_OS_GROUP** specifica il gruppo di sistemi operativi del database clonato.

  Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito.

  Esempio: Oinstall

- **SC_TARGET_DB_PORT** specifica la porta del database clonato.

  Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito.

  Esempio: 1521

Per informazioni sui delimitatori, vedere "Delimitatori supportati".

Requisiti per la clonazione di un database Oracle

Prima di clonare un database Oracle, è necessario assicurarsi che i prerequisiti siano stati completati.

- È necessario aver creato un backup del database utilizzando SnapCenter.

  Per eseguire correttamente l'operazione di cloning, è necessario aver creato correttamente backup di dati e log online o backup offline (montaggio o arresto).

- Se si desidera personalizzare il file di controllo o ripetere i percorsi dei file di log, è necessario aver preconfigurato il file system o il gruppo di dischi ASM (Automatic Storage Management) richiesto.

Per impostazione predefinita, i file di log e di controllo del database clonato vengono creati nel gruppo di dischi ASM o nel file system fornito da SnapCenter per i file di dati del database clone.

- Se si utilizza ASM su NFS, aggiungere */var/opt/snapcenter/scu/cloni/*/** al percorso esistente definito nel parametro asm_diskstring.
- Nel parametro asm_diskstring, configurare *AFD:** se si utilizza ASMFD o configurare *ORCL:** se si utilizza ASMLIB.

  Per informazioni su come modificare il parametro asm_diskstring, vedere "Come aggiungere i percorsi dei dischi ad asm_diskstring".

- Se si crea il clone su un host alternativo, l'host alternativo deve soddisfare i seguenti requisiti:
  - Il plug-in SnapCenter per database Oracle deve essere installato sull'host alternativo.
  - L'host clone deve essere in grado di rilevare LUN dallo storage primario o secondario.
    - Se si esegue la clonazione dallo storage primario o secondario (Vault o Mirror) a un host alternativo, assicurarsi che sia stata stabilita una sessione iSCSI tra lo storage secondario e l'host alternativo o che sia stata inserita correttamente la zoning per FC.
    - Se si esegue la clonazione dallo storage Vault o Mirror allo stesso host, assicurarsi che sia stata stabilita una sessione iSCSI tra lo storage Vault o Mirror e l'host oppure che sia stata creata una zoning corretta per FC.
    - Se si esegue la clonazione in un ambiente virtualizzato, assicurarsi che venga stabilita una sessione iSCSI tra lo storage primario o secondario e il server ESX che ospita l'host alternativo o che venga eseguita la zoning appropriata per FC.

      Per informazioni, fare riferimento alla "documentazione delle utility host".

  - Se il database di origine è un database ASM:
    - L'istanza di ASM deve essere attiva e in esecuzione sull'host in cui verrà eseguito il clone.
    - Il provisioning del gruppo di dischi ASM deve essere eseguito prima dell'operazione di clonazione se si desidera inserire i file di log di archiviazione del database clonato in un gruppo di dischi ASM dedicato.
    - Il nome del gruppo di dischi dati può essere configurato, ma assicurarsi che il nome non sia utilizzato da altri gruppi di dischi ASM sull'host in cui verrà eseguito il clone.

      I file di dati che risiedono nel gruppo di dischi ASM vengono forniti come parte del flusso di lavoro dei cloni di SnapCenter.

  - Per NVMe, è necessario installare NVMe util
- Il tipo di protezione per il LUN dei dati e il LUN del log, ad esempio mirror, vault o vault mirror, deve essere lo stesso per rilevare i locatori secondari durante la clonazione su un host alternativo utilizzando i backup del log.
- Impostare IL valore di exclude_seed_cdb_view su FALSE nel file dei parametri del database di origine per recuperare le informazioni relative a PDB seme per clonare un backup del database 12_c_.

  La PDB seme è un modello fornito dal sistema che la CDB può utilizzare per creare PDB. La PDB seme è denominata SEME PDB. Per informazioni sul VALORE DI INIZIALIZZAZIONE PDB, consultare l'Oracle Doc ID 1940806.1.

  Impostare il valore prima di eseguire il backup del database 12_c_.

- SnapCenter supporta il backup dei file system gestiti dal sottosistema autofs. Se si esegue la clonazione del database, assicurarsi che i punti di montaggio dei dati non si trovino sotto la radice del punto di montaggio autofs, perché l'utente root dell'host plug-in non dispone dell'autorizzazione per creare directory sotto la radice del punto di montaggio autofs.

  Se i file di log di controllo e ripristino si trovano sotto il punto di montaggio dei dati, modificare il percorso del file di controllo e quindi ripetere il percorso del file di log di conseguenza.

  È possibile registrare manualmente i nuovi punti di montaggio clonati con il sottosistema autofs. I nuovi punti di montaggio clonati non verranno registrati automaticamente.

- Se si dispone di un TDE (accesso automatico) e si desidera clonare il database sullo stesso host o su un host alternativo, copiare il portafoglio (file chiave) sotto */etc/ORACLE/WALLET/€ORACLE_SID* dal database di origine al database clonato.
- Impostare il valore di use_lvmetad = 0 in */etc/lvm/lvm.conf* e arrestare il servizio lvm2-lvmetad per eseguire correttamente la clonazione in ambienti SAN (Storage Area Network) su Oracle Linux 7 o versione successiva o Red Hat Enterprise Linux (RHEL) 7 o versione successiva.
- Installare la patch Oracle 13366202 se si utilizza il database Oracle 11.2.0.3 o versione successiva e l'ID del database per l'istanza ausiliaria viene modificato utilizzando uno script NID.
- Assicurarsi che gli aggregati che ospitano i volumi siano inclusi nell'elenco degli aggregati assegnati della macchina virtuale di storage (SVM).
- Per NVMe, se una porta di destinazione deve essere esclusa dalla connessione, aggiungere il nome del nodo di destinazione e il nome della porta nel file /var/opt/snapcenter/scu/etc/nvme.conf.

  Se il file non esiste, crearlo come illustrato nell'esempio seguente:

```
blacklist {
nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- Assicurarsi che il LUN non sia mappato all'host AIX utilizzando iGroup costituito da protocolli misti iSCSI e FC. Per ulteriori informazioni, vedere "Operazione non riuscita con errore Impossibile rilevare il dispositivo per il LUN".

Clonare un backup del database Oracle

È possibile utilizzare SnapCenter per clonare un database Oracle utilizzando il backup del database.

Prima di iniziare

Se il plug-in è stato installato come utente non root, è necessario assegnare manualmente le autorizzazioni di esecuzione alle directory prescrittt e postscript.

A proposito di questa attività

- L'operazione di cloning crea una copia dei file di dati del database e crea nuovi file di log di ripristino e file di controllo online. Il database può essere ripristinato a un orario specifico, in base alle opzioni di ripristino

specificate.

> La clonazione non riesce se si tenta di clonare un backup creato su un host Linux su un host AIX o viceversa.

SnapCenter crea un database standalone quando viene clonato da un backup di database Oracle RAC. SnapCenter supporta la creazione di cloni dal backup di database di standby Data Guard e Active Data Guard.

Durante la clonazione, SnapCenter monta il numero ottimale di backup dei log in base a SCN o dat e il tempo necessario per le operazioni di recovery. Dopo il ripristino, il backup del registro viene disinstallato. Tutti questi cloni sono montati sotto */var/opt/snapcenter/scu/cloni/*. Se si utilizza ASM su NFS, aggiungere */var/opt/snapcenter/scu/cloni/*/** al percorso esistente definito nel parametro asm_diskstring.

Durante la clonazione di un backup di un database ASM in un ambiente SAN, le regole udev per i dispositivi host clonati vengono create in */etc/udev/rules.d/999-scu-netapp.rules*. Queste regole udev associate ai dispositivi host clonati vengono eliminate quando si elimina il clone.

> In una configurazione di Flex ASM, non è possibile eseguire l'operazione di cloni sui nodi Leaf se la cardinalità è inferiore al numero di nodi nel cluster RAC.

- Per i criteri abilitati per SnapLock, per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco Snapshot, i cloni creati dagli Snapshot a prova di manomissione come parte del ripristino ereditano il tempo di scadenza SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

4. Dalla vista Manage Copies (Gestisci copie), selezionare i backup da Local Copies (copie locali) (primarie), Mirror Copies (copie mirror) (secondarie) o Vault Copies (copie vault) (secondarie).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su * *  .
6. Nella pagina Name (Nome), eseguire una delle seguenti operazioni:

Se si desidera…	Fasi…
Clonare un database (CDB o non CDB)	a. Specificare il SID del clone. Il SID clone non è disponibile per impostazione predefinita e la lunghezza massima del SID è di 8 caratteri. Assicurarsi che non esista alcun database con lo stesso SID sull'host in cui verrà creato il clone.
Clonare un database collegabile (PDB)	a. Selezionare **Copia PDB**. b. Specificare il PDB che si desidera clonare. c. Specificare il nome della PDB clonata. Per informazioni dettagliate sulla clonazione di un PDB, vedere "Clonare un database collegabile".

Quando si selezionano dati mirrorati o del vault:

- se non è presente alcun backup del log nel mirror o nel vault, non viene selezionato nulla e i locatori sono vuoti.
- se i backup del log esistono nel mirror o nel vault, viene selezionato l'ultimo backup del log e viene visualizzato il localizzatore corrispondente.

Se il backup del log selezionato esiste sia nella posizione del mirror che nel vault, vengono visualizzati entrambi i locator.

7. Nella pagina Locations (posizioni), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Clonare l'host	Per impostazione predefinita, l'host del database di origine viene popolato. Se si desidera creare il clone su un host alternativo, selezionare l'host con la stessa versione di Oracle e del sistema operativo dell'host del database di origine.

Per questo campo…	Eseguire questa operazione…
Posizioni dei file di dati	Per impostazione predefinita, la posizione del file dati viene popolata. La convenzione di denominazione predefinita di SnapCenter per i file system SAN o NFS è FileSystemNameofsourcedatabase_CLONESID. La convenzione di denominazione predefinita di SnapCenter per i gruppi di dischi ASM è SC_HASHCODEODISKGROUP_CLONESID. HASHCODEofDISKGROUP è un numero generato automaticamente (da 2 a 10 cifre) univoco per ciascun gruppo di dischi ASM. Se si sta personalizzando il nome del gruppo di dischi ASM, assicurarsi che la lunghezza del nome sia conforme alla lunghezza massima supportata da Oracle. Se si desidera specificare un percorso diverso, è necessario immettere i punti di montaggio dei file di dati o i nomi dei gruppi di dischi ASM per il database clone. Quando si personalizza il percorso del file di dati, è necessario modificare anche il file di controllo e ripetere i nomi dei gruppi di dischi ASM o del file system del file di registro con lo stesso nome utilizzato per i file di dati o con un file system o gruppi di dischi ASM esistente.

Per questo campo…	Eseguire questa operazione…
File di controllo	Per impostazione predefinita, il percorso del file di controllo viene popolato. I file di controllo sono posizionati nello stesso gruppo di dischi ASM o file system dei file di dati. Se si desidera eseguire l'override del percorso del file di controllo, è possibile specificare un percorso diverso del file di controllo. Il file system o il gruppo di dischi ASM dovrebbe esistere sull'host. Per impostazione predefinita, il numero di file di controllo sarà uguale a quello del database di origine. È possibile modificare il numero di file di controllo, ma per clonare il database è necessario almeno un file di controllo. È possibile personalizzare il percorso del file di controllo su un file system diverso (esistente) rispetto a quello del database di origine.

Per questo campo…	Eseguire questa operazione…
Registri di ripristino	Per impostazione predefinita, vengono popolati il gruppo di file di log di ripristino, il percorso e le relative dimensioni. I log di ripristino vengono posizionati nello stesso gruppo di dischi ASM o file system dei file di dati del database clonato. Se si desidera eseguire l'override del percorso del file di log di ripristino, è possibile personalizzare il percorso del file di log di ripristino in un file system diverso da quello del database di origine. Il nuovo file system o il gruppo di dischi ASM dovrebbe esistere sull'host. Per impostazione predefinita, il numero di gruppi di log di ripristino, i file di log di ripristino e le relative dimensioni saranno identici a quelli del database di origine. È possibile modificare i seguenti parametri: • Numero di gruppi di log di ripristino Per clonare il database sono necessari almeno due gruppi di log di ripristino. • Ripristinare i file di log di ciascun gruppo e il relativo percorso È possibile personalizzare il percorso del file di log di ripristino su un file system diverso (esistente) da quello del database di origine. Per clonare il database, è necessario un minimo di un file di log di ripristino nel gruppo di log di ripristino. • Dimensioni del file di log di ripristino

8. Nella pagina credenziali, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale per l'utente sys	Selezionare la credenziale da utilizzare per definire la password utente sys del database clone. Se SQLNET.AUTHENTICATION_SERVICES è impostato su NONE nel file sqlnet.ora sull'host di destinazione, non selezionare **None** come credenziale nell'interfaccia grafica di SnapCenter.
Nome credenziale istanza ASM	Selezionare **None** se l'autenticazione del sistema operativo è abilitata per la connessione all'istanza ASM sull'host clone. In caso contrario, selezionare la credenziale Oracle ASM configurata con l'utente "sys" o con il privilegio "sysasm" applicabile all'host clone.

La home page, il nome utente e i dettagli del gruppo Oracle vengono compilati automaticamente dal database di origine. È possibile modificare i valori in base all'ambiente Oracle dell'host in cui verrà creato il clone.

9. Nella pagina PreOps, attenersi alla seguente procedura:

   a. Inserire il percorso e gli argomenti della prescrizione che si desidera eseguire prima dell'operazione di clonazione.

      È necessario memorizzare la prescrizione in */var/opt/snapcenter/spl/scripts* o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso */var/opt/snapcenter/spl/scripts* viene compilato. Se lo script è stato inserito in qualsiasi cartella all'interno di questo percorso, è necessario fornire il percorso completo fino alla cartella in cui è inserito lo script.

      SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono il prescrittivo e postscript. "Scopri di più"

   b. Nella sezione Database Parameter Settings (Impostazioni dei parametri del database), modificare i valori dei parametri del database prepopolati utilizzati per inizializzare il database.

      È possibile aggiungere altri parametri facendo clic su * *  .

      Se si utilizza Oracle Standard Edition e il database è in esecuzione in modalità Archive log o si desidera ripristinare un database dal log di ripristino dell'archivio, aggiungere i parametri e specificare il percorso.

      - LOG_ARCHIVE_DEST
      - LOG_ARCHIVE_DUPLEX_DEST

      L'area di recupero rapido (fra) non è definita nei parametri del database prepopolati. È possibile configurare fra aggiungendo i relativi parametri.

Il valore predefinito di log_archive_dest_1 è €ORACLE_HOME/clone_sid e i log di archiviazione del database clonato verranno creati in questa posizione. Se il parametro log_archive_dest_1 è stato eliminato, la posizione del log di archiviazione viene determinata da Oracle. È possibile definire una nuova posizione per il log di archiviazione modificando log_archive_dest_1, ma assicurarsi che il file system o il gruppo di dischi siano esistenti e resi disponibili sull'host.

a. Fare clic su **Reset** (Ripristina) per visualizzare le impostazioni predefinite dei parametri del database.

10. Per impostazione predefinita, nella pagina PostOps, sono selezionate le opzioni **Recover database** (Ripristina database) e **until Cancel** (Annulla) per eseguire il ripristino del database clonato.

    SnapCenter esegue il ripristino montando l'ultimo backup del registro con la sequenza ininterrotta di registri di archivio dopo il backup dei dati selezionato per la clonazione. Il backup di log e dati deve essere sullo storage primario per eseguire il clone sullo storage primario e il backup di log e dati deve essere sullo storage secondario per eseguire il clone sullo storage secondario.

    Le opzioni **Recover database** (Ripristina database) e **until Cancel** (Annulla) non sono selezionate se SnapCenter non riesce a trovare i backup di log appropriati. È possibile specificare la posizione del registro di archiviazione esterno se il backup del registro non è disponibile in **specificare le posizioni esterne del registro di archiviazione**. È possibile specificare più posizioni del registro.

    Se si desidera clonare un database di origine configurato per supportare flash recovery area (fra) e Oracle Managed Files (OMF), anche la destinazione del log per il ripristino deve aderire alla struttura di directory OMF.

    La pagina PostOps non viene visualizzata se il database di origine è un database di standby Data Guard o un database di standby Active Data Guard. Per lo standby di Data Guard o un database di standby di Active Data Guard, SnapCenter non fornisce un'opzione per selezionare il tipo di ripristino nell'interfaccia grafica di SnapCenter, ma il database viene ripristinato utilizzando fino al tipo di ripristino Annulla senza applicare alcun registro.

Nome del campo	Descrizione
Fino a Annulla	SnapCenter esegue il ripristino montando l'ultimo backup del registro con la sequenza ininterrotta di registri di archivio dopo il backup dei dati selezionato per il cloning. Il database clonato viene recuperato fino a quando il file di log non è mancante o corrotto.
Data e ora	SnapCenter ripristina il database fino a una data e un'ora specificate. Il formato accettato è mm/gg/aaaa hh:mm:ss. L'ora può essere specificata in formato 24 ore.
Fino a SCN (System Change Number)	SnapCenter ripristina il database fino a un numero SCN (System Change Number) specificato.

Nome del campo	Descrizione
Specificare le posizioni esterne del registro di archiviazione	Se il database viene eseguito in modalità ARCHIVELOG, SnapCenter identifica e monta il numero ottimale di backup dei log in base al numero SCN specificato o alla data e all'ora selezionate. È inoltre possibile specificare la posizione del registro di archiviazione esterno. SnapCenter non identificherà e monterà automaticamente i backup del registro se è stato selezionato fino a quando non viene selezionato Annulla.
Creare un nuovo DBID	Per impostazione predefinita, la casella di controllo **Create new DBID** (Crea nuovo DBID) è selezionata per generare un numero univoco (DBID) per il database clonato che lo differenzia dal database di origine. Deselezionare la casella di controllo se si desidera assegnare il DBID del database di origine al database clonato. In questo scenario, se si desidera registrare il database clonato con il catalogo RMAN esterno in cui il database di origine è già registrato, l'operazione non riesce.
Creare un file di tempfile per tablespace temporaneo	Selezionare questa casella di controllo se si desidera creare un file di tempesta per lo spazio tabella temporaneo predefinito del database clonato. Se la casella di controllo non è selezionata, il clone del database verrà creato senza il file di tempesta.
Inserire le voci sql da applicare quando viene creato il clone	Aggiungere le voci sql che si desidera applicare al momento della creazione del clone.

Nome del campo	Descrizione
Inserire gli script da eseguire dopo l'operazione di clonazione	Specificare il percorso e gli argomenti del postscript che si desidera eseguire dopo l'operazione di clonazione. Il postscript deve essere memorizzato in */var/opt/snapcenter/spl/scripts* o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso */var/opt/snapcenter/spl/scripts* viene compilato. Se lo script è stato inserito in qualsiasi cartella all'interno di questo percorso, è necessario fornire il percorso completo fino alla cartella in cui è inserito lo script. Se l'operazione di cloni non riesce, i postscript non vengono eseguiti e le attività di cleanup vengono attivate direttamente.

11. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

    È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report**.

    Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

12. Esaminare il riepilogo, quindi fare clic su **fine**.

    Durante l'esecuzione del ripristino come parte dell'operazione di creazione dei cloni, anche se il ripristino non riesce, il clone viene creato con un avviso. È possibile eseguire un ripristino manuale su questo clone per portare il database clone allo stato coerente.

13. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Risultato

Dopo aver clonato il database, è possibile aggiornare la pagina delle risorse per elencare il database clonato come una delle risorse disponibili per il backup. Il database clonato può essere protetto come qualsiasi altro database utilizzando il flusso di lavoro di backup standard o può essere incluso in un gruppo di risorse (appena creato o esistente). Il database clonato può essere ulteriormente clonato (clone di cloni).

Dopo la clonazione, non rinominare mai il database clonato.

Se non è stato eseguito il ripristino durante la clonazione, il backup del database clonato potrebbe non riuscire a causa di un ripristino non corretto e potrebbe essere necessario eseguire un ripristino manuale. Il backup del log può anche avere esito negativo se la posizione predefinita popolata per i log di archiviazione si trova su uno storage non NetApp o se il sistema di storage non è configurato con SnapCenter.

Nell'installazione di AIX, è possibile utilizzare il comando lkdev per bloccare e il comando rendev per rinominare i dischi su cui risiedeva il database clonato.

Il blocco o la ridenominazione dei dispositivi non influisce sull'operazione di eliminazione dei cloni. Per i layout LVM AIX costruiti sui dispositivi SAN, la ridenominazione dei dispositivi non sarà supportata per i dispositivi SAN clonati.

Ulteriori informazioni

- "Il ripristino o la clonazione non riesce e viene visualizzato il messaggio di errore ora-00308"
- "Ripristino di un database clonato non riuscito"
- "Parametri personalizzabili per operazioni di backup, ripristino e clonazione su sistemi AIX"

Clonare un database collegabile

È possibile clonare un database collegabile (PDB) su un CDB di destinazione diverso o uguale sullo stesso host o su un host alternativo. È inoltre possibile ripristinare il PDB clonato a un SCN desiderato o a una data e un'ora.

Prima di iniziare

Se il plug-in è stato installato come utente non root, è necessario assegnare manualmente le autorizzazioni di esecuzione alle directory prescrittt e postscript.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database di tipo istanza singola (multi-tenant) dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

4. Dalla vista Manage Copies (Gestisci copie), selezionare i backup da Local Copies (copie locali) (primarie), Mirror Copies (copie mirror) (secondarie) o Vault Copies (copie vault) (secondarie).
5. Selezionare il backup dalla tabella, quindi fare clic su * *  .
6. Nella pagina Name (Nome), eseguire le seguenti operazioni:
   a. Selezionare **Copia PDB**.
   b. Specificare il PDB che si desidera clonare.

      È possibile clonare un solo PDB alla volta.

c. Specificare il nome del clone PDB.

7. Nella pagina Locations (posizioni), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Clonare l'host	Per impostazione predefinita, l'host del database di origine viene popolato. Se si desidera creare il clone su un host alternativo, selezionare l'host con la stessa versione di Oracle e del sistema operativo dell'host del database di origine.
CDB di destinazione	Selezionare il CDB in cui si desidera includere il PDB clonato. Assicurarsi che la CDB di destinazione sia in esecuzione.
Stato del database	Selezionare la casella di controllo **Open the cloned PDB in READ-WRITE mode** (Apri la PDB clonata in modalità DI LETTURA/SCRITTURA) se si desidera aprire la PDB in modalità DI LETTURA/SCRITTURA.
Posizioni dei file di dati	Per impostazione predefinita, la posizione del file dati viene popolata. La convenzione di denominazione predefinita di SnapCenter per i file system SAN o NFS è FileSystemNameofsourcedatabase_SCJOBID. La convenzione di naming predefinita di SnapCenter per i gruppi di dischi ASM è SC_HASHCODEofDISKGROUP_SCJOBID. HASHCODEofDISKGROUP è un numero generato automaticamente (da 2 a 10 cifre) univoco per ciascun gruppo di dischi ASM. Se si sta personalizzando il nome del gruppo di dischi ASM, assicurarsi che la lunghezza del nome sia conforme alla lunghezza massima supportata da Oracle. Se si desidera specificare un percorso diverso, è necessario immettere i punti di montaggio dei file di dati o i nomi dei gruppi di dischi ASM per il database clone.

La home page, il nome utente e i dettagli del gruppo Oracle vengono compilati automaticamente dal database di origine. È possibile modificare i valori in base all'ambiente Oracle dell'host in cui verrà creato il

clone.

8. Nella pagina PreOps, attenersi alla seguente procedura:

   a. Inserire il percorso e gli argomenti della prescrizione che si desidera eseguire prima dell'operazione di clonazione.

      Si consiglia di memorizzare la prescrizione in /var/opt/snapcenter/spl/scripts o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso /var/opt/snapcenter/spl/scripts viene compilato. Se lo script è stato inserito in qualsiasi cartella all'interno di questo percorso, è necessario fornire il percorso completo fino alla cartella in cui è inserito lo script.

   SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono il prescrittivo e postscript. "Scopri di più"

   a. Nella sezione Auxiliary CDB clone database parameters (Impostazioni dei parametri del database dei cloni CDB ausiliari), modificare i valori dei parametri del database prepopolati utilizzati per inizializzare il database.

9. Fare clic su **Reset** (Ripristina) per visualizzare le impostazioni predefinite dei parametri del database.
10. Per impostazione predefinita, nella pagina PostOps, viene selezionato **fino a quando non viene eseguito Annulla** per eseguire il ripristino del database clonato.

    Se SnapCenter non riesce a trovare i backup di log appropriati, l'opzione **fino a Annulla** non viene selezionata. È possibile specificare la posizione del registro di archiviazione esterno se il backup del registro non è disponibile in **specificare le posizioni esterne del registro di archiviazione**. È possibile specificare più posizioni del registro.

    Se si desidera clonare un database di origine configurato per supportare flash recovery area (fra) e Oracle Managed Files (OMF), anche la destinazione del log per il ripristino deve aderire alla struttura di directory OMF.

Nome del campo	Descrizione
Fino a Annulla	SnapCenter esegue il ripristino montando l'ultimo backup del registro con la sequenza ininterrotta di registri di archivio dopo il backup dei dati selezionato per il cloning. Il backup di log e dati deve essere sullo storage primario per eseguire il clone sullo storage primario e il backup di log e dati deve essere sullo storage secondario per eseguire il clone sullo storage secondario. Il database clonato viene recuperato fino a quando il file di log non è mancante o corrotto.
Data e ora	SnapCenter ripristina il database fino a una data e un'ora specificate. L'ora può essere specificata in formato 24 ore.

Nome del campo	Descrizione
Fino a SCN (System Change Number)	SnapCenter ripristina il database fino a un numero SCN (System Change Number) specificato.
Specificare le posizioni esterne del registro di archiviazione	Specificare la posizione del log di archiviazione esterno.
Creare un nuovo DBID	Per impostazione predefinita, la casella di controllo **Create new DBID** (Crea nuovo DBID) non è selezionata per il database dei cloni ausiliari. Selezionare questa casella di controllo se si desidera generare un numero univoco (DBID) per il database clonato ausiliario differenziandolo dal database di origine.
Creare un file di tempfile per tablespace temporaneo	Selezionare questa casella di controllo se si desidera creare un file di tempesta per lo spazio tabella temporaneo predefinito del database clonato. Se la casella di controllo non è selezionata, il clone del database verrà creato senza il file di tempesta.
Inserire le voci sql da applicare quando viene creato il clone	Aggiungere le voci sql che si desidera applicare al momento della creazione del clone.
Inserire gli script da eseguire dopo l'operazione di clonazione	Specificare il percorso e gli argomenti del postscript che si desidera eseguire dopo l'operazione di clonazione. Il postscript deve essere memorizzato in */var/opt/snapcenter/spl/scripts* o in qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, il percorso */var/opt/snapcenter/spl/scripts* viene compilato. Se lo script è stato inserito in qualsiasi cartella all'interno di questo percorso, è necessario fornire il percorso completo fino alla cartella in cui è inserito lo script. Se l'operazione di cloni non riesce, i postscript non vengono eseguiti e le attività di cleanup vengono attivate direttamente.

11. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report**.

> Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

12. Esaminare il riepilogo, quindi fare clic su **fine**.
13. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Al termine

Se si desidera creare un backup del PDB clonato, è necessario eseguire il backup del CDB di destinazione in cui viene clonato il PDB, poiché non è possibile eseguire il backup solo del PDB clonato. Se si desidera creare il backup con una relazione secondaria, è necessario creare una relazione secondaria per la CDB di destinazione.

In una configurazione RAC, lo storage per la PDB clonata è collegato solo al nodo in cui è stato eseguito il clone PDB. I PDB sugli altri nodi del RAC sono in STATO DI MONTAGGIO. Se si desidera che la PDB clonata sia accessibile dagli altri nodi, è necessario collegare manualmente lo storage agli altri nodi.

Ulteriori informazioni

- "Il ripristino o la clonazione non riesce e viene visualizzato il messaggio di errore ora-00308"
- "Parametri personalizzabili per operazioni di backup, ripristino e clonazione su sistemi AIX"

Clonare i backup dei database Oracle utilizzando i comandi UNIX

Il flusso di lavoro dei cloni include la pianificazione, l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

A proposito di questa attività

Eseguire i seguenti comandi per creare il file di specifica del clone del database Oracle e avviare l'operazione di clone.

Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al comando software SnapCenter".

Fasi

1. Creare una specifica di clone del database Oracle da un backup specificato: *New-SmOracleCloneSpecification*

   > Se il criterio di protezione dei dati secondario è un vault unificato, specificare Only -IncludeSecondaryDetails. Non è necessario specificare -SecondaryStorageType.

   Questo comando crea automaticamente un file di specifica del clone del database Oracle per il database di origine specificato e il relativo backup. È inoltre necessario fornire un SID del database clone in modo che il file di specifica creato abbia i valori generati automaticamente per il database clone che si desidera creare.

Il file di specifica del clone viene creato in */var/opt/snapcenter/sco/clone_specs*.

2. Avviare un'operazione di clone da un gruppo di risorse clone o da un backup esistente: *New-SmClone*

   Questo comando avvia un'operazione di clonazione. È inoltre necessario fornire un percorso del file di specifica del clone Oracle per l'operazione di clonazione. È inoltre possibile specificare le opzioni di ripristino, l'host in cui eseguire l'operazione di clonazione, le prescrizioni, i postscript e altri dettagli.

   Per impostazione predefinita, il file di destinazione del log di archiviazione per il database dei cloni viene popolato automaticamente in _ Oracle_HOME/CLONE_SID_.

Separare un clone di database Oracle

È possibile utilizzare SnapCenter per separare una risorsa clonata dalla risorsa principale. Il clone diviso diventa indipendente dalla risorsa padre.

A proposito di questa attività

- Non è possibile eseguire l'operazione di suddivisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato il clone1 da un backup del database, è possibile creare un backup del clone1 e clonare il backup (clone2). Dopo aver creato il clone2, il clone1 è un clone intermedio e non è possibile eseguire l'operazione di suddivisione del clone sul clone1. Tuttavia, è possibile eseguire l'operazione di suddivisione dei cloni sul clone2.

  Dopo aver diviso il clone2, è possibile eseguire l'operazione di divisione del clone sul clone1, poiché il clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup del clone vengono eliminate.
- Per informazioni sulle limitazioni delle operazioni di suddivisione clone, vedere "Guida alla gestione dello storage logico di ONTAP 9".
- Assicurarsi che il volume o l'aggregato sul sistema di storage sia online.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** dall'elenco **View** (Visualizza).
3. Selezionare la risorsa clonata, ad esempio il database o il LUN, quindi fare clic su  .
4. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
5. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

   L'operazione di suddivisione del clone non risponde se il servizio SMCore viene riavviato e i database su cui è stata eseguita l'operazione di suddivisione del clone vengono elencati come cloni nella pagina risorse. Eseguire il cmdlet *Stop-SmJob* per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione di suddivisione del clone.

   Se si desidera un tempo di polling più lungo o più breve per controllare se il clone è diviso o meno, è possibile modificare il valore del parametro CloneSplitStatusCheckPollTime nel file SMCoreServiceHost.exe.config per impostare l'intervallo di tempo in cui SMCore deve eseguire il polling

per lo stato dell'operazione di suddivisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

Ad esempio,

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'operazione di avvio del clone split non riesce se sono in corso operazioni di backup, ripristino o altro clone split. È necessario riavviare l'operazione di suddivisione dei cloni solo al termine delle operazioni in esecuzione.

Clone separato di un database collegabile

È possibile utilizzare SnapCenter per suddividere un database clonato collegabile (PDB).

A proposito di questa attività

Se è stato creato un backup del CDB di destinazione in cui viene clonato il PDB, quando si divide il clone del PDB, il PDB clonato viene rimosso anche da tutti i backup del CDB di destinazione contenente il PDB clonato.

I cloni PDB non vengono visualizzati nella vista dell'inventario o delle risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Selezionare il database dei container di origine (CDB) dalla vista delle risorse o dei gruppi di risorse.
3. Dalla vista Manage Copies (Gestisci copie), selezionare **cloni** dai sistemi di storage primario o secondario (mirrorati o replicati).
4. Selezionare il clone PDB (targetCDB:PDBClone), quindi fare clic su  .
5. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
6. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Monitorare le operazioni di clonazione del database Oracle

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

-  In corso
-  Completato correttamente

- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Clone**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato del clone.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro clone, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

Aggiornare un clone

È possibile aggiornare il clone eseguendo il comando *Refresh-SmClone*. Questo comando crea un backup del database, elimina il clone esistente e crea un clone con lo stesso nome.

Non è possibile aggiornare un clone PDB.

Cosa ti serve

- Creare un backup completo online o una policy di backup dei dati offline senza backup pianificati attivati.
- Configurare la notifica e-mail nel criterio solo per gli errori di backup.
- Definire il numero di conservazione per i backup on-demand in modo appropriato per garantire che non vi siano backup indesiderati.
- Assicurarsi che al gruppo di risorse identificato per l'operazione di aggiornamento dei cloni sia associato solo un backup completo online o una policy di backup dei dati offline.
- Creare un gruppo di risorse con un solo database.
- Se viene creato un job cron per il comando di aggiornamento dei cloni, assicurarsi che le pianificazioni SnapCenter e cron non si sovrappongano per il gruppo di risorse del database.

  Per un job cron creato per il comando di refresh del clone, assicurarsi di eseguire Open-SmConnection ogni 24 ore.

- Assicurarsi che il SID clone sia univoco per un host.

  Se più operazioni di refresh clone utilizzano lo stesso file di specifica del clone o il file di specifica del clone con lo stesso SID del clone, il clone esistente con il SID sull'host verrà cancellato e il clone verrà creato.

- Assicurarsi che il criterio di backup sia abilitato con la protezione secondaria e che il file di specifica del clone sia creato con “-IncludeSecondaryDetails” per creare i cloni utilizzando i backup secondari.
  - Se viene specificato il file di specifica del clone primario ma l’opzione di aggiornamento secondario del criterio è selezionata, il backup viene creato e l’aggiornamento viene trasferito al file secondario. Tuttavia, il clone verrà creato dal backup primario.
  - Se viene specificato il file di specifica del clone primario e non è stata selezionata l’opzione di aggiornamento secondario per il criterio, il backup verrà creato sul primario e il clone verrà creato dal primario.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico: *Open-SmConnection*
2. Creare una specifica di clone del database Oracle da un backup specificato: *New-SmOracleCloneSpecification*

   Se il criterio di protezione dei dati secondario è un vault unificato, specificare Only -IncludeSecondaryDetails. Non è necessario specificare -SecondaryStorageType.

   Questo comando crea automaticamente un file di specifica del clone del database Oracle per il database di origine specificato e il relativo backup. È inoltre necessario fornire un SID del database clone in modo che il file di specifica creato abbia i valori generati automaticamente per il database clone che si desidera creare.

   Il file di specifica del clone viene creato in */var/opt/snapcenter/sco/clone_specs*.

3. Eseguire *Refresh-SmClone*.

   Se l’operazione non riesce con i messaggi di errore "PL-SCO-20032: Operazione CanExecute non riuscita con l’errore: PL-SCO-30031: File di log di ripristino +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log esiste", specificare un valore più alto per *-WaitToTriggerClone*.

   Per informazioni dettagliate sui comandi UNIX, vedere "Guida di riferimento al comando software SnapCenter".

Eliminare il clone di un database collegabile

È possibile eliminare il clone di un database collegabile (PDB) se non è più necessario.

Se è stato creato un backup del CDB di destinazione in cui viene clonato il PDB, quando si elimina il clone del PDB, anche il PDB clonato viene rimosso dal backup del CDB di destinazione.

I cloni PDB non vengono visualizzati nella vista dell’inventario o delle risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall’elenco.
2. Selezionare il database dei container di origine (CDB) dalla vista delle risorse o dei gruppi di risorse.
3. Dalla vista Manage Copies (Gestisci copie), selezionare **cloni** dai sistemi di storage primario o secondario

(mirrorati o replicati).

4. Selezionare il clone PDB (targetCDB:PDBClone), quindi fare clic su .
5. Fare clic su **OK**.

Gestire i volumi delle applicazioni

Che cosa sono i volumi delle applicazioni

I volumi delle applicazioni sono lo storage in cui sono memorizzate informazioni quali configurazione, programma di installazione e altri file non dati correlati al database Oracle.

Il plug-in SnapCenter per database Oracle consente di creare un backup coerente dei volumi delle applicazioni (volumi non di dati) con i database Oracle.

Il plug-in automatizza backup e cloning dei volumi delle applicazioni.

- Proteggere i volumi delle applicazioni e i volumi dei database Oracle in un singolo gruppo di risorse.
- Creare backup dei volumi di applicazioni.
- Crea backup di database Oracle e volumi applicativi.
- Crea cloni di database e volumi applicativi fino a un point-in-time.
- Pianificare le operazioni di backup.
- Monitorare tutte le operazioni.
- Visualizzazione di report sulle operazioni di backup e cloning.

Aggiungere volumi applicativi

SnapCenter supporta il backup e la clonazione dei volumi applicativi del database Oracle. Aggiungere manualmente i volumi dell'applicazione. Il rilevamento automatico dei volumi delle applicazioni non è supportato.

I volumi applicativi supportano solo connessioni dirette NFS e iSCSI.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Resources**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Fare clic su **Add Application Volume** (Aggiungi volume applicazione).
3. Nella pagina Name (Nome), eseguire le seguenti operazioni:
   - Nel campo Name (Nome), immettere il nome del volume dell'applicazione.
   - Nel campo host Name (Nome host), immettere il nome dell'host.
4. Nella pagina Storage Footprint, inserire il nome del sistema di storage, selezionare uno o volumi e specificare i LUN o le Qtree associati.

   È possibile aggiungere più sistemi storage.

5. Esaminare il riepilogo, quindi fare clic su **fine**.
6. Nella pagina Resources (risorse), selezionare **Application Volume** (Volume applicazione) dall'elenco **View** (Visualizza) per visualizzare tutti i volumi delle applicazioni aggiunti.

Modificare il volume dell'applicazione

Se non vengono creati backup, è possibile modificare tutti i valori specificati durante l'aggiunta del volume dell'applicazione. Se il backup viene creato, è possibile modificare solo i dettagli del sistema di storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Resources**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Application Volume** (Volume applicazione) dall'elenco **View** (Visualizza).
3. Fare clic su  per modificare i valori.

Eliminare il volume dell'applicazione

Quando si elimina un volume dell'applicazione, se sono presenti backup associati al volume dell'applicazione, il volume dell'applicazione viene messo in modalità di manutenzione e non vengono creati nuovi backup e non vengono conservati backup precedenti. Se non sono associati backup, tutti i metadati verranno eliminati.

Se necessario, SnapCenter consente di annullare l'operazione di eliminazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Resources**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Application Volume** (Volume applicazione) dall'elenco **View** (Visualizza).
3. Fare clic su  per modificare i valori.

Volumi applicativi di backup

Eseguire il backup del volume dell'applicazione

Se il volume dell'applicazione non fa parte di alcun gruppo di risorse, è possibile eseguire il backup del volume dell'applicazione dalla pagina risorse.

A proposito di questa attività

Per impostazione predefinita, vengono creati i backup del gruppo di coerenza (CG). Se si desidera creare backup basati su volume, impostare il valore **EnableOracleNdvVolumeBasedBackup** su true nel file *web.config*.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Resources**, quindi selezionare il plug-in Oracle Database dall'elenco.

2. Nella pagina Resources (risorse), selezionare **Application Volume** (Volume applicazione) dall'elenco **View** (Visualizza).
3. Fare clic su , quindi selezionare il nome host e il tipo di database per filtrare le risorse.

   È quindi possibile fare clic su * * per chiudere il riquadro del filtro.

4. Selezionare il volume dell'applicazione di cui si desidera eseguire il backup.

   Viene visualizzata la pagina Application volume-Protect.

5. Nella pagina Resource, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
USA il formato nome personalizzato per la copia Snapshot	Selezionare questa casella di controllo, quindi immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea. Ad esempio, customtext__policy_hostname o resource_hostname. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.
Escludi le destinazioni del registro di archiviazione dal backup	Specificare le destinazioni dei file di log dell'archivio di cui non si desidera eseguire il backup.

6. Nella pagina Criteri, attenersi alla seguente procedura:

   a. Selezionare uno o più criteri dall'elenco a discesa.

      È inoltre possibile creare un criterio facendo clic su .

      Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

   b. Fare clic nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.

      policy_name è il nome del criterio selezionato.

   Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

7. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di backup eseguita sulla risorsa, quindi selezionare **Allega report del processo**.

Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

8. Esaminare il riepilogo, quindi fare clic su **fine**.

   Viene visualizzata la pagina della topologia del volume dell'applicazione.

9. Fare clic su **Esegui backup ora**.
10. Nella pagina Backup, attenersi alla seguente procedura:
    a. Se sono stati applicati più criteri alla risorsa, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.
    b. Fare clic su **Backup**.
11. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Eseguire il backup del gruppo di risorse dei volumi dell'applicazione

È possibile eseguire il backup del gruppo di risorse contenente solo volumi applicativi o una combinazione di volumi applicativi e database. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

Se il gruppo di risorse dispone di più volumi di applicazioni, tutti i volumi di applicazioni devono disporre di una policy di replica SnapMirror o SnapVault.

A proposito di questa attività

Per impostazione predefinita, vengono creati i backup del gruppo di coerenza (CG). Se si desidera creare backup basati su volume, impostare il valore **EnableOracleNdvVolumeBasedBackup** su true nel file *web.config*.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Resources**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).

   È possibile eseguire una ricerca nel gruppo di risorse immettendo il nome del gruppo di risorse nella casella di ricerca oppure facendo clic su , quindi selezionando il tag. È quindi possibile fare clic su per chiudere il riquadro del filtro.

3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi fare clic su **Esegui backup ora**.
4. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se sono stati associati più criteri al gruppo di risorse, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

b. Fare clic su **Backup**.

5. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

L'operazione di verifica verrà eseguita solo per i database e non per i volumi dell'applicazione.

Clonare il backup del volume dell'applicazione

È possibile utilizzare SnapCenter per clonare i backup dei volumi dell'applicazione.

Prima di iniziare

Se il plug-in è stato installato come utente non root, è necessario assegnare manualmente le autorizzazioni di esecuzione alle directory prescrittt e postscript.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Resources**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Application Volume** (Volume applicazione) dall'elenco **View** (Visualizza).
3. Selezionare il volume dell'applicazione dalla vista dettagli volume dell'applicazione o dalla vista dettagli gruppo di risorse.

   Viene visualizzata la pagina della topologia del volume dell'applicazione.

4. Dalla vista Manage Copies (Gestisci copie), selezionare i backup da Local Copies (copie locali) (primarie), Mirror Copies (copie mirror) (secondarie) o Vault Copies (copie vault) (secondarie).
5. Selezionare il backup dalla tabella, quindi fare clic su * *  .
6. Nella pagina Location (posizione), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Host plug-in	Selezionare l'host in cui si desidera creare il clone.
Nome risorsa di destinazione	Specificare il nome della risorsa.

7. Nella pagina script, specificare i nomi degli script da eseguire prima della clonazione, i comandi per montare un file system e i nomi degli script da eseguire dopo la clonazione.
8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report**.

Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

9. Esaminare il riepilogo, quindi fare clic su **fine**.

Dividere un clone di un volume applicativo

È possibile utilizzare SnapCenter per separare una risorsa clonata dalla risorsa principale. Il clone diviso diventa indipendente dalla risorsa padre.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Resources**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Application Volume** (Volume applicazione) dall'elenco **View** (Visualizza).
3. Selezionare la risorsa clonata e fare clic su  .
4. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
5. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Eliminare un clone del volume dell'applicazione

È possibile eliminare i cloni se non sono più necessari. Non è possibile eliminare cloni che agiscono come origine per altri cloni.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Resources**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Application Volume** (Volume applicazione) dall'elenco **View** (Visualizza).
3. Selezionare la risorsa o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **cloni** dai sistemi di storage primario o secondario (mirrorati o replicati).
5. Selezionare il clone, quindi fare clic su  .
6. Nella pagina Delete Clone (Elimina clone), eseguire le seguenti operazioni:
   a. Nel campo **Pre clone delete**, immettere i nomi degli script da eseguire prima di eliminare il clone.
   b. Nel campo **Unmount**, immettere i comandi per smontare il clone prima di eliminarlo.
7. Fare clic su **OK**.

Proteggere i file system Windows

Concetti relativi al plug-in SnapCenter per Microsoft Windows

Panoramica del plug-in SnapCenter per Microsoft Windows

Il plug-in SnapCenter per Microsoft Windows è un componente sul lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati applicativa delle risorse del file system Microsoft. Inoltre, fornisce il provisioning dello storage, la coerenza di Snapshot e il recupero di spazio per file system Windows. Il plug-in per Windows automatizza le operazioni di backup, ripristino e clonazione del file system nell'ambiente SnapCenter.

Una volta installato il plug-in per Windows, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror dei set di backup su un altro volume e con la tecnologia NetApp SnapVault per eseguire la replica del backup disk-to-disk per l'archiviazione o la conformità agli standard.

Operazioni che è possibile eseguire con il plug-in SnapCenter per Microsoft Windows

Una volta installato il plug-in per Windows nell'ambiente, è possibile utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei file system Windows. È inoltre possibile eseguire attività a supporto di tali operazioni.

- Scopri le risorse
- Eseguire il backup dei file system Windows
- Pianificare le operazioni di backup
- Ripristinare i backup del file system
- Clonare i backup del file system
- Monitorare le operazioni di backup, ripristino e clonazione

Il plug-in per Windows non supporta il backup e il ripristino dei file system sulle condivisioni SMB.

Funzionalità del plug-in SnapCenter per Windows

Il plug-in per Windows si integra con la tecnologia Snapshot di NetApp nel sistema di storage. Per utilizzare il plug-in per Windows, utilizzare l'interfaccia SnapCenter.

Il plug-in per Windows include le seguenti funzionalità principali:

- **Interfaccia utente grafica unificata con tecnologia SnapCenter**

  L'interfaccia SnapCenter offre standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia di SnapCenter consente di completare processi di backup e ripristino coerenti tra i plug-in, utilizzare report

centralizzati, utilizzare visualizzazioni dashboard a colpo d'occhio, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi in tutti i plug-in. SnapCenter offre inoltre la pianificazione centralizzata e la gestione delle policy per supportare le operazioni di backup e clonazione.

- **Amministrazione centrale automatizzata**

  È possibile pianificare backup di routine del file system, configurare la conservazione dei backup basata su policy e impostare le operazioni di ripristino. È inoltre possibile monitorare in modo proattivo l'ambiente del file system configurando SnapCenter per l'invio di avvisi e-mail.

- **Tecnologia istantanea NetApp senza interruzioni**

  Il plug-in per Windows utilizza la tecnologia Snapshot di NetApp. In questo modo, è possibile eseguire il backup dei file system in pochi secondi e ripristinarli rapidamente senza interrompere la linea dell'host. Le snapshot consumano una quantità minima di spazio storage.

Oltre a queste funzionalità principali, il plug-in per Windows offre i seguenti vantaggi:

- Supporto del workflow di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli
- Creazione di copie efficienti in termini di spazio dei file system di produzione per il test o l'estrazione dei dati utilizzando la tecnologia FlexClone di NetApp

  Per informazioni sulle licenze di FlexClone, vedere "Licenze SnapCenter".

- Possibilità di eseguire più backup contemporaneamente su più server
- Cmdlet PowerShell per lo scripting delle operazioni di backup, ripristino e clonazione
- Supporto per il backup di file system e dischi di macchine virtuali (VMDK)
- Supporto per infrastrutture fisiche e virtualizzate
- Supporto per iSCSI, Fibre Channel, FCoE, RDM (raw device mapping), ALM (Asymmetric LUN Mapping), VMDK su NFS e VMFS e FC virtuale

Come SnapCenter esegue il backup dei file system Windows

SnapCenter utilizza la tecnologia Snapshot per eseguire il backup delle risorse del file system Windows che risiedono su LUN, volumi CSV (Cluster Shared Volumes), volumi RDM (raw device mapping), ALM (Asymmetric LUN mapping) nei cluster Windows e VMDK basati su VMFS/NFS (VMware Virtual Machine file System using NFS).

SnapCenter crea backup creando Snapshot dei file system. I backup federati, in cui un volume contiene LUN da più host, sono più rapidi ed efficienti rispetto ai backup di ogni singolo LUN, in quanto viene creata una sola Snapshot del volume rispetto alle singole Snapshot di ogni file system.

Quando SnapCenter crea una Snapshot, l'intero volume del sistema storage viene acquisito nella Snapshot. Tuttavia, il backup è valido solo per il server host per il quale è stato creato il backup.

Se i dati di altri server host si trovano sullo stesso volume, non è possibile ripristinarli dalla Snapshot.

Se un file system Windows contiene un database, il backup del file system non equivale a quello del database. Per eseguire il backup di un database, è necessario utilizzare uno dei plug-in del database.

Tipi di storage supportati dai plug-in SnapCenter per Microsoft Windows

SnapCenter supporta un'ampia gamma di tipi di storage su macchine fisiche e virtuali. Prima di installare il pacchetto per l'host, è necessario verificare se il supporto è disponibile per il tipo di storage in uso.

Il provisioning SnapCenter e il supporto per la protezione dei dati sono disponibili su Windows Server. Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Macchina	Tipo di storage	Eseguire il provisioning utilizzando	Note di supporto
Server fisico	LUN connessi a FC	Interfaccia grafica utente (GUI) o cmdlet PowerShell di SnapCenter	
Server fisico	LUN connessi a iSCSI	GUI SnapCenter o cmdlet PowerShell	
Server fisico	Condivisioni SMB3 (CIFS) che risiedono su una macchina virtuale di storage (SVM)	GUI SnapCenter o cmdlet PowerShell	Supporto solo per il provisioning. Non è possibile utilizzare SnapCenter per eseguire il backup di dati o condivisioni utilizzando il protocollo SMB.
Macchina virtuale VMware	LUN RDM collegati da un HBA FC o iSCSI	Cmdlet PowerShell	
Macchina virtuale VMware	LUN iSCSI collegati direttamente al sistema guest dall'iniziatore iSCSI	GUI SnapCenter o cmdlet PowerShell	
Macchina virtuale VMware	Virtual Machine file Systems (VMFS) o datastore NFS	VMware vSphere	

Macchina	Tipo di storage	Eseguire il provisioning utilizzando	Note di supporto
Macchina virtuale VMware	Un sistema guest connesso alle condivisioni SMB3 che risiedono su una SVM	GUI SnapCenter o cmdlet PowerShell	Supporto solo per il provisioning. Non è possibile utilizzare SnapCenter per eseguire il backup di dati o condivisioni utilizzando il protocollo SMB.
Macchina virtuale Hyper-V.	LUN Virtual FC (VFC) collegate da uno switch Fibre Channel virtuale	GUI SnapCenter o cmdlet PowerShell	È necessario utilizzare Hyper-V Manager per eseguire il provisioning dei LUN Virtual FC (VFC) collegati da uno switch Fibre Channel virtuale. I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti sullo storage NetApp non sono supportati.
Macchina virtuale Hyper-V.	LUN iSCSI collegati direttamente al sistema guest dall'iniziatore iSCSI	GUI SnapCenter o cmdlet PowerShell	I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti sullo storage NetApp non sono supportati.

Macchina	Tipo di storage	Eseguire il provisioning utilizzando	Note di supporto
Macchina virtuale Hyper-V.	Un sistema guest connesso alle condivisioni SMB3 che risiedono su una SVM	GUI SnapCenter o cmdlet PowerShell	Supporto solo per il provisioning. Non è possibile utilizzare SnapCenter per eseguire il backup di dati o condivisioni utilizzando il protocollo SMB. I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti sullo storage NetApp non sono supportati.

Privilegi minimi di ONTAP richiesti per il plug-in di Windows

I privilegi minimi di ONTAP richiesti variano in base ai plug-in di SnapCenter utilizzati per la protezione dei dati.

- All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
  - event generate-autosupport-log
  - mostra la cronologia dei lavori
  - interruzione del lavoro
  - lun
  - lun create (crea lun)
  - lun delete (elimina lun)
  - lun igroup add
  - lun igroup create
  - lun igroup delete (elimina igroup lun)
  - lun igroup rename (rinomina lun igroup)
  - lun igroup show
  - lun mapping add-reporting-node
  - creazione mappatura lun
  - eliminazione della mappatura lun

- nodi di remove-reporting-mapping lun
- visualizzazione della mappatura del lun
- modifica del lun
- lun move-in-volume
- lun offline
- lun online
- ridimensionamento del lun
- lun seriale
- lun show
- regola aggiuntiva del criterio snapmirror
- regola-modifica del criterio snapmirror
- regola di rimozione del criterio snapmirror
- policy di snapmirror
- ripristino di snapmirror
- spettacolo di snapmirror
- storia di snapmirror
- aggiornamento di snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione del clone del volume
- visualizzazione del clone del volume
- avvio della divisione del clone del volume
- interruzione della divisione del clone del volume
- creazione del volume
- distruggere il volume
- creazione del clone del file di volume
- file di volume show-disk-usage
- volume offline
- volume online
- modifica del volume
- creazione del qtree del volume
- eliminazione del qtree del volume
- modifica del qtree del volume
- visualizzazione del qtree del volume
- limitazione del volume
- presentazione del volume

    - creazione di snapshot di volume
    - eliminazione dello snapshot del volume
    - modifica dello snapshot del volume
    - rinominare lo snapshot del volume
    - ripristino dello snapshot del volume
    - file di ripristino dello snapshot del volume
    - visualizzazione di snapshot di volume
    - smontare il volume
    - cifs vserver
    - creazione condivisione cifs vserver
    - eliminazione condivisione cifs vserver
    - vserver cifs shadowcopy mostra
    - show di condivisione di vserver cifs
    - vserver cifs show
    - policy di esportazione di vserver
    - creazione policy di esportazione vserver
    - eliminazione della policy di esportazione di vserver
    - creazione della regola dei criteri di esportazione di vserver
    - visualizzazione della regola dei criteri di esportazione di vserver
    - visualizzazione della policy di esportazione di vserver
    - iscsi vserver
    - visualizzazione della connessione iscsi del vserver
    - show di vserver
- Comandi di sola lettura: Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete
    - visualizzazione dell'interfaccia di rete
    - server virtuale

Preparazione dei sistemi storage per la replica di SnapMirror e SnapVault

È possibile utilizzare un plug-in SnapCenter con la tecnologia SnapMirror di ONTAP per creare copie mirror dei set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replica del backup disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti di SnapMirror e SnapVault al termine dell'operazione di Snapshot. Gli aggiornamenti di SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter; non creare una pianificazione ONTAP separata.

Se vieni a SnapCenter da un prodotto NetApp SnapManager e sei soddisfatto delle relazioni di protezione dei dati che hai configurato, puoi saltare questa sezione.

Una relazione di protezione dei dati replica i dati sullo storage primario (il volume di origine) nello storage secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui fa riferimento il volume di origine al volume di destinazione.

SnapCenter non supporta le relazioni a cascata tra SnapMirror e i volumi SnapVault (**primario** > **Mirror** > **Vault**). Si consiglia di utilizzare le relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per ulteriori informazioni sulle relazioni di SnapMirror flessibili per la versione e sulla loro configurazione, vedere la "Documentazione ONTAP".

SnapCenter non supporta la replica **Sync_mirror**.

Definire una strategia di backup per i file system Windows

La definizione di una strategia di backup prima della creazione dei backup fornisce i backup necessari per ripristinare o clonare correttamente i file system. Il tuo SLA (Service-Level Agreement), RTO (Recovery Time Objective) e RPO (Recovery Point Objective) determinano in gran parte la tua strategia di backup.

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. RTO è il momento in cui un processo di business deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

Pianificazioni di backup per file system Windows

La frequenza di backup viene specificata nei criteri; nella configurazione del gruppo di risorse viene specificata una pianificazione di backup. Il fattore più critico per determinare una frequenza o una pianificazione di backup è il tasso di cambiamento per la risorsa e l'importanza dei dati. È possibile eseguire il backup di una risorsa utilizzata in modo pesante ogni ora, mentre è possibile eseguire il backup di una risorsa utilizzata raramente una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo Service Level Agreement (SLA) e il tuo Recover Point Objective (RPO).

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. Un RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA e RPO contribuiscono alla strategia di protezione dei dati.

Anche per una risorsa molto utilizzata, non è necessario eseguire un backup completo più di una o due volte al giorno.

Le pianificazioni dei backup sono in due parti, come segue:

- Frequenza di backup

  La frequenza di backup (con quale frequenza devono essere eseguiti i backup), denominata *tipo di pianificazione* per alcuni plug-in, fa parte di una configurazione di policy. Ad esempio, è possibile

configurare la frequenza di backup come orario, giornaliero, settimanale o mensile oppure specificare **Nessuno** che rende la policy una policy solo on-demand. Puoi accedere alle policy facendo clic su **Impostazioni** > **politiche**.

- Pianificazioni di backup

  Le pianificazioni di backup (esattamente quando devono essere eseguiti i backup) fanno parte di una configurazione di gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione per il backup ogni giovedì alle 10:00. È possibile accedere alle pianificazioni dei gruppi di risorse facendo clic su **risorse** > **gruppi di risorse**.

Numero di backup necessari per i file system Windows

I fattori che determinano il numero di backup necessari includono le dimensioni del file system Windows, il numero di volumi utilizzati, la velocità di modifica del file system e il contratto SLA (Service Level Agreement).

Convenzione di naming del backup per i file system Windows

I backup dei file system di Windows utilizzano la convenzione di denominazione predefinita di Snapshot. La convenzione di denominazione predefinita dei backup aggiunge un indicatore data e ora ai nomi Snapshot che consente di identificare quando le copie sono state create.

L'istantanea utilizza la seguente convenzione di denominazione predefinita: Resourcegroupname_hostname_timestamp

È necessario assegnare un nome logico ai gruppi di risorse di backup, come nell'esempio seguente:

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

In questo esempio, gli elementi di sintassi hanno i seguenti significati:

- `dts1` è il nome del gruppo di risorse.
- `mach1x88` è il nome host.
- `03-12-2016_23.17.26` indica la data e l'ora.

Quando si crea un backup, è possibile aggiungere anche un tag descrittivo per identificare il backup. Al contrario, se si desidera utilizzare una convenzione di denominazione del backup personalizzata, è necessario rinominare il backup al termine dell'operazione.

Opzioni di conservazione del backup

È possibile scegliere il numero di giorni per i quali conservare le copie di backup o specificare il numero di copie di backup che si desidera conservare, fino a un massimo di 255 copie ONTAP. Ad esempio, l'organizzazione potrebbe richiedere di conservare 10 giorni di copie di backup o 130 copie di backup.

Durante la creazione di un criterio, è possibile specificare le opzioni di conservazione per il tipo di backup e il tipo di pianificazione.

Se si imposta la replica di SnapMirror, il criterio di conservazione viene mirrorato sul volume di destinazione.

SnapCenter elimina i backup conservati con etichette di conservazione corrispondenti al tipo di pianificazione.

Se il tipo di pianificazione è stato modificato per la risorsa o il gruppo di risorse, i backup con la vecchia etichetta del tipo di pianificazione potrebbero rimanere nel sistema.

Per la conservazione a lungo termine delle copie di backup, è necessario utilizzare il backup di SnapVault.

Origini e destinazioni dei cloni per file system Windows

È possibile clonare un backup del file system dallo storage primario o secondario. È inoltre possibile scegliere la destinazione che supporta i requisiti, ovvero la posizione di backup originale o una destinazione diversa sullo stesso host o su un host diverso. La destinazione deve trovarsi sullo stesso volume del backup di origine del clone.

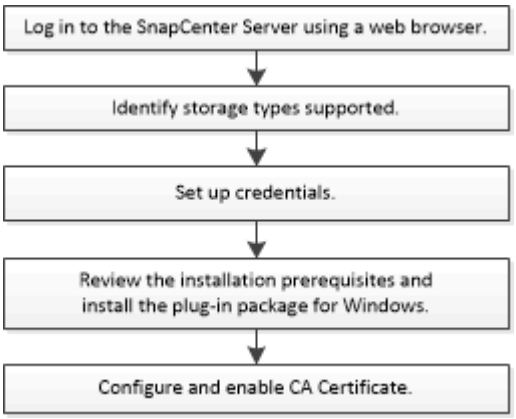
Clonare la destinazione	Descrizione
Originale, origine, posizione	Per impostazione predefinita, SnapCenter memorizza il clone nella stessa posizione e nello stesso host del backup clonato.
Posizione diversa	È possibile memorizzare il clone in una posizione diversa sullo stesso host o su un altro host. L'host deve disporre di una connessione configurata alla macchina virtuale di storage (SVM).

È possibile rinominare il clone una volta completata l'operazione.

Installare il plug-in SnapCenter per Microsoft Windows

Workflow di installazione del plug-in SnapCenter per Microsoft Windows

Se si desidera proteggere i file di SnapCenter che non sono file di database, è necessario installare e configurare il plug-in di Microsoft Windows.



Requisiti di installazione del plug-in SnapCenter per Microsoft Windows

Prima di installare il plug-in per Windows, è necessario conoscere alcuni requisiti di installazione.

Prima di iniziare a utilizzare il plug-in per Windows, l'amministratore di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività dei prerequisiti.

- Per installare il plug-in per Windows, è necessario disporre dei privilegi di amministratore di SnapCenter.

  Il ruolo di amministratore di SnapCenter deve disporre dei privilegi di amministratore.

- È necessario aver installato e configurato il server SnapCenter.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.
- Se si desidera eseguire la replica di backup, è necessario configurare SnapMirror e SnapVault.

Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario conoscere alcuni requisiti di base relativi allo spazio del sistema host e al dimensionamento.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	5 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.

Elemento	Requisiti
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp". Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet."

Impostare le credenziali per il plug-in per Windows

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. È necessario creare credenziali per l'installazione dei plug-in di SnapCenter e credenziali aggiuntive per l'esecuzione delle operazioni di protezione dei dati sui file system di Windows.

Cosa ti serve

- Prima di installare i plug-in, è necessario impostare le credenziali di Windows.
- È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore, sull'host remoto.
- Se si impostano le credenziali per singoli gruppi di risorse e l'utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup all'utente.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.
4. Nella pagina Credential, effettuare le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale	Immettere un nome per le credenziali.

Per questo campo…	Eseguire questa operazione…
Nome utente/Password	Immettere il nome utente e la password utilizzati per l'autenticazione. • Amministratore di dominio o qualsiasi membro del gruppo di amministratori Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono i seguenti: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Amministratore locale (solo per gruppi di lavoro) Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host. Il formato valido per il campo Nome utente è il seguente: `UserName` Non utilizzare virgolette doppie (") o backtick (`) nelle password. Non utilizzare il valore inferiore a (<) e il punto esclamativo (!) simboli insieme nelle password. Ad esempio, meno di<!10, meno di 10<!, backtick`12.
Password	Inserire la password utilizzata per l'autenticazione.

5. Fare clic su **OK**.

   Al termine dell'impostazione delle credenziali, è possibile assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina User and Access (utenti e accesso).

Configurare gMSA su Windows Server 2012 o versione successiva

Windows Server 2012 o versione successiva consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatica delle password dell'account di servizio da un account di dominio gestito.

Prima di iniziare

- È necessario disporre di un controller di dominio Windows Server 2012 o versione successiva.
- È necessario disporre di un host Windows Server 2012 o versione successiva, membro del dominio.

Fasi

1. Creare una chiave root KDS per generare password univoche per ogni oggetto in gMSA.
2. Per ciascun dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Creare e configurare gMSA:
   a. Creare un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo di utenti appena creato per creare gMSA.
```

   Ad esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Eseguire `Get-ADServiceAccount` il comando per verificare
l'account del servizio.
```

4. Configurare gMSA sugli host:
   a. Attivare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

   A tale scopo, eseguire il seguente comando da PowerShell:

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

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


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

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Riavviare l'host.

b. Installare gMSA sull'host eseguendo il comando seguente dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verificare il proprio account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter.

   Il server SnapCenter installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

Aggiungere host e installare il plug-in SnapCenter per Microsoft Windows

È possibile utilizzare la pagina Aggiungi host di SnapCenter per aggiungere host Windows. Il plug-in SnapCenter per Microsoft Windows viene installato automaticamente sull'host specificato. Questo è il metodo consigliato per installare i plug-in. È possibile aggiungere un host e installare un plug-in per un singolo host o per un cluster.

Prima di iniziare

- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.
- L'utente SnapCenter deve essere aggiunto al ruolo "accesso come servizio" del server Windows.
- Assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi

amministrativi.

"Configurare l'account di servizio gestito di gruppo su Windows Server 2012 o versione successiva per il file system di Windows"

A proposito di questa attività

- Non è possibile aggiungere un server SnapCenter come host plug-in a un altro server SnapCenter.
- Plug-in di Windows
  - Microsoft Windows
  - Server Microsoft Exchange
  - Microsoft SQL Server
  - SAP HANA
  - Plug-in personalizzati
- Installazione dei plug-in su un cluster

  Se si installano plug-in su un cluster (WSFC, Oracle RAC o Exchange DAG), questi vengono installati su tutti i nodi del cluster.

- Storage e-Series

  Non è possibile installare il plug-in per Windows su un host Windows connesso allo storage e-series.

SnapCenter non supporta l'aggiunta dello stesso host (host plug-in) a SnapCenter se l'host fa già parte di un gruppo di lavoro e viene modificato in un altro dominio o viceversa. Se si desidera aggiungere lo stesso host, rimuovere l'host da SnapCenter e aggiungerlo di nuovo.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Assicurarsi che nella parte superiore sia selezionato **Managed hosts**.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, effettuare le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare il tipo di host **Windows**. Il server SnapCenter aggiunge l'host e installa il plug-in per Windows, se non è già installato sull'host.

Per questo campo…	Eseguire questa operazione…
Nome host	Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire il nome di dominio completo (FQDN). È possibile immettere gli indirizzi IP o il nome FQDN di uno dei seguenti elementi: • Host standalone • Clustering di failover di Windows Server (WSFC) Se si aggiunge un host utilizzando SnapCenter e fa parte di un sottodominio, è necessario fornire l'FQDN.
Credenziali	Selezionare il nome della credenziale creata o creare le nuove credenziali. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere la sezione relativa alla creazione di una credenziale. I dettagli relativi alle credenziali, inclusi nome utente, dominio e tipo di host, vengono visualizzati posizionando il cursore sul nome della credenziale fornito. La modalità di autenticazione è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare i plug-in da installare.

   Per le nuove implementazioni, non sono elencati pacchetti plug-in.

6. (Facoltativo) fare clic su **altre opzioni**.

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.
Percorso di installazione	Il percorso predefinito è C:/Program Files/NetApp/SnapCenter. È possibile personalizzare il percorso. Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C: File di programma. Tuttavia, se lo si desidera, è possibile personalizzare il percorso predefinito.
Aggiungere tutti gli host nel cluster	Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un WSFC.
Ignorare i controlli di preinstallazione	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.
Utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in	Selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in. Fornire il nome gMSA nel seguente formato: *Domainname/accountName*. GMSA verrà utilizzato come account del servizio di accesso solo per il servizio del plug-in SnapCenter per Windows.

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo **Ignora controlli preliminari**, l'host viene convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione PowerShell, . La versione NETTA e la posizione vengono convalidate in base ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati.

Se l'errore è relativo allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in `C:\Program Files\NetApp\SnapCenter` WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

In una configurazione ha, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Monitorare l'avanzamento dell'installazione.

Installare il plug-in SnapCenter per Microsoft Windows su più host remoti utilizzando i cmdlet PowerShell

Se si desidera installare il plug-in SnapCenter per Microsoft Windows su più host contemporaneamente, è possibile utilizzare il `Install-SmHostPackage` cmdlet PowerShell.

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare i plug-in.

Fasi

1. Avviare PowerShell.
2. Sull'host del server SnapCenter, stabilire una sessione utilizzando il `Open-SmConnection` cmdlet, quindi immettere le credenziali.
3. Aggiungere l'host standalone o il cluster a SnapCenter utilizzando il `Add-SmHost` cmdlet e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

4. Installare il plug-in su più host utilizzando il `Install-SmHostPackage` cmdlet e i parametri richiesti.

   È possibile utilizzare `-skipprecheck` l'opzione quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

Installare il plug-in SnapCenter per Microsoft Windows in modo invisibile dalla riga di comando

È possibile installare il plug-in SnapCenter per Microsoft Windows localmente su un host Windows se non si riesce a installare il plug-in in remoto dall'interfaccia grafica di SnapCenter. È possibile eseguire il plug-in SnapCenter per il programma di installazione di Microsoft Windows senza supervisione, in modalità silenziosa, dalla riga di comando di Windows.

Prima di iniziare

- È necessario aver installato Microsoft .Net 4.7.2 o versione successiva.
- PowerShell 4.0 o versione successiva deve essere installato.
- È necessario aver attivato la funzione di accodamento dei messaggi di Windows.

- È necessario essere un amministratore locale dell'host.

Fasi

1. Scaricare il plug-in SnapCenter per Microsoft Windows dal percorso di installazione.

   Ad esempio, il percorso di installazione predefinito è C: ProgramData/NetApp/SnapCenter/Package Repository.

   Questo percorso è accessibile dall'host in cui è installato il server SnapCenter.

2. Copiare il file di installazione nell'host su cui si desidera installare il plug-in.
3. Dal prompt dei comandi, accedere alla directory in cui è stato scaricato il file di installazione.
4. Immettere il seguente comando, sostituendo le variabili con i dati:

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   Ad esempio:

   ```
   `"C:\ProgramData\NetApp\SnapCenter\Package Repository
   \snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
   \HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
   SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
   BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW`
   ```

   Tutti i parametri passati durante l'installazione del plug-in per Windows sono sensibili al maiuscolo/minuscolo.

   Inserire i valori per le seguenti variabili:

Variabile	Valore
/debuglog"<Debug_Log_Path>	Specificare il nome e la posizione del file di log del programma di installazione della suite, come nell'esempio seguente: setup.exe /debuglog"C: PathToLog setupexe.log".
PORTA_BI_SNAPCENTER	Specificare la porta su cui SnapCenter comunica con SMCore.
SUITE_INSTALLDIR	Specificare la directory di installazione del pacchetto del plug-in host.
BI_SERVICEACCOUNT	Specificare il plug-in SnapCenter per l'account del servizio Web Microsoft Windows.

Variabile	Valore
BI_SERVICEPWD	Specificare la password per l'account del servizio Web di SnapCenter per il plug-in Microsoft Windows.
ISFeatureInstall	Specificare la soluzione da implementare da SnapCenter sull'host remoto.

Il parametro *debuglog* include il percorso del file di log per SnapCenter. La scrittura in questo file di log è il metodo preferito per ottenere informazioni sulla risoluzione dei problemi, poiché il file contiene i risultati dei controlli eseguiti dall'installazione per verificare i prerequisiti del plug-in.

Se necessario, è possibile trovare ulteriori informazioni per la risoluzione dei problemi nel file di registro del pacchetto SnapCenter per Windows. I file di log per il pacchetto sono elencati (per primi quelli meno recenti) nella cartella *%Temp%*, ad esempio _C:.

L'installazione del plug-in per Windows registra il plug-in sull'host e non sul server SnapCenter. È possibile registrare il plug-in sul server SnapCenter aggiungendo l'host utilizzando l'interfaccia grafica di SnapCenter o il cmdlet PowerShell. Una volta aggiunto l'host, il plug-in viene rilevato automaticamente.

Monitorare lo stato di installazione del pacchetto plug-in SnapCenter

È possibile monitorare lo stato di avanzamento dell'installazione del pacchetto plug-in di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento dell'installazione per determinare quando è completa o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filter** (filtro).
   b. Facoltativo: Specificare la data di inizio e di fine.

c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).
d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.
e. Fare clic su **Apply** (Applica).

4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Configurare il certificato CA

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare una CSR, vedere "Come generare il file CSR del certificato CA".

Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato del file di importazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
   c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
   d. Copiare i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

      Get-ChildItem -Path Certate: LocalMachine/My

   b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

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

   Ad esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in
   dell'host Windows eseguendo i seguenti comandi:
   ```

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

   Ad esempio:

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

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.

3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.
5. Selezionare **attiva convalida certificato**.

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- * * Indica che il certificato CA non è né abilitato né assegnato all'host del plug-in.
- * * Indica che il certificato CA è stato convalidato correttamente.
- * * Indica che il certificato CA non può essere convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Installare il plug-in SnapCenter per VMware vSphere

Se il database o il file system sono memorizzati su macchine virtuali (VM), o se si desidera proteggere macchine virtuali e datastore, è necessario implementare il plug-in SnapCenter per l'appliance virtuale VMware vSphere.

Per informazioni sulla distribuzione, vedere "Panoramica sull'implementazione".

Implementare il certificato CA

Per configurare il certificato CA con il plug-in SnapCenter per VMware vSphere, vedere "Creare o importare un certificato SSL".

Configurare il file CRL

Il plug-in SnapCenter per VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il plug-in SnapCenter per VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Eseguire il backup dei file system Windows

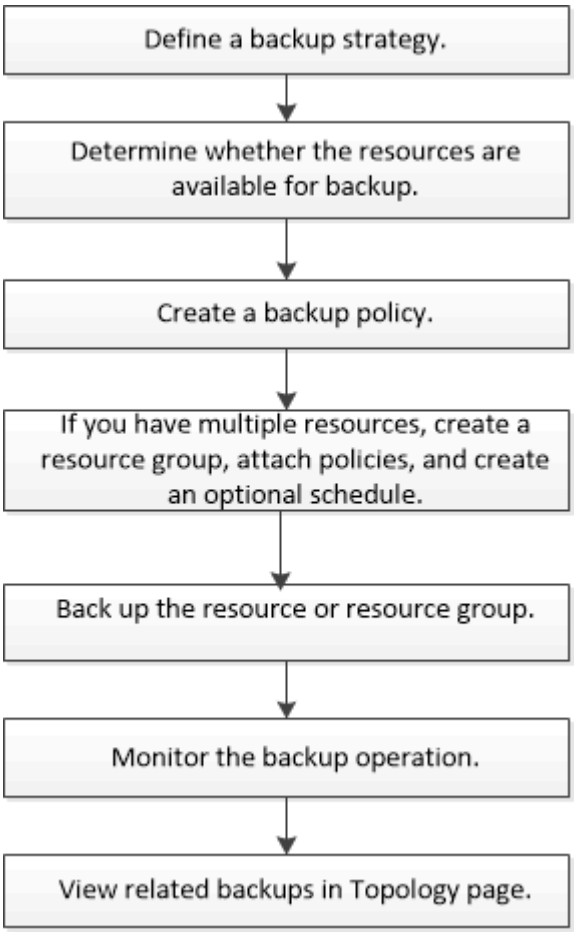
Eseguire il backup dei file system Windows

Quando si installa il plug-in SnapCenter per Microsoft Windows nell'ambiente in uso, è possibile utilizzare SnapCenter per eseguire il backup dei file system Windows. È possibile eseguire il backup di un singolo file system o di un gruppo di risorse che contiene più file system. È possibile eseguire il backup on-demand o in base a un programma di protezione definito.

È possibile pianificare più backup per l'esecuzione simultanea tra i server. Le operazioni di backup e ripristino

non possono essere eseguite contemporaneamente sulla stessa risorsa.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di backup:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida dei cmdlet di SnapCenter o "Guida di riferimento al cmdlet del software SnapCenter" contiene informazioni dettagliate sui cmdlet di PowerShell.

Determinare la disponibilità delle risorse per i file system Windows

Le risorse sono le LUN e i componenti simili nel file system gestiti dai plug-in installati. È possibile aggiungere tali risorse ai gruppi di risorse in modo da poter eseguire lavori di protezione dei dati su più risorse, ma prima è necessario identificare le risorse disponibili. La ricerca delle risorse disponibili verifica inoltre che l'installazione del plug-in sia stata completata correttamente.

Prima di iniziare

- È necessario aver già completato attività come l'installazione del server SnapCenter, l'aggiunta di host, la creazione di connessioni alle macchine virtuali di storage (SVM) e l'aggiunta di credenziali.
- Se i file risiedono su LUN o VMDK VMware RDM, è necessario implementare il plug-in SnapCenter per VMware vSphere e registrare il plug-in con SnapCenter. Per ulteriori informazioni, vedere "Plug-in SnapCenter per la documentazione di VMware vSphere".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **file Systems** dall'elenco.
3. Selezionare l'host per filtrare l'elenco di risorse, quindi fare clic su **Refresh Resources** (Aggiorna risorse).

   I file system appena aggiunti, rinominati o cancellati vengono aggiornati all'inventario del server SnapCenter.

   È necessario aggiornare le risorse se i database vengono rinominati al di fuori di SnapCenter.

Creare criteri di backup per i file system Windows

È possibile creare un nuovo criterio di backup per le risorse prima di utilizzare SnapCenter per eseguire il backup dei file system Windows oppure creare un nuovo criterio di backup al momento della creazione di un gruppo di risorse o del backup di una risorsa.

Prima di iniziare

- È necessario aver definito la strategia di backup. "Scopri di più"
- Devi essere preparato per la protezione dei dati.

  Per prepararsi alla protezione dei dati, è necessario completare attività come l'installazione di SnapCenter, l'aggiunta di host, il rilevamento delle risorse e la creazione di connessioni di storage virtual machine (SVM).

- Se si stanno replicando Snapshot in uno storage secondario mirror o vault, l'amministratore di SnapCenter deve aver assegnato le SVM per i volumi di origine e di destinazione.
- Se si desidera eseguire gli script PowerShell in prescripts e postscripts, impostare il valore del parametro usePowershellProcessforScripts su true nel file web.config.

  Il valore predefinito è false

- Per SnapMirror Business Continuity (SM-BC), per ulteriori informazioni sui prerequisiti e sulle limitazioni, fare riferimento a "Limiti a oggetti per la business continuity di SnapMirror".

A proposito di questa attività

- IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

  Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

  È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- SnapLock
  - Se è selezionata l'opzione "conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere minore o uguale ai giorni di conservazione menzionati.

- La specifica di un periodo di blocco snapshot impedisce l'eliminazione delle istantanee fino alla scadenza del periodo di conservazione. Questo potrebbe portare a mantenere un numero di Snapshot maggiore del conteggio specificato nel criterio.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Le impostazioni SnapLock primarie vengono gestite nel criterio di backup SnapCenter e le impostazioni SnapLock secondarie vengono gestite da ONTAP.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Per determinare se è possibile utilizzare un criterio esistente, selezionare il nome del criterio e fare clic su **Dettagli**.

   Dopo aver esaminato i criteri esistenti, è possibile eseguire una delle seguenti operazioni:

   - Utilizzare una policy esistente.
   - Copiare un criterio esistente e modificare la configurazione del criterio.
   - Creare una nuova policy.
4. Per creare un nuovo criterio, fare clic su **nuovo**.
5. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
6. Nella pagina Backup Options (Opzioni di backup), eseguire le seguenti operazioni:

   a. Selezionare un'impostazione di backup.

Opzione	Descrizione
Backup coerente del file system	Scegliere questa opzione se si desidera che SnapCenter termini l'unità disco su cui si trova il file system prima dell'inizio dell'operazione di backup, quindi ripristini l'unità disco al termine dell'operazione di backup.
Backup coerente con il file system Crash	Scegliere questa opzione se non si desidera che SnapCenter disattivi il disco su cui risiede il file system.

   b. Selezionare una frequenza di pianificazione (chiamata anche tipo di policy).

      Il criterio specifica solo la frequenza di backup. La pianificazione di protezione specifica per il backup viene definita nel gruppo di risorse. Pertanto, due o più gruppi di risorse possono condividere la stessa policy e la stessa frequenza di backup, ma hanno diverse pianificazioni di backup.

      Se sono previste le 2:00, la programmazione non verrà attivata durante l'ora legale (DST).
7. Nella pagina di conservazione, specificare le impostazioni di conservazione per i backup on-demand e per

ciascuna frequenza di pianificazione selezionata.

Opzione	Descrizione
Copie Snapshot totali da conservare	Scegliere questa opzione se si desidera specificare il numero di archivi SnapCenter istantanee prima di eliminarli automaticamente.
Elimina copie Snapshot precedenti a.	Scegliere questa opzione se si desidera specificare il numero di giorni in cui SnapCenter conserva una copia di backup prima di eliminarla.
Periodo di blocco della copia snapshot	Selezionare periodo di blocco istantanea e selezionare giorni, mesi o anni. Il periodo di conservazione di SnapLock deve essere inferiore a 100 anni.

È necessario impostare il conteggio di conservazione su 2 o superiore. Il valore minimo per il conteggio di conservazione è 2.

Il valore massimo di conservazione è 1018 per le risorse su ONTAP 9.4 o versioni successive e 254 per le risorse su ONTAP 9.3 o versioni precedenti. I backup non avranno esito positivo se la conservazione viene impostata su un valore superiore a quello supportato dalla versione di ONTAP sottostante.

8. Nella pagina Replication (Replica), specificare la replica nel sistema di storage secondario:

Per questo campo…	Eseguire questa operazione…
Aggiornare SnapMirror dopo aver creato una copia Snapshot locale	Selezionare questa opzione per creare copie mirror dei set di backup su un altro volume (SnapMirror). Questa opzione deve essere abilitata per SnapMirror Business Continuity (SM-BC). Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante **Aggiorna** nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP. Vedere "Visualizzare i backup e i cloni correlati nella pagina topologia".

Per questo campo…	Eseguire questa operazione…
Aggiornare SnapVault dopo aver creato una copia Snapshot	Selezionare questa opzione per eseguire la replica del backup disk-to-disk. Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante Aggiorna nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP. Quando SnapLock è configurato solo sul secondario da ONTAP noto come vault di SnapLock, facendo clic sul pulsante Aggiorna nella pagina topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP. Per ulteriori informazioni sul vault di SnapLock, vedere "Assegnare le copie Snapshot a WORM su una destinazione del vault"
Etichetta del criterio secondario	Selezionare un'etichetta Snapshot. A seconda dell'etichetta Snapshot selezionata, ONTAP applica la politica di conservazione Snapshot secondaria corrispondente all'etichetta. Se è stato selezionato **Update SnapMirror dopo la creazione di una copia Snapshot locale**, è possibile specificare l'etichetta del criterio secondario. Tuttavia, se è stato selezionato **Aggiorna SnapVault dopo la creazione di una copia Snapshot locale**, è necessario specificare l'etichetta del criterio secondario.
Numero tentativi di errore	Immettere il numero di tentativi di replica che devono verificarsi prima dell'arresto del processo.

È necessario configurare il criterio di conservazione SnapMirror in ONTAP per lo storage secondario, in modo da evitare di raggiungere il limite massimo di Snapshot sullo storage secondario.

9. Nella pagina script, immettere il percorso del prescrittore o del postscript che si desidera venga eseguito dal server SnapCenter rispettivamente prima o dopo l'operazione di backup e un limite di tempo che SnapCenter attende l'esecuzione dello script prima del timeout.

   Ad esempio, è possibile eseguire uno script per aggiornare i trap SNMP, automatizzare gli avvisi e inviare i registri.

Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

10. Esaminare il riepilogo, quindi fare clic su **fine**.

Creare gruppi di risorse per i file system Windows

Un gruppo di risorse è il container a cui è possibile aggiungere più file system che si desidera proteggere. È inoltre necessario associare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire, quindi specificare la pianificazione del backup.

A proposito di questa attività

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.
- L'aggiunta di nuovi file system senza SM-BC a un gruppo di risorse esistente che contiene risorse con SM-BC non è supportata.
- L'aggiunta di nuovi file system a un gruppo di risorse esistente in modalità di failover di SM-BC non è supportata. È possibile aggiungere risorse al gruppo di risorse solo in stato normale o di failback.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **file Systems** dall'elenco.

   Se di recente è stato aggiunto un file system a SnapCenter, fare clic su **Aggiorna risorse** per visualizzare la risorsa appena aggiunta.

3. Fare clic su **New Resource Group** (nuovo gruppo di risorse).
4. Nella pagina Nome della procedura guidata, effettuare le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere il nome del gruppo di risorse. Il nome del gruppo di risorse non deve superare i 250 caratteri.
USA il formato nome personalizzato per la copia Snapshot	Opzionale: Immettere un nome e un formato dell'istantanea personalizzato. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

Per questo campo…	Eseguire questa operazione…
Tag	Inserire un tag descrittivo per facilitare la ricerca di un gruppo di risorse.

5. Nella pagina risorse, eseguire le seguenti operazioni:

   a. Selezionare l'host per filtrare l'elenco delle risorse.

      Le risorse aggiunte di recente vengono visualizzate nell'elenco delle risorse disponibili solo dopo l'aggiornamento dell'elenco delle risorse.

   b. Nella sezione risorse disponibili, fare clic sui file system di cui si desidera eseguire il backup, quindi fare clic sulla freccia destra per spostarli nella sezione aggiunta.

      Se si seleziona l'opzione **selezione automatica di tutte le risorse sullo stesso volume di storage**, vengono selezionate tutte le risorse dello stesso volume. Quando vengono spostate nella sezione aggiunta, tutte le risorse del volume vengono spostate insieme.

   Per aggiungere un singolo file system, deselezionare l'opzione **selezione automatica di tutte le risorse sullo stesso volume di storage** e selezionare i file system da spostare nella sezione aggiunta.

6. Nella pagina Criteri, eseguire le seguenti operazioni:

   a. Selezionare uno o più criteri dall'elenco a discesa.

      È possibile selezionare qualsiasi policy esistente e fare clic su **Dettagli** per determinare se è possibile utilizzare tale policy.

      Se nessun criterio esistente soddisfa i propri requisiti, è possibile creare un nuovo criterio facendo clic su * * per avviare la procedura guidata dei criteri.

      I criteri selezionati sono elencati nella colonna Policy della sezione Configure schedules for selected policies.

   b. Nella sezione Configura pianificazioni per i criteri selezionati, fare clic su * * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare la pianificazione.

   c. Se il criterio è associato a più tipi di pianificazione (frequenze), selezionare la frequenza che si desidera configurare.

   d. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione specificando la data di inizio, la data di scadenza e la frequenza, quindi fare clic su **fine**.

      Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate) della sezione Configure schedules for selected policies (Configura pianificazioni per criteri selezionati).

   Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup di SnapCenter. Non modificare le pianificazioni da Task Scheduler di Windows e SQL Server Agent.

7. Nella pagina Notification (notifica), fornire le informazioni di notifica, come indicato di seguito:

Per questo campo…	Eseguire questa operazione…
Preferenza e-mail	Selezionare **Always**, **on Failure** o **on failure or warning**, per inviare e-mail ai destinatari dopo la creazione di gruppi di risorse di backup, l'aggiunta di criteri e la configurazione delle pianificazioni. Immettere il server SMTP, l'oggetto e-mail predefinito e gli indirizzi e-mail a e da.
Da	Indirizzo e-mail
A.	Indirizzo e-mail
Soggetto	Oggetto e-mail predefinito

8. Esaminare il riepilogo, quindi fare clic su **fine**.

   È possibile eseguire un backup su richiesta o attendere che venga eseguito il backup pianificato.

Eseguire il backup di una singola risorsa on-demand per i file system Windows

Se una risorsa non si trova in un gruppo di risorse, è possibile eseguire il backup su richiesta dalla pagina risorse.

A proposito di questa attività

Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con lo storage secondario, il ruolo assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

Quando si esegue il backup di un file system, SnapCenter non esegue il backup dei LUN montati su un punto di montaggio del volume (VMP) nel file system di cui si sta eseguendo il backup.

Se si lavora in un contesto di file system Windows, non eseguire il backup dei file di database. In questo modo si crea un backup incoerente e una possibile perdita di dati durante il ripristino. Per proteggere i file di database, è necessario utilizzare il plug-in SnapCenter appropriato per il database (ad esempio, il plug-in SnapCenter per Microsoft SQL Server, il plug-in SnapCenter per Microsoft Exchange Server o un plug-in personalizzato per i file di database).

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare il tipo di risorsa file system, quindi selezionare la risorsa di cui si desidera eseguire il backup.
3. Se la procedura guidata file system - Protect non si avvia automaticamente, fare clic su **Protect** per avviare la procedura guidata.

   Specificare le impostazioni di protezione, come descritto nella sezione creazione dei gruppi di risorse.

4. Facoltativo: Nella pagina risorse della procedura guidata, immettere un formato nome personalizzato per l'istantanea.

   Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

5. Nella pagina Criteri, eseguire le seguenti operazioni:

   a. Selezionare uno o più criteri dall'elenco a discesa.

      È possibile selezionare qualsiasi criterio esistente, quindi fare clic su **Dettagli** per determinare se è possibile utilizzarlo.

      Se nessun criterio esistente soddisfa i propri requisiti, è possibile copiare e modificare un criterio esistente oppure creare un nuovo criterio facendo clic su  per avviare la procedura guidata.

      I criteri selezionati sono elencati nella colonna Policy della sezione Configure schedules for selected policies.

   b. Nella sezione Configura pianificazioni per i criteri selezionati, fare clic  nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare la pianificazione.

   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione specificando la data di inizio, la data di scadenza e la frequenza, quindi fare clic su **fine**.

      Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate) della sezione Configure schedules for selected policies (Configura pianificazioni per criteri selezionati).

   "Le operazioni pianificate potrebbero non riuscire"

6. Nella pagina Notification (notifica), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Preferenza e-mail	Selezionare **Always**, **on Failure**, oppure **on failure or warning**, per inviare e-mail ai destinatari dopo la creazione di gruppi di risorse di backup, l'aggiunta di criteri e la configurazione delle pianificazioni. Immettere le informazioni sul server SMTP, l'oggetto e-mail predefinito e gli indirizzi e-mail "a" e "da".
Da	Indirizzo e-mail
A.	Indirizzo e-mail
Soggetto	Oggetto e-mail predefinito

7. Esaminare il riepilogo, quindi fare clic su **fine**.

   Viene visualizzata la pagina della topologia del database.

8. Fare clic su **Esegui backup ora**.
9. Nella pagina Backup, attenersi alla seguente procedura:
    a. Se sono stati applicati più criteri alla risorsa, dall'elenco a discesa Policy (criterio), selezionare il criterio da utilizzare per il backup.

       Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Fare clic su **Backup**.
10. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Eseguire il backup dei gruppi di risorse per i file system Windows

Un gruppo di risorse è un insieme di risorse su un host o cluster. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse. È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina risorse. Se un gruppo di risorse dispone di un criterio associato e di una pianificazione configurata, i backup vengono eseguiti automaticamente in base alla pianificazione.

Prima di iniziare

- È necessario aver creato un gruppo di risorse con un criterio allegato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con lo storage secondario, il ruolo assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Se un gruppo di risorse dispone di più database di host diversi, l'operazione di backup su alcuni host potrebbe attivarsi in ritardo a causa di problemi di rete. È necessario configurare il valore di MaxRetryForUninitializedHosts in web.config utilizzando il cmdlet Set-SmConfigSettings PowerShell

Quando si esegue il backup di un file system, SnapCenter non esegue il backup dei LUN montati su un punto di montaggio del volume (VMP) nel file system di cui si sta eseguendo il backup.

Se si lavora in un contesto di file system Windows, non eseguire il backup dei file di database. In questo modo si crea un backup incoerente e una possibile perdita di dati durante il ripristino. Per proteggere i file di database, è necessario utilizzare il plug-in SnapCenter appropriato per il database (ad esempio, il plug-in SnapCenter per Microsoft SQL Server, il plug-in SnapCenter per Microsoft Exchange Server o un plug-in personalizzato per i file di database).

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).

   È possibile eseguire una ricerca nel gruppo di risorse immettendo il nome del gruppo di risorse nella casella di ricerca oppure facendo clic  e selezionando il tag. È quindi possibile fare clic su  per chiudere il riquadro del filtro.

3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi fare clic su **Esegui backup ora**.

> Per il plug-in SnapCenter per database Oracle, se si dispone di un gruppo di risorse federate con due database e uno di essi dispone di un file di dati su uno storage non NetApp, l'operazione di backup viene interrotta anche se l'altro database si trova su uno storage NetApp.

4. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se sono stati associati più criteri al gruppo di risorse, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Fare clic su **Backup**.
5. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.
   - Nelle configurazioni MetroCluster, SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

     "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover di MetroCluster"

   - Se si esegue il backup dei dati delle applicazioni su VMDK e la dimensione dell'heap Java per il plug-in SnapCenter per VMware vSphere non è sufficiente, il backup potrebbe non riuscire. Per aumentare le dimensioni dell'heap di Java, individuare il file di script `/opt/netapp/init_scripts/scvservice`. In tale script, il `do_start method` comando avvia il servizio plug-in VMware di SnapCenter. Aggiornare il comando al seguente indirizzo: `Java -jar -Xmx8192M -Xms4096M`.

Creare una connessione al sistema storage e una credenziale utilizzando i cmdlet PowerShell

È necessario creare una connessione SVM (Storage Virtual Machine) e una credenziale prima di utilizzare i cmdlet PowerShell per eseguire operazioni di protezione dei dati.

Prima di iniziare

- L'ambiente PowerShell dovrebbe essere stato preparato per l'esecuzione dei cmdlet PowerShell.
- Per creare le connessioni storage, è necessario disporre delle autorizzazioni necessarie nel ruolo Infrastructure Admin.
- Assicurarsi che le installazioni dei plug-in non siano in corso.

  Le installazioni dei plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage perché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nella GUI di SnapCenter come "non disponibile per il backup" o "non su storage NetApp".

- I nomi dei sistemi di storage devono essere univoci.

  SnapCenter non supporta più sistemi storage con lo stesso nome su cluster diversi. Ogni sistema storage supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF di gestione univoco.

Fasi

1. Avviare una sessione di connessione PowerShell utilizzando il cmdlet Open-SmConnection.

   Questo esempio apre una sessione PowerShell:

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

2. Creare una nuova connessione al sistema di storage utilizzando il cmdlet Add-SmStorageConnection.

   Questo esempio crea una nuova connessione al sistema di storage:

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

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   In questo esempio viene creata una nuova credenziale denominata FinanceAdmin con credenziali Windows:

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Eseguire il backup delle risorse utilizzando i cmdlet PowerShell

È possibile utilizzare i cmdlet PowerShell per eseguire il backup dei database SQL Server o dei file system Windows. Il backup di un database o di un file system di SQL Server include la connessione con il server SnapCenter, il rilevamento delle istanze o dei file system di SQL Server, l'aggiunta di un criterio, la creazione di un gruppo di risorse di backup, il backup e la verifica del backup.

Prima di iniziare

- È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- È necessario aver aggiunto la connessione al sistema di storage e creato una credenziale.
- È necessario aggiungere host e rilevare risorse.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

Viene visualizzato il prompt di nome utente e password.

2. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   In questo esempio viene creata una nuova policy di backup con un tipo di backup completo SQL:

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

   Questo esempio crea una nuova policy di backup con un tipo di backup del file system Windows di CrashConsistent:

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

3. Individuare le risorse host utilizzando il cmdlet Get-SmResources.

   In questo esempio vengono illustrate le risorse per il plug-in Microsoft SQL sull'host specificato:

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

   In questo esempio vengono illustrate le risorse per i file system Windows sull'host specificato:

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

4. Aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   Questo esempio crea un nuovo gruppo di risorse di backup del database SQL con i criteri e le risorse specificati:

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

   Questo esempio crea un nuovo gruppo di risorse di backup del file system Windows con i criteri e le risorse specificati:

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

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

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

6. Visualizzare lo stato del processo di backup utilizzando il cmdlet Get-SmBackupReport.

   Questo esempio visualizza un report di riepilogo di tutti i lavori eseguiti alla data specificata:

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di backup

È possibile monitorare l'avanzamento di diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere necessario controllare i progressi per determinare quando sono stati completati o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, attenersi alla seguente procedura:

a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
b. Specificare le date di inizio e di fine.
c. Dall'elenco a discesa **tipo**, selezionare **Backup**.
d. Dal menu a discesa **Status** (Stato), selezionare lo stato del backup.
e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.

4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

> Sebbene venga visualizzato lo stato del processo di backup , quando si fa clic sui dettagli del processo, è possibile che alcune delle attività secondarie dell'operazione di backup siano ancora in corso o contrassegnate da segnali di avviso.

5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Monitorare le operazioni nel riquadro attività

Il riquadro Activity (attività) visualizza le cinque operazioni più recenti eseguite. Il riquadro Activity (attività) visualizza anche il momento in cui l'operazione è stata avviata e lo stato dell'operazione.

Il riquadro Activity (attività) visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli commessa**.

Annullare le operazioni di backup

È possibile annullare le operazioni di backup inserite nella coda.

Cosa ti serve

- Per annullare le operazioni, è necessario accedere come amministratore SnapCenter o come proprietario del processo.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- Per annullare le operazioni di backup, è possibile utilizzare l'interfaccia grafica utente di SnapCenter, i cmdlet PowerShell o i comandi CLI.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di backup in coda degli altri membri durante l'utilizzo di tale ruolo.

Fasi

1. Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	a. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**.
Riquadro delle attività	a. Dopo aver avviato l'operazione di backup, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. b. Selezionare l'operazione. c. Nella pagina Dettagli processo, fare clic su **Annulla processo**.

L'operazione viene annullata e la risorsa viene riportata allo stato precedente.

Visualizzare i backup e i cloni correlati nella pagina topologia

Quando si prepara il backup o la clonazione di una risorsa, è possibile visualizzare una rappresentazione grafica di tutti i backup e cloni sullo storage primario e secondario. Nella pagina topologia, è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e selezionarli per eseguire le operazioni di protezione dei dati.

A proposito di questa attività

È possibile esaminare le seguenti icone nella vista Manage Copies (Gestisci copie) per determinare se i backup e i cloni sono disponibili sullo storage primario o secondario (copie Mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- Visualizza il numero di backup e cloni su cui viene eseguito il mirroring dello storage secondario utilizzando la tecnologia SnapMirror.

  I cloni di un backup di un mirror flessibile della versione su un volume di tipo mirror-vault vengono visualizzati nella vista della topologia, ma il numero di backup mirror nella vista della topologia non include il backup flessibile della versione.

- Visualizza il numero di backup e cloni replicati sullo storage secondario utilizzando la tecnologia SnapVault.

- Il numero di backup visualizzati include i backup eliminati dallo storage secondario. Ad esempio, se sono stati creati 6 backup utilizzando un criterio per conservare solo 4 backup, il numero di backup visualizzati è 6.
- Se è stato eseguito l'aggiornamento da SnapCenter 1.1, i cloni sul secondario (mirror o vault) non vengono visualizzati in copie mirrorate o copie del vault nella pagina topologia. Tutti i cloni creati con SnapCenter 1.1 vengono visualizzati nelle copie locali di SnapCenter 3.0.

I cloni di un backup di un mirror flessibile della versione su un volume di tipo mirror-vault vengono visualizzati nella vista della topologia, ma il numero di backup mirror nella vista della topologia non include il backup flessibile della versione.

Se disponi di una relazione secondaria come SnapMirror Business Continuity (SM-BC), puoi visualizzare le seguenti icone aggiuntive:

-  implica che il sito di replica è attivo.
-  implica che il sito di replica non è attivo.
-  implica che la relazione del mirror secondario o del vault non è stata ristabilita.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Consulta la scheda Summary per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione Summary Card (scheda di riepilogo) visualizza il numero totale di backup e cloni. Solo per il database Oracle, la sezione Summary Card (scheda di riepilogo) visualizza anche il numero totale di backup del registro.

   Facendo clic sul pulsante **Refresh** viene avviata una query dello storage per visualizzare un conteggio accurato.

   Se viene eseguito il backup abilitato SnapLock, facendo clic sul pulsante **Aggiorna** si aggiornano i tempi di scadenza SnapLock primari e secondari recuperati da ONTAP. Inoltre, una pianificazione settimanale aggiorna il tempo di scadenza SnapLock primario e secondario recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza del SnapLock per il backup sarà il tempo di scadenza del SnapLock più lungo impostato per una Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Per SnapMirror Business Continuity (SM-BC), facendo clic sul pulsante **Refresh** (Aggiorna) viene aggiornato l'inventario di backup di SnapCenter eseguendo una query su ONTAP per i siti principali e di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti relazioni SM-BC.

- Per le relazioni SM-BC, Async Mirror, Vault o MirrorVault con la nuova destinazione primaria deve essere configurato manualmente dopo il failover.
- Dopo il failover, è necessario creare un backup affinché SnapCenter sia consapevole del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista Gestisci copie, fare clic su **backup** o **cloni** dallo storage primario o secondario per visualizzare i dettagli di un backup o clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione, ridenominazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nel sistema di storage secondario.

   Se si utilizzano plug-in personalizzati di SnapCenter, non è possibile rinominare i backup presenti nel sistema di storage primario.

   - Se si seleziona un backup di una risorsa o di un gruppo di risorse Oracle, è anche possibile eseguire operazioni di montaggio e smontaggio.
   - Se è stato selezionato un backup del registro di una risorsa o di un gruppo di risorse Oracle, è possibile eseguire operazioni di ridenominazione, montaggio, disinstallazione ed eliminazione.
   - Se si utilizza il pacchetto di plug-in SnapCenter per Linux e il backup è stato catalogato utilizzando Gestione ripristino Oracle (RMAN), non è possibile rinominare i backup catalogati.

7. Se si desidera eliminare un clone, selezionarlo dalla tabella e fare clic per eliminarlo.

Esempio di visualizzazione di backup e cloni sullo storage primario

Rimuovere i backup utilizzando i cmdlet PowerShell

È possibile utilizzare il cmdlet Remove-SmBackup per eliminare i backup se non sono più necessari per altre operazioni di protezione dei dati.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet

Open-SmConnection.

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

2. Eliminare uno o più backup utilizzando il cmdlet Remove-SmBackup.

   Questo esempio elimina due backup utilizzando i relativi ID di backup:

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

Ripulire il numero di backup secondari utilizzando i cmdlet PowerShell

È possibile utilizzare il cmdlet Remove-SmBackup per eliminare il conteggio dei backup per i backup secondari che non dispongono di snapshot. È possibile utilizzare questo cmdlet quando le istantanee totali visualizzate nella topologia Manage Copies (Gestisci copie) non corrispondono all'impostazione di conservazione Snapshot dello storage secondario.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Eliminare il numero di backup secondari utilizzando il parametro -CleanupSecondaryBackups.

   Nell'esempio riportato di seguito viene eliminato il conteggio dei backup per i backup secondari senza istantanee:

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

Ripristinare i file system di Windows

Ripristinare i backup del file system di Windows

È possibile utilizzare SnapCenter per ripristinare i backup del file system. Il ripristino del file system è un processo multifase che copia tutti i dati da un backup specificato nella posizione originale del file system.

Prima di iniziare

- È necessario aver eseguito il backup del file system.
- Se è in corso un'operazione pianificata, ad esempio un'operazione di backup, per un file system, tale operazione deve essere annullata prima di poter avviare un'operazione di ripristino.
- È possibile ripristinare solo un backup del file system nella posizione originale e non in un percorso alternativo.

  Non è possibile ripristinare un singolo file da un backup perché il file system ripristinato sovrascrive qualsiasi dato nella posizione originale del file system. Per ripristinare un singolo file da un backup del file system, è necessario clonare il backup e accedere al file nel clone.

- Non è possibile ripristinare un volume di sistema o di avvio.
- SnapCenter può ripristinare i file system in un cluster Windows senza disattivare il gruppo di cluster.

A proposito di questa attività

- IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

  Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

  È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- Per l'operazione di ripristino SnapMirror Business Continuity (SM-BC), devi selezionare il backup dalla posizione principale.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Per filtrare l'elenco delle risorse, selezionare le opzioni file system (file system) e Resource Group (Gruppo di risorse).
3. Selezionare un gruppo di risorse dall'elenco, quindi fare clic su **Ripristina**.
4. Nella pagina Backup, selezionare se si desidera eseguire il ripristino da sistemi di storage primari o secondari, quindi selezionare un backup da ripristinare.
5. Selezionare le opzioni desiderate nella procedura guidata di ripristino.

6. È possibile immettere il percorso e gli argomenti del prescrittt o del postscript che si desidera eseguire SnapCenter rispettivamente prima o dopo l'operazione di ripristino.

   Ad esempio, è possibile eseguire uno script per aggiornare i trap SNMP, automatizzare gli avvisi, inviare i registri e così via.

   > Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

7. Nella pagina Notification (notifica), selezionare una delle seguenti opzioni:

Per questo campo…	Eseguire questa operazione…
Registrare gli eventi del server SnapCenter nel syslog del sistema di storage	Selezionare questa opzione per registrare gli eventi del server SnapCenter nel syslog del sistema di storage.
Invia al sistema di storage la notifica AutoSupport per le operazioni non riuscite	Selezionare questa opzione per inviare a NetApp informazioni su operazioni non riuscite utilizzando AutoSupport.
Preferenza e-mail	Selezionare **Always**, **on Failure** o **on failure or warning** per inviare messaggi e-mail ai destinatari dopo il ripristino dei backup. Immettere il server SMTP, l'oggetto e-mail predefinito e gli indirizzi e-mail a e da.

8. Esaminare il riepilogo, quindi fare clic su **fine**.
9. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

> Se il file system ripristinato contiene un database, è necessario ripristinarlo. Se il database non viene ripristinato, potrebbe essere in uno stato non valido. Per informazioni sul ripristino dei database, consultare la Data Protection Guide relativa al database.

Ripristinare le risorse utilizzando i cmdlet PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con il server SnapCenter, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Recuperare le informazioni relative a uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio mostra informazioni su tutti i backup disponibili:

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

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

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

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

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

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

3. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di ripristino

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

gli stati di post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi altra azione di ripristino che è possibile eseguire.

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Ripristina**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato di ripristino.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Annullare le operazioni di ripristino

È possibile annullare i processi di ripristino in coda.

Per annullare le operazioni di ripristino, è necessario accedere come amministratore SnapCenter o come proprietario del processo.

A proposito di questa attività

- È possibile annullare un'operazione di ripristino in coda dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione di ripristino in corso.
- È possibile utilizzare l'interfaccia grafica di SnapCenter, i cmdlet PowerShell o i comandi CLI per annullare le operazioni di ripristino in coda.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni di ripristino che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di ripristino in coda degli altri membri durante l'utilizzo di tale ruolo.

Fase

Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. 2. Selezionare il lavoro e fare clic su **Annulla lavoro**.
Riquadro delle attività	1. Dopo aver avviato l'operazione di ripristino, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. 2. Selezionare l'operazione. 3. Nella pagina Dettagli processo, fare clic su **Annulla processo**.

Clonare i file system Windows

Clonare da un backup del file system Windows

È possibile utilizzare SnapCenter per clonare un backup del file system Windows. Se si desidera una copia di un singolo file che è stata erroneamente eliminata o modificata, è possibile clonare un backup e accedere a tale file nel clone.

Prima di iniziare

- Dovresti aver preparato per la protezione dei dati completando attività come l'aggiunta di host, l'identificazione delle risorse e la creazione di connessioni alle macchine virtuali di storage (SVM).
- Si dovrebbe disporre di un backup del file system.
- Assicurarsi che gli aggregati che ospitano i volumi siano inclusi nell'elenco degli aggregati assegnati della macchina virtuale di storage (SVM).
- Non è possibile clonare un gruppo di risorse. È possibile clonare solo backup di file system singoli.
- Se un backup risiede su una macchina virtuale con un disco VMDK, SnapCenter non può clonare il backup su un server fisico.
- Se si clona un cluster Windows (ad esempio, un LUN condiviso o un LUN del volume condiviso del cluster (CSV)), il clone viene memorizzato come LUN dedicato sull'host specificato.
- Per un'operazione di cloning, la directory principale del punto di montaggio del volume non può essere una directory condivisa.
- Non è possibile creare un clone su un nodo che non è il nodo principale per l'aggregato.
- Non è possibile pianificare operazioni ricorrenti di cloni (ciclo di vita dei cloni) per i file system Windows; è possibile clonare un backup solo su richiesta.
- Se si sposta un LUN contenente un clone in un nuovo volume, SnapCenter non supporta più il clone. Ad esempio, non è possibile utilizzare SnapCenter per eliminare il clone.
- Non è possibile clonare in più ambienti. Ad esempio, la clonazione da un disco fisico a un disco virtuale o viceversa.

A proposito di questa attività

- IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel

file SMCoreServiceHost.exe.Config dell'host del plug-in.

Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **file Systems** dall'elenco.
3. Selezionare l'host.

   La vista della topologia viene visualizzata automaticamente se la risorsa è protetta.

4. Dall'elenco delle risorse, selezionare il backup che si desidera clonare, quindi fare clic sull'icona del clone.
5. Nella pagina Opzioni, procedere come segue:

Per questo campo…	Eseguire questa operazione…
Server clone	Scegliere l'host su cui creare il clone.
"Auto assign mount point" o "Auto assign volume mount point under path"	Scegliere se assegnare automaticamente un punto di montaggio o un punto di montaggio del volume sotto un percorso. Auto assign volume mount point under path (assegnazione automatica del punto di montaggio del volume sotto il percorso): Il punto di montaggio sotto un percorso consente di fornire una directory specifica in cui verranno creati i punti di montaggio. Prima di scegliere questa opzione, verificare che la directory sia vuota. Se nella directory è presente un backup, il backup non sarà valido dopo l'operazione di montaggio.
Percorso di archiviazione	Scegliere un percorso di archiviazione se si desidera clonare un backup secondario.

6. Nella pagina script, specificare eventuali prescritture o postscript da eseguire.

   Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

7. Esaminare il riepilogo, quindi fare clic su **fine**.

8. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Clonare i backup utilizzando i cmdlet PowerShell

Il flusso di lavoro dei cloni include la pianificazione, l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Elencare i backup che possono essere clonati utilizzando il cmdlet Get-SmBackup o Get-SmResourceGroup.

   Questo esempio mostra informazioni su tutti i backup disponibili:

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

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

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   Nell'esempio riportato di seguito vengono visualizzate informazioni su un gruppo di risorse specificato, sulle relative risorse e sui criteri associati:

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

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
```

```
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
```

```
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. Avviare un'operazione di clonazione da un backup esistente utilizzando il cmdlet New-SmClone.

   Questo esempio crea un clone da un backup specificato con tutti i log:

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

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

In questo esempio viene creato un clone per un'istanza specifica di Microsoft SQL Server:

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

4. Visualizzare lo stato del processo clone utilizzando il cmdlet Get-SmCloneReport.

   Questo esempio visualizza un report clone per l'ID lavoro specificato:

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                   Sally_DRAPER}
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di clonazione

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Clone**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato del clone.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro clone, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

Annullare le operazioni di clonazione

È possibile annullare le operazioni di clonazione inserite nella coda.

Per annullare le operazioni di clonazione, accedere come amministratore SnapCenter o come proprietario del processo.

A proposito di questa attività

- È possibile annullare un'operazione di clonazione in coda dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione clone in esecuzione.
- È possibile utilizzare l'interfaccia grafica di SnapCenter, i cmdlet PowerShell o i comandi CLI per annullare le operazioni di clonazione in coda.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di cloni in coda degli altri membri durante l'utilizzo di tale ruolo.

Fase

Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. 2. Selezionare l'operazione e fare clic su **Annulla lavoro**.
Riquadro delle attività	1. Dopo aver avviato l'operazione di clonazione, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. 2. Selezionare l'operazione. 3. Nella pagina **Dettagli processo**, fare clic su **Annulla processo**.

Separare un clone

È possibile utilizzare SnapCenter per separare una risorsa clonata dalla risorsa principale. Il clone diviso diventa indipendente dalla risorsa padre.

A proposito di questa attività

- Non è possibile eseguire l'operazione di suddivisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato il clone1 da un backup del database, è possibile creare un backup del clone1 e clonare il backup (clone2). Dopo aver creato il clone2, il clone1 è un clone intermedio e non è possibile eseguire l'operazione di suddivisione del clone sul clone1. Tuttavia, è possibile eseguire l'operazione di suddivisione dei cloni sul clone2.

  Dopo aver diviso il clone2, è possibile eseguire l'operazione di divisione del clone sul clone1, poiché il clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i lavori di clonazione del clone vengono eliminati.
- Per informazioni sulle limitazioni delle operazioni di suddivisione clone, vedere "Guida alla gestione dello storage logico di ONTAP 9".
- Assicurarsi che il volume o l'aggregato sul sistema di storage sia online.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **risorse**, selezionare l'opzione appropriata dall'elenco Visualizza:

Opzione	Descrizione
Per applicazioni di database	Selezionare **Database** dall'elenco View (Visualizza).
Per file system	Selezionare **Path** dall'elenco View (Visualizza).

3. Selezionare la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Nella vista **Gestisci copie**, selezionare la risorsa clonata (ad esempio, il database o il LUN), quindi fare clic su * *  .
5. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
6. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

   Se il servizio SMCore viene riavviato, l'operazione di split clone smette di rispondere. Eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione di suddivisione del clone.

   Se si desidera un tempo di polling più lungo o più breve per controllare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo in cui SMCore deve eseguire il polling per lo stato dell'operazione di suddivisione del clone. Il valore è espresso in millisecondi e il valore

predefinito è 5 minuti.

Ad esempio:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'operazione di avvio del clone split non riesce se sono in corso operazioni di backup, ripristino o altro clone split. È necessario riavviare l'operazione di suddivisione dei cloni solo al termine delle operazioni in esecuzione.

Informazioni correlate

"Il clone o la verifica di SnapCenter non riesce e l'aggregato non esiste"

Proteggere i database di Microsoft Exchange Server

Concetti relativi al plug-in SnapCenter per Microsoft Exchange Server

Panoramica del plug-in SnapCenter per il server Microsoft Exchange

Il plug-in SnapCenter per Microsoft Exchange Server è un componente sul lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati basata sulle applicazioni dei database Exchange. Il plug-in per Exchange automatizza il backup e il ripristino dei database Exchange nell'ambiente SnapCenter.

Una volta installato il plug-in per Exchange, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror dei set di backup su un altro volume e con la tecnologia NetApp SnapVault per eseguire la replica del backup disk-to-disk a scopo di conformità agli standard o di archiviazione.

Se si desidera ripristinare e ripristinare i messaggi e-mail o le caselle postali al posto del database Exchange completo, è possibile utilizzare il software SMBR (Single Mailbox Recovery). Il ripristino di una singola casella postale di NetApp® è giunto alla fine della disponibilità (EOA) il 12 maggio 2023. NetApp continuerà a supportare i clienti che hanno acquistato capacità, manutenzione e supporto della casella postale attraverso i codici marketing introdotti il 24 giugno 2020, per tutta la durata del diritto al supporto.

Il servizio di ripristino di una singola casella postale di NetApp è un prodotto partner fornito da Ontrack. Ontrack PowerControl offre funzionalità simili a quelle del ripristino di una singola casella postale di NetApp. I clienti possono acquistare nuove licenze software Ontrack PowerControls e rinnovi di assistenza e manutenzione Ontrack PowerControls da Ontrack (fino a licensingteam@ontrack.com) per il ripristino granulare della mailbox.

Operazioni che è possibile eseguire con il plug-in SnapCenter per Microsoft Exchange Server

È possibile utilizzare il plug-in per Exchange per eseguire il backup e il ripristino dei database di Exchange Server.

- Visualizzare e gestire un inventario attivo di DAG (Database Availability Group), database e set di repliche di Exchange
- Definire le policy che forniscono le impostazioni di protezione per l'automazione del backup
- Assegnare i criteri ai gruppi di risorse
- Proteggere singoli DAG e database
- Eseguire il backup dei database delle cassette postali di Exchange primario e secondario
- Ripristinare i database dai backup primari e secondari

Tipi di storage supportati dal plug-in SnapCenter per Microsoft Windows e per Microsoft Exchange Server

SnapCenter supporta un'ampia gamma di tipi di storage su macchine fisiche e virtuali.

Prima di installare il pacchetto per l'host, è necessario verificare se il supporto è disponibile per il tipo di storage in uso.

Il provisioning SnapCenter e il supporto per la protezione dei dati sono disponibili su Windows Server. Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Macchina	Tipo di storage	Eseguire il provisioning utilizzando	Note di supporto
Server fisico	LUN connessi a FC	Interfaccia grafica utente (GUI) o cmdlet PowerShell di SnapCenter	
Server fisico	LUN connessi a iSCSI	GUI SnapCenter o cmdlet PowerShell	
Macchina virtuale VMware	LUN RDM collegati da un HBA FC o iSCSI	Cmdlet PowerShell	Solo compatibilità fisica I VMDK non sono supportati.
Macchina virtuale VMware	LUN iSCSI collegati direttamente al sistema guest dall'iniziatore iSCSI	GUI SnapCenter o cmdlet PowerShell	I VMDK non sono supportati.
Macchina virtuale Hyper-V.	LUN Virtual FC (VFC) collegate da uno switch Fibre Channel virtuale	GUI SnapCenter o cmdlet PowerShell	È necessario utilizzare Hyper-V Manager per eseguire il provisioning dei LUN Virtual FC (VFC) collegati da uno switch Fibre Channel virtuale. I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti sullo storage NetApp non sono supportati.

Macchina	Tipo di storage	Eseguire il provisioning utilizzando	Note di supporto
Macchina virtuale Hyper-V.	LUN iSCSI collegati direttamente al sistema guest dall'iniziatore iSCSI	GUI SnapCenter o cmdlet PowerShell	I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti sullo storage NetApp non sono supportati.

Privilegi minimi di ONTAP richiesti per il plug-in Exchange

I privilegi minimi di ONTAP richiesti variano in base ai plug-in di SnapCenter utilizzati per la protezione dei dati.

- All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
  - event generate-autosupport-log
  - mostra la cronologia dei lavori
  - interruzione del lavoro
  - lun
  - lun create (crea lun)
  - lun create (crea lun)
  - lun create (crea lun)
  - lun delete (elimina lun)
  - lun igroup add
  - lun igroup create
  - lun igroup delete (elimina igroup lun)
  - lun igroup rename (rinomina lun igroup)
  - lun igroup rename (rinomina lun igroup)
  - lun igroup show
  - lun mapping add-reporting-node
  - creazione mappatura lun
  - eliminazione della mappatura lun
  - nodi di remove-reporting-mapping lun
  - visualizzazione della mappatura del lun
  - modifica del lun

- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- ridimensionamento del lun
- lun seriale
- lun show
- regola aggiuntiva del criterio snapmirror
- regola-modifica del criterio snapmirror
- regola di rimozione del criterio snapmirror
- policy di snapmirror
- ripristino di snapmirror
- spettacolo di snapmirror
- storia di snapmirror
- aggiornamento di snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione del clone del volume
- visualizzazione del clone del volume
- avvio della divisione del clone del volume
- interruzione della divisione del clone del volume
- creazione del volume
- distruggere il volume
- creazione del clone del file di volume
- file di volume show-disk-usage
- volume offline
- volume online
- modifica del volume
- creazione del qtree del volume
- eliminazione del qtree del volume
- modifica del qtree del volume
- visualizzazione del qtree del volume
- limitazione del volume
- presentazione del volume
- creazione di snapshot di volume
- eliminazione dello snapshot del volume

- modifica dello snapshot del volume
- rinominare lo snapshot del volume
- ripristino dello snapshot del volume
- file di ripristino dello snapshot del volume
- visualizzazione di snapshot di volume
- smontare il volume
- cifs vserver
- creazione condivisione cifs vserver
- eliminazione condivisione cifs vserver
- vserver cifs shadowcopy mostra
- show di condivisione di vserver cifs
- vserver cifs show
- policy di esportazione di vserver
- creazione policy di esportazione vserver
- eliminazione della policy di esportazione di vserver
- creazione della regola dei criteri di esportazione di vserver
- visualizzazione della regola dei criteri di esportazione di vserver
- visualizzazione della policy di esportazione di vserver
- iscsi vserver
- visualizzazione della connessione iscsi del vserver
- show di vserver

- Comandi di sola lettura: Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
  - interfaccia di rete
  - visualizzazione dell'interfaccia di rete
  - server virtuale

Preparazione dei sistemi storage per la replica di SnapMirror e SnapVault

È possibile utilizzare un plug-in SnapCenter con la tecnologia SnapMirror di ONTAP per creare copie mirror dei set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replica del backup disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti di SnapMirror e SnapVault al termine dell'operazione di Snapshot. Gli aggiornamenti di SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter; non creare una pianificazione ONTAP separata.

Se vieni a SnapCenter da un prodotto NetApp SnapManager e sei soddisfatto delle relazioni di protezione dei dati che hai configurato, puoi saltare questa sezione.

Una relazione di protezione dei dati replica i dati sullo storage primario (il volume di origine) nello storage secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui fa riferimento il volume di origine al volume di destinazione.

SnapCenter non supporta le relazioni a cascata tra SnapMirror e i volumi SnapVault (**primario** > **Mirror** > **Vault**). Si consiglia di utilizzare le relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per ulteriori informazioni sulle relazioni di SnapMirror flessibili per la versione e sulla loro configurazione, vedere la "Documentazione ONTAP".

SnapCenter non supporta la replica **Sync_mirror**.

Definire una strategia di backup per le risorse di Exchange Server

La definizione di una strategia di backup prima di creare i processi di backup consente di garantire la presenza dei backup necessari per ripristinare correttamente i database. Il Service Level Agreement (SLA), l'RTO (Recovery Time Objective) e l'RPO (Recovery Point Objective) determinano in gran parte la strategia di backup.

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. L'RTO è il momento in cui un processo di business deve essere ripristinato dopo un'interruzione del servizio. Un RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di backup.

Tipi di backup supportati per il database Exchange

Il backup delle cassette postali Exchange mediante SnapCenter richiede la scelta del tipo di risorsa, ad esempio database e gruppi di disponibilità database (DAG). La tecnologia Snapshot viene sfruttata per creare copie online di sola lettura dei volumi in cui risiedono le risorse.

Tipo di backup	Descrizione
Backup completo e del log	Esegue il backup dei database e di tutti i log delle transazioni, inclusi i log troncati. Al termine di un backup completo, Exchange Server tronca i log delle transazioni già impegnati nel database. In genere, scegliere questa opzione. Tuttavia, se il tempo di backup è breve, è possibile scegliere di non eseguire un backup del log delle transazioni con un backup completo.
Backup completo	Esegue il backup di database e log delle transazioni. Non viene eseguito il backup dei log delle transazioni troncati.

Tipo di backup	Descrizione
Backup del log	Esegue il backup di tutti i log delle transazioni. Non viene eseguito il backup dei log troncati che sono già stati impegnati nel database. Se si pianificano backup frequenti del log delle transazioni tra backup completi del database, è possibile scegliere punti di ripristino granulari.

Pianificazioni di backup per i plug-in del database

La frequenza di backup (tipo di pianificazione) viene specificata nei criteri; nella configurazione del gruppo di risorse viene specificata una pianificazione di backup. Il fattore più critico per determinare una frequenza o una pianificazione di backup è il tasso di cambiamento per la risorsa e l'importanza dei dati. È possibile eseguire il backup di una risorsa utilizzata in modo pesante ogni ora, mentre è possibile eseguire il backup di una risorsa utilizzata raramente una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo Service Level Agreement (SLA) e il tuo Recover Point Objective (RPO).

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. Un RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA e RPO contribuiscono alla strategia di protezione dei dati.

Anche per una risorsa molto utilizzata, non è necessario eseguire un backup completo più di una o due volte al giorno. Ad esempio, i backup regolari del log delle transazioni potrebbero essere sufficienti per garantire la disponibilità dei backup necessari. Più spesso si esegue il backup dei database, minore è il numero di log delle transazioni che SnapCenter deve utilizzare al momento del ripristino, con conseguente accelerazione delle operazioni di ripristino.

Le pianificazioni dei backup sono in due parti, come segue:

- Frequenza di backup

  La frequenza di backup (con quale frequenza devono essere eseguiti i backup), denominata *tipo di pianificazione* per alcuni plug-in, fa parte di una configurazione di policy. È possibile selezionare ogni ora, ogni giorno, ogni settimana o ogni mese come frequenza di backup per la policy. Se non si seleziona una di queste frequenze, la policy creata è solo on-demand. Puoi accedere alle policy facendo clic su **Impostazioni** > **politiche**.

- Pianificazioni di backup

  Le pianificazioni di backup (esattamente quando devono essere eseguiti i backup) fanno parte di una configurazione di gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione per il backup ogni giovedì alle 10:00. È possibile accedere alle pianificazioni dei gruppi di risorse facendo clic su **risorse** > **gruppi di risorse**.

Numero di processi di backup necessari per i database

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, il tasso di cambiamento della risorsa e il contratto SLA (Service Level Agreement).

Convenzioni di denominazione del backup

È possibile utilizzare la convenzione di naming predefinita di Snapshot o una convenzione di naming personalizzata. La convenzione di denominazione predefinita dei backup aggiunge un indicatore data e ora ai nomi Snapshot che consente di identificare quando le copie sono state create.

L'istantanea utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

È necessario assegnare un nome logico ai gruppi di risorse di backup, come nell'esempio seguente:

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

In questo esempio, gli elementi di sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* indica data e ora.

In alternativa, è possibile specificare il formato del nome dell'istantanea mentre si proteggono le risorse o i gruppi di risorse selezionando **Usa il formato del nome personalizzato per la copia dell'istantanea**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso dell'indicatore data e ora viene aggiunto al nome dell'istantanea.

Opzioni di conservazione del backup

È possibile scegliere il numero di giorni per i quali conservare le copie di backup o specificare il numero di copie di backup che si desidera conservare, fino a un massimo di 255 copie ONTAP. Ad esempio, l'organizzazione potrebbe richiedere di conservare 10 giorni di copie di backup o 130 copie di backup.

Durante la creazione di un criterio, è possibile specificare le opzioni di conservazione per il tipo di backup e il tipo di pianificazione.

Se si imposta la replica di SnapMirror, il criterio di conservazione viene mirrorato sul volume di destinazione.

SnapCenter elimina i backup conservati con etichette di conservazione corrispondenti al tipo di pianificazione. Se il tipo di pianificazione è stato modificato per la risorsa o il gruppo di risorse, i backup con la vecchia etichetta del tipo di pianificazione potrebbero rimanere nel sistema.

> Per la conservazione a lungo termine delle copie di backup, è necessario utilizzare il backup di SnapVault.

Per quanto tempo conservare i backup del log delle transazioni sul volume di storage di origine per Exchange Server

Il plug-in SnapCenter per Microsoft Exchange Server richiede backup del log delle transazioni per eseguire operazioni di ripristino aggiornate al minuto, che ripristinano il database a un intervallo di tempo compreso tra due backup completi.

Ad esempio, se Plug-in for Exchange ha eseguito un backup completo del registro delle transazioni Plus alle 8:00:5:00 e un altro backup completo del registro delle transazioni Plus alle 17:00, potrebbe utilizzare l'ultimo

backup del registro delle transazioni per ripristinare il database in qualsiasi momento tra le 8:00 e le 5:00. se i registri delle transazioni non sono disponibili, Plug-in for Exchange può eseguire solo operazioni di ripristino point-in-time, che ripristina un database al momento in cui Plug-in for Exchange ha completato un backup completo.

In genere, è necessario eseguire operazioni di ripristino fino al minuto per uno o due giorni. Per impostazione predefinita, SnapCenter conserva un minimo di due giorni.

Definire una strategia di ripristino per i database Exchange

La definizione di una strategia di ripristino per Exchange Server consente di ripristinare correttamente il database.

Origini di un'operazione di ripristino in Exchange Server

È possibile ripristinare un database Exchange Server da una copia di backup sullo storage primario.

È possibile ripristinare i database solo dallo storage primario.

Tipi di operazioni di ripristino supportate per Exchange Server

È possibile utilizzare SnapCenter per eseguire diversi tipi di operazioni di ripristino sulle risorse Exchange.

- Ripristino up-to-the-minute
- Ripristinare un punto precedente

Ripristino fino al minuto

In un'operazione di ripristino up-to-the-minute, i database vengono ripristinati fino al punto di errore. SnapCenter esegue questa operazione eseguendo la seguente sequenza:

1. Ripristina i database dal backup completo del database selezionato.
2. Applica tutti i log delle transazioni di cui è stato eseguito il backup, nonché tutti i nuovi log creati dopo il backup più recente.

   I log delle transazioni vengono spostati in avanti e applicati a qualsiasi database selezionato.

   Exchange crea una nuova catena di log al termine di un ripristino.

   Best practice: si consiglia di eseguire un nuovo backup completo e di log al termine di un ripristino.

   Un'operazione di ripristino aggiornata al minuto richiede un set contiguo di log delle transazioni.

   Dopo aver eseguito un ripristino up-to-the-minute, il backup utilizzato per il ripristino è disponibile solo per le operazioni di ripristino point-in-time.

   Se non è necessario mantenere una funzionalità di ripristino aggiornata al minuto per tutti i backup, è possibile configurare la conservazione del backup del log delle transazioni del sistema attraverso le policy di backup.

Ripristinare un punto precedente

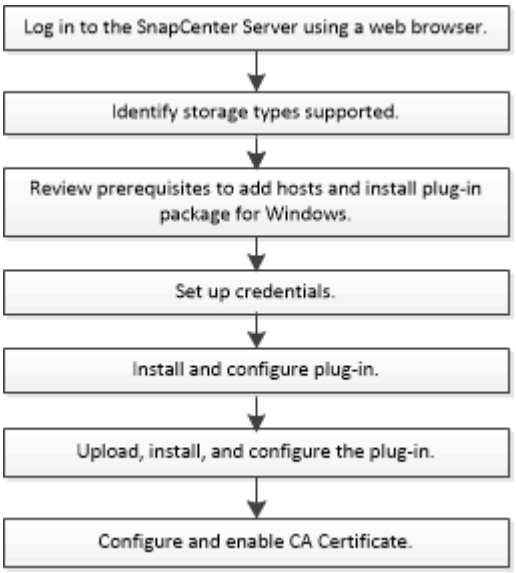
In un'operazione di ripristino point-in-time, i database vengono ripristinati solo a un'ora specifica rispetto al passato. Un'operazione di ripristino point-in-time si verifica nelle seguenti situazioni di ripristino:

- Il database viene ripristinato a un determinato intervallo di tempo in un log delle transazioni di cui è stato eseguito il backup.
- Il database viene ripristinato e viene applicato solo un sottoinsieme di log delle transazioni di cui è stato eseguito il backup.

Installare il plug-in SnapCenter per Microsoft Exchange Server

Workflow di installazione del plug-in SnapCenter per Microsoft Exchange Server

Se si desidera proteggere i database di SnapCenter, è necessario installare e configurare il plug-in di Exchange.



Prerequisiti per aggiungere host e installare il plug-in SnapCenter per Microsoft Exchange Server

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario completare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È necessario disporre di un utente di dominio con privilegi di amministratore locale con autorizzazioni di accesso locale sull'host remoto.
- È necessario utilizzare Microsoft Exchange Server 2013, 2016 o 2019 per le configurazioni standalone e Database Availability Group.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.

- Se si gestiscono i nodi del cluster in SnapCenter, è necessario disporre di un utente con privilegi amministrativi per tutti i nodi del cluster.
- È necessario disporre di un utente con autorizzazioni amministrative su Exchange Server.
- Se SnapManager per Microsoft Exchange Server e SnapDrive per Windows sono già installati, è necessario annullare la registrazione del provider hardware VSS utilizzato da SnapDrive per Windows prima di installare il plug-in per Exchange sullo stesso server Exchange per garantire la corretta protezione dei dati utilizzando SnapCenter.
- Se SnapManager per Microsoft Exchange Server e il plug-in per Exchange sono installati sullo stesso server, è necessario sospendere o eliminare da Windows Scheduler tutte le pianificazioni create da SnapManager per Microsoft Exchange Server.
- L'host deve essere risolvibile con il nome di dominio completo (FQDN) dal server. Se il file hosts viene modificato in modo da renderlo risolvibile e se nel file hosts sono specificati sia il nome breve che l'FQDN, creare una voce nel file hosts di SnapCenter nel seguente formato: *<ip_address> <host_fqdn> <host_name>*.
- Assicurarsi che le seguenti porte non siano bloccate nel firewall, altrimenti l'operazione di aggiunta dell'host non riesce. Per risolvere questo problema, è necessario configurare l'intervallo di porte dinamiche. Per ulteriori informazioni, vedere "Documentazione Microsoft".
  - Intervallo di porte 50000 - 51000 per Windows 2016 ed Exchange 2016
  - Intervallo di porte 6000 - 6500 per Windows 2012 R2 ed Exchange 2013
  - Intervallo di porte 49152 - 65536 per Windows 2019

> Per identificare l'intervallo di porte, eseguire i seguenti comandi:
>
> - netsh int ipv4 mostra il tcp dinamico
> - netsh int ipv4 mostra l'udp di dinamicport
> - netsh int ipv6 mostra il tcp dinamico
> - netsh int ipv6 mostra l'udp di dinamicport

Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario conoscere alcuni requisiti di base relativi allo spazio del sistema host e al dimensionamento.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".
RAM minima per il plug-in SnapCenter sull'host	1 GB

Elemento	Requisiti
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	5 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp". Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet."

Privilegi di Exchange Server richiesti

Per consentire a SnapCenter di aggiungere Exchange Server o DAG e installare il plug-in SnapCenter per Microsoft Exchange Server su un host o DAG, è necessario configurare SnapCenter con le credenziali per un utente con un set minimo di privilegi e autorizzazioni.

È necessario disporre di un utente di dominio con privilegi di amministratore locale e con autorizzazioni di accesso locale sull'host Exchange remoto, nonché di autorizzazioni amministrative su tutti i nodi del DAG. L'utente di dominio richiede le seguenti autorizzazioni minime:

- Add-MailboxDatabaseCopy
- Smontare il database
- Get-AdServerSettings
- Get-DatabaseAvailabilitàGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics

- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly: Vero
- Mount-Database
- New-MailboxDatabase
- New-PublicFolderDatabase
- Remove-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Remove-PublicFolderDatabase
- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore: Veritiero
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario conoscere alcuni requisiti di base relativi allo spazio del sistema host e al dimensionamento.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	5 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.

Elemento	Requisiti
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp". Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet."

Impostare le credenziali per il plug-in SnapCenter per Windows

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. È necessario creare credenziali per l'installazione del pacchetto plug-in e credenziali aggiuntive per l'esecuzione delle operazioni di protezione dei dati sui database.

A proposito di questa attività

È necessario impostare le credenziali per l'installazione dei plug-in sugli host Windows. Sebbene sia possibile creare credenziali per Windows dopo la distribuzione degli host e l'installazione dei plug-in, la procedura consigliata consiste nel creare credenziali dopo l'aggiunta di SVM, prima di distribuire gli host e installare i plug-in.

Impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup al nome utente.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.

   Viene visualizzata la finestra credenziale.

4. Nella pagina Credential, effettuare le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale	Immettere un nome per la credenziale.

Per questo campo…	Eseguire questa operazione…
Nome utente	Inserire il nome utente utilizzato per l'autenticazione. • Amministratore di dominio o qualsiasi membro del gruppo di amministratori Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Amministratore locale (solo per gruppi di lavoro) Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host. Il formato valido per il campo Nome utente è: `UserName`
Password	Inserire la password utilizzata per l'autenticazione.
Autenticazione	Selezionare Windows come modalità di autenticazione.

5. Fare clic su **OK**.

Configurare gMSA su Windows Server 2012 o versione successiva

Windows Server 2012 o versione successiva consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatica delle password dell'account di servizio da un account di dominio gestito.

Prima di iniziare

- È necessario disporre di un controller di dominio Windows Server 2012 o versione successiva.
- È necessario disporre di un host Windows Server 2012 o versione successiva, membro del dominio.

Fasi

1. Creare una chiave root KDS per generare password univoche per ogni oggetto in gMSA.
2. Per ciascun dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey

-EffectiveImmediately

3. Creare e configurare gMSA:
   a. Creare un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo di utenti appena creato per creare gMSA.
```

   Ad esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Eseguire `Get-ADServiceAccount` il comando per verificare
l'account del servizio.
```

4. Configurare gMSA sugli host:
   a. Attivare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

   A tale scopo, eseguire il seguente comando da PowerShell:

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

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


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

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

   a. Riavviare l'host.
   b. Installare gMSA sull'host eseguendo il comando seguente dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`
   c. Verificare il proprio account gMSA eseguendo il seguente comando: `Test-AdServiceAccount`

```
<gMSA>
```

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter.

   Il server SnapCenter installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

Aggiungere host e installare il plug-in per Exchange

È possibile utilizzare la pagina Aggiungi host di SnapCenter per aggiungere host Windows. Il plug-in per Exchange viene installato automaticamente sull'host specificato. Questo è il metodo consigliato per installare i plug-in. È possibile aggiungere un host e installare un plug-in per un singolo host o per un cluster.

Prima di iniziare

- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio SnapCenter Admin
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.
- Il servizio di accodamento dei messaggi deve essere in esecuzione.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi. Per informazioni, vedere "Configurare account di servizio gestito di gruppo su Windows Server 2012 o versione successiva per Microsoft Exchange Server".

A proposito di questa attività

- Non è possibile aggiungere un server SnapCenter come host plug-in a un altro server SnapCenter.
- È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster.
- Se un nodo Exchange fa parte di un DAG, non è possibile aggiungere un solo nodo al server SnapCenter.
- Se si installano plug-in su un cluster (Exchange DAG), questi vengono installati su tutti i nodi del cluster anche se alcuni nodi non dispongono di database su LUN NetApp.

A partire da SnapCenter 4.6, SCE supporta la multi-tenancy ed è possibile aggiungere un host utilizzando i seguenti metodi:

Aggiunta dell'operazione host	4,5 e precedenti	4,6 e successivi
Aggiungere DAG senza IP in un dominio diverso o incrociato	Non supportato	Supportato
Aggiungere più DAG IP con nomi univoci, residenti nello stesso dominio o tra domini	Supportato	Supportato
Aggiungere più DAG IP o IP-less con gli stessi nomi host e/o nome DB in più domini	Non supportato	Supportato

Aggiunta dell'operazione host	4,5 e precedenti	4,6 e successivi
Aggiungere più DAG IP/IP-less con lo stesso nome e lo stesso dominio incrociato	Non supportato	Supportato
Aggiungere più host standalone con lo stesso nome e più domini	Non supportato	Supportato

Il plug-in per Exchange dipende dal pacchetto di plug-in SnapCenter per Windows e le versioni devono essere le stesse. Durante l'installazione del plug-in per Exchange, il pacchetto plug-in SnapCenter per Windows viene selezionato per impostazione predefinita e viene installato insieme al provider hardware VSS.

Se SnapManager per Microsoft Exchange Server e SnapDrive per Windows sono già installati, Se si desidera installare il plug-in per Exchange sullo stesso server Exchange, è necessario annullare la registrazione del provider hardware VSS utilizzato da SnapDrive per Windows, poiché non è compatibile con il provider hardware VSS installato con il plug-in per Exchange e il pacchetto plug-in SnapCenter per Windows. Per ulteriori informazioni, vedere "Come registrare manualmente il provider hardware VSS di Data ONTAP".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Verificare che l'opzione **Managed hosts** sia selezionata nella parte superiore.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, effettuare le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare **Windows** come tipo di host. Il server SnapCenter aggiunge l'host e installa sull'host il plug-in per Windows e il plug-in per Exchange, se non sono già installati. Il plug-in per Windows e il plug-in per Exchange devono essere della stessa versione. Se in precedenza è stata installata una versione diversa del plug-in per Windows, SnapCenter aggiorna la versione come parte dell'installazione.

Per questo campo…	Eseguire questa operazione…
Nome host	Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire il nome di dominio completo (FQDN). Un indirizzo IP è supportato per gli host di dominio non attendibili solo se viene risolto nell'FQDN. Se si aggiunge un host utilizzando SnapCenter e fa parte di un sottodominio, è necessario fornire l'FQDN. È possibile immettere gli indirizzi IP o il nome FQDN di uno dei seguenti elementi: • Host standalone • DAG Exchange Per un DAG Exchange, è possibile: ◦ Aggiungere un DAG fornendo il nome del DAG, l'indirizzo IP del DAG, il nome del nodo o l'indirizzo IP del nodo. ◦ Aggiungere il cluster IP less DAG fornendo l'indirizzo IP o l'FQDN di uno dei nodi del cluster DAG. ◦ Aggiungere IP senza DAG che risiede nello stesso dominio o in un dominio diverso. È inoltre possibile aggiungere più indirizzi IP/IP senza DAG con lo stesso nome ma con domini diversi. Per un host standalone o un DAG Exchange (tra domini o stesso dominio), si consiglia di fornire l'FQDN o l'indirizzo IP dell'host o del DAG.

Per questo campo…	Eseguire questa operazione…
Credenziali	Selezionare il nome della credenziale creata o creare le nuove credenziali. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere la sezione relativa alla creazione di una credenziale. È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome specificato. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare i plug-in da installare.

   Quando si seleziona il plug-in per Exchange, il plug-in SnapCenter per Microsoft SQL Server viene deselezionato automaticamente. Microsoft consiglia di non installare SQL Server ed Exchange Server sullo stesso sistema a causa della quantità di memoria utilizzata e dell'utilizzo di altre risorse richiesto da Exchange.

6. (Facoltativo) fare clic su **altre opzioni**.

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.
Percorso di installazione	Il percorso predefinito è `C:\Program Files\NetApp\SnapCenter`. È possibile personalizzare il percorso.
Aggiungere tutti gli host nel DAG	Selezionare questa casella di controllo quando si aggiunge un DAG.

Per questo campo…	Eseguire questa operazione…
Ignorare i controlli di preinstallazione	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.
Utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in	Selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in. Fornire il nome gMSA nel seguente formato: *Domainname/accountName*. GMSA verrà utilizzato come account del servizio di accesso solo per il servizio del plug-in SnapCenter per Windows.

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo Ignora controlli preliminari, l'host viene convalidato per determinare se soddisfa i requisiti per installare il plug-in. Se i requisiti minimi non sono soddisfatti, vengono visualizzati i messaggi di errore o di avvertenza appropriati.

   Se l'errore è relativo allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in `C:\Program Files\NetApp\SnapCenter` WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione ha, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Monitorare l'avanzamento dell'installazione.

Installare il plug-in per Exchange dall'host del server SnapCenter utilizzando i cmdlet PowerShell

Installare il plug-in per Exchange dall'interfaccia grafica di SnapCenter. Se non si desidera utilizzare la GUI, è possibile utilizzare i cmdlet PowerShell sull'host del server SnapCenter o su un host remoto.

Prima di iniziare

- Il server SnapCenter deve essere stato installato e configurato.
- È necessario essere un amministratore locale dell'host o un utente con privilegi amministrativi.
- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di plug-in, installazione e disinstallazione, ad esempio SnapCenter Admin
- Prima di installare il plug-in per Exchange, è necessario aver esaminato i requisiti di installazione e i tipi di configurazioni supportate.
- L'host su cui si desidera installare il plug-in per Exchange deve essere un host Windows.

Fasi

1. Sull'host del server SnapCenter, stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
2. Aggiungere l'host su cui si desidera installare il plug-in per Exchange utilizzando il cmdlet *Add-SmHost* con i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

   L'host può essere un host standalone o un DAG. Se si specifica un DAG, il parametro *-ISDAG* è obbligatorio.

3. Installare il plug-in per Exchange utilizzando il cmdlet *Install-SmHostPackage* con i parametri richiesti.

   Questo comando installa il plug-in per Exchange sull'host specificato, quindi registra il plug-in con SnapCenter.

Installare il plug-in SnapCenter per Exchange in modo invisibile dalla riga di comando

Installare il plug-in per Exchange dall'interfaccia utente di SnapCenter. Tuttavia, se per qualche motivo non è possibile eseguire il programma di installazione del plug-in per Exchange in modalità automatica dalla riga di comando di Windows.

Prima di iniziare

- È necessario aver eseguito il backup delle risorse di Microsoft Exchange Server.
- È necessario aver installato i pacchetti dei plug-in di SnapCenter.
- Prima di eseguire l'installazione, è necessario eliminare la versione precedente del plug-in SnapCenter per Microsoft SQL Server.

  Per ulteriori informazioni, vedere "Come installare un plug-in SnapCenter manualmente e direttamente dall'host del plug-in".

Fasi

1. Verificare se la cartella *C:/temp* esiste sull'host del plug-in e se l'utente che ha effettuato l'accesso dispone dell'accesso completo.
2. Scarica il plug-in SnapCenter per Microsoft Windows da *C:/ProgramData/NetApp/SnapCenter/Package* Repository.

   Questo percorso è accessibile dall'host in cui è installato il server SnapCenter.

3. Copiare il file di installazione nell'host su cui si desidera installare il plug-in.
4. Dal prompt dei comandi di Windows sull'host locale, accedere alla directory in cui sono stati salvati i file di installazione del plug-in.
5. Immettere il seguente comando per installare il plug-in.

   Snapcenter_Windows_host_plugin.exe"/silent /debuglog"<Debug_Log_Path>" /log"<Log_Path>" BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLDIR="<Install_Directory_Path>" BI_SERVICEACCOUNT=<domain\administrator> BI_SERVICEPWD=<password>

ISFeatureInstall=HPPW,SCW,SCE

Ad esempio:

_C: /ProgramData/NetApp/SnapCenter/Package Repository/Snapcenter_Windows_host_plugin.exe"/silent /debuglog"C: HPPW_SCSQL_Install.log" /log"C: Temp" BI_SMAPCENTER_PORT=8145 SUITE_INSTALLDIR="C: File del programma NetApp SnapCenter=Installazione_dominio_SERVISVISPSCI_SERVISSE_SERVISSE=Password_SERVISVISTUDI_SERVISTUDI_SERVISICA_SERVISICA_SERVISICA_SERVISICA_SPI

Tutti i parametri passati durante l'installazione del plug-in per Exchange sono sensibili al maiuscolo/minuscolo.

Inserire i seguenti valori per le variabili:

Variabile	Valore
/debuglog"<Debug_Log_Path>	Specificare il nome e la posizione del file di log del programma di installazione della suite, come nell'esempio seguente: *Setup.exe /debuglog"C: PathToLog.setupexe.log*
PORTA_BI_SNAPCENTER	Specificare la porta su cui SnapCenter comunica con SMCore.
SUITE_INSTALLDIR	Specificare la directory di installazione del pacchetto del plug-in host.
BI_SERVICEACCOUNT	Specificare il plug-in SnapCenter per l'account del servizio Web Microsoft Windows.
BI_SERVICEPWD	Specificare la password per l'account del servizio Web di SnapCenter per il plug-in Microsoft Windows.
ISFeatureInstall	Specificare la soluzione da implementare da SnapCenter sull'host remoto.

6. Monitorare il Task Scheduler di Windows, il file di log dell'installazione principale *C: Installdebug.log* e i file di installazione aggiuntivi in *C:/Temp*.
7. Monitorare la directory *%temp%* per verificare se i programmi di installazione *msiexe.exe* stanno installando il software senza errori.

L'installazione del plug-in per Exchange registra il plug-in sull'host e non sul server SnapCenter. È possibile registrare il plug-in sul server SnapCenter aggiungendo l'host utilizzando l'interfaccia grafica di SnapCenter o il cmdlet PowerShell. Una volta aggiunto l'host, il plug-in viene rilevato automaticamente.

Monitorare lo stato di installazione del pacchetto plug-in SnapCenter

È possibile monitorare lo stato di avanzamento dell'installazione del pacchetto plug-in di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento dell'installazione per determinare quando è completa o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filter** (filtro).
   b. Facoltativo: Specificare la data di inizio e di fine.
   c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).
   d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.
   e. Fare clic su **Apply** (Applica).
4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Configurare il certificato CA

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare una CSR, vedere "Come generare il file CSR del certificato CA".

Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato del file di importazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
   c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
   d. Copiare i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

      Get-ChildItem -Path Certate: LocalMachine/My

   b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

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

   Ad esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in
   dell'host Windows eseguendo i seguenti comandi:
   ```

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

   Ad esempio:

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

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.
5. Selezionare **attiva convalida certificato**.

Al termine

L’host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l’host del plug-in.

- * * Indica che il certificato CA non è né abilitato né assegnato all’host del plug-in.
- * * Indica che il certificato CA è stato convalidato correttamente.
- * * Indica che il certificato CA non può essere convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Configurare SnapManager 7.x per Exchange e SnapCenter in modo che coesistano

Per consentire la coesistenza del plug-in SnapCenter per Microsoft Exchange Server con SnapManager per Microsoft Exchange Server, è necessario installare il plug-in SnapCenter per Microsoft Exchange Server sullo stesso server Exchange su cui è installato SnapManager per Microsoft Exchange Server, disattivare SnapManager per le

pianificazioni Exchange, E configurare nuove pianificazioni e backup utilizzando il plug-in SnapCenter per Microsoft Exchange Server.

Prima di iniziare

- SnapManager per Microsoft Exchange Server e SnapDrive per Windows sono già installati e i backup di SnapManager per Microsoft Exchange Server sono presenti nel sistema e nella directory SnapInfo.
- Dovresti aver eliminato o recuperato i backup di SnapManager per Microsoft Exchange Server che non hai più bisogno.
- Tutte le pianificazioni create da SnapManager per Microsoft Exchange Server dovrebbero essere state sospese o eliminate dal programma di pianificazione di Windows.
- Il plug-in SnapCenter per Exchange Server e SnapManager per Microsoft Exchange Server possono coesistere sullo stesso server, ma non è possibile aggiornare le installazioni SnapManager per Microsoft Exchange Server esistenti a SnapCenter.

  SnapCenter non fornisce un'opzione per l'aggiornamento.

- SnapCenter non supporta il ripristino dei database Exchange da SnapManager per il backup di Microsoft Exchange Server.

  Se non si disinstalla SnapManager per Microsoft Exchange Server dopo l'installazione del plug-in SnapCenter e si desidera ripristinare un backup di SnapManager per Microsoft Exchange Server in un secondo momento, è necessario eseguire ulteriori operazioni.

Fasi

1. Utilizzando PowerShell su tutti i nodi DAG, determinare se il provider hardware SnapDrive per Windows VSS è registrato: *Provider elenco vssadmin*

   ```
   C:\Program Files\NetApp\SnapDrive>vssadmin list providers
   vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
   tool
   (C) Copyright 2001-2013 Microsoft Corp.

   Provider name: 'Data ONTAP VSS Hardware Provider'
      Provider type: Hardware
      Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
      Version: 7. 1. 4. 6845
   ```

2. Dalla directory SnapDrive, annullare la registrazione del provider hardware VSS da SnapDrive per Windows: *navssprv.exe -r service –u*
3. Verificare che il provider hardware VSS sia stato rimosso: *Provider elenco vssadmin*
4. Aggiungere l'host Exchange a SnapCenter, quindi installare il plug-in SnapCenter per Microsoft Windows e il plug-in SnapCenter per Microsoft Exchange Server.
5. Dalla directory del plug-in SnapCenter per Microsoft Windows su tutti i nodi DAG, verificare che il provider hardware VSS sia registrato: *Provider elenco vssadmin*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
   Version: 7. 0. 0. 5561
```

6. Interrompere le pianificazioni di backup di SnapManager per Microsoft Exchange Server.
7. Utilizzando l'interfaccia grafica di SnapCenter, creare backup on-demand, configurare backup pianificati e configurare le impostazioni di conservazione.
8. Disinstallare SnapManager per Microsoft Exchange Server.

   Se non si disinstalla SnapManager per Microsoft Exchange Server ora e successivamente si desidera ripristinare un backup di SnapManager per Microsoft Exchange Server:

   a. Annullare la registrazione del plug-in SnapCenter per Microsoft Exchange Server da tutti i nodi DAG: *navssprv.exe -r service -u*

      ```
      C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
      Windows>navssprv.exe -r service -u
      ```

   b. Dalla directory *C: Programmi NetApp, registrare SnapDrive per Windows su tutti i nodi DAG: _navssprv.exe -r service -a hostname -p password*

Installare il plug-in SnapCenter per VMware vSphere

Se il database o il file system sono memorizzati su macchine virtuali (VM), o se si desidera proteggere macchine virtuali e datastore, è necessario implementare il plug-in SnapCenter per l'appliance virtuale VMware vSphere.

Per informazioni sulla distribuzione, vedere "Panoramica sull'implementazione".

Implementare il certificato CA

Per configurare il certificato CA con il plug-in SnapCenter per VMware vSphere, vedere "Creare o importare un certificato SSL".

Configurare il file CRL

Il plug-in SnapCenter per VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il plug-in SnapCenter per VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Prepararsi alla protezione dei dati

Prima di eseguire qualsiasi operazione di protezione dei dati, ad esempio operazioni di backup, clonazione o ripristino, è necessario definire la strategia e impostare l'ambiente. È inoltre possibile configurare il server SnapCenter in modo che utilizzi le tecnologie SnapMirror e SnapVault.

Per sfruttare i vantaggi delle tecnologie SnapVault e SnapMirror, è necessario configurare e inizializzare una relazione di protezione dei dati tra i volumi di origine e di destinazione sul dispositivo di storage. È possibile utilizzare NetAppSystem Manager oppure la riga di comando della console di storage per eseguire queste attività.

Ulteriori informazioni

"Introduzione a REST API"

Prerequisiti per l'utilizzo del plug-in SnapCenter per Microsoft Exchange Server

Prima di utilizzare il plug-in per Exchange, l'amministratore di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività necessarie.

- Installare e configurare il server SnapCenter.
- Accedere a SnapCenter.
- Configurare l'ambiente SnapCenter aggiungendo o assegnando connessioni al sistema di storage e creando una credenziale.

  SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM supportata da SnapCenter deve avere un nome univoco.

- Aggiungere host, installare il plug-in SnapCenter per Microsoft Windows e il plug-in SnapCenter per Microsoft Exchange Server e individuare (aggiornare) le risorse.
- Eseguire il provisioning dello storage sul lato host utilizzando il plug-in SnapCenter per Microsoft Windows.
- Se si utilizza un server SnapCenter per proteggere i database Exchange che risiedono su LUN VMware RDM, è necessario implementare il plug-in SnapCenter per VMware vSphere e registrare il plug-in con SnapCenter. Il plug-in SnapCenter per la documentazione di VMware vSphere contiene ulteriori informazioni.

  I VMDK non sono supportati.

- Spostare un database Microsoft Exchange Server esistente da un disco locale allo storage supportato utilizzando gli strumenti di Microsoft Exchange.
- Impostare le relazioni di SnapMirror e SnapVault, se si desidera eseguire la replica del backup.

Per gli utenti di SnapCenter 4.1.1, la documentazione del plug-in SnapCenter per VMware vSphere 4.1.1 contiene informazioni sulla protezione dei database e dei file system virtualizzati. Per gli utenti di SnapCenter 4.2.x, NetApp Data Broker 1.0 e 1.0.1, la documentazione contiene informazioni sulla protezione dei database virtualizzati e dei file system mediante il plug-in SnapCenter per VMware vSphere fornito dall'appliance virtuale NetApp Data Broker basata su Linux (formato di appliance virtuale aperta). Per gli utenti di SnapCenter 4.3.x, la documentazione relativa al plug-in SnapCenter per VMware vSphere 4.3 contiene informazioni sulla protezione dei database e dei file system virtualizzati mediante il plug-in SnapCenter basato su Linux per

l'appliance virtuale VMware vSphere (formato appliance virtuale aperta).

"Plug-in SnapCenter per la documentazione di VMware vSphere"

Modalità di utilizzo delle risorse, dei gruppi di risorse e dei criteri per la protezione di Exchange Server

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, ripristino e reed che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- In genere, le risorse sono database di cassette postali o DAG (Database Availability Group) di Microsoft Exchange di cui si esegue il backup con SnapCenter.
- Un gruppo di risorse SnapCenter è un insieme di risorse su un host o un DAG Exchange e il gruppo di risorse può includere un intero DAG o singoli database.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

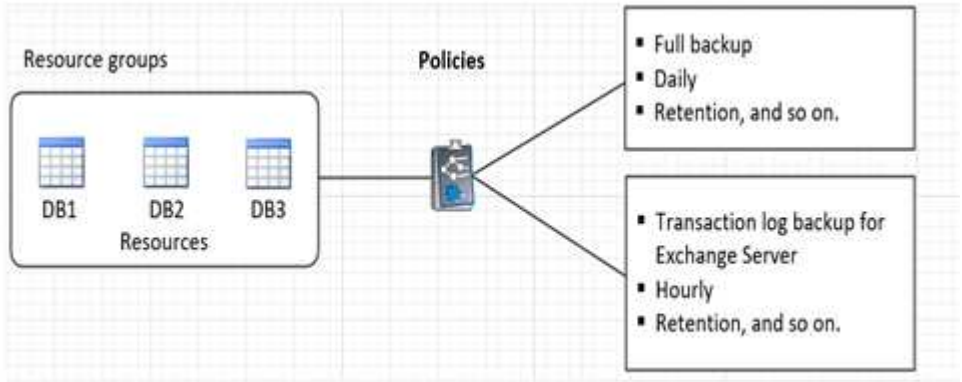
  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È inoltre possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

  I gruppi di risorse erano precedentemente noti come set di dati.

- I criteri specificano la frequenza di backup, la conservazione delle copie, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano uno o più criteri per tale gruppo. È inoltre possibile selezionare uno o più criteri quando si esegue un backup su richiesta per una singola risorsa.

Un gruppo di risorse definisce *cosa* si desidera proteggere e quando si desidera proteggerlo in termini di giorno e ora. Pensa a una policy come a definire *come* la vuoi proteggere. Ad esempio, se si esegue il backup di tutti i database di un host, è possibile creare un gruppo di risorse che includa tutti i database dell'host. È quindi possibile associare due criteri al gruppo di risorse: Una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si allegano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno e un altro programma che esegua i backup del registro ogni ora. L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i database:



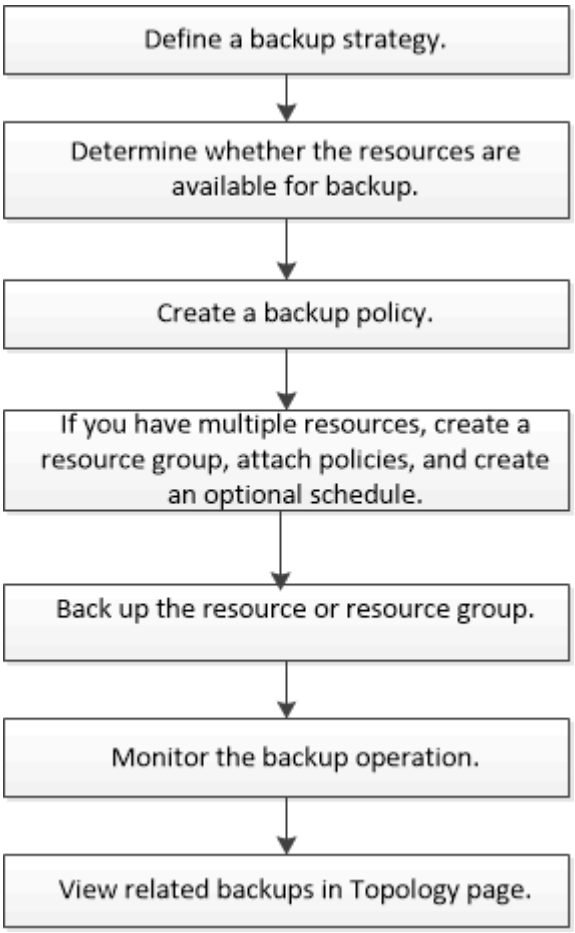
Eseguire il backup delle risorse Exchange

Workflow di backup

Quando si installa il plug-in SnapCenter per Microsoft Exchange Server nell'ambiente in uso, è possibile utilizzare SnapCenter per eseguire il backup delle risorse Exchange.

È possibile pianificare più backup per l'esecuzione simultanea tra i server. Le operazioni di backup e ripristino non possono essere eseguite contemporaneamente sulla stessa risorsa. Le copie di backup attive e passive sullo stesso volume non sono supportate.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:



Verifica del database e del backup di Exchange

Il plug-in SnapCenter per Microsoft Exchange Server non fornisce la verifica del backup; tuttavia, è possibile utilizzare lo strumento Eseutil fornito con Exchange per verificare i database e i backup di Exchange.

Lo strumento Microsoft Exchange Eseutil è un'utilità della riga di comando inclusa nel server Exchange. L'utility consente di eseguire controlli di coerenza per verificare l'integrità dei database e dei backup di Exchange.

Best practice: non è necessario eseguire controlli di coerenza sui database che fanno parte di una configurazione DAG (Database Availability Group) con almeno due repliche.

Per ulteriori informazioni, vedere "Documentazione di Microsoft Exchange Server".

Determinare se le risorse Exchange sono disponibili per il backup

Le risorse sono i database, i gruppi di disponibilità dei database Exchange gestiti dai plug-in installati. È possibile aggiungere tali risorse ai gruppi di risorse in modo da poter eseguire lavori di protezione dei dati, ma prima occorre identificare le risorse disponibili. La determinazione delle risorse disponibili verifica inoltre che l'installazione del plug-in sia stata completata correttamente.

Prima di iniziare

- È necessario aver già completato attività come l'installazione del server SnapCenter, l'aggiunta di host, la creazione di connessioni al sistema di storage, l'aggiunta di credenziali e l'installazione del plug-in per Exchange.
- Per sfruttare le funzionalità del software Single Mailbox Recovery, è necessario che il database attivo sia stato posizionato sul server Exchange in cui è installato il software Single Mailbox Recovery.
- Se i database risiedono su LUN VMware RDM, è necessario implementare il plug-in SnapCenter per VMware vSphere e registrare il plug-in con SnapCenter. "Plug-in SnapCenter per la documentazione di VMware vSphere"Dispone di ulteriori informazioni.

A proposito di questa attività

- Non è possibile eseguire il backup dei database se l'opzione **Stato generale** nella pagina Dettagli è impostata su non disponibile per il backup. L'opzione **Stato generale** è impostata su non disponibile per il backup quando si verifica una delle seguenti condizioni:
  - I database non si trovano su un LUN NetApp.
  - I database non sono in stato normale.

    I database non sono in stato normale quando sono in stato di mount, unmount, reseed o recovery pending.
- Se si dispone di un DAG (Database Availability Group), è possibile eseguire il backup di tutti i database del gruppo eseguendo il processo di backup dal DAG.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare **Microsoft Exchange Server** dall'elenco a discesa dei plug-in situato nell'angolo superiore sinistro della pagina risorse.
2. Nella pagina risorse, selezionare **Database**, **Database Availability Group** o **Resource Group** dall'elenco a discesa **View**.

   Tutti i database e i DAG vengono visualizzati con i relativi nomi host o DAG in formato FQDN, in modo da poter distinguere tra più database.

   Fare clic su  e selezionare il nome host e il server Exchange per filtrare le risorse. È quindi possibile fare clic su  per chiudere il riquadro del filtro.
3. Fare clic su **Aggiorna risorse**.

   Le risorse appena aggiunte, rinominate o eliminate vengono aggiornate nell'inventario del server SnapCenter.

È necessario aggiornare le risorse se i database vengono rinominati al di fuori di SnapCenter.

Le risorse vengono visualizzate insieme a informazioni quali nome della risorsa, nome del gruppo disponibilità database, server in cui il database è attualmente attivo, server con copie, ora dell'ultimo backup e stato generale.

- Se il database si trova su uno storage non NetApp, nella colonna Stato generale viene visualizzato non disponibile per il backup.

  In un DAG, se la copia del database attiva si trova su uno storage non NetApp e se almeno una copia passiva del database si trova sullo storage NetApp, nella colonna **Stato generale** viene visualizzato non protetto.

Non è possibile eseguire operazioni di protezione dei dati su un database che si trova su un tipo di storage non NetApp.

- Se il database si trova sullo storage NetApp e non è protetto, nella colonna **Stato generale** viene visualizzato non protetto.
- Se il database si trova su un sistema storage NetApp e viene protetto, l'interfaccia utente visualizza il messaggio Backup not run (Backup non eseguito) nella colonna **Overall Status** (Stato generale).
- Se il database si trova su un sistema storage NetApp ed è protetto e se il backup viene attivato per il database, l'interfaccia utente visualizza il messaggio Backup riuscito nella colonna **Stato generale**.

Creare criteri di backup per i database di Exchange Server

È possibile creare un criterio di backup per le risorse di Exchange o per i gruppi di risorse prima di utilizzare SnapCenter per eseguire il backup delle risorse di Exchange Server oppure creare un criterio di backup al momento della creazione di un gruppo di risorse o del backup di una singola risorsa.

Prima di iniziare

- Devi aver definito la tua strategia di protezione dei dati.

  Per ulteriori informazioni, vedere la sezione relativa alla definizione di una strategia di protezione dei dati per i database Exchange.

- Devi essere preparato per la protezione dei dati completando attività come l'installazione di SnapCenter, l'aggiunta di host, l'identificazione delle risorse e la creazione di connessioni al sistema di storage.
- È necessario aver aggiornato (rilevato) le risorse di Exchange Server.
- Se si stanno replicando Snapshot in un mirror o un vault, l'amministratore della SnapCenter deve aver assegnato le Storage Virtual Machine (SVM) per entrambi i volumi di origine e di destinazione.
- Se si desidera eseguire gli script PowerShell in prescritts e postscripts, è necessario impostare il valore del `usePowershellProcessforScripts` parametro su true nel `web.config` file.

  Il valore predefinito è false

A proposito di questa attività

- Un criterio di backup è un insieme di regole che regolano la gestione e la conservazione dei backup e la frequenza con cui viene eseguito il backup delle risorse o del gruppo di risorse. Inoltre, è possibile

specificare le impostazioni dello script. La specifica delle opzioni in un criterio consente di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.

- La conservazione completa del backup è specifica di una determinata policy. Un database o una risorsa che utilizza il criterio A con una conservazione completa del backup di 4 conserva 4 backup completi e non ha alcun effetto sul criterio B per lo stesso database o risorsa, che potrebbe avere una conservazione di 3 per conservare 3 backup completi.
- La conservazione del backup dei log è efficace in tutti i criteri e si applica a tutti i backup dei log di un database o di una risorsa. Pertanto, quando si esegue un backup completo utilizzando il criterio B, l'impostazione di conservazione del registro influisce sui backup del registro creati dal criterio A sullo stesso database o risorsa. Allo stesso modo, l'impostazione di conservazione dei log per il criterio A influisce sui backup dei log creati dal criterio B sullo stesso database.
- IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

  Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

  È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

  Best practice: è meglio configurare il criterio di conservazione secondario in base al numero di backup completi e di log che si desidera conservare. Quando si configurano policy di conservazione secondarie, occorre ricordare che quando database e registri si trovano in volumi diversi, ogni backup può avere tre snapshot, e quando database e log si trovano nello stesso volume, ogni backup può avere due snapshot.

- SnapLock
  - Se è selezionata l'opzione "conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere minore o uguale ai giorni di conservazione menzionati.

    La specifica di un periodo di blocco snapshot impedisce l'eliminazione delle istantanee fino alla scadenza del periodo di conservazione. Questo potrebbe portare a mantenere un numero di Snapshot maggiore del conteggio specificato nel criterio.

    Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

  Le impostazioni SnapLock primarie vengono gestite nel criterio di backup SnapCenter e le impostazioni SnapLock secondarie vengono gestite da ONTAP.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **nuovo**.
4. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
5. Nella pagina Backup Type (tipo di backup), attenersi alla seguente procedura:

   a. Scegliere il tipo di backup:

Se si desidera…	Eseguire questa operazione…
Eseguire il backup dei file di database e dei registri delle transazioni richiesti	Selezionare **Backup completo e Backup del registro**. Il backup dei database viene eseguito con il troncamento del log e viene eseguito il backup di tutti i log, inclusi quelli troncati. Si tratta del tipo di backup consigliato.
Eseguire il backup dei file di database e dei log delle transazioni non assegnate	Selezionare **Backup completo**. Il backup dei database viene eseguito con il troncamento del log e non viene eseguito il backup dei log troncati.
Eseguire il backup di tutti i log delle transazioni	Selezionare **Log backup**. Viene eseguito il backup di tutti i log delle transazioni nel file system attivo e non viene eseguito alcun troncamento del log. Sullo stesso disco del log live viene creata una directory *scebackupinfo*. Questa directory contiene il puntatore alle modifiche incrementali per il database Exchange e non è equivalente ai file di log completi.
Eseguire il backup di tutti i file di database e dei log delle transazioni senza troncare i file di log delle transazioni	Selezionare **Copy Backup** (Copia backup). Viene eseguito il backup di tutti i database e di tutti i registri e non viene eseguito alcun troncamento del registro. In genere, si utilizza questo tipo di backup per eseguire di nuovo la configurazione di una replica o per verificare o diagnosticare un problema.

È necessario definire lo spazio necessario per i backup dei log in base alla conservazione completa del backup e non in base alla conservazione up-to-the-minute (UTM).

Creare policy di vault separate per log e database quando si gestiscono volumi Exchange (LUN) e impostare il mantenimento (conservazione) del criterio di log sul doppio del numero per ciascuna etichetta del criterio di database, utilizzando le stesse etichette. Per ulteriori informazioni, vedere, "I backup di SnapCenter per Exchange conservano solo la metà delle istantanee sul volume di log di destinazione del vault"

b. Nella sezione Database Availability Group Settings (Impostazioni gruppo disponibilità database), selezionare un'azione:

Per questo campo…	Eseguire questa operazione…
Eseguire il backup delle copie attive	Selezionare questa opzione per eseguire il backup solo delle copie attive del database selezionato. Per i DAG (Database Availability Group), questa opzione esegue il backup solo delle copie attive di tutti i database nel DAG. Non viene eseguito il backup delle copie passive.
Copie di backup sui server da selezionare al momento della creazione del processo di backup	Selezionare questa opzione per eseguire il backup delle copie dei database sui server selezionati, sia attive che passive. Per i DAG, questa opzione consente di eseguire il backup delle copie attive e passive di tutti i database sui server selezionati.

Nelle configurazioni del cluster, i backup vengono conservati in ciascun nodo del cluster in base alle impostazioni di conservazione impostate nel criterio. Se il nodo proprietario del cluster cambia, i backup del nodo proprietario precedente verranno conservati. La conservazione è applicabile solo a livello di nodo.

c. Nella sezione Schedule frequency (frequenza pianificazione), selezionare uno o più tipi di frequenza: **On demand**, **Hourly**, **Daily**, **Weekly** e **Monthly**.

È possibile specificare la pianificazione (data di inizio, data di fine) per le operazioni di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e frequenza di backup, ma consente di assegnare diverse pianificazioni di backup a ciascun criterio.

Se sono previste le 2:00, la programmazione non verrà attivata durante l'ora legale (DST).

6. Nella pagina di conservazione, configurare le impostazioni di conservazione.

Le opzioni visualizzate dipendono dal tipo di backup e dal tipo di frequenza precedentemente selezionati.

Il valore massimo di conservazione è 1018 per le risorse su ONTAP 9.4 o versioni successive e 254 per le risorse su ONTAP 9.3 o versioni precedenti. I backup non avranno esito positivo se la conservazione viene impostata su un valore superiore a quello supportato dalla versione di ONTAP sottostante.

Se si intende attivare la replica SnapVault, è necessario impostare il numero di conservazione su 2 o superiore. Se si imposta il conteggio della conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è il Snapshot di riferimento per la relazione SnapVault fino a quando una snapshot più recente non viene replicata nella destinazione.

a. Nella sezione Impostazioni conservazione backup registro, selezionare una delle seguenti opzioni:

Se si desidera…	Eseguire questa operazione…
Conserva solo un numero specifico di backup del log	Selezionare **numero di backup completi per i quali vengono conservati i registri** e specificare il numero di backup completi per i quali si desidera eseguire un ripristino up-to-the-minute. La conservazione UTM (up-to-the-minute) si applica al backup del registro creato tramite backup completo o del registro. Ad esempio, se le impostazioni di conservazione UTM sono configurate per conservare i backup dei log degli ultimi 5 backup completi, i backup dei log degli ultimi 5 backup completi vengono conservati. Le cartelle di log create come parte dei backup completi e dei log vengono automaticamente eliminate come parte di UTM. Non è possibile eliminare manualmente le cartelle di log. Ad esempio, se l'impostazione di conservazione Full (completa) o Full (completa) e Log Backup (Backup registro) è impostata su 1 mese e UTM Retention (conservazione UTM) è impostata su 10 giorni, la cartella di registro creata come parte di questi backup verrà eliminata come da UTM. Di conseguenza, saranno presenti solo cartelle di log di 10 giorni e tutti gli altri backup saranno contrassegnati per il ripristino point-in-time. È possibile impostare il valore di conservazione UTM su 0, se non si desidera eseguire un ripristino up-to-the-minute. In questo modo si attiva l'operazione di ripristino point-in-time. **Procedura consigliata:** è consigliabile che l'impostazione sia uguale all'impostazione per Total Snapshots (backup completi) nella sezione Impostazioni di conservazione del backup completo. In questo modo, i file di registro vengono conservati per ogni backup completo.
Conservare le copie di backup per un numero specifico di giorni	Selezionare l'opzione **Mantieni backup registro per ultimo** e specificare il numero di giorni in cui conservare le copie di backup del registro. I backup del registro vengono conservati fino al numero di giorni di backup completi.

Se si desidera…	Eseguire questa operazione…
Periodo di blocco delle istantanee	Selezionare **periodo blocco copia istantanea**, quindi giorni, mesi o anni. Il periodo di conservazione di SnapLock deve essere inferiore a 100 anni.

Se è stato selezionato **Log backup** come tipo di backup, i backup dei log vengono conservati come parte delle impostazioni di conservazione aggiornate al minuto per i backup completi.

b. Nella sezione Full backup retention settings (Impostazioni di conservazione backup complete), selezionare una delle seguenti opzioni per i backup on-demand, quindi selezionarne una per i backup completi:

Per questo campo…	Eseguire questa operazione…
Conserva solo un numero specifico di snapshot	Se si desidera specificare il numero di backup completi da conservare, selezionare l'opzione **Total Snapshot Copies to Keep** (copie snapshot totali da conservare) e specificare il numero di snapshot (backup completi) da conservare. Se il numero di backup completi supera il numero specificato, i backup completi che superano il numero specificato vengono eliminati, con le copie meno recenti eliminate per prime.
Conserva backup completi per un numero specifico di giorni	Selezionare l'opzione **Mantieni copie snapshot per** e specificare il numero di giorni in cui conservare le istantanee (backup completi).
Periodo di blocco delle istantanee	Selezionare **periodo blocco copia istantanea**, quindi giorni, mesi o anni. Il periodo di conservazione di SnapLock deve essere inferiore a 100 anni.

Se si dispone di un database con solo backup di log e nessun backup completo su un host in una configurazione DAG, i backup di log vengono conservati nei seguenti modi:

- Per impostazione predefinita, SnapCenter trova il backup completo più vecchio per questo database in tutti gli altri host del DAG ed elimina tutti i backup del registro su questo host che sono stati eseguiti prima del backup completo.
- È possibile eseguire l'override del comportamento di conservazione predefinito di un database su un host in un DAG con solo backup di log aggiungendo la chiave **MaxLogBackupOnlyCountWithoutFullBackup** nel file *C: File di programma/NetApp/SnapCenter WebApp/web.config*.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

Nell'esempio, il valore 10 significa che si mantengono fino a 10 backup del log sull'host.

7. Nella pagina Replication (Replica), selezionare una o entrambe le seguenti opzioni di replica secondaria:

Per questo campo…	Eseguire questa operazione…
Update SnapMirror dopo la creazione di una snapshot locale Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante **Aggiorna** nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP. Vedere "Visualizzare i backup di Exchange nella pagina topologia".	Selezionare questa opzione per conservare le copie mirror dei set di backup su un altro volume (SnapMirror).
Aggiornare SnapVault dopo aver creato un'istantanea locale	Selezionare questa opzione per eseguire la replica del backup disk-to-disk.
Etichetta del criterio secondario	Selezionare un'etichetta Snapshot. A seconda dell'etichetta Snapshot selezionata, ONTAP applica la politica di conservazione Snapshot secondaria corrispondente all'etichetta. Se è stato selezionato **Update SnapMirror dopo la creazione di una copia Snapshot locale**, è possibile specificare l'etichetta del criterio secondario. Tuttavia, se è stato selezionato **Aggiorna SnapVault dopo la creazione di una copia Snapshot locale**, è necessario specificare l'etichetta del criterio secondario.
Numero tentativi di errore	Immettere il numero di tentativi di replica che devono verificarsi prima dell'arresto del processo.

È necessario configurare il criterio di conservazione SnapMirror in ONTAP per lo storage secondario, in modo da evitare di raggiungere il limite massimo di Snapshot sullo storage secondario.

8. Nella pagina script, immettere il percorso e gli argomenti del prespt o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di backup.
   - Gli argomenti di backup prescrittivi includono "` database`" e "``` ServerInstance".
   - Gli argomenti di backup PostScript includono "` database`", "` ServerInstance`", "` BackupName`", "` LogDirectory`" e "``` LogSnapshot".

     È possibile eseguire uno script per aggiornare i trap SNMP, automatizzare gli avvisi, inviare i registri e così via.

     Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.
9. Esaminare il riepilogo, quindi fare clic su **fine**.

Creare gruppi di risorse e associare criteri per i server Exchange

Per qualsiasi lavoro di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario associare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire e la pianificazione della protezione.

A proposito di questa attività

- IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

  Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

  È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in Microsoft Exchange Server dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** dall'elenco **View** (Visualizza).

   Se di recente è stata aggiunta una risorsa a SnapCenter, fare clic su **Aggiorna risorse** per visualizzare la risorsa appena aggiunta.
3. Fare clic su **New Resource Group** (nuovo gruppo di risorse).
4. Nella pagina Name (Nome), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere il nome del gruppo di risorse. Il nome del gruppo di risorse non deve superare i 250 caratteri.
Tag	Inserire una o più etichette per facilitare la ricerca del gruppo di risorse in un secondo momento. Ad esempio, se si aggiunge HR come tag a più gruppi di risorse, è possibile trovare in seguito tutti i gruppi di risorse associati al tag HR.
USA il formato nome personalizzato per la copia Snapshot	Opzionale: Immettere un nome e un formato dell'istantanea personalizzato. Ad esempio, *customtext_resourcegroup_policy_hostname* o *resourcegroup_hostname*. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

5. Nella pagina risorse, attenersi alla seguente procedura:
   a. Selezionare il tipo di risorsa e gli elenchi a discesa Database Availability Group from (Gruppo disponibilità database da) per filtrare l'elenco delle risorse disponibili.

      Le risorse aggiunte di recente vengono visualizzate nell'elenco delle risorse disponibili solo dopo l'aggiornamento dell'elenco delle risorse.

      Nelle sezioni Available Resources (risorse disponibili) e Selected Resources (risorse selezionate), il nome del database viene visualizzato con l'FQDN dell'host. Questo FQDN indica solo che il database è attivo su quell'host specifico e potrebbe non eseguire il backup su questo host. Selezionare uno o più server di backup dall'opzione Server selection (selezione server), in cui si desidera eseguire il backup nel caso in cui sia stata selezionata l'opzione **Backup delle copie sui server da selezionare al momento della creazione del processo di backup** nel criterio.

   b. Digitare il nome della risorsa nella casella di testo di ricerca oppure scorrere per individuare una risorsa.
   c. Per spostare le risorse dalla sezione risorse disponibili alla sezione risorse selezionate, eseguire una delle seguenti operazioni:
      - Selezionare **selezione automatica di tutte le risorse sullo stesso volume di storage** per spostare tutte le risorse dello stesso volume nella sezione risorse selezionate.
      - Selezionare le risorse dalla sezione risorse disponibili, quindi fare clic sulla freccia destra per spostarle nella sezione risorse selezionate.

        I gruppi di risorse di SnapCenter per Microsoft Exchange Server non possono avere più di 30 database per snapshot. Se sono presenti più di 30 database in un gruppo di risorse, viene creata una seconda istantanea per i database aggiuntivi. Pertanto, vengono creati 2 job secondari nel processo di backup principale. Per i backup con replica secondaria, mentre è in corso

l'aggiornamento di SnapMirror o SnapVault, potrebbero esserci scenari in cui l'aggiornamento per entrambi i lavori secondari si sovrappone. Il processo di backup principale rimane in esecuzione per sempre anche se i registri indicano che il processo è stato completato.

6. Nella pagina Criteri, attenersi alla seguente procedura:

   a. Selezionare uno o più criteri dall'elenco a discesa.

      È anche possibile creare una policy facendo clic su * *  .

      Se un criterio contiene l'opzione **Backup delle copie sui server da selezionare al momento della creazione del processo di backup**, viene visualizzata un'opzione di selezione del server per selezionare uno o più server. L'opzione di selezione del server elenca solo il server in cui il database selezionato si trova sullo storage NetApp.

      Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

   b. Nella sezione Configura pianificazioni per i criteri selezionati, fare clic su *  **nella colonna *Configura pianificazioni** per il criterio per il quale si desidera configurare la pianificazione.

   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione specificando la data di inizio, la data di scadenza e la frequenza, quindi fare clic su **OK**.

      È necessario eseguire questa operazione per ciascuna frequenza elencata nella policy. I piani di lavoro configurati sono elencati nella colonna **piani di lavoro applicati** della sezione Configura piani di lavoro per i criteri selezionati.

   Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup di SnapCenter.

7. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report**.

   Per la notifica e-mail, è necessario specificare i dettagli del server SMTP utilizzando la GUI o il comando PowerShell `Set-SmSmtpServer`.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

8. Esaminare il riepilogo, quindi fare clic su **fine**.

Eseguire il backup dei database Exchange

Se un database non fa parte di alcun gruppo di risorse, è possibile eseguire il backup del database o del gruppo disponibilità database dalla pagina risorse.

Prima di iniziare

- È necessario aver creato una policy di backup.
- È necessario assegnare l'aggregato utilizzato dall'operazione di backup alla SVM utilizzata dal database.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con uno storage secondario, il ruolo assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Se si desidera eseguire il backup di un database o di un Database Availability Group con copia del database attiva/passiva su uno storage NetApp e non NetApp, Inoltre, è stata selezionata l'opzione **Backup delle copie attive** o **Backup delle copie sui server da selezionare durante l'ora di creazione del processo di backup** nel criterio, i processi di backup passano allo stato di avviso. Il backup avrà esito positivo per la copia del database attiva/passiva sullo storage NetApp e il backup non avrà esito positivo per la copia del database attiva/passiva su storage non NetApp.

  Best practice: non eseguire contemporaneamente backup di database attivi e passivi. Può verificarsi una race condition e uno dei backup potrebbe non riuscire.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare **plug-in Microsoft Exchange Server** dall'elenco.
2. Nella pagina risorse, selezionare **Database** o **Database Availability Group** dall'elenco **View**.

   Nella pagina Resources, l'  icona indica che il database si trova su sistemi di storage non NetApp.

   In un DAG, se una copia del database attiva si trova su uno storage non NetApp e almeno una copia passiva del database risiede su uno storage NetApp, è possibile proteggere il database.

Fare clic su  , quindi selezionare il nome host e il tipo di database per filtrare le risorse. È quindi possibile fare clic su  per chiudere il riquadro del filtro.

- Se si desidera eseguire il backup di un database, fare clic sul nome del database.
  a. Se viene visualizzata la vista topologia, fare clic su **Protect** (protezione).
  b. Se viene visualizzata la procedura guidata Database - Protect Resource, passare alla fase 3.
- Se si desidera eseguire il backup di un gruppo di disponibilità database, fare clic sul nome del gruppo di disponibilità database.
  a. Se si desidera specificare un nome istantanea personalizzato, nella pagina risorse selezionare la casella di controllo **Usa formato nome personalizzato per copia istantanea**, quindi immettere un formato nome personalizzato che si desidera utilizzare per il nome istantanea.

     Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

  b. Nella pagina Criteri, attenersi alla seguente procedura:
     i. Selezionare uno o più criteri dall'elenco a discesa.

     È inoltre possibile creare un criterio facendo clic su  .

Se un criterio contiene l'opzione **Backup delle copie sui server da selezionare al momento della creazione del processo di backup**, viene visualizzata un'opzione di selezione del server per selezionare uno o più server. L'opzione di selezione del server elenca solo il server in cui il database selezionato si trova su uno storage NetApp.

Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

c. Fare clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

d. Nella finestra Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.

Dove *policy_name* è il nome del criterio selezionato.

Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate). . Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

+ è inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di backup eseguita sulla risorsa, selezionare **Attach Job Report**.

+ NOTA: Per la notifica tramite e-mail, è necessario specificare i dettagli del server SMTP utilizzando la GUI o il comando PowerShell set-SmtpServer.

i. Esaminare il riepilogo, quindi fare clic su **fine**.

Viene visualizzata la pagina della topologia del database.

ii. Fare clic su **Esegui backup ora**.

iii. Nella pagina Backup, attenersi alla seguente procedura:

e. Se sono stati applicati più criteri alla risorsa, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

f. Fare clic su **Backup**.

i. Monitorare l'avanzamento del backup facendo doppio clic sul processo nel riquadro attività nella parte inferiore della pagina per visualizzare la pagina Dettagli lavoro.

- Nelle configurazioni MetroCluster, SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

  Per informazioni, vedere: "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover di MetroCluster"

- Se si esegue il backup dei dati delle applicazioni su VMDK e la dimensione dell'heap Java per il plug-in SnapCenter per VMware vSphere non è sufficiente, il backup potrebbe non riuscire.

Per aumentare la dimensione dell'heap Java, individuare il file script */opt/netapp/init_scripts/scvservice*. In questo script, il comando *do_start method* avvia il servizio plug-in VMware di SnapCenter. Aggiornare il comando al seguente: *Java -jar -Xmx8192M -Xms4096M*

Eseguire il backup dei gruppi di risorse di Exchange

Un gruppo di risorse è una raccolta di risorse su un host o su un DAG Exchange e il gruppo di risorse può includere un intero DAG o singoli database. È possibile eseguire il backup dei gruppi di risorse dalla pagina risorse.

Prima di iniziare

- È necessario aver creato un gruppo di risorse con un criterio allegato.
- È necessario assegnare l'aggregato utilizzato dall'operazione di backup alla SVM (Storage Virtual Machine) utilizzata dal database.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con uno storage secondario, il ruolo assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Se un gruppo di risorse dispone di più database provenienti da host diversi, l'operazione di backup su alcuni host potrebbe iniziare in ritardo a causa di problemi di rete. È necessario configurare il valore di `MaxRetryForUninitializedHosts` in `web.config` utilizzando il `Set-SmConfigSettings` cmdlet PowerShell.
- In un gruppo di risorse, se si include un database o un gruppo di disponibilità del database con copia del database attiva/passiva su uno storage NetApp e non NetApp e si è selezionata l'opzione **Backup delle copie attive** o **Backup delle copie sui server da selezionare durante il tempo di creazione del processo di backup** nella policy, i processi di backup passano quindi allo stato di avviso.

  Il backup avrà esito positivo per la copia del database attiva/passiva sullo storage NetApp e il backup non avrà esito positivo per la copia del database attiva/passiva su storage non NetApp.

A proposito di questa attività

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina risorse. Se un gruppo di risorse dispone di un criterio associato e di una pianificazione configurata, i backup vengono eseguiti automaticamente in base alla pianificazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare **plug-in Microsoft Exchange Server** dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).

   È possibile eseguire una ricerca nel gruppo di risorse immettendo il nome del gruppo di risorse nella casella di ricerca oppure facendo clic su , quindi selezionando il tag. È quindi possibile fare clic su per chiudere il riquadro del filtro.

3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi fare clic su **Esegui backup ora**.
4. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se sono stati associati più criteri al gruppo di risorse, selezionare il criterio da utilizzare per il backup

dall'elenco a discesa **Policy**.

Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

b. Fare clic su **Backup**.

5. Monitorare l'avanzamento del backup facendo doppio clic sul processo nel riquadro attività nella parte inferiore della pagina per visualizzare la pagina Dettagli lavoro.

Creare una connessione al sistema di storage e una credenziale utilizzando i cmdlet PowerShell per Exchange Server

Prima di utilizzare i cmdlet PowerShell per eseguire il backup e il ripristino, è necessario creare una connessione SVM (Storage Virtual Machine) e una credenziale.

Prima di iniziare

- L'ambiente PowerShell dovrebbe essere stato preparato per l'esecuzione dei cmdlet PowerShell.
- Per creare le connessioni storage, è necessario disporre delle autorizzazioni necessarie nel ruolo Infrastructure Admin.
- Assicurarsi che le installazioni dei plug-in non siano in corso.

  Le installazioni dei plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage perché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nella GUI di SnapCenter come "non disponibile per il backup" o "non su storage NetApp".

- I nomi dei sistemi di storage devono essere univoci.

  SnapCenter non supporta più sistemi storage con lo stesso nome su cluster diversi. Ogni sistema storage supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dei dati univoco.

Fasi

1. Avviare una sessione di connessione PowerShell con il `Open-SmConnection` cmdlet.

   Questo esempio apre una sessione PowerShell:

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

2. Creare una nuova connessione al sistema di storage utilizzando il `Add-SmStorageConnection` cmdlet.

   Questo esempio crea una nuova connessione al sistema di storage:

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

3. Creare un nuovo account Esegui come utilizzando il `Add-Credential` cmdlet.

In questo esempio viene creato un nuovo account Run As denominato ExchangeAdmin con credenziali Windows:

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Eseguire il backup delle risorse Exchange utilizzando i cmdlet PowerShell

Il backup di un database di Exchange Server include la connessione con il server SnapCenter, il rilevamento del database, l'aggiunta di un criterio, la creazione di un gruppo di risorse di backup, il backup e la visualizzazione dello stato del backup.

Prima di iniziare

- È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- È necessario aver aggiunto la connessione al sistema di storage e creato una credenziale.
- È necessario aggiungere host e rilevare risorse.

Il plug-in per Exchange non supporta le operazioni di cloni, pertanto il parametro CloneType per il cmdlet Add-SmPolicy non è supportato per il plug-in per Exchange

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

   Viene visualizzato il prompt di nome utente e password.

2. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   In questo esempio viene creata una nuova policy di backup con un backup completo e un tipo di backup di log Exchange:

   ```
   C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
   -PolicyType Backup -PluginPolicytype SCE -SceBackupType
   FullBackupAndLogBackup -BackupActiveCopies
   ```

   In questo esempio viene creata una nuova policy di backup con un backup orario completo e un tipo di backup di log Exchange:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly
-RetentionSettings
@{'BackupType'='DATA';'ScheduleType'='Hourly';'RetentionCount'='10'}
```

Questo esempio crea un nuovo criterio di backup per eseguire il backup solo dei registri di Exchange:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Individuare le risorse host utilizzando il cmdlet Get-SmResources.

   In questo esempio vengono illustrate le risorse per il plug-in di Microsoft Exchange Server sull'host specificato:

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

4. Aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   In questo esempio viene creato un nuovo gruppo di risorse di backup del database Exchange Server con i criteri e le risorse specificati:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bk
p_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange
Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-
w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

   In questo esempio viene creato un nuovo gruppo di risorse di backup di Exchange Database Availability Group (DAG) con i criteri e le risorse specificati:

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode SCE
-Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bk
p_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability
Group";"Names"="DAGSCE0102"}
```

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

Questo esempio crea un nuovo backup sullo storage secondario:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Visualizzare lo stato del processo di backup utilizzando il cmdlet Get-SmBackupReport.

Questo esempio visualizza un report di riepilogo di tutti i lavori eseguiti alla data specificata:

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

Questo esempio visualizza un report di riepilogo del lavoro per un ID lavoro specifico:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, vedere "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di backup

È possibile monitorare l'avanzamento di diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere necessario controllare i progressi per determinare quando sono stati completati o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, attenersi alla seguente procedura:
   a. Fare clic  per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Status** (Stato), selezionare lo stato del backup.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene venga visualizzato lo stato del processo di backup , quando si fa clic sui dettagli del processo, è possibile che alcune delle attività secondarie dell'operazione di backup siano ancora in corso o contrassegnate da segnali di avviso.

5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Monitorare le operazioni nel riquadro attività

Il riquadro Activity (attività) visualizza le cinque operazioni più recenti eseguite. Il riquadro Activity (attività) visualizza anche il momento in cui l'operazione è stata avviata e lo stato dell'operazione.

Il riquadro Activity (attività) visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Fare clic  sul riquadro attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli commessa**.

Annullare le operazioni di backup per il database Exchange

È possibile annullare le operazioni di backup inserite nella coda.

Cosa ti serve

- Per annullare le operazioni, è necessario accedere come amministratore SnapCenter o come proprietario del processo.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- Per annullare le operazioni di backup, è possibile utilizzare l'interfaccia grafica utente di SnapCenter, i cmdlet PowerShell o i comandi CLI.

- Il pulsante **Annulla lavoro** è disattivato per le operazioni che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di backup in coda degli altri membri durante l'utilizzo di tale ruolo.

Fasi

1. Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	a. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**.
Riquadro delle attività	a. Dopo aver avviato l'operazione di backup, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. b. Selezionare l'operazione. c. Nella pagina Dettagli processo, fare clic su **Annulla processo**.

L'operazione viene annullata e la risorsa viene riportata allo stato precedente.

Rimuovere i backup di Exchange utilizzando i cmdlet PowerShell

È possibile utilizzare il cmdlet Remove-SmBackup per eliminare i backup di Exchange se non sono più necessari per altre operazioni di protezione dei dati.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Eliminare uno o più backup utilizzando il `Remove-SmBackup` cmdlet.

   Questo esempio elimina due backup utilizzando i relativi ID di backup:

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

Visualizzare i backup di Exchange nella pagina topologia

Quando si prepara il backup di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup sullo storage primario e secondario.

A proposito di questa attività

Nella pagina topologia, è possibile visualizzare tutti i backup disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e selezionarli per eseguire le operazioni di protezione dei dati.

È possibile esaminare la seguente icona nella vista Manage Copies (Gestisci copie) per determinare se i backup sono disponibili sullo storage primario o secondario (copie Mirror o copie Vault).

-  visualizza il numero di backup disponibili sullo storage primario.
-  Visualizza il numero di backup di cui viene eseguito il mirroring sullo storage secondario utilizzando la tecnologia SnapMirror.
-  Visualizza il numero di backup replicati sullo storage secondario utilizzando la tecnologia SnapVault.
    - Il numero di backup visualizzati include i backup eliminati dallo storage secondario.

      Ad esempio, se sono stati creati 6 backup utilizzando un criterio per conservare solo 4 backup, il numero di backup visualizzato è 6.

Best practice: per garantire che venga visualizzato il numero corretto di backup replicati, si consiglia di aggiornare la topologia.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare il database, la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina topologia della risorsa selezionata.

4. Consultare la sezione Summary Card (scheda di riepilogo) per visualizzare un riepilogo del numero di backup disponibili sullo storage primario e secondario.

   La sezione Summary Card (scheda di riepilogo) visualizza il numero totale di backup e il numero totale di backup del registro.

   Facendo clic sul pulsante **Refresh** viene avviata una query dello storage per visualizzare un conteggio accurato.

   Se viene eseguito il backup abilitato SnapLock, facendo clic sul pulsante **Aggiorna** si aggiornano i tempi di scadenza SnapLock primari e secondari recuperati da ONTAP. Inoltre, una pianificazione settimanale aggiorna il tempo di scadenza SnapLock primario e secondario recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza del SnapLock per il backup sarà il tempo di scadenza del SnapLock più lungo impostato per una Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Dopo il backup su richiesta, facendo clic sul pulsante **Refresh** (Aggiorna) vengono aggiornati i dettagli del backup o della clonazione.

5. Nella vista Manage Copies (Gestisci copie), fare clic su **Backup** dallo storage primario o secondario per visualizzare i dettagli di un backup.

   I dettagli dei backup vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, ridenominazione ed eliminazione.

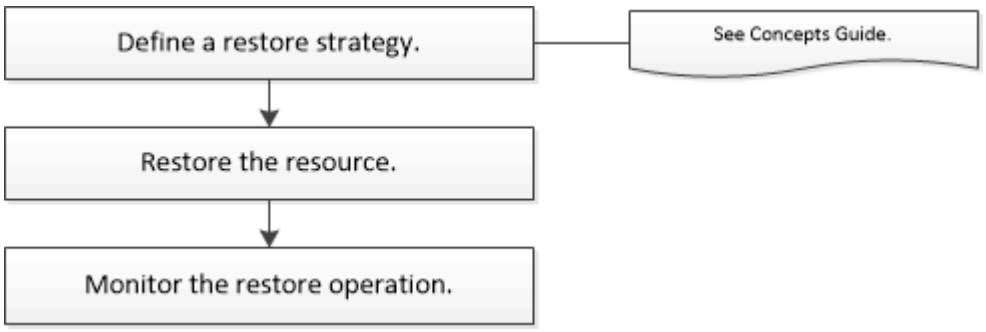
   Non è possibile rinominare o eliminare i backup presenti nello storage secondario. L'eliminazione delle istantanee viene gestita dalle impostazioni di conservazione di ONTAP.

Ripristinare le risorse Exchange

Ripristinare il flusso di lavoro

È possibile utilizzare SnapCenter per ripristinare i database Exchange ripristinando uno o più backup nel file system attivo.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di ripristino del database di Exchange:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup

e ripristino. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la Guida dei cmdlet di SnapCenter o consultare "Guida di riferimento al cmdlet del software SnapCenter".

Requisiti per il ripristino di un database Exchange

Prima di ripristinare un database di Exchange Server da un plug-in SnapCenter per il backup di Microsoft Exchange Server, è necessario assicurarsi che siano soddisfatti diversi requisiti.

Per utilizzare completamente la funzionalità di ripristino, è necessario aggiornare il server SnapCenter e il plug-in SnapCenter per il database Exchange alla versione 4.6.

- Exchange Server deve essere in linea e in esecuzione prima di poter ripristinare un database.
- I database devono essere presenti su Exchange Server.

  Il ripristino dei database cancellati non è supportato.

- Le pianificazioni SnapCenter per il database devono essere sospese.
- Il server SnapCenter e il plug-in SnapCenter per l'host devono essere connessi allo storage primario e secondario contenente i backup che si desidera ripristinare.

Ripristinare i database Exchange

È possibile utilizzare SnapCenter per ripristinare i database Exchange di cui è stato eseguito il backup.

Prima di iniziare

- È necessario aver eseguito il backup dei gruppi di risorse, del database o dei DAG (Database Availability Group).
- Quando il database Exchange viene migrato in un'altra posizione, l'operazione di ripristino non funziona per i backup precedenti.
- Se si stanno replicando Snapshot in un mirror o un vault, l'amministratore di SnapCenter deve aver assegnato le SVM sia per i volumi di origine che per quelli di destinazione.
- In un DAG, se una copia del database attiva si trova su uno storage non NetApp e si desidera eseguire il ripristino dal backup passivo della copia del database presente su uno storage NetApp, eseguire la copia passiva (storage NetApp) come copia attiva, aggiornare le risorse ed eseguire l'operazione di ripristino.

  Eseguire `Move-ActiveMailboxDatabase` il comando per creare la copia passiva del database come copia attiva del database.

  ```
  https://docs.microsoft.com/en-us/powershell/module/exchange/move-
  activemailboxdatabase?view=exchange-ps["Documentazione
  Microsoft"^]Contiene informazioni su questo comando.
  ```

A proposito di questa attività

- Quando si esegue un'operazione di ripristino su un database, il database viene montato nuovamente sullo stesso host e non viene creato alcun nuovo volume.

- I backup a livello DI DAG devono essere ripristinati da singoli database.
- Il ripristino completo del disco non è supportato quando esistono file diversi dal file di database Exchange (.edb).

  Il plug-in per Exchange non esegue un ripristino completo su un disco se il disco contiene file Exchange come quelli utilizzati per la replica. Quando un ripristino completo potrebbe influire sulla funzionalità di Exchange, Plug-in per Exchange esegue una singola operazione di ripristino dei file.

- Il plug-in per Exchange non è in grado di ripristinare le unità crittografate di BitLocker.
- IL PERCORSO_SCRIPT viene definito utilizzando la chiave PredesedWindowsScriptsDirectory situata nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Si consiglia di utilizzare il percorso predefinito per la protezione.

  Il valore della chiave può essere visualizzato da swagger attraverso l'API: API /4.7/configsettings

  È possibile utilizzare L'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Resources** nell'angolo superiore sinistro della pagina Resource.
2. Selezionare il plug-in di Exchange Server dall'elenco a discesa.
3. Nella pagina Resources (risorse), selezionare **Database** dall'elenco View (Visualizza).
4. Selezionare il database dall'elenco.
5. Nella vista Gestisci copie, selezionare **backup**, dalla tabella Backup primari, quindi fare clic su * *  .
6. Nella pagina Opzioni, selezionare una delle seguenti opzioni di backup del registro:

Opzione	Descrizione
Tutti i backup dei log	Scegliere **All log backups** (tutti i backup dei log) per eseguire un'operazione di backup di ripristino aggiornata al minuto per ripristinare tutti i backup dei log disponibili dopo il backup completo.

Opzione	Descrizione
In base ai backup dei log fino a.	Scegliere **by log backups until** per eseguire un'operazione di ripristino point-in-time, che ripristina il database in base ai backup dei log fino al log selezionato. Il numero di registri visualizzati nell'elenco a discesa si basa su UTM. Ad esempio, se la conservazione completa del backup è 5 e la conservazione UTM è 3, il numero di backup del registro disponibili è 5, ma nell'elenco a discesa vengono elencati solo 3 registri per eseguire l'operazione di ripristino.
Per data specifica fino al	Scegliere **per data specifica fino a** per specificare la data e l'ora in cui i registri delle transazioni vengono applicati al database ripristinato. Questa operazione di ripristino point-in-time ripristina le voci del log delle transazioni registrate fino all'ultimo backup nella data e nell'ora specificate.
Nessuno	Scegliere **None** (Nessuno) quando è necessario ripristinare solo il backup completo senza alcun backup del registro.

È possibile eseguire una delle seguenti operazioni:

- **Recover and mount database after restore (Ripristina e monta database dopo il ripristino)** - questa opzione è selezionata per impostazione predefinita.
- **Non verificare l'integrità dei log delle transazioni nel backup prima del ripristino** - per impostazione predefinita, SnapCenter verifica l'integrità dei log delle transazioni in un backup prima di eseguire un'operazione di ripristino.

  Best practice: non selezionare questa opzione.

7. Nella pagina script, immettere il percorso e gli argomenti del prespt o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di ripristino.

   Gli argomenti prescrittivi del ripristino includono il database e l'istanza del server.

   Gli argomenti relativi al ripristino postscript includono: Database, ServerInstance, BackupName, LogDirectory e TargetServerInstance.

   È possibile eseguire uno script per aggiornare i trap SNMP, automatizzare gli avvisi, inviare i registri e così via.

Il percorso prescripts o postscripts non deve includere dischi o condivisioni. Il percorso deve essere relativo al PERCORSO_SCRIPT.

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail.

9. Esaminare il riepilogo, quindi fare clic su **fine**.
10. È possibile visualizzare lo stato del processo di ripristino espandendo il pannello attività nella parte inferiore della pagina.

    È necessario monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

Quando si ripristina un database attivo da un backup, il database passivo potrebbe andare in stato di sospensione o di errore se si verifica un ritardo tra la replica e il database attivo.

La modifica dello stato può verificarsi quando la catena di log del database attivo passa e inizia una nuova filiale che interrompe la replica. Exchange Server tenta di correggere la replica, ma se non è in grado di farlo, dopo il ripristino, è necessario creare un nuovo backup e quindi eseguire nuovamente il reeeding della replica.

Ripristino granulare di e-mail e mailbox

Il software SMBR (Single Mailbox Recovery) consente di ripristinare e ripristinare i messaggi e-mail o le caselle postali anziché l'intero database Exchange.

Il ripristino di un database completo solo per recuperare un singolo messaggio di posta consumerà molto tempo e risorse. SMBR consente di recuperare rapidamente i messaggi di posta creando una copia clone di Snapshot e utilizzando le API Microsoft per montare la casella di posta in SMBR. Per informazioni su come utilizzare SMBR, vedere "Guida all'amministrazione SMBR".

Per ulteriori informazioni su SMBR, fare riferimento a quanto segue:

- "Come ripristinare manualmente un singolo elemento con SMBR (applicabile anche per i ripristini Ontrack Power Control)"
- "Come eseguire il ripristino dallo storage secondario in SMBR con SnapCenter"
- "Ripristino della posta di Microsoft Exchange da SnapVault utilizzando SMBR"

Ripristinare un database Exchange Server dallo storage secondario

È possibile ripristinare un database Exchange Server di cui è stato eseguito il backup dallo storage secondario (mirror o vault).

È necessario aver replicato le istantanee dallo storage primario a uno secondario.

A proposito di questa attività

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare **plug-in Microsoft Exchange Server** dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco a discesa **View** (Visualizza).
3. Selezionare il database o il gruppo di risorse.

   Viene visualizzata la pagina della topologia del database o del gruppo di risorse.
4. Nella sezione Gestisci copie, selezionare **backup** dal sistema di storage secondario (mirror o vault).
5. Selezionare il backup dall'elenco, quindi fare clic su  .
6. Nella pagina Location (percorso), scegliere il volume di destinazione per il ripristino della risorsa selezionata.
7. Completare la procedura guidata di ripristino, esaminare il riepilogo, quindi fare clic su **fine**.

Ripristinare le risorse Exchange utilizzando i cmdlet PowerShell

Il ripristino di un database Exchange include l'avvio di una sessione di connessione con il server SnapCenter, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

A proposito di questa attività

Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specificato utilizzando il `Open-SmConnection` cmdlet.

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

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando il `Get-SmBackup` cmdlet.

   Questo esempio mostra informazioni su tutti i backup disponibili:

```
PS C:\> Get-SmBackup

BackupId                      BackupName                    BackupTime
BackupType
--------                      ----------                    ----------
----------
341                           ResourceGroup_36304978_UTM... 12/8/2017
4:13:24 PM          Full Backup
342                           ResourceGroup_36304978_UTM... 12/8/2017
4:16:23 PM          Full Backup
355                           ResourceGroup_06140588_UTM... 12/8/2017
6:32:36 PM          Log Backup
356                           ResourceGroup_06140588_UTM... 12/8/2017
6:36:20 PM          Full Backup
```

3. Ripristinare i dati dal backup utilizzando il `Restore-SmBackup` cmdlet.

   Questo esempio ripristina un backup up-to-the-minute:

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341 -IsRecoverMount:$true
```

   Questo esempio ripristina un backup point-in-time:

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341 -IsRecoverMount:$true
-LogRestoreType ByTransactionLogs -LogCount 2
```

   Questo esempio ripristina un backup sullo storage secondario nella storia principale:

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2' -BackupId
81 -IsRecoverMount:$true -Confirm:$false
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}
-logrestoretype All
```

   Il `-archive` parametro consente di specificare i volumi primari e secondari da utilizzare per il ripristino.

   Il `-IsRecoverMount:$true` parametro consente di montare il database dopo il ripristino.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Eseguire nuovamente la configurazione di una replica passiva del nodo Exchange

Se è necessario eseguire di nuovo il reeed di una copia della replica, ad esempio quando una copia è danneggiata, è possibile eseguire nuovamente il reeed del backup più recente utilizzando la funzione di reeed di SnapCenter.

Prima di iniziare

- È necessario utilizzare il server SnapCenter 4.1 o versione successiva e il plug-in per Exchange 4.1 o versione successiva.

  Il reseeding di una replica non è supportato nelle versioni di SnapCenter precedenti alla 4.1.

- È necessario aver creato un backup del database che si desidera reconfigurare.

Best practice: per evitare ritardi tra i nodi, si consiglia di creare un nuovo backup prima di eseguire un'operazione di riseed o di scegliere l'host con il backup più recente.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare **plug-in Microsoft Exchange Server** dall'elenco.
2. Nella pagina risorse, selezionare l'opzione appropriata dall'elenco Visualizza:

Opzione	Descrizione
Per eseguire di nuovo la configurazione di un singolo database	Selezionare **Database** dall'elenco View (Visualizza).
Per eseguire nuovamente il reeeding dei database in un DAG	Selezionare **Database Availability Group** (Gruppo disponibilità database) dall'elenco View (Visualizza).

3. Selezionare la risorsa da reconfigurare.
4. Nella pagina Manage Copies (Gestisci copie), fare clic su **Reseed** (Ripristina).
5. Dall'elenco delle copie dei database non integre nella procedura guidata di riseed, selezionare quella che si desidera riseedare, quindi fare clic su **Avanti**.
6. Nella finestra host, selezionare l'host con il backup da cui si desidera eseguire nuovamente il reeed, quindi fare clic su **Avanti**.
7. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail.

8. Esaminare il riepilogo, quindi fare clic su **fine**.
9. È possibile visualizzare lo stato del lavoro espandendo il pannello attività nella parte inferiore della pagina.

L'operazione di riseed non è supportata se la copia passiva del database risiede su uno storage non NetApp.

Eseguire di nuovo il reeeding di una replica utilizzando i cmdlet PowerShell per il database Exchange

È possibile utilizzare i cmdlet PowerShell per ripristinare una replica non sana utilizzando la copia più recente sullo stesso host o la copia più recente da un host alternativo.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specificato utilizzando il `Open-SmConnection` cmdlet.

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

2. Il database è stato ripristinato utilizzando il `reseed-SmDagReplicaCopy` cmdlet.

   In questo esempio viene reeseguita la copia non riuscita del database denominata execdb sull'host "mva-rx200.netapp.com" utilizzando l'ultimo backup su tale host.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

   In questo esempio viene reinstallata la copia non riuscita del database denominata execdb utilizzando l'ultimo backup del database (produzione/copia) su un host alternativo "mva-rx201.netapp.com."

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

Monitorare le operazioni di ripristino

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

gli stati di post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi altra azione di ripristino che è possibile eseguire.

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente

- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Ripristina**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato di ripristino.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Annulla le operazioni di ripristino per il database Exchange

È possibile annullare i processi di ripristino in coda.

Per annullare le operazioni di ripristino, è necessario accedere come amministratore SnapCenter o come proprietario del processo.

A proposito di questa attività

- È possibile annullare un'operazione di ripristino in coda dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione di ripristino in corso.
- È possibile utilizzare l'interfaccia grafica di SnapCenter, i cmdlet PowerShell o i comandi CLI per annullare le operazioni di ripristino in coda.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni di ripristino che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di ripristino in coda degli altri membri durante l'utilizzo di tale ruolo.

Fase

Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. 2. Selezionare il lavoro e fare clic su **Annulla lavoro**.
Riquadro delle attività	1. Dopo aver avviato l'operazione di ripristino, fare clic  sul riquadro attività per visualizzare le cinque operazioni più recenti. 2. Selezionare l'operazione. 3. Nella pagina Dettagli processo, fare clic su **Annulla processo**.

Proteggere le applicazioni personalizzate

Plug-in personalizzati di SnapCenter

Panoramica sui plug-in personalizzati di SnapCenter

È possibile sviluppare plug-in personalizzati per le applicazioni utilizzate e quindi utilizzare SnapCenter per eseguire il backup, il ripristino o la clonazione di tali applicazioni. Come altri plug-in SnapCenter, i plug-in personalizzati agiscono come componenti lato host del software NetApp SnapCenter, consentendo la protezione dei dati e la gestione delle risorse applicative.

Una volta installati i plug-in personalizzati, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror dei set di backup su un altro volume e utilizzare la tecnologia NetApp SnapVault per eseguire la replica del backup disk-to-disk. I plug-in personalizzati possono essere utilizzati in ambienti Windows e Linux.

SnapCenterCLI non supporta i comandi dei plug-in personalizzati di SnapCenter.

NetApp fornisce il plug-in di storage per eseguire operazioni di protezione dei dati del volume di dati sullo storage ONTAP utilizzando il framework plug-in personalizzato integrato in SnapCenter.

È possibile installare il plug-in e il plug-in di storage personalizzati dalla pagina Add host (Aggiungi host).

"Aggiungere host e installare pacchetti plug-in su host remoti."

NetApp offre inoltre MySQL, MAXDB, DB2, SYBASE, DPGLUE, Plug-in personalizzati MongoDB, ORASCPM e PostgreSQL.

I criteri di supporto di SnapCenter riguarderanno il supporto per il framework del plug-in personalizzato di SnapCenter, il motore principale e le API associate. Il supporto non copre il codice sorgente del plug-in e gli script associati creati sul framework del plug-in personalizzato.

È possibile creare plug-in personalizzati facendo riferimento a "Sviluppare un plug-in per l'applicazione".

Operazioni che è possibile eseguire con i plug-in e i plug-in di storage personalizzati di SnapCenter

È possibile utilizzare i plug-in personalizzati di SnapCenter per le operazioni di protezione dei dati.

Plug-in personalizzato

- Aggiungere risorse come database, istanze, documenti o spazi tabella.
- Creare backup.
- Ripristinare dai backup.
- Clonare i backup.
- Pianificare le operazioni di backup.

- Monitorare le operazioni di backup, ripristino e clonazione.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

Plug-in di storage

È possibile utilizzare il plug-in di storage per le operazioni di protezione dei dati.

- Crea snapshot di gruppo di coerenza dei volumi di storage nei cluster ONTAP.
- Eseguire il backup delle applicazioni personalizzate utilizzando il framework pre e post-scripting integrato

  È possibile eseguire il backup di un volume ONTAP, di un LUN o di un Qtree.

- Update delle Snapshot acquisite nel primario in un secondario ONTAP, sfruttando la relazione di replica esistente (SnapVault/SnapMirror/replica unificata) utilizzando la policy SnapCenter

  ONTAP primario e secondario possono essere ONTAP FAS, AFF, All SAN Array (ASA), Select o Cloud ONTAP.

- Ripristinare il volume, il LUN o i file ONTAP completi.

  È necessario specificare manualmente il percorso del file corrispondente, poiché le funzioni di ricerca o indicizzazione non sono integrate nel prodotto.

  Il ripristino di qtree o directory non è supportato, ma è possibile clonare ed esportare solo il Qtree se l'ambito di backup è definito a livello di Qtree.

Funzionalità dei plug-in personalizzati di SnapCenter

SnapCenter si integra con l'applicazione plug-in e con le tecnologie NetApp del sistema storage. Per utilizzare i plug-in personalizzati, utilizzare l'interfaccia grafica utente di SnapCenter.

- **Interfaccia utente grafica unificata**

  L'interfaccia SnapCenter offre standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia di SnapCenter consente di completare operazioni di backup, ripristino, ripristino e clonazione coerenti tra i plug-in, utilizzare report centralizzati, utilizzare visualizzazioni dashboard a colpo d'occhio, impostare RBAC (role-based access control) e monitorare i processi in tutti i plug-in.

- **Amministrazione centrale automatizzata**

  È possibile pianificare le operazioni di backup, configurare la conservazione dei backup basata su policy ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per l'invio di avvisi e-mail.

- **Tecnologia istantanea NetApp senza interruzioni**

  SnapCenter utilizza la tecnologia Snapshot di NetApp con i plug-in personalizzati di SnapCenter per eseguire il backup delle risorse. Le snapshot consumano una quantità minima di spazio storage.

L'utilizzo della funzione Custom Plug-ins offre anche i seguenti vantaggi:

- Supporto per flussi di lavoro di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È inoltre possibile impostare le credenziali in modo che gli utenti SnapCenter autorizzati dispongano delle autorizzazioni a livello di applicazione.

- Creazione di copie delle risorse efficienti in termini di spazio e point-in-time per il test o l'estrazione dei dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema storage in cui si desidera creare il clone.

- Supporto della funzionalità di snapshot del gruppo di coerenza (CG) di ONTAP durante la creazione dei backup.
- Possibilità di eseguire più backup contemporaneamente su più host di risorse

  In una singola operazione, le Snapshot vengono consolidate quando le risorse di un singolo host condividono lo stesso volume.

- Possibilità di creare snapshot utilizzando comandi esterni.
- Capacità di creare Snapshot coerenti con il file system negli ambienti Windows.

Tipi di storage supportati dai plug-in personalizzati di SnapCenter

SnapCenter supporta un'ampia gamma di tipi di storage su macchine fisiche e virtuali. Prima di installare i plug-in personalizzati di SnapCenter, è necessario verificare il supporto per il tipo di storage in uso.

Macchina	Tipo di storage
Montaggi fisici e diretti NFS sugli host VM (VMDK e LUN RDM non sono supportati).	LUN connessi a FC
Montaggi fisici e diretti NFS sugli host VM (VMDK e LUN RDM non sono supportati).	LUN connessi a iSCSI
Montaggi fisici e diretti NFS sugli host VM (VMDK e LUN RDM non sono supportati).	Volumi connessi a NFS

Privilegi minimi di ONTAP richiesti per il plug-in personalizzato

I privilegi minimi di ONTAP richiesti variano in base ai plug-in di SnapCenter utilizzati per la protezione dei dati.

- All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
  - event generate-autosupport-log
  - mostra la cronologia dei lavori
  - interruzione del lavoro
  - visualizzazione dell'attributo lun

- lun create (crea lun)
- lun delete (elimina lun)
- geometria del lun
- lun igroup add
- lun igroup create
- lun igroup delete (elimina igroup lun)
- lun igroup rename (rinomina lun igroup)
- lun igroup show
- lun mapping add-reporting-node
- creazione mappatura lun
- eliminazione della mappatura lun
- nodi di remove-reporting-mapping lun
- visualizzazione della mappatura del lun
- modifica del lun
- lun move-in-volume
- lun offline
- lun online
- ridimensionamento del lun
- lun seriale
- lun show
- interfaccia di rete
- regola aggiuntiva del criterio snapmirror
- regola-modifica del criterio snapmirror
- regola di rimozione del criterio snapmirror
- policy di snapmirror
- ripristino di snapmirror
- spettacolo di snapmirror
- storia di snapmirror
- aggiornamento di snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione del clone del volume
- visualizzazione del clone del volume
- avvio della divisione del clone del volume
- interruzione della divisione del clone del volume
- creazione del volume

    - distruggere il volume
    - creazione del clone del file di volume
    - file di volume show-disk-usage
    - volume offline
    - volume online
    - modifica del volume
    - creazione del qtree del volume
    - eliminazione del qtree del volume
    - modifica del qtree del volume
    - visualizzazione del qtree del volume
    - limitazione del volume
    - presentazione del volume
    - creazione di snapshot di volume
    - eliminazione dello snapshot del volume
    - modifica dello snapshot del volume
    - rinominare lo snapshot del volume
    - ripristino dello snapshot del volume
    - file di ripristino dello snapshot del volume
    - visualizzazione di snapshot di volume
    - smontare il volume
    - cifs vserver
    - creazione condivisione cifs vserver
    - eliminazione condivisione cifs vserver
    - vserver cifs shadowcopy mostra
    - show di condivisione di vserver cifs
    - vserver cifs show
    - creazione policy di esportazione vserver
    - eliminazione della policy di esportazione di vserver
    - creazione della regola dei criteri di esportazione di vserver
    - visualizzazione della regola dei criteri di esportazione di vserver
    - visualizzazione della policy di esportazione di vserver
    - visualizzazione della connessione iscsi del vserver
    - show di vserver
- Comandi di sola lettura: Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete

Preparazione dei sistemi storage per la replica di SnapMirror e SnapVault per plug-in personalizzati

È possibile utilizzare un plug-in SnapCenter con la tecnologia SnapMirror di ONTAP per creare copie mirror dei set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replica del backup disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti di SnapMirror e SnapVault al termine dell'operazione di Snapshot. Gli aggiornamenti di SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter; non creare una pianificazione ONTAP separata.

Se vieni a SnapCenter da un prodotto NetApp SnapManager e sei soddisfatto delle relazioni di protezione dei dati che hai configurato, puoi saltare questa sezione.

Una relazione di protezione dei dati replica i dati sullo storage primario (il volume di origine) nello storage secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui fa riferimento il volume di origine al volume di destinazione.

SnapCenter non supporta le relazioni a cascata tra SnapMirror e i volumi SnapVault (**primario** > **Mirror** > **Vault**). Si consiglia di utilizzare le relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per ulteriori informazioni sulle relazioni di SnapMirror flessibili per la versione e sulla loro configurazione, vedere la "Documentazione ONTAP".

SnapCenter non supporta la replica **Sync_mirror**.

Definire una strategia di backup

La definizione di una strategia di backup prima della creazione dei processi di backup garantisce la disponibilità dei backup necessari per ripristinare o clonare correttamente le risorse. Il tuo SLA (Service-Level Agreement), RTO (Recovery Time Objective) e RPO (Recovery Point Objective) determinano in gran parte la tua strategia di backup.

A proposito di questa attività

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. RTO è il momento in cui un processo di business deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

Fasi

1. Stabilire quando eseguire il backup delle risorse.
2. Decidere il numero di processi di backup necessari.
3. Decidere come assegnare un nome ai backup.

4. Decidere se si desidera creare snapshot del gruppo di coerenza e decidere le opzioni appropriate per l'eliminazione degli snapshot del gruppo di coerenza.
5. Decidere se utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.
6. Determina il periodo di conservazione per gli Snapshot sul sistema di storage di origine e sulla destinazione di SnapMirror.
7. Determinare se si desidera eseguire qualsiasi comando prima o dopo l'operazione di backup e fornire una prescrizione o postscript.

Strategia di backup per plug-in personalizzati

Pianificazioni di backup di risorse plug-in personalizzate

Il fattore più critico per determinare una pianificazione di backup è il tasso di cambiamento per la risorsa. Più spesso si esegue il backup delle risorse, minore è il numero di log di archiviazione che SnapCenter deve utilizzare per il ripristino, che può comportare operazioni di ripristino più rapide.

È possibile eseguire il backup di una risorsa utilizzata in modo pesante ogni ora, mentre è possibile eseguire il backup di una risorsa utilizzata raramente una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo SLA (Service Level Agreement) e l'RPO (Recovery Point Objective).

SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA e RPO contribuiscono alla strategia di protezione dei dati.

Le pianificazioni dei backup sono in due parti, come segue:

- Frequenza di backup

  La frequenza di backup (frequenza con cui devono essere eseguiti i backup), chiamata anche tipo di pianificazione per alcuni plug-in, fa parte di una configurazione di policy. Ad esempio, è possibile configurare la frequenza di backup come orario, giornaliero, settimanale o mensile. È possibile accedere ai criteri nella GUI di SnapCenter facendo clic su **Impostazioni** > **Criteri**.

- Pianificazioni di backup

  Le pianificazioni dei backup (esattamente quando devono essere eseguiti i backup) fanno parte di una configurazione di risorsa o gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione per il backup ogni giovedì alle 10:00. È possibile accedere alle pianificazioni dei gruppi di risorse nella GUI di SnapCenter facendo clic su **risorse**, quindi selezionando il plug-in appropriato, e fare clic su **Visualizza** > **Gruppo di risorse**.

Numero di processi di backup necessari

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, il tasso di cambiamento della risorsa e il contratto SLA (Service Level Agreement).

Il numero di processi di backup scelti dipende in genere dal numero di volumi da cui sono state collocate le risorse. Ad esempio, se si dispone un gruppo di piccole risorse su un volume e una grande risorsa su un altro volume, è possibile creare un processo di backup per le piccole risorse e un processo di backup per le grandi risorse.

Tipi di strategie di ripristino supportate per risorse plug-in personalizzate aggiunte manualmente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per le risorse plug-in personalizzate aggiunte manualmente.

Non è possibile ripristinare le risorse plug-in personalizzate aggiunte manualmente.

Ripristino completo delle risorse

- Ripristina tutti i volumi, le qtree e le LUN di una risorsa

Se la risorsa contiene volumi o qtree, gli Snapshot acquisiti dopo la Snapshot selezionata per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata.

Ripristino a livello di file

- Ripristina i file da volumi, qtree o directory
- Ripristina solo i LUN selezionati

Sviluppare un plug-in per l'applicazione

Panoramica

Il server SnapCenter consente di implementare e gestire le applicazioni come plug-in per SnapCenter. È possibile collegare al server SnapCenter applicazioni di vostra scelta per la protezione e la gestione dei dati.

SnapCenter consente di sviluppare plug-in personalizzati utilizzando diversi linguaggi di programmazione. È possibile sviluppare un plug-in personalizzato utilizzando Perl, Java, BATCH o altri linguaggi di scripting.

Per utilizzare plug-in personalizzati in SnapCenter, è necessario eseguire le seguenti operazioni:

- Creare un plug-in per l'applicazione seguendo le istruzioni di questa guida
- Creare un file di descrizione
- Esportare il plug-in personalizzato per installarlo sull'host SnapCenter
- Caricare il file zip del plug-in nel server SnapCenter

Gestione di plug-in generici in tutte le chiamate API

Per ogni chiamata API, utilizzare le seguenti informazioni:

- Parametri del plug-in
- Codici di uscita
- Registrare i messaggi di errore
- Coerenza dei dati

Utilizzare i parametri del plug-in

Un insieme di parametri viene passato al plug-in come parte di ogni chiamata API effettuata. La seguente tabella elenca le informazioni specifiche per i parametri.

Parametro	Scopo
AZIONE	Determina il nome del flusso di lavoro. Ad esempio, Discover, backup, fileOrVolRestore o cloneVolAndLun
RISORSE	Elenca le risorse da proteggere. Una risorsa è identificata da UID e Type. L'elenco viene presentato al plug-in nel seguente formato: "<UID>,<TYPE>;<UID>,<TYPE>". Ad esempio, "Instance1,Instance;Instance2,DB1,Database"
NOME_APP	Determina quale plug-in viene utilizzato. Ad esempio, DB2, MYSQL. Il server SnapCenter dispone di un supporto integrato per le applicazioni elencate. Questo parametro fa distinzione tra maiuscole e minuscole.
APP_IGNORE_ERROR	(Y o N) questo causa l'uscita di SnapCenter quando si verifica un errore dell'applicazione. Ciò è utile quando si esegue il backup di più database e non si desidera che un singolo errore interrompa l'operazione di backup.
<RESOURCE_NAME>__APP_INSTANCE_USERNAME	La credenziale SnapCenter è impostata per la risorsa.
<RESOURCE_NAME>_APP_INSTANCE_PASSWORD	La credenziale SnapCenter è impostata per la risorsa.
<RESOURCE_NAME>_<CUSTOM_PARAM>	Ogni valore della chiave personalizzata a livello di risorsa è disponibile per i plug-in con prefisso "<RESOURCE_NAME>_". Ad esempio, se una chiave personalizzata è "MASTER_SLAVE" per una risorsa denominata "MySQLDB", sarà disponibile come MySQLDB_MASTER_SLAVE

Utilizzare i codici di uscita

Il plug-in restituisce lo stato dell'operazione all'host mediante i codici di uscita. Ciascun codice ha un significato

specifico e il plug-in utilizza il codice di uscita corretto per indicare lo stesso.

La tabella seguente illustra i codici di errore e il relativo significato.

Codice di uscita	Scopo
0	Operazione riuscita.
99	L'operazione richiesta non è supportata o implementata.
100	Operazione non riuscita, ignorare e uscire. Unquiesce è per impostazione predefinita.
101	Operazione non riuscita, continuare con l'operazione di backup.
altro	Operazione non riuscita, eseguire senza problemi e uscire.

Registrare i messaggi di errore

I messaggi di errore vengono passati dal plug-in al server SnapCenter. Il messaggio include il messaggio, il livello di registrazione e l'indicazione dell'ora.

La tabella seguente elenca i livelli e i relativi scopi.

Parametro	Scopo
INFO	messaggio informativo
ATTENZIONE	messaggio di avviso
ERRORE	messaggio di errore
DEBUG	messaggio di debug
TRACCIA	messaggio di traccia

Preservare la coerenza dei dati

I plug-in personalizzati mantengono i dati tra le operazioni della stessa esecuzione del workflow. Ad esempio, un plug-in può memorizzare i dati alla fine di quiesce, che possono essere utilizzati durante un'operazione senza problemi.

I dati da conservare vengono impostati come parte dell'oggetto risultato dal plug-in. Segue un formato specifico ed è descritto in dettaglio in ogni stile di sviluppo plug-in.

Sviluppo BASATO SU PERL

È necessario seguire alcune convenzioni durante lo sviluppo del plug-in con PERL.

- Il contenuto deve essere leggibile
- Devono implementare le operazioni obbligatorie setenv, quiesce e senza richieste
- Deve utilizzare una sintassi specifica per restituire i risultati all'agente
- Il contenuto deve essere salvato come file <PLUGIN_NAME>.pm

Le operazioni disponibili sono

- Setenv
- versione
- quiesce
- non fare domande
- clone_pre, clone_post
- restore_pre, ripristino
- pulizia

Gestione generale dei plug-in

Utilizzo dell'oggetto Results

Ogni operazione di plug-in personalizzata deve definire l'oggetto Results. Questo oggetto invia messaggi, codice di uscita, stdout e stderr all'agente host.

Oggetto Results (risultati):

```
my $result = {
```

```
      exit_code => 0,
      stdout => "",
      stderr => "",
};
```

Restituzione dell'oggetto Results:

```
return $result;
```

Preservare la coerenza dei dati

È possibile conservare i dati tra le operazioni (eccetto la pulizia) come parte della stessa esecuzione del flusso di lavoro. Ciò avviene utilizzando coppie chiave-valore. Le coppie chiave-valore dei dati vengono impostate come parte dell'oggetto risultato e vengono conservate e disponibili nelle successive operazioni dello stesso flusso di lavoro.

Il seguente esempio di codice imposta i dati da conservare:

```
my $result = {
  exit_code => 0,
  stdout => "",
  stderr => "",
};
  $result->{env}->{'key1'} = 'value1';
  $result->{env}->{'key2'} = 'value2';
  ….
  return $result
```

Il codice precedente imposta due coppie chiave-valore, che sono disponibili come input nell'operazione successiva. Le due coppie chiave-valore sono accessibili utilizzando il seguente codice:

```
sub setENV {
    my ($self, $config) = @_;
    my $first_value = $config->{'key1'};
    my $second_value = $config->{'key2'};
    …
}
```

```
 === Logging error messages
Ciascuna operazione può inviare i messaggi all'agente host, che visualizza
e memorizza il contenuto. Un messaggio contiene il livello del messaggio,
un indicatore data e ora e un testo del messaggio. Sono supportati i
messaggi multilinea.
```

```
Load the SnapCreator::Event Class:
my $msgObj = new SnapCreator::Event();
my @message_a = ();
```

Utilizzare msgObj per acquisire un messaggio utilizzando il metodo Collect.

```
$msgObj->collect(\@message_a, INFO, "My INFO Message");
$msgObj->collect(\@message_a, WARN, "My WARN Message");
$msgObj->collect(\@message_a, ERROR, "My ERROR Message");
$msgObj->collect(\@message_a, DEBUG, "My DEBUG Message");
$msgObj->collect(\@message_a, TRACE, "My TRACE Message");
```

Applicare i messaggi all'oggetto Results:

```
$result->{message} = \@message_a;
```

Utilizzo di stub plug-in

I plug-in personalizzati devono esporre gli stub plug-in. Questi sono i metodi che il server SnapCenter chiama, in base a un flusso di lavoro.

Stub plug-in	Opzionale/obbligatorio	Scopo
Setenv	obbligatorio	Questo stub imposta l'ambiente e l'oggetto di configurazione. Qualsiasi analisi o gestione dell'ambiente deve essere eseguita qui. Ogni volta che viene chiamato uno stub, lo stub setenv viene chiamato poco prima. È necessario solo per i plug-in PERL-style.
Versione	Opzionale	Questo stub viene utilizzato per ottenere la versione dell'applicazione.
Scopri	Opzionale	Questo stub viene utilizzato per rilevare gli oggetti dell'applicazione come istanze o database ospitati sull'agente o sull'host. Il plug-in restituirà gli oggetti dell'applicazione rilevati in un formato specifico come parte della risposta. Questo stub viene utilizzato solo nel caso in cui l'applicazione sia integrata con SnapDrive per Unix. Il file system Linux (Linux Flavors) è supportato. AIX/Solaris (Unix Flavors) non sono supportati.

Stub plug-in	Opzionale/obbligatorio	Scopo
discovery_complete	Opzionale	Questo stub viene utilizzato per rilevare gli oggetti dell'applicazione come istanze o database ospitati sull'agente o sull'host. Il plug-in restituirà gli oggetti dell'applicazione rilevati in un formato specifico come parte della risposta. Questo stub viene utilizzato solo nel caso in cui l'applicazione sia integrata con SnapDrive per Unix. Il file system Linux (Linux Flavors) è supportato. AIX e Solaris (versioni Unix) non sono supportati.
Quiesce	obbligatorio	Questa stub è responsabile dell'esecuzione di una pausa, il che significa posizionare l'applicazione in uno stato in cui è possibile creare una snapshot. Questo viene chiamato prima dell'operazione istantanea. I metadati dell'applicazione da conservare devono essere impostati come parte della risposta, che verranno restituiti durante le operazioni di cloning o ripristino successive sul Snapshot di storage corrispondente sotto forma di parametri di configurazione.
Senza richieste	obbligatorio	Questo stub è responsabile dell'esecuzione di un'operazione senza oggetto, il che significa mettere l'applicazione in uno stato normale. Questa operazione viene richiamata dopo la creazione di un'istantanea.

Stub plug-in	Opzionale/obbligatorio	Scopo
clone_pre	opzionale	Questo stub è responsabile dell'esecuzione delle attività di precolona. Ciò presuppone che si stia utilizzando l'interfaccia di clonazione del server SnapCenter integrata e che venga attivata durante l'esecuzione dell'operazione di clonazione.
clone_post	opzionale	Questo stub è responsabile dell'esecuzione delle attività post-clone. Ciò presuppone che si stia utilizzando l'interfaccia di clonazione del server SnapCenter integrata e che venga attivata solo quando si esegue un'operazione di clonazione.
ripristina_pre	opzionale	Questo stub è responsabile dell'esecuzione delle attività di prerestore. Ciò presuppone che si stia utilizzando l'interfaccia di ripristino del server SnapCenter integrata e che venga attivata durante l'esecuzione dell'operazione di ripristino.
Ripristinare	opzionale	Questo stub è responsabile dell'esecuzione delle attività di ripristino delle applicazioni. Questo presuppone che si stia utilizzando l'interfaccia di ripristino del server SnapCenter integrata e viene attivato solo quando si esegue l'operazione di ripristino.

Stub plug-in	Opzionale/obbligatorio	Scopo
Pulizia	opzionale	Questo stub è responsabile dell'esecuzione della pulizia dopo le operazioni di backup, ripristino o clonazione. La pulizia può avvenire durante la normale esecuzione del flusso di lavoro o in caso di errore del flusso di lavoro. È possibile dedurre il nome del flusso di lavoro con cui viene chiamata la pulizia facendo riferimento ALL'AZIONE del parametro di configurazione, che può essere backup, cloneVolAndLun o fileOrVolRestore. Il parametro di configurazione ERROR_MESSAGE indica se si è verificato un errore durante l'esecuzione del flusso di lavoro. Se ERROR_MESSAGE è definito e NON NULL, la pulitura viene richiamata durante l'esecuzione di un errore del workflow.
versione_app	Opzionale	Questo stub viene utilizzato da SnapCenter per gestire i dettagli della versione dell'applicazione dal plug-in.

Informazioni sul pacchetto plug-in

Ogni plug-in deve avere le seguenti informazioni:

```
package MOCK;
our @ISA = qw(SnapCreator::Mod);
=head1 NAME
MOCK - class which represents a MOCK module.
=cut
=head1 DESCRIPTION
MOCK implements methods which only log requests.
=cut
use strict;
use warnings;
use diagnostics;
use SnapCreator::Util::Generic qw ( trim isEmpty );
use SnapCreator::Util::OS qw ( isWindows isUnix getUid
createTmpFile );
use SnapCreator::Event qw ( INFO ERROR WARN DEBUG COMMENT ASUP
CMD DUMP );
my $msgObj = new SnapCreator::Event();
my %config_h = ();
```

Operazioni

È possibile codificare diverse operazioni come setenv, Version, Quiesce e Unquiesce, supportate dai plug-in personalizzati.

Operazione setenv

L'operazione setenv è necessaria per i plug-in creati utilizzando PERL. È possibile impostare ENV e accedere facilmente ai parametri del plug-in.

```
sub setENV {
    my ($self, $obj) = @_;
    %config_h = %{$obj};
    my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
    };
    return $result;
}
```

Funzionamento della versione

L'operazione di versione restituisce le informazioni sulla versione dell'applicazione.

```
sub version {
  my $version_result = {
    major => 1,
    minor => 2,
    patch => 1,
    build => 0
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $version_result->{message} = \@message_a;
  return $version_result;
}
```

Interrompere le operazioni

L'operazione quiesce esegue l'operazione di quiesce dell'applicazione sulle risorse elencate nel parametro RESOURCES.

```
sub quiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

Operazione senza problemi

L'operazione Unquiesce è necessaria per interrompere l'applicazione. L'elenco delle risorse è disponibile nel parametro RESOURCES.

```
sub unquiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::unquiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

Stile NATIVO

SnapCenter supporta linguaggi di programmazione o scripting non PERL per creare plug-in. Questa è nota come programmazione in stile NATIVO, che può essere un file script o BATCH.

I plug-in DI stile NATIVO devono seguire alcune convenzioni fornite di seguito:

Il plug-in deve essere eseguibile

- Per i sistemi Unix, l'utente che esegue l'agente deve disporre dei privilegi di esecuzione sul plug-in
- Per i sistemi Windows, i plug-in PowerShell devono avere il suffisso .ps1, gli altri script di Windows devono avere il suffisso .cmd o .bat e devono essere eseguibili dall'utente
- I plug-in devono reagire a argomenti della riga di comando come "-quiesce", "-unquiesce"
- I plug-in devono restituire il codice di uscita 99 nel caso in cui un'operazione o una funzione non sia implementata
- I plug-in devono utilizzare una sintassi specifica per restituire i risultati al server

Gestione generale dei plug-in

Registrazione dei messaggi di errore

Ogni operazione può inviare messaggi al server, che visualizza e memorizza il contenuto. Un messaggio contiene il livello del messaggio, un indicatore data e ora e un testo del messaggio. Sono supportati i messaggi multilinea.

Formato:

```
SC_MSG#<level>#<timestamp>#<message>
SC_MESSAGE#<level>#<timestamp>#<message>
```

Utilizzo di stub plug-in

I plug-in SnapCenter devono implementare i plug-in stub. Si tratta di metodi richiamati dal server SnapCenter in base a un flusso di lavoro specifico.

Stub plug-in	Opzionale/obbligatorio	Scopo
quiesce	obbligatorio	Questo stub è responsabile dell'esecuzione di un quiesce. Posiziona l'applicazione in uno stato in cui è possibile creare un'istantanea. Questo viene chiamato prima dell'operazione di snapshot di storage.
non fare domande	obbligatorio	Questo stub è responsabile dell'esecuzione di una richiesta. Pone l'applicazione in uno stato normale. Questo viene chiamato dopo l'operazione snapshot di storage.
clone_pre	opzionale	Questo stub è responsabile dell'esecuzione delle attività pre-clonate. Questo presuppone che si stia utilizzando l'interfaccia di cloning SnapCenter integrata e che venga attivata solo durante l'esecuzione dell'azione "clone_vol o clone_lun".
clone_post	Opzionale	Questo stub è responsabile dell'esecuzione delle attività post-clone. Questo presuppone che si stia utilizzando l'interfaccia di cloning SnapCenter integrata e che venga attivata solo durante l'esecuzione delle operazioni "clone_vol o clone_lun".
ripristina_pre	Opzionale	Questo stub è responsabile dell'esecuzione delle attività di pre-ripristino. Ciò presuppone che si stia utilizzando l'interfaccia di ripristino SnapCenter integrata e che venga attivata solo durante l'esecuzione dell'operazione di ripristino.

Stub plug-in	Opzionale/obbligatorio	Scopo
ripristinare	opzionale	Questo stub è responsabile dell'esecuzione di tutte le azioni di ripristino. Ciò presuppone che non si stia utilizzando un'interfaccia di ripristino integrata. Viene attivato durante l'esecuzione dell'operazione di ripristino.

Esempi

Windows PowerShell

Controllare se lo script può essere eseguito sul sistema. Se non è possibile eseguire lo script, impostare il bypass Set-ExecutionPolicy per lo script e riprovare l'operazione.

```
if ($args.length -ne 1) {
  write-warning "You must specify a method";
  break;
}
function log ($level, $message) {
  $d = get-date
  echo "SC_MSG#$level#$d#$message"
}
function quiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Quiescing application using script $app_name";
  log "INFO" "Quiescing application finished successfully"
}
function unquiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Unquiescing application using script $app_name";
  log "INFO" "Unquiescing application finished successfully"
}
  switch ($args[0]) {
    "-quiesce" {
    quiesce;
}
"-unquiesce" {
    unquiesce;
}
default {
    write-error "Function $args[0] is not implemented";
    exit 99;
  }
}
exit 0;
```

Stile Java

Un plug-in personalizzato Java interagisce direttamente con un'applicazione come database, istanze e così via.

Limitazioni

Esistono alcune limitazioni che è necessario tenere presenti durante lo sviluppo di un plug-in utilizzando il linguaggio di programmazione Java.

Caratteristica del plug-in	Plug-in Java
Complessità	Da basso a medio

Caratteristica del plug-in	Plug-in Java
Impatto della memoria	Fino a 10-20 MB
Dipendenze da altre librerie	Librerie per la comunicazione applicativa
Numero di thread	1
Runtime del thread	Meno di un'ora

Motivo delle limitazioni Java

L'obiettivo dell'agente SnapCenter è garantire un'integrazione applicativa continua, sicura e solida. Grazie al supporto dei plug-in Java, è possibile che i plug-in introducano perdite di memoria e altri problemi indesiderati. Questi problemi sono difficili da affrontare, soprattutto quando l'obiettivo è quello di mantenere le cose semplici da utilizzare. Se la complessità di un plug-in non è troppo complessa, è molto meno probabile che gli sviluppatori abbiano introdotto gli errori. Il pericolo che il plug-in Java venga eseguito nella stessa JVM dell'agente SnapCenter. In caso di crash o perdita di memoria, il plug-in potrebbe avere un impatto negativo sull'Agent.

Metodi supportati

Metodo	Obbligatorio	Descrizione	Chiamate quando e da chi?
Versione	Sì	Deve restituire la versione del plug-in.	Dal server o dall'agente SnapCenter per richiedere la versione del plug-in.
Quiesce	Sì	Deve eseguire un quiesce sull'applicazione. Nella maggior parte dei casi, ciò significa mettere l'applicazione in uno stato in cui il server SnapCenter può creare un backup (ad esempio, un'istantanea).	Prima che il server SnapCenter crei una copia Snapshot o esegua un backup in generale.
Senza richieste	Sì	Deve eseguire un'operazione senza domande sull'applicazione. Nella maggior parte dei casi, ciò significa riportare l'applicazione in uno stato operativo normale.	Dopo che il server SnapCenter ha creato uno snapshot o ha eseguito un backup in generale.

Metodo	Obbligatorio	Descrizione	Chiamate quando e da chi?
Pulizia	No	Responsabile della pulizia di qualsiasi elemento che il plug-in deve pulire.	Al termine di un flusso di lavoro sul server SnapCenter (con esito positivo o con errore).
ClonePre	No	Dovrebbe eseguire azioni che devono essere eseguite prima di eseguire un'operazione di clonazione.	Quando un utente attiva un'azione "cloneVol" o "cloneLun" e utilizza la procedura guidata di cloning integrata (GUI/CLI).
ClonePost	No	Dovrebbe eseguire azioni che devono avvenire dopo l'esecuzione di un'operazione di clonazione.	Quando un utente attiva un'azione "cloneVol" o "cloneLun" e utilizza la procedura guidata di cloning integrata (GUI/CLI).
RestorePre	No	Dovrebbe eseguire le azioni che devono essere eseguite prima di richiamare l'operazione di ripristino.	Quando un utente attiva un'operazione di ripristino.
Ripristinare	No	Responsabile dell'esecuzione di un ripristino/ripristino dell'applicazione.	Quando un utente attiva un'operazione di ripristino.
AppVersion	No	Per recuperare la versione dell'applicazione gestita dal plug-in.	Come parte della raccolta di dati ASUP in ogni flusso di lavoro come Backup/Restore/Clone.

Esercitazione

In questa sezione viene descritto come creare un plug-in personalizzato utilizzando il linguaggio di programmazione Java.

Configurare l'eclissi

1. Creare un nuovo progetto Java "TutorialPlugin" in Eclipse
2. Fare clic su **fine**
3. Fare clic con il pulsante destro del mouse su **nuovo progetto** → **Proprietà** → **Java Build Path** → **Librerie** → **Aggiungi jar esterni**
4. Accedere alla cartella ../lib/ dell'agente host e selezionare jars scAgent-5.0-core.jar e common-5.0.jar

5. Selezionare il progetto e fare clic con il pulsante destro del mouse sulla cartella **src** → **New** → **Package** e creare un nuovo pacchetto con il nome com.netapp.snapcreator.agent.plugin.TutorialPlugin
6. Fare clic con il pulsante destro del mouse sul nuovo pacchetto e selezionare New → Java Class.
   a. Immettere il nome come TutorialPlugin.
   b. Fare clic sul pulsante di ricerca delle superclassi e cercare "*AbstractPlugin". Dovrebbe essere visualizzato un solo risultato:

```
 "AbstractPlugin - com.netapp.snapcreator.agent.nextgen.plugin".
.. Fare clic su *fine*.
.. Classe Java:
```

```
package com.netapp.snapcreator.agent.plugin.TutorialPlugin;
import
com.netapp.snapcreator.agent.nextgen.common.result.Describe
Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.VersionR
esult;
import
com.netapp.snapcreator.agent.nextgen.context.Context;
import
com.netapp.snapcreator.agent.nextgen.plugin.AbstractPlugin;
public class TutorialPlugin extends AbstractPlugin {
  @Override
  public DescribeResult describe(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result quiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result unquiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public VersionResult version() {
    // TODO Auto-generated method stub
    return null;
  }
}
```

Implementazione dei metodi richiesti

Quiesce, unquiesce e version sono metodi obbligatori che ogni plug-in Java personalizzato deve implementare.

Di seguito viene riportato un metodo di versione per restituire la versione del plug-in.

```
@Override
public VersionResult version() {
    VersionResult versionResult = VersionResult.builder()
                                                .withMajor(1)
                                                .withMinor(0)
                                                .withPatch(0)
                                                .withBuild(0)
                                                .build();
    return versionResult;
}
```

```
Below is the implementation of quiesce and unquiesce method. These will be
interacting with   the application, which is being protected by SnapCenter
Server. As this is just a tutorial, the
application part is not explained, and the focus is more on the
functionality that SnapCenter   Agent provides the following to the plug-
in developers:
```

```
@Override
  public Result quiesce(Context context) {
    final Logger logger = context.getLogger();
    /*
      * TODO: Add application interaction here
    */
```

```
logger.error("Something bad happened.");
logger.info("Successfully handled application");
```

```
    Result result = Result.builder()
                    .withExitCode(0)
                    .withMessages(logger.getMessages())
                    .build();
    return result;
}
```

Il metodo viene passato in un oggetto di contesto. Contiene più assistenti, ad esempio un Logger e un archivio di contesto, nonché le informazioni sull'operazione corrente (workflow-ID, job-ID). Possiamo ottenere il logger chiamando il logger finale = Context.GetLogger();. L'oggetto logger fornisce metodi simili noti da altri framework di logging, ad esempio logback. Nell'oggetto risultato, è anche possibile specificare il codice di uscita. In questo esempio, viene restituito zero, poiché non si è verificato alcun problema. Altri codici di uscita possono essere associati a diversi scenari di guasto.

Utilizzo dell'oggetto risultato

L'oggetto Result contiene i seguenti parametri:

Parametro	Predefinito	Descrizione
Config	Config. Vuota	Questo parametro può essere utilizzato per inviare nuovamente i parametri di configurazione al server. Possono essere parametri che il plug-in desidera aggiornare. Se questa modifica viene effettivamente riflessa nella configurazione sul server SnapCenter dipende dal parametro APP_CONF_PERSISTENCY=Y o N nella configurazione.
ExitCode	0	Indica lo stato dell'operazione. "0" indica che l'operazione è stata eseguita correttamente. Altri valori indicano errori o avvisi.
Stdout	Elenco vuoto	Questa funzione può essere utilizzata per trasmettere messaggi stdout al server SnapCenter.
Stderr	Elenco vuoto	Questa opzione può essere utilizzata per ritrasmettere i messaggi stderr al server SnapCenter.
Messaggi	Elenco vuoto	Questo elenco contiene tutti i messaggi che un plug-in desidera restituire al server. Il server SnapCenter visualizza questi messaggi nella CLI o nella GUI.

L'agente SnapCenter fornisce i costruttori ("Modello di costruttore") per tutti i tipi di risultati. Questo rende l'utilizzo molto semplice:

```
Result result = Result.builder()
                    .withExitCode(0)
                    .withStdout(stdout)
                    .withStderr(stderr)
                    .withConfig(config)
                    .withMessages(logger.getMessages())
                    .build()
```

Ad esempio, impostare il codice di uscita su 0, impostare gli elenchi per stdout e stderr, impostare i parametri

di configurazione e aggiungere anche i messaggi di registro che verranno rinviati al server. Se non sono necessari tutti i parametri, inviare solo quelli necessari. Poiché ogni parametro ha un valore predefinito, se si rimuove .withExitCode(0) dal codice riportato di seguito, il risultato non viene influenzato:

```
Result result = Result.builder()
                      .withExitCode(0)
                      .withMessages(logger.getMessages())
                      .build();
```

VersionResult

VersionResult informa il server SnapCenter della versione del plug-in. Poiché eredita anche dal risultato, contiene i parametri config, exitCode, stdout, stderr e messaggi.

Parametro	Predefinito	Descrizione
Maggiore	0	Principale campo di versione del plug-in.
Minore	0	Campo versione minore del plug-in.
Patch	0	Campo della versione della patch del plug-in.
Costruire	0	Campo della versione di build del plug-in.

Ad esempio:

```
VersionResult result = VersionResult.builder()
                                    .withMajor(1)
                                    .withMinor(0)
                                    .withPatch(0)
                                    .withBuild(0)
                                    .build();
```

Utilizzo dell'oggetto di contesto

L'oggetto Context fornisce i seguenti metodi:

Metodo di contesto	Scopo
Stringa getWorkflowId();	Restituisce l'id del flusso di lavoro utilizzato dal server SnapCenter per il flusso di lavoro corrente.

Metodo di contesto	Scopo
Config getConfig();	Restituisce la configurazione inviata dal server SnapCenter all'agente.

ID flusso di lavoro

L'ID del flusso di lavoro è l'id utilizzato dal server SnapCenter per fare riferimento a un flusso di lavoro in esecuzione specifico.

Config

Questo oggetto contiene la maggior parte dei parametri che un utente può impostare nella configurazione sul server SnapCenter. Tuttavia, per motivi di sicurezza, alcuni di questi parametri potrebbero essere filtrati sul lato server. Di seguito viene riportato un esempio su come accedere alla configurazione e recuperare un parametro:

```
final Config config = context.getConfig();
String myParameter =
config.getParameter("PLUGIN_MANDATORY_PARAMETER");
```

""// myParameter" ora contiene il parametro letto dalla configurazione sul server SnapCenter se una chiave del parametro di configurazione non esiste, restituirà una stringa vuota ("").

Esportazione del plug-in

È necessario esportare il plug-in per installarlo sull'host SnapCenter.

In Eclipse eseguire le seguenti operazioni:

1. Fare clic con il pulsante destro del mouse sul pacchetto di base del plug-in (nell'esempio com.netapp.snapcreator.agent.plugin.TutorialPlugin).
2. Selezionare **Export → Java → jar file**
3. Fare clic su **Avanti**.
4. Nella finestra seguente, specificare il percorso del file jar di destinazione: tutorial_plugin.jar la classe di base del plug-in è denominata TutorialPlugin.class, il plug-in deve essere aggiunto a una cartella con lo stesso nome.

Se il plug-in dipende da librerie aggiuntive, è possibile creare la seguente cartella: Lib/

È possibile aggiungere file jar, da cui dipende il plug-in (ad esempio, un driver di database). Quando SnapCenter carica il plug-in, associa automaticamente tutti i file jar presenti in questa cartella e li aggiunge al classpath.

Plug-in personalizzato in SnapCenter

Plug-in personalizzato in SnapCenter

Il plug-in personalizzato creato utilizzando Java, PERL o lo stile NATIVO può essere installato sull'host utilizzando il server SnapCenter per abilitare la protezione dei dati dell'applicazione. È necessario esportare il

plug-in per installarlo sull'host SnapCenter utilizzando la procedura fornita in questo tutorial.

Creazione di un file di descrizione del plug-in

Per ogni plug-in creato, è necessario disporre di un file di descrizione. Il file di descrizione descrive i dettagli del plug-in. Il nome del file deve essere Plugin_descriptor.xml.

Utilizzo degli attributi del file del descrittore del plug-in e del relativo significato

Attributo	Descrizione
Nome	Nome del plug-in. Sono consentiti caratteri alfanumerici. Ad esempio, DB2, MYSQL, MongoDB Per i plug-in creati in stile NATIVO, assicurarsi di non fornire l'estensione del file. Ad esempio, se il nome del plug-in è MongoDB.sh, specificare il nome come MongoDB.
Versione	Versione del plug-in. Può includere sia la versione principale che quella secondaria. Ad esempio, 1.0, 1.1, 2.0, 2.1
DisplayName	Il nome del plug-in da visualizzare nel server SnapCenter. Se vengono scritte più versioni dello stesso plug-in, assicurarsi che il nome visualizzato sia lo stesso per tutte le versioni.
Tipo di plug-in	Lingua utilizzata per creare il plug-in. I valori supportati sono Perl, Java e Native. Il tipo di plug-in nativo include shell script Unix/Linux, script Windows, Python o qualsiasi altro linguaggio di scripting.
Nome dell'OSName	Il nome del sistema operativo host in cui è installato il plug-in. I valori validi sono Windows e Linux. È possibile che un singolo plug-in sia disponibile per l'implementazione su diversi tipi di sistemi operativi, come IL plug-in DI TIPO PERL.
Versione del sistema operativo	La versione del sistema operativo host in cui è installato il plug-in.
ResourceName	Nome del tipo di risorsa supportato dal plug-in. Ad esempio, database, istanze, raccolte.
Origine	Nel caso in cui ResourceName dipenda gerarchicamente da un altro tipo di risorsa, quindi Parent determina il tipo di risorsa principale. Ad esempio, il plug-in DB2, ResourceName "Database" ha un'istanza padre.

Attributo	Descrizione
RequireFileSystemPlugin	Sì o No Determina se la scheda Recovery (Ripristino) viene visualizzata nella procedura guidata di ripristino.
ResourceRequiresAuthentication	Sì o No Determina se le risorse, rilevate automaticamente o non rilevate automaticamente, necessitano delle credenziali per eseguire le operazioni di protezione dati dopo il rilevamento dello storage.
RequireFileSystemClone	Sì o No Determina se il plug-in richiede l'integrazione del plug-in del file system per il flusso di lavoro dei cloni.

Un esempio del file Plugin_descriptor.xml per il plug-in personalizzato DB2 è il seguente:

```
<Plugin>
<SMSServer></SMSServer>
<Name>DB2</Name>
<Version>1.0</Version>
<PluginType>Perl</PluginType>
<DisplayName>Custom DB2 Plugin</DisplayName>
<SupportedOS>
<OS>
<OSName>windows</OSName>
<OSVersion>2012</OSVersion>
</OS>
<OS>
<OSName>Linux</OSName>
<OSVersion>7</OSVersion>
</OS>
</SupportedOS>
<ResourceTypes>
<ResourceType>
<ResourceName>Database</ResourceName>
<Parent>Instance</Parent>
</ResourceType>
<ResourceType>
<ResourceName>Instance</ResourceName>
</ResourceType>
</ResourceTypes>
<RequireFileSystemPlugin>no</RequireFileSystemPlugin>
<ResourceRequiresAuthentication>yes</ResourceRequiresAuthentication>
<SupportsApplicationRecovery>yes</SupportsApplicationRecovery>
</Plugin>
```

Creazione di un file ZIP

Dopo aver sviluppato un plug-in e creato un file descrittore, è necessario aggiungere i file plug-in e Plugin_descriptor.xml a una cartella e comprimerli.

Prima di creare un file ZIP, è necessario prendere in considerazione quanto segue:

- Il nome dello script deve essere uguale al nome del plug-in.
- Per IL plug-in PERL, la cartella ZIP deve contenere una cartella con il file script e il file descrittore deve essere esterno a questa cartella. Il nome della cartella deve essere uguale al nome del plug-in.
- Per i plug-in diversi dal plug-in PERL, la cartella ZIP deve contenere il descrittore e i file di script.
- La versione del sistema operativo deve essere un numero.

Esempi:

- Plug-in DB2: Aggiungere i file DB2.pm e Plugin_descriptor.xml a "DB2.zip".
- Plug-in sviluppato utilizzando Java: Aggiungere file jar, file jar dipendenti e file Plugin_descriptor.xml in una cartella e comprimerli.

Caricamento del file ZIP del plug-in

È necessario caricare il file ZIP del plug-in sul server SnapCenter in modo che il plug-in sia disponibile per la distribuzione sull'host desiderato.

È possibile caricare il plug-in utilizzando l'interfaccia utente o i cmdlet.

UI:

- Caricare il file ZIP del plug-in come parte della procedura guidata del flusso di lavoro **Add** o **Modify host**
- Fare clic su **"Select to upload custom plug-in"**

PowerShell:

- Cmdlet Upload-SmPluginPackage

  Ad esempio, PS> Upload-SmPluginPackage -AbsolutePath c: DB2_1.zip

  Per informazioni dettagliate sui cmdlet PowerShell, consultare la guida in linea del cmdlet di SnapCenter o le informazioni di riferimento del cmdlet.

"Guida di riferimento al cmdlet del software SnapCenter".

Implementazione dei plug-in personalizzati

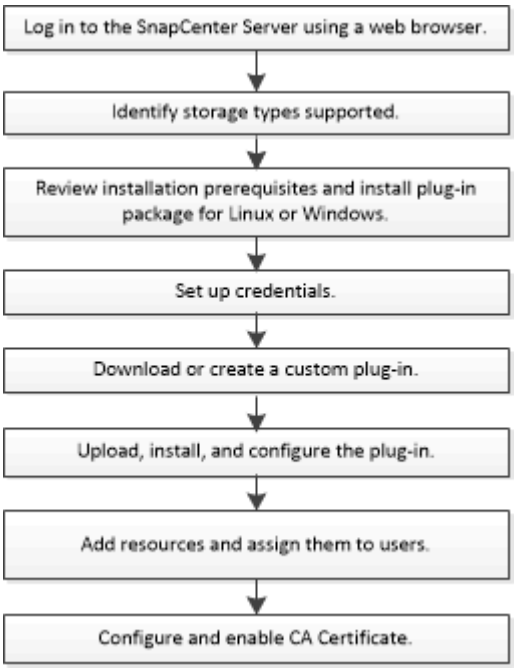
Il plug-in personalizzato caricato è ora disponibile per la distribuzione sull'host desiderato come parte del flusso di lavoro **Add** e **Modify host**. È possibile caricare più versioni dei plug-in sul server SnapCenter ed è possibile selezionare la versione desiderata da implementare su un host specifico.

Per ulteriori informazioni su come caricare il plug-in, vedere, "Aggiungere host e installare pacchetti plug-in su host remoti"

Preparare l’installazione dei plug-in personalizzati di SnapCenter

Workflow di installazione dei plug-in personalizzati di SnapCenter

Se si desidera proteggere le risorse dei plug-in personalizzati, è necessario installare e configurare i plug-in personalizzati di SnapCenter.



"Sviluppare un plug-in per l’applicazione"

Prerequisiti per l’aggiunta di host e l’installazione dei plug-in personalizzati di SnapCenter

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario completare tutti i requisiti. I plug-in personalizzati possono essere utilizzati in ambienti Windows e Linux.

- È necessario aver creato un plug-in personalizzato. Per ulteriori informazioni, vedere le informazioni sullo sviluppatore.

  "Sviluppare un plug-in per l’applicazione"

- Se si desidera gestire applicazioni MySQL o DB2, è necessario aver scaricato i plug-in personalizzati MySQL e DB2 forniti da NetApp.
- È necessario aver installato Java 1.8 o Java 11 (64 bit) sull’host Linux o Windows.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l’utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell’account utente sull’host.
- I plug-in personalizzati devono essere disponibili sull’host client da cui viene eseguita l’operazione di aggiunta dell’host.

Generale

Se si utilizza iSCSI, il servizio iSCSI dovrebbe essere in esecuzione.

Hash SHA512

- Per i plug-in personalizzati forniti da NetApp, assicurarsi di aver aggiunto l'hash SHA512 del file del plug-in personalizzato al file *custom_plugin_checksum_list*.
  - Per l'host Linux, l'hash SHA512 si trova in */var/opt/snapcenter/scc/custom_plugin_checksum_list.txt*
  - Per gli host Windows, l'hash SHA512 si trova in *C: File di programma NetApp, SnapCenter Plug-in Creator, ecc. custom_plugin_checksum_list.txt*

    Per il percorso di installazione personalizzato, l'hash SHA512 si trova in *<custom path>/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/custom_plugin_checksum_list.txt*

  Custom_plugin_checksum_list fa parte dell'installazione del plug-in personalizzato sull'host da parte di SnapCenter.

- Per i plug-in personalizzati creati per l'applicazione, è necessario eseguire le seguenti operazioni:

  a. Ha generato l'hash SHA512 del file zip del plug-in.

     È possibile utilizzare strumenti online come "Hash SHA512".

  b. Aggiunto l'hash SHA512 generato al file custom_plugin_checksum_list in una nuova riga.

     I commenti iniziano con il simbolo n. per identificare il plug-in a cui appartiene l'hash.

     Di seguito è riportato un esempio di una voce di hash SHA512 nel file checksum:

```
#ORASCPM
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63
d6e6777a2b2a1ec068bb0a93a59a8ade71587182f8bccbe81f7e0ba6
```

Host Windows

- È necessario disporre di un utente di dominio con privilegi di amministratore locale con autorizzazioni di accesso locale sull'host remoto.
- Se si gestiscono i nodi del cluster in SnapCenter, è necessario disporre di un utente con privilegi amministrativi per tutti i nodi del cluster.

Host Linux

- È necessario aver attivato la connessione SSH basata su password per l'utente root o non root.
- È necessario aver installato Java 1.8 o Java 11 (64 bit) sull'host Linux.

  Se si utilizza Windows Server 2019 o Windows Server 2016 per l'host del server SnapCenter, è necessario installare Java 1.8 o Java 11 (64 bit). Lo strumento matrice di interoperabilità (IMT) contiene le informazioni più recenti sui requisiti.

"Download Java per tutti i sistemi operativi"

"Tool di matrice di interoperabilità NetApp"

- Per consentire l'accesso a diversi percorsi, è necessario configurare i privilegi sudo per l'utente non root. Aggiungere le seguenti righe al file /etc/sudoers usando l'utility visudo Linux.

  Assicurarsi di utilizzare sudo versione 1.8.7 o successiva.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

  LINUX_USER è il nome dell'utente non root creato.

  È possibile ottenere il *checksum_value* dal file **oracle_checksum.txt**, che si trova in *C:/ProgramData/NetApp/SnapCenter/Package Repository*.

  L'esempio deve essere utilizzato solo come riferimento per la creazione di dati personali.

Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario conoscere alcuni requisiti di base relativi allo spazio del sistema host e al dimensionamento.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Elemento	Requisiti
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	5 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp". Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet."

Requisiti dell'host per l'installazione del pacchetto di plug-in SnapCenter per Linux

Assicurarsi che l'host soddisfi i requisiti prima di installare il pacchetto di plug-in SnapCenter per Linux.

Elemento	Requisiti
Sistemi operativi	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
RAM minima per il plug-in SnapCenter sull'host	1 GB

Elemento	Requisiti
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	Java 1,8 (64 bit) Oracle Java o OpenJDK Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.

Per informazioni aggiornate sulle versioni supportate, consultare la "Tool di matrice di interoperabilità NetApp"

Impostare le credenziali per i plug-in personalizzati di SnapCenter

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per l'esecuzione delle operazioni di protezione dei dati su database o file system Windows.

Prima di iniziare

- Host Linux

  È necessario impostare le credenziali per l'installazione dei plug-in sugli host Linux.

  Per installare e avviare il processo di plug-in, è necessario impostare le credenziali per l'utente root o per un utente non root che dispone dei privilegi di sudo.

  Best practice: sebbene sia consentito creare credenziali per Linux dopo l'implementazione degli host e l'installazione dei plug-in, la Best practice consiste nel creare credenziali dopo l'aggiunta di SVM, prima di distribuire host e installare plug-in.

- Host Windows

  Prima di installare i plug-in, è necessario impostare le credenziali di Windows.

  È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

- Applicazioni plug-in personalizzate

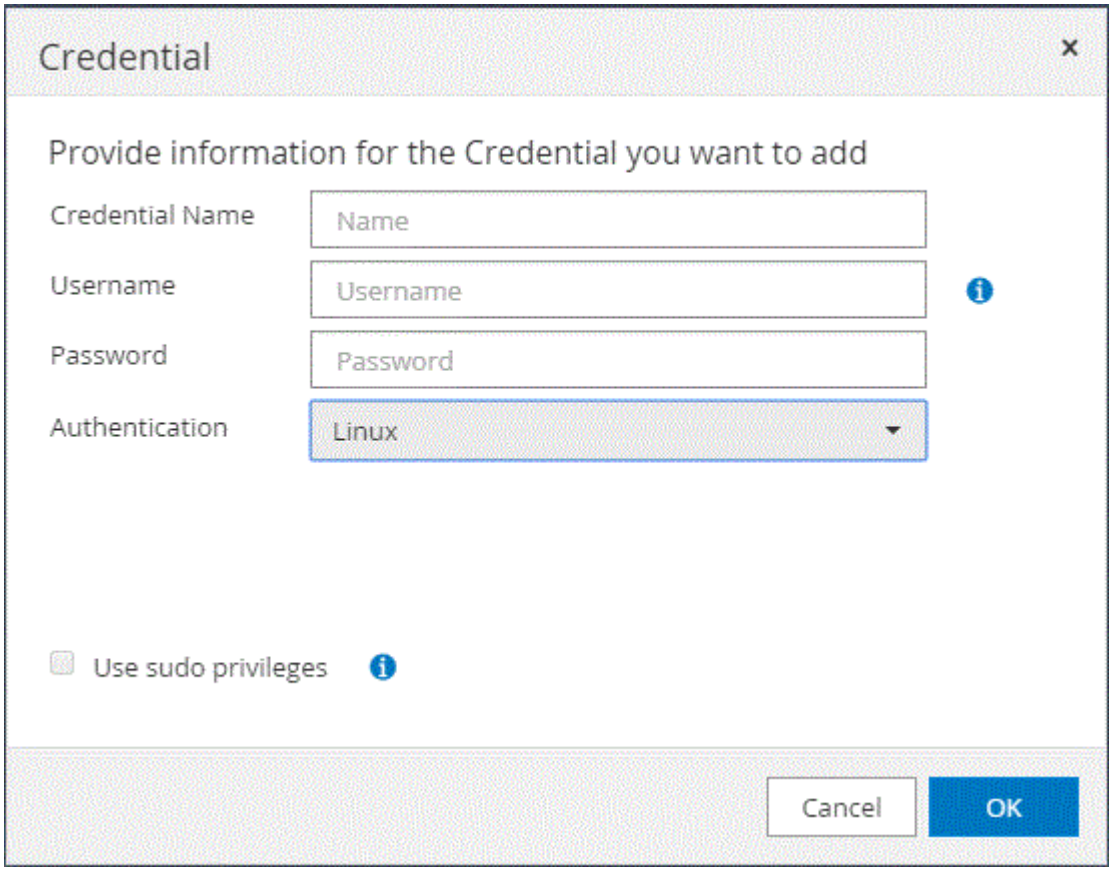
  Il plug-in utilizza le credenziali selezionate o create durante l'aggiunta di una risorsa. Se una risorsa non richiede credenziali durante le operazioni di protezione dei dati, è possibile impostare le credenziali su **None**.

A proposito di questa attività

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup al nome utente.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.



4. Nella pagina **credenziale**, specificare le informazioni necessarie per la configurazione delle credenziali:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale	Immettere un nome per le credenziali.

Per questo campo…	Eseguire questa operazione…
Nome utente	Immettere il nome utente e la password da utilizzare per l'autenticazione. • Amministratore di dominio o qualsiasi membro del gruppo di amministratori Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono: ◦ *NetBIOS/nome utente* ◦ *Dominio FQDN/nome utente* • Amministratore locale (solo per gruppi di lavoro) Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host. Il formato valido per il campo Nome utente è: *Nome utente*
Password	Inserire la password utilizzata per l'autenticazione.
Modalità di autenticazione	Selezionare la modalità di autenticazione che si desidera utilizzare.
Utilizzare i privilegi sudo	Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root. Applicabile solo agli utenti Linux.

5. Fare clic su **OK**.

Al termine dell'impostazione delle credenziali, è possibile assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina User and Access (utenti e accesso).

Configurare gMSA su Windows Server 2012 o versione successiva

Windows Server 2012 o versione successiva consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatica delle password dell'account di servizio da un account di dominio gestito.

Prima di iniziare

- È necessario disporre di un controller di dominio Windows Server 2012 o versione successiva.
- È necessario disporre di un host Windows Server 2012 o versione successiva, membro del dominio.

Fasi

1. Creare una chiave root KDS per generare password univoche per ogni oggetto in gMSA.
2. Per ciascun dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Creare e configurare gMSA:
   a. Creare un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo di utenti appena creato per creare gMSA.
```

   Ad esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Eseguire `Get-ADServiceAccount` il comando per verificare
l'account del servizio.
```

4. Configurare gMSA sugli host:
   a. Attivare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

   A tale scopo, eseguire il seguente comando da PowerShell:

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

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


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

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Riavviare l'host.

b. Installare gMSA sull'host eseguendo il comando seguente dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verificare il proprio account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter.

   Il server SnapCenter installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

Installare i plug-in personalizzati di SnapCenter

Aggiungere host e installare pacchetti plug-in su host remoti

Utilizzare la pagina SnapCenterAdd host per aggiungere host e installare i pacchetti plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere un host e installare i pacchetti plug-in per un singolo host o per un cluster.

Prima di iniziare

- Si dovrebbe essere un utente assegnato a un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.
- Assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare l'account di servizio gestito di gruppo su Windows Server 2012 o versione successiva per le applicazioni personalizzate"

A proposito di questa attività

Non è possibile aggiungere un server SnapCenter come host plug-in a un altro server SnapCenter.

Se si installano plug-in su un cluster (WSFC), i plug-in vengono installati su tutti i nodi del cluster.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata nella parte superiore.
3. Selezionare **Aggiungi**.
4. Nella pagina host, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare il tipo di host: • Windows • Linux I plug-in personalizzati possono essere utilizzati in ambienti Windows e Linux.
Nome host	Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire l'FQDN. Per gli ambienti Windows, l'indirizzo IP è supportato per gli host di dominio non attendibili solo se viene risolto nell'FQDN. È possibile inserire gli indirizzi IP o il nome FQDN di un host standalone. Se si aggiunge un host utilizzando SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN.

Per questo campo…	Eseguire questa operazione…
Credenziali	Selezionare il nome della credenziale creata o creare nuove credenziali. Le credenziali devono disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere le informazioni sulla creazione delle credenziali. È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome specificato. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione **Seleziona plug-in da installare**, selezionare i plug-in da installare.
6. (Facoltativo) selezionare **altre opzioni**.

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito oppure specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.

Per questo campo…	Eseguire questa operazione…
Percorso di installazione	I plug-in personalizzati possono essere installati su un sistema Windows o Linux. • Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C: In alternativa, è possibile personalizzare il percorso. • Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è `/opt/NetApp/snapcenter`. In alternativa, è possibile personalizzare il percorso. • Per i plug-in personalizzati di SnapCenter: i. Nella sezione Custom Plug-in (Plug-in personalizzati), selezionare **Browse** (Sfoglia) e selezionare la cartella dei plug-in personalizzati compressi. La cartella zippata contiene il codice del plug-in personalizzato e il file .xml descrittore. Per il plug-in di archiviazione, accedere alla *`C:\ProgramData\NetApp\SnapCenter\Package Repository`* cartella e selezionarla `Storage.zip` . ii. Selezionare **Upload**. Il file .xml descrittore nella cartella dei plug-in personalizzati compressi viene validato prima del caricamento del pacchetto. Vengono elencati i plug-in personalizzati caricati sul server SnapCenter. Se si desidera gestire applicazioni MySQL o DB2, è possibile utilizzare i plug-in personalizzati MySQL e DB2 forniti da NetApp.
Ignorare i controlli di preinstallazione	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

Per questo campo…	Eseguire questa operazione…
Utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in	Per l'host Windows, selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in. Fornire il nome gMSA nel seguente formato: Nome dominio/nome account. GMSA verrà utilizzato come account del servizio di accesso solo per il servizio del plug-in SnapCenter per Windows.

7. Selezionare **Invia**.

   Se non è stata selezionata la casella di controllo **Ignora controlli preliminari**, l'host viene convalidato per verificare se l'host soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione PowerShell, . La versione NET, la posizione (per i plug-in Windows) e la versione Java (per i plug-in Linux) sono convalidate in base ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati.

   Se l'errore riguarda lo spazio su disco o la RAM, è possibile aggiornare il file web.config che si trova in C: File di programma NetApp SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione ha, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi selezionare **Confirm and Submit** (Conferma e invia).

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

   I file di registro specifici dell'installazione si trovano nei `/custom_location/snapcenter/` registri.

Installare i pacchetti plug-in SnapCenter per Linux o Windows su più host remoti utilizzando i cmdlet

È possibile installare i pacchetti plug-in SnapCenter per Linux o Windows su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage PowerShell.

Prima di iniziare

L'utente che aggiunge un host deve disporre dei diritti amministrativi sull'host.

Fasi

1. Avviare PowerShell.
2. Sull'host del server SnapCenter, stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in su più host utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

   È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.
4. Inserire le credenziali per l'installazione remota.

Installare i plug-in personalizzati di SnapCenter sugli host Linux utilizzando l'interfaccia della riga di comando

Installare i plug-in personalizzati di SnapCenter utilizzando l'interfaccia utente di SnapCenter. Se l'ambiente in uso non consente l'installazione remota del plug-in dall'interfaccia utente di SnapCenter, è possibile installare i plug-in personalizzati in modalità console o in modalità silenziosa utilizzando l'interfaccia a riga di comando (CLI).

Fasi

1. Copiare il file di installazione del pacchetto plug-in SnapCenter per Linux (Snapcenter_linux_host_plugin.bin) da C: ProgramData/NetApp SnapCenter/Package Repository all'host in cui si desidera installare i plug-in personalizzati.

   È possibile accedere a questo percorso dall'host in cui è installato il server SnapCenter.
2. Dal prompt dei comandi, accedere alla directory in cui è stato copiato il file di installazione.
3. Installare il plug-in: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

   - -DPORT specifica la porta di comunicazione HTTPS SMCore.
   - -DSERVER_IP specifica l'indirizzo IP del server SnapCenter.
   - -DSERVER_HTTPS_PORT specifica la porta HTTPS del server SnapCenter.
   - -DUSER_INSTALL_DIR specifica la directory in cui si desidera installare il pacchetto di plug-in SnapCenter per Linux.
   - DINSTALL_LOG_NAME specifica il nome del file di log.

   ```
   /tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
   -DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
   -DUSER_INSTALL_DIR=/opt
   -DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
   -DCHOSEN_FEATURE_LIST=CUSTOM
   ```
4. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

5. Accedere a SnapCenter e caricare il plug-in personalizzato dall'interfaccia utente o utilizzando i cmdlet PowerShell.

   È possibile caricare il plug-in personalizzato dall'interfaccia utente facendo riferimento alla "Aggiungere host e installare pacchetti plug-in su host remoti" sezione .

   La guida in linea del cmdlet di SnapCenter e le informazioni di riferimento del cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell.

   "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare lo stato di installazione dei plug-in personalizzati

È possibile monitorare lo stato di avanzamento dell'installazione del pacchetto plug-in di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento dell'installazione per determinare quando è completa o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filter** (filtro).
   b. Facoltativo: Specificare la data di inizio e di fine.
   c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).
   d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.
   e. Fare clic su **Apply** (Applica).
4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Configurare il certificato CA

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare una CSR, vedere "Come generare il file CSR del certificato CA".

Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato del file di importazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
   c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
   d. Copiare i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

      Get-ChildItem -Path Certate: LocalMachine/My

   b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

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

Ad esempio:

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. Associare il certificato appena installato ai servizi plug-in
dell'host Windows eseguendo i seguenti comandi:
```

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

Ad esempio:

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

Configurare il certificato CA per il servizio plug-in personalizzati di SnapCenter sull'host Linux

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file 'keystore.jks', che si trova in */opt/NetApp/snapcenter/scc/etc* sia come Trust-store che come keystore.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Modificare la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle chiavi private nel
keystore con la stessa password utilizzata per il keystore:
```

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

Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.

> La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato: /Opt/NetApp/snapcenter/scc/ecc.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

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

4. Aggiungere un certificato root o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Riavviare il servizio dopo aver configurato i certificati root o
intermedi in un archivio di trust plug-in personalizzato.
```

> Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato /opt/NetApp/snapcenter/scc/ecc.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

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

4. Aggiungere il certificato CA con chiave pubblica e privata.

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

5. Elencare i certificati aggiunti nel keystore.

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

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Se il nome alias nel certificato CA è lungo e contiene spazi o
   caratteri speciali ("*",","), modificare il nome alias con un nome
   semplice:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configurare il nome alias del certificato CA nel file
   agent.properties.
   ```

   Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è ' opt/NetApp/snapcenter/scc/etc/crl'.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

   È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Configurare il certificato CA per il servizio plug-in personalizzati di SnapCenter sull'host Windows

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file *keystore.jks*, che si trova in _C: File di programma NetApp, SnapCenter, Snapcenter Plug-in Creator, ecc., sia come archivio di fiducia che come archivio chiavi.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Modificare la password del keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se il comando "keytool" non viene riconosciuto dal prompt dei comandi di Windows, sostituire il comando keytool con il relativo percorso completo.

   C: File di programma Java <jdk_version> keytool.exe" -storepasswd -keystore keystore.jks

3. Modificare la password per tutti gli alias delle chiavi private nel keystore con la stessa password utilizzata per il keystore:

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

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.

   > La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato _C: File di programma/NetApp/SnapCenter/Snapcenter Plug-in Creator
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungere un certificato root o intermedio:

   Keytool -import -trustcaacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Riavviare il servizio dopo aver configurato i certificati root o intermedi in un archivio di trust plug-in personalizzato.

Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato _C: File di programma/NetApp/SnapCenter/Snapcenter Plug-in Creator
2. Individuare il file *keystore.jks*.
3. Elencare i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungere il certificato CA con chiave pubblica e privata.

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

5. Elencare i certificati aggiunti nel keystore.

   keytool -list -v -keystore keystore.jks

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file agent.properties.

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

8. Configurare il nome alias del certificato CA nel file *agent.properties*.

   Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- Per scaricare il file CRL più recente per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoca dei certificati nel certificato CA di SnapCenter".
- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è _'C: File di programma, NetApp, SnapCenter, SnapCenter Plug-in Creator, ecc.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave CRL_PATH.
2. È possibile inserire più file CRL in questa directory.

I certificati in entrata verranno verificati per ciascun CRL.

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.
5. Selezionare **attiva convalida certificato**.

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- * * Indica che il certificato CA non è né abilitato né assegnato all'host del plug-in.
- * * Indica che il certificato CA è stato convalidato correttamente.
- * * Indica che il certificato CA non può essere convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Prepararsi alla protezione dei dati

Prerequisiti per l'utilizzo dei plug-in personalizzati di SnapCenter

Prima di utilizzare i plug-in personalizzati di SnapCenter, l'amministratore di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività necessarie.

- Installare e configurare il server SnapCenter.
- Accedere al server SnapCenter.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di storage e creando credenziali, se applicabili.

- Aggiungere host e installare e caricare i plug-in.
- Se applicabile, installare Java 1.7 o Java 1.8 sull'host del plug-in.
- Se si dispone di più percorsi dati (LIF) o di una configurazione DNFS, è possibile eseguire le seguenti operazioni utilizzando l'interfaccia utente di SnapCenter sull'host del database:
  - Per impostazione predefinita, tutti gli indirizzi IP dell'host del database vengono aggiunti alla policy di esportazione dello storage NFS in SVM (Storage Virtual Machine) per i volumi clonati. Se si desidera avere un indirizzo IP specifico o limitare un sottoinsieme di indirizzi IP, eseguire la CLI Set-PreferredHostIPsInStorageExportPolicy.
  - Se si dispone di più percorsi di dati (LIF) in SVM, SnapCenter sceglie il percorso di dati appropriato per il montaggio del volume clonato NFS. Tuttavia, se si desidera specificare un percorso dati specifico (LIF), è necessario eseguire la CLI Set-SvmPreferredDataPath. Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al comando software SnapCenter".
- Impostare SnapMirror e SnapVault, se si desidera eseguire la replica del backup.
- Assicurarsi che la porta 9090 non sia utilizzata da altre applicazioni sull'host.

  La porta 9090 deve essere riservata per l'utilizzo da parte dei plug-in personalizzati SnapCenter oltre alle altre porte richieste da SnapCenter.

Utilizzo di risorse, gruppi di risorse e policy per la protezione delle risorse plug-in personalizzate

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- In genere, le risorse sono database, file system Windows o macchine virtuali di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è un insieme di risorse su un host o cluster.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È inoltre possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- I criteri specificano la frequenza di backup, la conservazione delle copie, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano uno o più criteri per tale gruppo. È inoltre possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

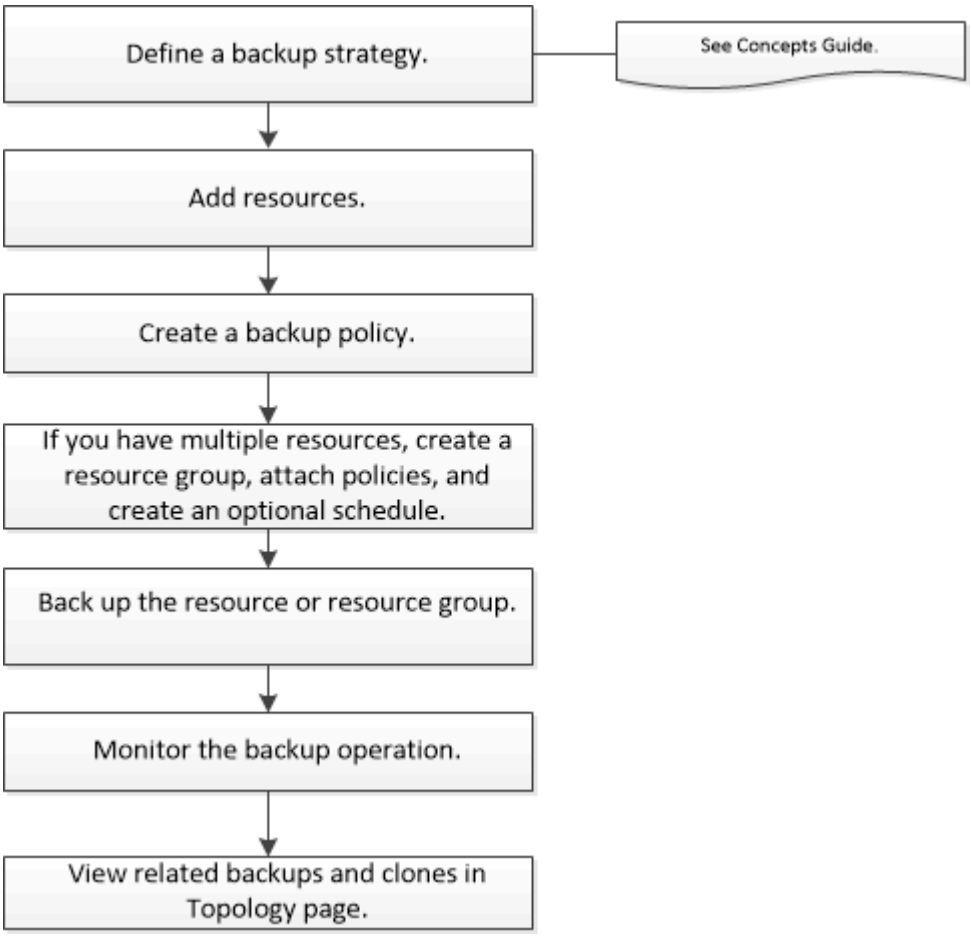
Un gruppo di risorse definisce *cosa* si desidera proteggere e quando si desidera proteggerlo in termini di giorno e ora. Pensa a una policy come a definire *come* la vuoi proteggere. Ad esempio, se si esegue il backup di tutti i database o di tutti i file system di un host, è possibile creare un gruppo di risorse che includa tutti i database o tutti i file system dell'host. È quindi possibile associare due criteri al gruppo di risorse: Una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si allegano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup basato su file ogni giorno e un altro programma che esegua il backup basato su Snapshot ogni ora.

Eseguire il backup delle risorse plug-in personalizzate

Eseguire il backup delle risorse plug-in personalizzate

Il workflow di backup include la pianificazione, l'identificazione delle risorse per il backup, la gestione delle policy di backup, la creazione di gruppi di risorse e l'aggiunta di policy, la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida dei cmdlet di SnapCenter o vedere la "Guida di riferimento al cmdlet del software SnapCenter"

Aggiungere risorse ai plug-in personalizzati di SnapCenter

È necessario aggiungere le risorse di cui si desidera eseguire il backup o la clonazione. A seconda dell'ambiente in uso, le risorse possono essere istanze di database o raccolte di cui si desidera eseguire il backup o la clonazione.

Prima di iniziare

- È necessario completare attività come l'installazione del server SnapCenter, l'aggiunta di host, la creazione di connessioni al sistema di storage e l'aggiunta di credenziali.

- È necessario disporre di "creazione di un plug-in personalizzato per l'applicazione".
- I plug-in devono essere stati caricati sul server SnapCenter.

A proposito di questa attività

È inoltre possibile aggiungere risorse per applicazioni MySQL e DB2.

Fasi

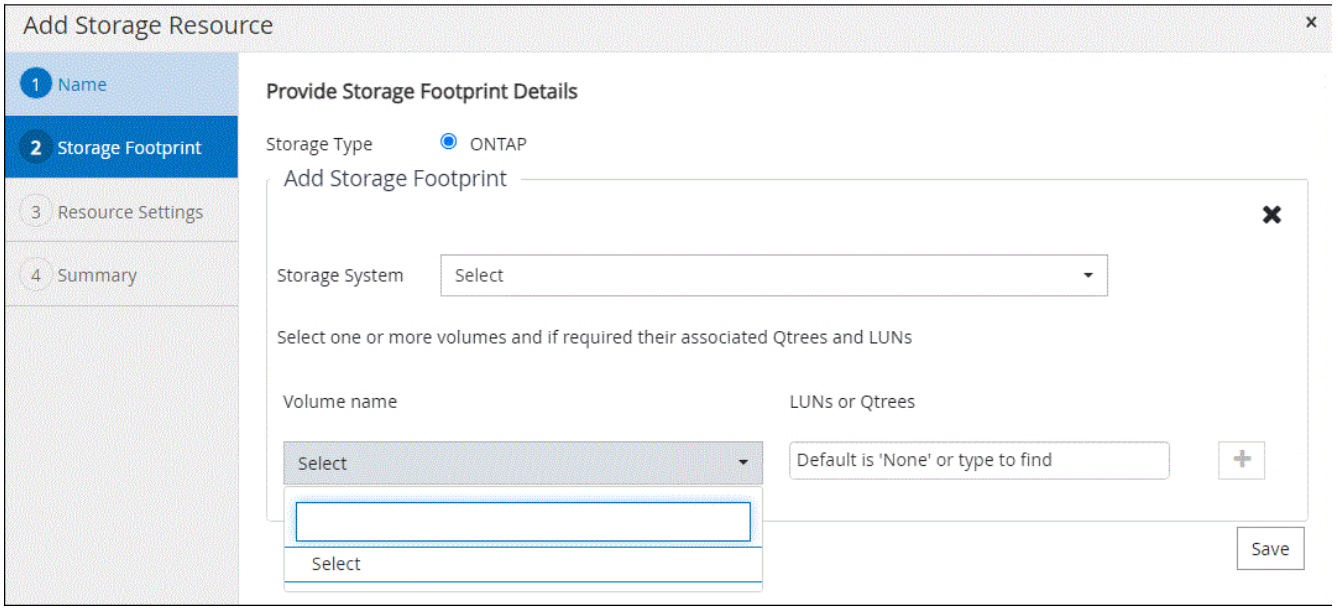
1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **Aggiungi risorsa**.
3. Nella pagina fornire dettagli sulle risorse, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere il nome della risorsa.
Nome host	Selezionare l'host.
Tipo	Selezionare il tipo. Il tipo è definito dall'utente in base al file di descrizione del plug-in. Ad esempio, database e istanze. Nel caso in cui il tipo selezionato abbia un padre, inserisci i dettagli dell'padre. Ad esempio, se il tipo è Database e il padre è istanza, inserire i dettagli dell'istanza.
Nome della credenziale	Selezionare credenziale o creare una nuova credenziale.
Percorsi di montaggio	Immettere i percorsi di montaggio in cui è montata la risorsa. Questo è valido solo per un host Windows.

4. Nella pagina fornire footprint dello storage, selezionare un sistema storage e scegliere uno o più volumi, LUN e qtree, quindi selezionare **Salva**.

   Opzionale: Seleziona l' + icona per aggiungere più volumi, LUN e qtree da altri sistemi storage.

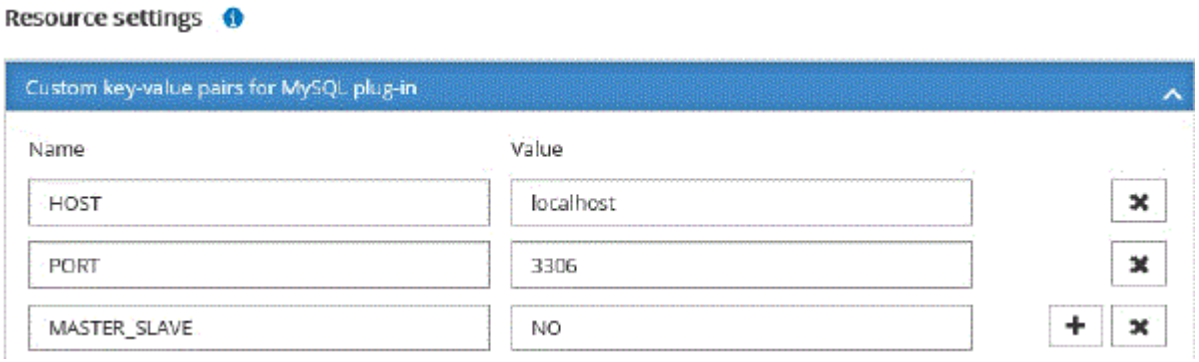
   I plug-in personalizzati di SnapCenter non supportano il rilevamento automatico delle risorse. Anche i dettagli dello storage degli ambienti fisici e virtuali non vengono rilevati automaticamente. Durante la creazione delle risorse, è necessario fornire le informazioni di storage per gli ambienti fisici e virtuali.



5. Nella pagina Resource Settings (Impostazioni risorse), fornire coppie chiave-valore personalizzate per la risorsa.

   Utilizzare le coppie chiave-valore personalizzate se si desidera passare informazioni specifiche della risorsa. Ad esempio, quando si utilizza il plug-in MySQL, è necessario specificare un HOST come HOST=hostname, PORT =port-NO usato per MySQL e configurazione master-slave come MASTER_SLAVE = “YES” o “NO” (il nome è MASTER_SLAVE e il valore è “YES” o “NO”).

   Assicurarsi che LE parole HOST e PORT siano in maiuscolo.



6. Esaminare il riepilogo, quindi selezionare **fine**.

Risultato

Le risorse vengono visualizzate insieme a informazioni quali tipo, nome host o cluster, criteri e gruppi di risorse associati e stato generale.

È necessario aggiornare le risorse se i database vengono rinominati al di fuori di SnapCenter.

Al termine

Se si desidera fornire l’accesso alle risorse ad altri utenti, l’amministratore di SnapCenter deve assegnare le risorse a tali utenti. In questo modo, gli utenti possono eseguire le azioni per le quali dispongono delle autorizzazioni per le risorse ad essi assegnate.

Dopo aver aggiunto le risorse, è possibile modificarne i dettagli. Se a una risorsa plug-in personalizzata sono associati backup, non è possibile modificare i seguenti campi: Nome risorsa, tipo di risorsa e nome host.

Creare policy per risorse plug-in personalizzate

Prima di utilizzare SnapCenter per eseguire il backup di risorse specifiche del plug-in personalizzato, è necessario creare un criterio di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup.

Prima di iniziare

- Dovresti aver definito la tua strategia di backup.

  Per ulteriori informazioni, consulta le informazioni sulla definizione di una strategia di protezione dei dati per i plug-in personalizzati.

- Dovresti aver preparato per la protezione dei dati.

  La preparazione per la protezione dei dati include attività come l'installazione di SnapCenter, l'aggiunta di host, la creazione di connessioni al sistema di storage e l'aggiunta di risorse.

- Le macchine virtuali di storage (SVM) devono essere assegnate all'utente per le operazioni di mirroring o vault.

  L'amministratore di SnapCenter deve aver assegnato le SVM per i volumi di origine e destinazione se si stanno replicando Snapshot in un mirror o un vault.

- Dovrebbero essere state aggiunte manualmente le risorse che si desidera proteggere.

A proposito di questa attività

- Un criterio di backup è un insieme di regole che regolano la gestione, la pianificazione e la conservazione dei backup. Inoltre, è possibile specificare le impostazioni di replica, script e applicazione.
- La specifica delle opzioni in un criterio consente di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.
- SnapLock
  - Se è selezionata l'opzione "conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere minore o uguale ai giorni di conservazione menzionati.
  - La specifica di un periodo di blocco snapshot impedisce l'eliminazione delle istantanee fino alla scadenza del periodo di conservazione. Questo potrebbe portare a mantenere un numero di Snapshot maggiore del conteggio specificato nel criterio.
  - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

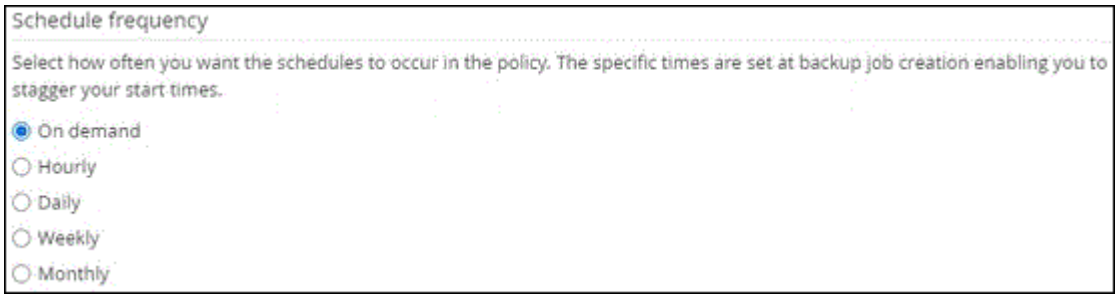
> Le impostazioni SnapLock primarie vengono gestite nel criterio di backup SnapCenter e le impostazioni SnapLock secondarie vengono gestite da ONTAP.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.

3. Fare clic su **nuovo**.
4. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
5. Nella pagina Impostazioni, attenersi alla seguente procedura:
   - Specificare il tipo di pianificazione selezionando **on demand**, **Hourly**, **Daily**, **Weekly** o **Monthly**.

     È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e frequenza di backup, ma consente di assegnare diverse pianificazioni di backup a ciascun criterio.



     Se sono previste le 2:00, la programmazione non verrà attivata durante l'ora legale (DST).

   - Nella sezione Custom backup settings (Impostazioni di backup personalizzate), fornire le impostazioni di backup specifiche che devono essere passate al plug-in in formato key-value. È possibile fornire più valori chiave da passare al plug-in.
6. Nella pagina **retention**, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionato nella pagina **Backup Type**:

Se si desidera…	Quindi…
Mantenere un certo numero di istantanee	Selezionare **totale copie snapshot da conservare**, quindi specificare il numero di istantanee che si desidera conservare. Se il numero di istantanee supera il numero specificato, le istantanee vengono eliminate con le copie meno recenti eliminate per prime. Se si intende attivare la replica SnapVault, è necessario impostare il numero di conservazione su 2 o superiore. Se si imposta il conteggio della conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è il Snapshot di riferimento per la relazione SnapVault fino a quando una snapshot più recente non viene replicata nella destinazione. Il valore massimo di conservazione è 1018 per le risorse su ONTAP 9.4 o versioni successive e 254 per le risorse su ONTAP 9.3 o versioni precedenti. I backup non avranno esito positivo se la conservazione viene impostata su un valore superiore a quello supportato dalla versione di ONTAP sottostante.
Conservare le istantanee per un determinato numero di giorni	Selezionare **Mantieni copie snapshot per**, quindi specificare il numero di giorni per i quali si desidera conservare le istantanee prima di eliminarle.
Periodo di blocco della copia snapshot	Selezionare periodo di blocco istantanea e selezionare giorni, mesi o anni. Il periodo di conservazione di SnapLock deve essere inferiore a 100 anni.

7. Nella pagina **Replica**, specificare le impostazioni di replica:

Per questo campo…	Eseguire questa operazione…
Aggiornare SnapMirror dopo aver creato una copia Snapshot locale	Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror). Se la relazione di protezione in ONTAP è di tipo Mirror e Vault e se si seleziona solo questa opzione, l'istantanea creata sul primario non verrà trasferita alla destinazione, ma sarà elencata nella destinazione. Se questa istantanea viene selezionata dalla destinazione per eseguire un'operazione di ripristino, viene visualizzato il seguente messaggio di errore: Posizione secondaria non disponibile per il backup a vault/mirror selezionato. Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante **Aggiorna** nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP. Vedere "Visualizza i backup e i cloni personalizzati relativi alle risorse plug-in nella pagina topologia".
Aggiornare SnapVault dopo aver creato una copia Snapshot locale	Selezionare questa opzione per eseguire la replica del backup disk-to-disk (backup SnapVault). Durante la replica secondaria, il tempo di scadenza del SnapLock carica il tempo di scadenza del SnapLock primario. Fare clic sul pulsante **Aggiorna** nella pagina topologia per aggiornare il tempo di scadenza SnapLock secondario e primario recuperato da ONTAP. Quando SnapLock è configurato solo sul secondario da ONTAP noto come vault di SnapLock, facendo clic sul pulsante **Aggiorna** nella pagina topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP. Per ulteriori informazioni sul vault di SnapLock, vedere commit Snapshot to WORM su una destinazione del vault Vedere "Visualizza i backup e i cloni personalizzati relativi alle risorse plug-in nella pagina topologia".

Per questo campo…	Eseguire questa operazione…
Etichetta del criterio secondario	Selezionare un'etichetta Snapshot. A seconda dell'etichetta Snapshot selezionata, ONTAP applica la politica di conservazione Snapshot secondaria corrispondente all'etichetta. Se è stato selezionato **Update SnapMirror dopo la creazione di una copia Snapshot locale**, è possibile specificare l'etichetta del criterio secondario. Tuttavia, se è stato selezionato **Aggiorna SnapVault dopo la creazione di una copia Snapshot locale**, è necessario specificare l'etichetta del criterio secondario.
Numero tentativi di errore	Immettere il numero massimo di tentativi di replica consentiti prima dell'interruzione dell'operazione.

È necessario configurare il criterio di conservazione SnapMirror in ONTAP per lo storage secondario, in modo da evitare di raggiungere il limite massimo di Snapshot sullo storage secondario.

8. Esaminare il riepilogo, quindi fare clic su **fine**.

Creare gruppi di risorse e allegare policy in SnapCenter

Un gruppo di risorse è il container al quale è necessario aggiungere risorse di cui si desidera eseguire il backup e la protezione. Consente di eseguire contemporaneamente il backup di tutti i dati associati a una determinata applicazione. È inoltre necessario associare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare nuovo gruppo di risorse.
3. Nella pagina Name (Nome), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere un nome per il gruppo di risorse. Nota: Il nome del gruppo di risorse non deve superare i 250 caratteri.

Per questo campo…	Eseguire questa operazione…
Tag	Inserire una o più etichette per facilitare la ricerca del gruppo di risorse in un secondo momento. Ad esempio, se si aggiunge HR come tag a più gruppi di risorse, è possibile trovare in seguito tutti i gruppi di risorse associati al tag HR.
USA il formato nome personalizzato per la copia Snapshot	Selezionare questa casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea. Ad esempio, *customtext_resource group_policy_hostname o resource group_hostname*. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

4. Facoltativo: Nella pagina risorse, selezionare un nome host dall'elenco a discesa **host** e il tipo di risorsa dall'elenco a discesa **tipo di risorsa**.

   In questo modo è possibile filtrare le informazioni sullo schermo.

5. Selezionare le risorse dalla sezione **risorse disponibili**, quindi selezionare la freccia destra per spostarle nella sezione **risorse selezionate**.
6. Facoltativo: Nella pagina **Impostazioni applicazione**, effettuare le seguenti operazioni:

   a. Selezionare la freccia Backup per impostare opzioni di backup aggiuntive:

      Abilitare il backup dei gruppi di coerenza ed eseguire le seguenti attività:

Per questo campo…	Eseguire questa operazione…
Tempo di attesa per il completamento dell'operazione Consistency Group Snapshot	Selezionare urgente, Medio o rilassato per specificare il tempo di attesa per il completamento dell'operazione istantanea. Urgente = 5 secondi, Medio = 7 secondi e rilassato = 20 secondi.
Disattiva sincronizzazione WAFL	Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL.

+

a. Selezionare la freccia Scripts (script) e immettere i comandi pre e post per le operazioni quiescenza, istantanea e inquiescenza. In caso di errore, è anche possibile inserire i pre-comandi da eseguire prima di uscire.

b. Selezionare la freccia Custom Configurations (configurazioni personalizzate) e immettere le coppie chiave-valore personalizzate richieste per tutte le operazioni di protezione dei dati che utilizzano questa risorsa.

Parametro	Impostazione	Descrizione
ARCHIVE_LOG_ENABLE	(S/N)	Consente alla gestione del log di archiviazione di eliminare i log di archiviazione.
ARCHIVE_LOG_RETENTION	numero_di_giorni	Specifica il numero di giorni in cui i registri di archiviazione vengono conservati. Questa impostazione deve essere uguale o superiore a NTAP_SNAPSHOT_ RETENTIONS.
ARCHIVE_LOG_DIR	change_info_directory/logs	Specifica il percorso della directory che contiene i log di archiviazione.

Parametro	Impostazione	Descrizione
ARCHIVE_LOG_EXT	estensione_file	Specifica la lunghezza dell'estensione del file di log dell'archivio. Ad esempio, se il log di archiviazione è log_backup_0_0_0_0.16151855 1942 9 e il valore di estensione_file è 5, l'estensione del log conserverà 5 cifre, ossia 16151.
ARCHIVE_LOG_RECURSIVE_ SE ARCH	(S/N)	Attiva la gestione dei log di archiviazione all'interno delle sottodirectory. Utilizzare questo parametro se i log di archiviazione si trovano nelle sottodirectory.

c. Selezionare la freccia **Snapshot Copy Tool** (strumento di copia istantanea) per selezionare lo strumento per creare le istantanee:

Se vuoi…	Quindi…
SnapCenter deve utilizzare il plug-in per Windows e mettere il file system in uno stato coerente prima di creare una Snapshot. Per le risorse Linux, questa opzione non è applicabile.	Selezionare **SnapCenter with file system Consistency**. Questa opzione non è applicabile al plug-in SnapCenter per database SAP HANA.
SnapCenter per creare una istantanea a livello di storage	Selezionare **SnapCenter senza coerenza del file system**.
Immettere il comando da eseguire sull'host per creare Snapshot.	Selezionare **Altro**, quindi immettere il comando da eseguire sull'host per creare un'istantanea.

7. Nella pagina Criteri, attenersi alla seguente procedura:

a. Selezionare uno o più criteri dall'elenco a discesa.

È inoltre possibile creare un criterio selezionando * * .

I criteri sono elencati nella sezione **Configura pianificazioni per i criteri selezionati**.

b. Nella colonna **Configura pianificazioni**, selezionare * * per il criterio che si desidera configurare.

c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione e

selezionare OK.

Dove policy_name è il nome del criterio selezionato.

Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate). Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup di SnapCenter.

8. Dall'elenco a discesa **Email preference** (Preferenze email) della pagina **Notification** (notifica), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Il server SMTP deve essere configurato in **Impostazioni** > **Impostazioni globali**.

9. Esaminare il riepilogo, quindi selezionare **fine**.

Eseguire il backup di singole risorse plug-in personalizzate

Se una singola risorsa plug-in personalizzata non fa parte di alcun gruppo di risorse, è possibile eseguire il backup della risorsa dalla pagina risorse. È possibile eseguire il backup della risorsa on-demand oppure, se la risorsa dispone di un criterio allegato e di una pianificazione configurata, i backup vengono eseguiti automaticamente in base alla pianificazione.

Prima di iniziare

- È necessario aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con uno storage secondario, il ruolo ONTAP assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, filtrare le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Fare clic su , quindi selezionare il nome host e il tipo di risorsa per filtrare le risorse. È quindi possibile fare clic su per chiudere il riquadro del filtro.

3. Fare clic sulla risorsa di cui si desidera eseguire il backup.
4. Nella pagina risorsa, se si desidera utilizzare un nome personalizzato, selezionare la casella di controllo **Usa formato nome personalizzato per copia istantanea** , quindi immettere un formato nome personalizzato per il nome dell'istantanea.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

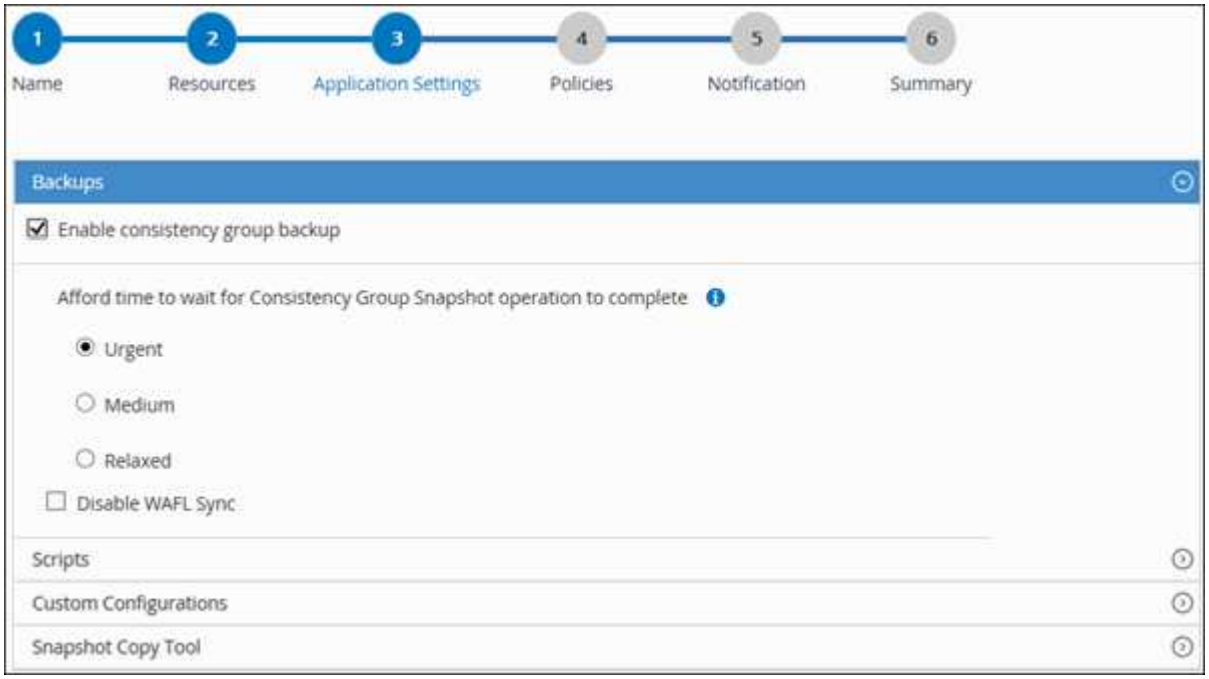
5. Nella pagina Impostazioni applicazione, effettuare le seguenti operazioni:

   a. Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

      Attivare il backup dei gruppi di coerenza, se necessario, ed eseguire le seguenti attività:

Per questo campo…	Eseguire questa operazione…
Tempo di attesa per il completamento dell'operazione Consistency Group Snapshot	Selezionare urgente, Medio o rilassato per specificare il tempo di attesa per il completamento dell'operazione istantanea. Urgente = 5 secondi, Medio = 7 secondi e rilassato = 20 secondi.
Disattiva sincronizzazione WAFL	Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL.

+



a. Fare clic sulla freccia **Scripts** per eseguire i comandi pre e post per le operazioni quiescenza, istantanea e inquiescenza. È inoltre possibile eseguire i comandi preliminari prima di uscire dall'operazione di backup.

   Le prescrizioni e i postscript vengono eseguiti nel server SnapCenter.

b. Fare clic sulla freccia **Custom Configurations** (configurazioni personalizzate), quindi immettere le coppie di valori personalizzate richieste per tutti i lavori che utilizzano questa risorsa.

c. Fare clic sulla freccia **Snapshot Copy Tool** per selezionare lo strumento per creare le istantanee:

Se vuoi…	Quindi…
SnapCenter per acquisire una snapshot a livello di storage	Selezionare **SnapCenter senza coerenza del file system**.
SnapCenter utilizza il plug-in per Windows per mettere il file system in uno stato coerente e quindi scattare una Snapshot	Selezionare **SnapCenter with file system Consistency**.

Se vuoi…	Quindi…
Per immettere il comando per creare un'istantanea	Selezionare **Altro**, quindi immettere il comando per creare un'istantanea.

6. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.

      È inoltre possibile creare un criterio facendo clic su + .

      Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

   b. Fare clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.

      Dove *policy_name* è il nome del criterio selezionato.

   Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

7. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. SMTP deve essere configurato anche in **Impostazioni** > **Impostazioni globali**.

8. Esaminare il riepilogo, quindi fare clic su **fine**.

   Viene visualizzata la pagina della topologia delle risorse.

9. Fare clic su **Esegui backup ora**.
10. Nella pagina Backup, attenersi alla seguente procedura:
    a. Se sono stati applicati più criteri alla risorsa, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

       Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Fare clic su **Backup**.
11. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Eseguire il backup di gruppi di risorse di plug-in personalizzati

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina risorse. Se un gruppo di risorse dispone di un criterio associato e di una pianificazione configurata, i

backup vengono eseguiti automaticamente in base alla pianificazione.

Prima di iniziare

- È necessario aver creato un gruppo di risorse con un criterio allegato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con lo storage secondario, il ruolo ONTAP assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).

   È possibile eseguire una ricerca nel gruppo di risorse immettendo il nome del gruppo di risorse nella casella di ricerca oppure facendo clic  e selezionando il tag. È quindi possibile fare clic su  per chiudere il riquadro del filtro.

3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi fare clic su **Esegui backup ora**.
4. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se sono stati associati più criteri al gruppo di risorse, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Fare clic su **Backup**.
5. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.
   - Nelle configurazioni MetroCluster, SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

     "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover di MetroCluster"

   - Se si esegue il backup dei dati delle applicazioni su VMDK e la dimensione dell'heap Java per il plug-in SnapCenter per VMware vSphere non è sufficiente, il backup potrebbe non riuscire. Per aumentare la dimensione dell'heap Java, individuare il file script /opt/netapp/init_scripts/scvservice. In tale script, il `do_start method` comando avvia il servizio plug-in VMware di SnapCenter. Aggiornare il comando al seguente indirizzo: `Java -jar -Xmx8192M -Xms4096M`.

Creare una connessione al sistema storage e una credenziale utilizzando i cmdlet PowerShell

È necessario creare una connessione SVM (Storage Virtual Machine) e una credenziale prima di utilizzare i cmdlet PowerShell per eseguire operazioni di protezione dei dati.

Prima di iniziare

- L'ambiente PowerShell dovrebbe essere stato preparato per l'esecuzione dei cmdlet PowerShell.
- Per creare le connessioni storage, è necessario disporre delle autorizzazioni necessarie nel ruolo

Infrastructure Admin.

- Assicurarsi che le installazioni dei plug-in non siano in corso.

  Le installazioni dei plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage perché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nella GUI di SnapCenter come "non disponibile per il backup" o "non su storage NetApp".

- I nomi dei sistemi di storage devono essere univoci.

  SnapCenter non supporta più sistemi storage con lo stesso nome su cluster diversi. Ogni sistema storage supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF di gestione univoco.

Fasi

1. Avviare una sessione di connessione PowerShell utilizzando il cmdlet Open-SmConnection.

   Questo esempio apre una sessione PowerShell:

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

2. Creare una nuova connessione al sistema di storage utilizzando il cmdlet Add-SmStorageConnection.

   Questo esempio crea una nuova connessione al sistema di storage:

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

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   In questo esempio viene creata una nuova credenziale denominata FinanceAdmin con credenziali Windows:

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Eseguire il backup delle risorse utilizzando i cmdlet PowerShell

Il backup di una risorsa include la connessione con il server SnapCenter, l'aggiunta di risorse, l'aggiunta di un criterio, la creazione di un gruppo di risorse di backup e il backup.

Prima di iniziare

- È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

- È necessario aver aggiunto la connessione al sistema di storage e creato una credenziale.

A proposito di questa attività

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

   Viene visualizzato il prompt di nome utente e password.

2. Aggiungere risorse utilizzando il cmdlet Add-SmResources.

   Questo esempio aggiunge risorse:

   ```
   Add-SmResource -HostName '10.232.206.248' -PluginCode 'DB2'
   -ResourceName NONREC1 -ResourceType Database -StorageFootPrint ( @
   {"VolumeName"="DB2_NONREC1DB";"LunName"="DB2_NONREC1DB";"Vserver"="vserv
   er_scauto_secondary"}) -Instance db2inst1
   ```

3. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   Questo esempio crea una nuova policy di backup:

   ```
   Add-SMPolicy -PolicyName 'db2VolumePolicy' -PolicyType 'Backup'
   -PluginPolicyType DB2  -description 'VolumePolicy'
   ```

4. Aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   In questo esempio viene creato un nuovo gruppo di risorse con le risorse e i criteri specificati:

   ```
   Add-SmResourceGroup -ResourceGroupName
   'Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix' -Resources @(@
   {"Host"="10.232.206.248";"Uid"="db2inst2\NONREC"},@{"Host"="10.232.206.2
   48";"Uid"="db2inst1\NONREC"}) -Policies db2ManualPolicy
   ```

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

```
New-SMBackup -DatasetName
Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix -Policy
db2ManualPolicy
```

6. Visualizzare lo stato del processo di backup utilizzando il cmdlet Get-SmBackupReport.

   Questo esempio visualizza un report di riepilogo di tutti i lavori eseguiti alla data specificata:

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

Monitorare le operazioni di backup delle risorse plug-in personalizzate

È possibile monitorare l'avanzamento di diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere necessario controllare i progressi per determinare quando sono stati completati o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Status** (Stato), selezionare lo stato del backup.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene venga visualizzato lo stato del processo di backup , quando si fa clic sui dettagli del processo, è possibile che alcune delle attività secondarie dell'operazione di backup siano ancora in corso o contrassegnate da segnali di avviso.

5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Annulla le operazioni di backup per i plug-in personalizzati

È possibile annullare le operazioni di backup inserite nella coda.

Cosa ti serve

- Per annullare le operazioni, è necessario accedere come amministratore SnapCenter o come proprietario del processo.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- Per annullare le operazioni di backup, è possibile utilizzare l'interfaccia grafica utente di SnapCenter, i cmdlet PowerShell o i comandi CLI.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di backup in coda degli altri membri durante l'utilizzo di tale ruolo.

Fasi

1. Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	a. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**.
Riquadro delle attività	a. Dopo aver avviato l'operazione di backup, fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti. b. Selezionare l'operazione. c. Nella pagina Dettagli processo, fare clic su **Annulla processo**.

L'operazione viene annullata e la risorsa viene riportata allo stato precedente.

Visualizza i backup e i cloni personalizzati relativi alle risorse plug-in nella pagina topologia

Quando si prepara il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e cloni sullo storage primario e secondario. Nella pagina topologia, è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e selezionarli per eseguire le operazioni di protezione dei dati.

A proposito di questa attività

È possibile esaminare le seguenti icone nella vista Manage Copies (Gestisci copie) per determinare se i backup e i cloni sono disponibili sullo storage primario o secondario (copie Mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- Visualizza il numero di backup e cloni su cui viene eseguito il mirroring dello storage secondario utilizzando la tecnologia SnapMirror.

  I cloni di un backup di un mirror flessibile della versione su un volume di tipo mirror-vault vengono visualizzati nella vista della topologia, ma il numero di backup mirror nella vista della topologia non include il backup flessibile della versione.

- Visualizza il numero di backup e cloni replicati sullo storage secondario utilizzando la tecnologia

SnapVault.

Il numero di backup visualizzati include i backup eliminati dallo storage secondario. Ad esempio, se sono stati creati 6 backup utilizzando un criterio per conservare solo 4 backup, il numero di backup visualizzati è 6.

> I cloni di un backup di un mirror flessibile della versione su un volume di tipo mirror-vault vengono visualizzati nella vista della topologia, ma il numero di backup mirror nella vista della topologia non include il backup flessibile della versione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Consulta la scheda Summary per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione Summary Card (scheda di riepilogo) visualizza il numero totale di backup e cloni.

   Facendo clic sul pulsante Refresh (Aggiorna), viene avviata una query dello storage per visualizzare un conteggio accurato.

   Se viene eseguito il backup abilitato SnapLock, facendo clic sul pulsante **Aggiorna** si aggiornano i tempi di scadenza SnapLock primari e secondari recuperati da ONTAP. Inoltre, una pianificazione settimanale aggiorna il tempo di scadenza SnapLock primario e secondario recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza del SnapLock per il backup sarà il tempo di scadenza del SnapLock più lungo impostato per una Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Dopo il backup su richiesta, facendo clic sul pulsante **Refresh** (Aggiorna) vengono aggiornati i dettagli del backup o della clonazione.

5. Nella vista Gestisci copie, fare clic su **backup** o **cloni** dallo storage primario o secondario per visualizzare i dettagli di un backup o clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione, ridenominazione ed eliminazione.

   > Non è possibile rinominare o eliminare i backup presenti nel sistema di storage secondario.

   > Non è possibile rinominare i backup presenti nel sistema di storage primario.

7. Se si desidera eliminare un clone, selezionarlo dalla tabella e fare clic per eliminarlo.

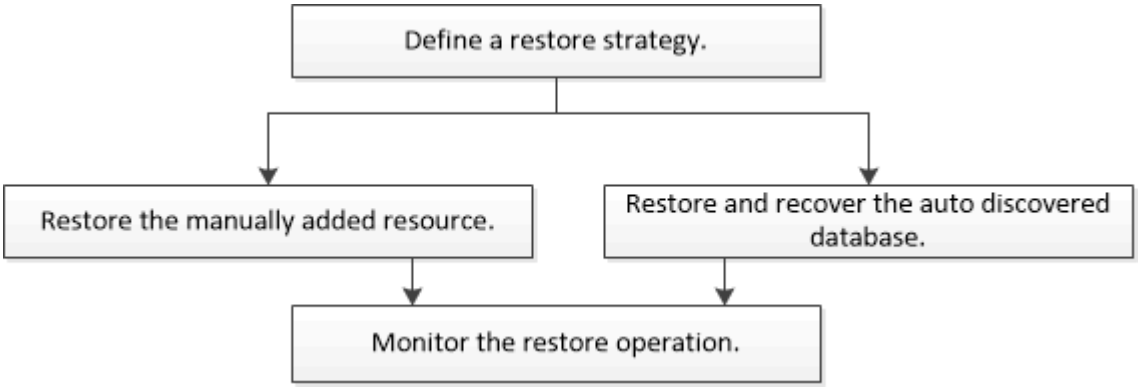
Ripristinare risorse plug-in personalizzate

Ripristinare risorse plug-in personalizzate

Il flusso di lavoro di ripristino e ripristino include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

A proposito di questa attività

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di ripristino:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. Per informazioni sui cmdlet di PowerShell, utilizzare la Guida dei cmdlet di SnapCenter o consultare la "Guida di riferimento al cmdlet del software SnapCenter".

Ripristinare un backup delle risorse

È possibile utilizzare SnapCenter per ripristinare le risorse. Le funzionalità delle operazioni di ripristino dipendono dal plug-in utilizzato.

Prima di iniziare

- È necessario aver eseguito il backup delle risorse o dei gruppi di risorse.
- Se si replicano Snapshot in un mirror o un vault, l'amministratore di SnapCenter deve aver assegnato le Storage Virtual Machine (SVM) sia per i volumi di origine che per quelli di destinazione.
- È necessario annullare qualsiasi operazione di backup attualmente in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.

A proposito di questa attività

- L'operazione di ripristino predefinita ripristina solo gli oggetti di storage. Le operazioni di ripristino a livello di applicazione possono essere eseguite solo se il plug-in personalizzato fornisce tale funzionalità.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, filtrare le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

Le risorse vengono visualizzate insieme a informazioni quali tipo, nome host o cluster, criteri e gruppi di risorse associati e stato.

> Anche se un backup potrebbe essere per un gruppo di risorse, quando si esegue il ripristino, è necessario selezionare le singole risorse da ripristinare.

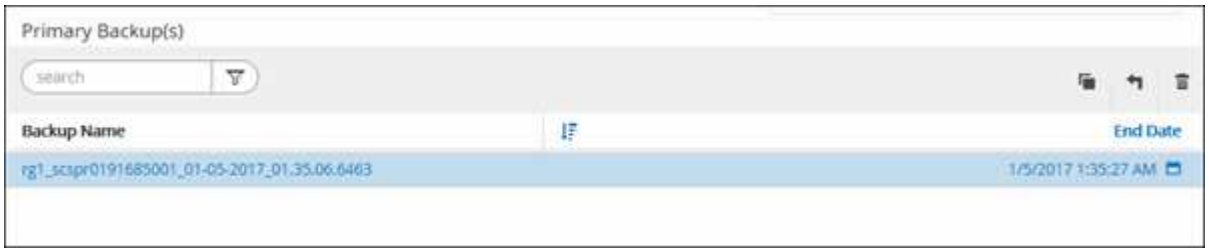
Se la risorsa non è protetta, nella colonna **Stato generale** viene visualizzato *non protetto*.

Lo stato *non protetto* nella colonna **Stato generale** può indicare che la risorsa non è protetta o che il backup della risorsa è stato eseguito da un altro utente.

3. Selezionare la risorsa o un gruppo di risorse, quindi selezionare una risorsa in tale gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, selezionare **backup** dai sistemi di storage primario o secondario (mirrorati o vault).
5. Nella tabella Backup primari, selezionare il backup da cui si desidera eseguire il ripristino, quindi fare clic su .



6. Nella pagina Restore Scope (ambito ripristino), selezionare **complete Resource** (completa risorsa) o **file Level** (livello file).
   a. Se si seleziona **completa risorsa**, il backup delle risorse viene ripristinato.

      Se la risorsa contiene volumi o qtree come Storage Footprint, snapshot più recenti su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata.

   b. Se è stato selezionato **file Level**, è possibile selezionare **All** (tutto) oppure selezionare Volumes (volumi) o qtree (qtree), quindi immettere il percorso relativo ai volumi o alle qtree selezionati separati da virgole.
      - È possibile selezionare più volumi e qtree.
      - Se il tipo di risorsa è LUN, viene ripristinato l'intero LUN. È possibile selezionare più LUN. + NOTA: Se si seleziona **All**, vengono ripristinati tutti i file presenti nei volumi, nei qtree o nei LUN.
7. Nella pagina **Recovery Type**, eseguire le seguenti operazioni: Selezionare l'opzione per applicare i registri. Assicurarsi che il plug-in supporti tutti i log e i log fino al tipo di ripristino prima di selezionarlo.

Se si desidera…	Eseguire questa operazione…
Ripristinare tutti i log	Selezionare **tutti i log**. Assicurarsi che il plug-in supporti **tutti i log**.

Se si desidera…	Eseguire questa operazione…
Ripristinare tutti i log fino all'ora specificata	Selezionare **Logs until**. Assicurarsi che il plug-in supporti **Logs until**.
Ripristinare il backup delle risorse	Selezionare **Nessuno**.

8. Nella pagina **operazioni preliminari**, immettere i comandi di pre-ripristino e disinstallazione da eseguire prima di eseguire un processo di ripristino.
9. Nella pagina **Post Ops**, immettere i comandi di mount e post restore da eseguire dopo l'esecuzione di un processo di ripristino.
10. Nella pagina **Notification**, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

    È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

11. Esaminare il riepilogo, quindi fare clic su **fine**.
12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Ripristinare le risorse utilizzando i cmdlet PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con il server SnapCenter, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Recuperare le informazioni relative a uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio mostra informazioni su tutti i backup disponibili:

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

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

Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

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

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

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

3. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

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

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di ripristino delle risorse plug-in personalizzate

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

gli stati di post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi altra azione di ripristino che è possibile eseguire.

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Ripristina**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato di ripristino.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Clonare i backup personalizzati delle risorse plug-in

Clonare i backup personalizzati delle risorse plug-in

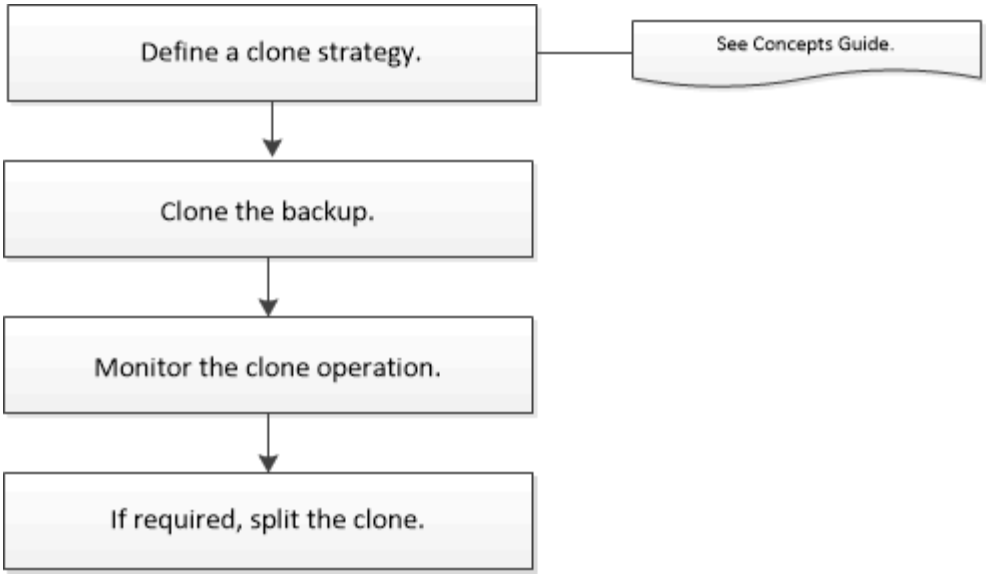
Il flusso di lavoro dei cloni include l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

A proposito di questa attività

È possibile clonare i backup delle risorse per i seguenti motivi:

- Per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo delle applicazioni
- Per l'estrazione e la manipolazione dei dati durante il popolamento dei data warehouse
- Per ripristinare i dati cancellati o modificati per errore

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di clonazione:



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la Guida dei cmdlet di SnapCenter o consultare la "Guida di riferimento al cmdlet del software SnapCenter".

Clonare da un backup

È possibile utilizzare SnapCenter per clonare un backup. È possibile clonare dal backup primario o secondario. Le funzionalità delle operazioni di clonazione dipendono dal plug-in utilizzato.

Prima di iniziare

- È necessario aver eseguito il backup delle risorse o del gruppo di risorse.
- L'operazione di cloni predefinita clona solo gli oggetti di storage. Le operazioni di clonazione a livello di applicazione possono essere eseguite solo se il plug-in personalizzato fornisce tale funzionalità.
- Assicurarsi che gli aggregati che ospitano i volumi siano inclusi nell'elenco degli aggregati assegnati della macchina virtuale di storage (SVM).

A proposito di questa attività

Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **risorse**, filtrare le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme a informazioni quali tipo, nome host o cluster, criteri e gruppi di risorse associati e stato.

3. Selezionare la risorsa o il gruppo di risorse.

   Selezionare una risorsa se si seleziona un gruppo di risorse.

Viene visualizzata la pagina della topologia di risorse o gruppi di risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primario o secondario (mirrorati o vault).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su  .
6. Nella pagina Locations (posizioni), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Server clone	Per impostazione predefinita, l'host di origine viene popolato. Se si desidera specificare un host diverso, selezionare l'host su cui montare il clone e installare il plug-in.
Suffisso clone	Questo è obbligatorio quando la destinazione del clone è la stessa dell'origine. Inserire un suffisso che verrà aggiunto al nome della risorsa appena clonata. Il suffisso garantisce che la risorsa clonata sia univoca sull'host. ad esempio, rs1_clone. Se si esegue la clonazione sullo stesso host della risorsa originale, è necessario fornire un suffisso per differenziare la risorsa clonata dalla risorsa originale; in caso contrario, l'operazione non riesce.

Se la risorsa selezionata è un LUN e si esegue la clonazione da un backup secondario, vengono elencati i volumi di destinazione. Una singola origine può avere più volumi di destinazione.

7. Nella pagina **Impostazioni**, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome dell'iniziatore	Immettere il nome dell'iniziatore host, ovvero un IQDN o WWPN.
Protocollo iGroup	Selezionare il protocollo iGroup.

La pagina delle impostazioni viene visualizzata solo se il tipo di storage è LUN.

8. Nella pagina script, immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clone. Immettere il comando mount per montare un file system su un host.

   Ad esempio:

   - Comando pre-clone: Elimina i database esistenti con lo stesso nome

- Comando post clone: Verifica di un database o avvia un database.

  Comando mount per un volume o un qtree su una macchina Linux: Mountanon <VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

9. Nella pagina **Notification**, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail.

10. Esaminare il riepilogo e fare clic su **fine**.
11. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Clonare i backup utilizzando i cmdlet PowerShell

Il flusso di lavoro dei cloni include la pianificazione, l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

Prima di iniziare

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Per informazioni sui cmdlet di PowerShell, utilizzare la Guida dei cmdlet di SnapCenter o consultare la "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

2. Elencare i backup che possono essere clonati utilizzando il cmdlet Get-SmBackup o Get-SmResourceGroup.

   Questo esempio mostra informazioni su tutti i backup disponibili:

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

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

   Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a un gruppo di risorse specificato:

```
```

```
PS C:\> Get-SmResourceGroup

    Description                 :
    CreationTime                : 10/10/2016 4:45:53 PM
    ModificationTime            : 10/10/2016 4:45:53 PM
    EnableEmail                 : False
    EmailSMTPServer             :
    EmailFrom                   :
    EmailTo                     :
    EmailSubject                :
    EnableSysLog                : False
    ProtectionGroupType         : Backup
    EnableAsupOnFailure         : False
    Policies                    : {}
    HostResourceMaping          : {}
    Configuration               : SMCoreContracts.SmCloneConfiguration
    LastBackupStatus            : Completed
    VerificationServer          :
    EmailBody                   :
    EmailNotificationPreference : Never
    VerificationServerInfo      :
    SchedulerSQLInstance        :
    CustomText                  :
    CustomSnapshotFormat        :
    SearchResources             : False
    ByPassCredential            : False
    IsCustomSnapshot            :
    MaintenanceStatus           : Production
    PluginProtectionGroupTypes  : {SMSQL}
    Tag                         :
    IsInternal                  : False
    EnableEmailAttachment       : False
    VerificationSettings        : {}
    Name                        : NFS_DB
    Type                        : Group
    Id                          : 2
    Host                        :
    UserName                    :
    Passphrase                  :
    Deleted                     : False
    Auth                        : SMCoreContracts.SmAuth
    IsClone                     : False
    CloneLevel                  : 0
    Hosts                       :
    StorageName                 :
    ResourceGroupNames          :
```

```
PolicyNames                 :

Description                 :
CreationTime                : 10/10/2016 4:51:36 PM
ModificationTime            : 10/10/2016 5:27:57 PM
EnableEmail                 : False
EmailSMTPServer             :
EmailFrom                   :
EmailTo                     :
EmailSubject                :
EnableSysLog                : False
ProtectionGroupType         : Backup
EnableAsupOnFailure         : False
Policies                    : {}
HostResourceMaping          : {}
Configuration               : SMCoreContracts.SmCloneConfiguration
LastBackupStatus            : Failed
VerificationServer          :
EmailBody                   :
EmailNotificationPreference : Never
VerificationServerInfo      :
SchedulerSQLInstance        :
CustomText                  :
CustomSnapshotFormat        :
SearchResources             : False
ByPassRunAs                 : False
IsCustomSnapshot            :
MaintenanceStatus           : Production
PluginProtectionGroupTypes  : {SMSQL}
Tag                         :
IsInternal                  : False
EnableEmailAttachment       : False
VerificationSettings        : {}
Name                        : Test
Type                        : Group
Id                          : 3
Host                        :
UserName                    :
Passphrase                  :
Deleted                     : False
Auth                        : SMCoreContracts.SmAuth
IsClone                     : False
CloneLevel                  : 0
Hosts                       :
StorageName                 :
ResourceGroupNames          :
```

```
    PolicyNames                :
```

3. Avviare un'operazione di clonazione da un gruppo di risorse clone o da un backup esistente utilizzando il cmdlet New-SmClone.

   Questo esempio crea un clone da un backup specificato con tutti i log:

```
New-SmClone -BackupName Verify_delete_clone_on_qtree_windows_scc54_10-
04-2016_19.05.48.0886 -Resources
@{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"}  -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'
```

4. Visualizzare lo stato del processo clone utilizzando il cmdlet Get-SmCloneReport.

   Questo esempio visualizza un report clone per l'ID lavoro specificato:

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

Monitorare le operazioni personalizzate di cloni delle risorse del plug-in

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter

utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Clone**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato del clone.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro clone, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

Proteggere i file system Unix

Cosa puoi fare con il plug-in SnapCenter per file system Unix

Quando il plug-in per i file system Unix è installato nel proprio ambiente, è possibile utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei file system Unix. È inoltre possibile eseguire attività a supporto di tali operazioni.

- Scopri le risorse
- Eseguire il backup dei file system Unix
- Pianificare le operazioni di backup
- Ripristinare i backup del file system
- Clonare i backup del file system
- Monitorare le operazioni di backup, ripristino e clonazione

Configurazioni supportate

Elemento	Configurazione supportata
Ambienti	• Server fisico • Server virtuale
Sistemi operativi	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
File system	• SAN: ◦ File system basati su LVM e non LVM ◦ LVM su VMDK ext3, ext4 e xfs • NFS: NFS v3, NFS v4.x
Protocolli	• FC • FCoE • ISCSI • NFS
Multipath	sì

Limitazioni

- La combinazione di RDM e dischi virtuali in un gruppo di volumi non è supportata.

- Il ripristino a livello di file non è supportato.

  Tuttavia, è possibile eseguire manualmente il ripristino a livello di file clonando il backup e copiando i file manualmente.

- La combinazione di file system distribuita tra VMDK provenienti dal datastore NFS e VMFS non è supportata.
- NVMe non è supportato.
- SnapMirror Business Continuity (SM-BC) non è supportato.
- Il provisioning non è supportato.

Installare il plug-in SnapCenter per i file system Unix

Prerequisiti per l'aggiunta di host e l'installazione di Plug-in Package per Linux

Prima di aggiungere un host e installare il pacchetto plug-in per Linux, è necessario completare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È possibile utilizzare l'autenticazione basata su password per l'utente root o non root oppure l'autenticazione basata su chiave SSH.

  Il plug-in SnapCenter per file system Unix può essere installato da un utente non root. Tuttavia, è necessario configurare i privilegi sudo per l'utente non root per installare e avviare il processo di plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utenti non root.

- Creare credenziali con la modalità di autenticazione come Linux per l'utente di installazione.
- È necessario aver installato Java 1,8.x o Java 11 a 64 bit sul proprio host Linux.

  Assicurarsi di aver installato solo L'edizione certificata DI JAVA 11 sull'host Linux.

  Per informazioni su come scaricare JAVA, vedere: "Download Java per tutti i sistemi operativi"

- Si dovrebbe avere **bash** come shell predefinita per l'installazione del plug-in.

Requisiti degli host Linux

Assicurarsi che l'host soddisfi i requisiti prima di installare il pacchetto di plug-in SnapCenter per Linux.

Elemento	Requisiti
Sistemi operativi	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
RAM minima per il plug-in SnapCenter sull'host	2 GB

Elemento	Requisiti
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	• Java 1,8.x (64 bit) Oracle Java e OpenJDK • Java 11 (64 bit) Oracle Java e OpenJDK Assicurarsi di aver installato solo L'edizione certificata DI JAVA 11 sull'host Linux. Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.

Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Aggiungere host e installare il pacchetto plug-in per Linux utilizzando la GUI

È possibile utilizzare la pagina Aggiungi host per aggiungere host e quindi installare il pacchetto di plug-in SnapCenter per Linux. I plug-in vengono installati automaticamente sugli host remoti.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata nella parte superiore.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare **Linux** come tipo di host.

Per questo campo…	Eseguire questa operazione…
Nome host	Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire l'FQDN. Se si aggiunge un host utilizzando SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN.
Credenziali	Selezionare il nome della credenziale creata o creare nuove credenziali. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere le informazioni sulla creazione delle credenziali. È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome specificato. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare **Unix file Systems**.
6. (Facoltativo) fare clic su **altre opzioni**.

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.

Per questo campo…	Eseguire questa operazione…
Percorso di installazione	Il percorso predefinito è */OPT/NetApp/Snapcenter*. È possibile personalizzare il percorso. Se si utilizza il percorso personalizzato, assicurarsi che il contenuto predefinito dei sudori sia aggiornato con il percorso personalizzato.
Ignorare i controlli opzionali di preinstallazione	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo Ignora precheck, l'host viene validato per verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

   Lo script di precheck non convalida lo stato del firewall della porta plug-in se specificato nelle regole di rifiuto del firewall.

   Se non vengono soddisfatti i requisiti minimi, vengono visualizzati messaggi di errore o di avviso appropriati. Se l'errore riguarda lo spazio su disco o la RAM, è possibile aggiornare il file web.config che si trova in *C: File di programma NetApp SnapCenter WebApp* per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione ha, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Verificare l'impronta digitale, quindi fare clic su **Confirm and Submit** (Conferma e invia).

   SnapCenter non supporta l'algoritmo ECDSA.

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

   I file di log specifici dell'installazione si trovano in */custom_location/snapcenter/logs*.

Risultato

Tutti i file system montati sull'host vengono automaticamente rilevati e visualizzati nella pagina risorse. Se non viene visualizzato alcun messaggio, fare clic su **Refresh Resources** (Aggiorna risorse).

Monitorare lo stato dell'installazione

È possibile monitorare lo stato di avanzamento dell'installazione del pacchetto plug-in di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento dell'installazione per determinare quando è completa o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filter** (filtro).
   b. Facoltativo: Specificare la data di inizio e di fine.
   c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).
   d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.
   e. Fare clic su **Apply** (Applica).
4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Configurare il servizio caricatore plug-in di SnapCenter

Il servizio caricatore plug-in SnapCenter carica il pacchetto plug-in affinché Linux possa interagire con il server SnapCenter. Il servizio caricatore plug-in SnapCenter viene installato quando si installa il pacchetto plug-in SnapCenter per Linux.

A proposito di questa attività

Dopo aver installato il pacchetto di plug-in SnapCenter per Linux, il servizio caricatore dei plug-in SnapCenter si avvia automaticamente. Se il servizio caricatore plug-in di SnapCenter non si avvia automaticamente, è necessario:

- Assicurarsi che la directory in cui opera il plug-in non venga eliminata
- Aumentare lo spazio di memoria assegnato alla Java Virtual Machine

Il file spl.properties, che si trova in */custom_location/NetApp/snapcenter/spl/etc/*, contiene i seguenti parametri. A questi parametri vengono assegnati valori predefiniti.

Nome del parametro	Descrizione
LOG_LEVEL	Visualizza i livelli di registro supportati. I valori possibili sono TRACE, DEBUG, INFO, WARN, ERROR, E FATALE.
PROTOCOLLO_SPL	Visualizza il protocollo supportato dal caricatore plug-in SnapCenter. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.
PROTOCOLLO_SERVER_SNAPCENTER	Visualizza il protocollo supportato dal server SnapCenter. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.
SKIP_JAVAHOME_UPDATE	Per impostazione predefinita, il servizio SPL rileva il percorso java e aggiorna IL parametro JAVA_HOME. Pertanto, il valore predefinito è IMPOSTATO SU FALSE. È possibile impostare SU TRUE se si desidera disattivare il comportamento predefinito e correggere manualmente il percorso java.
SPL_KEYSTORE_PASS	Visualizza la password del file keystore. È possibile modificare questo valore solo se si modifica la password o si crea un nuovo file keystore.
SPL_PORT	Visualizza il numero di porta su cui è in esecuzione il servizio caricatore plug-in di SnapCenter. È possibile aggiungere il valore se manca il valore predefinito. Non modificare il valore dopo l'installazione dei plug-in.
SNAPCENTER_SERVER_HOST	Visualizza l'indirizzo IP o il nome host del server SnapCenter.
SPL_KEYSTORE_PATH	Visualizza il percorso assoluto del file keystore.
PORTA_SERVER_SNAPCENTER	Visualizza il numero di porta su cui è in esecuzione il server SnapCenter.

Nome del parametro	Descrizione
LOG_MAX_COUNT	Visualizza il numero di file di log del caricatore plug-in SnapCenter conservati nella cartella */custom_location/snapcenter/spl/logs*. Il valore predefinito è 5000. Se il conteggio supera il valore specificato, vengono conservati gli ultimi 5000 file modificati. Il controllo del numero di file viene eseguito automaticamente ogni 24 ore dall'avvio del servizio caricatore plug-in di SnapCenter. Se si elimina manualmente il file spl.properties, il numero di file da conservare viene impostato su 9999.
JAVA_HOME	Visualizza il percorso assoluto della directory DI JAVA_HOME che viene utilizzato per avviare il servizio SPL. Questo percorso viene determinato durante l'installazione e come parte dell'avvio di SPL.
LOG_MAX_SIZE	Visualizza la dimensione massima del file di log del lavoro. Una volta raggiunta la dimensione massima, il file di registro viene compresso e i registri vengono scritti nel nuovo file del lavoro.
RETAIN_LOGS_OF_LAST_DAYS	Visualizza il numero di giorni in cui i registri vengono conservati.
ENABLE_CERTIFICATE_VALIDATION	Viene visualizzato true quando la convalida del certificato CA è attivata per l'host. È possibile attivare o disattivare questo parametro modificando il file spl.properties o utilizzando l'interfaccia grafica o il cmdlet di SnapCenter.

Se uno di questi parametri non è assegnato al valore predefinito o se si desidera assegnare o modificare il valore, è possibile modificare il file spl.properties. È inoltre possibile verificare il file spl.properties e modificarlo per risolvere eventuali problemi relativi ai valori assegnati ai parametri. Dopo aver modificato il file spl.properties, riavviare il servizio caricatore plug-in di SnapCenter.

Fasi

1. Eseguire una delle seguenti operazioni, secondo necessità:
   - Avviare il servizio caricatore plug-in SnapCenter:
     - Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl start`

- Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`

◦ Arrestare il servizio caricatore plug-in di SnapCenter:

- Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
- Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

> È possibile utilizzare l'opzione -force con il comando stop per arrestare con forza il servizio caricatore plug-in di SnapCenter. Tuttavia, prima di eseguire questa operazione, è necessario prestare attenzione, in quanto termina anche le operazioni esistenti.

◦ Riavviare il servizio caricatore plug-in di SnapCenter:

- Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`

◦ Individuare lo stato del servizio caricatore plug-in di SnapCenter:

- Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
- Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ Individuare la modifica nel servizio caricatore plug-in di SnapCenter:

- Come utente root, eseguire: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- Come utente non root, eseguire: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurare il certificato CA con il servizio caricatore plug-in (SPL) di SnapCenter sull'host Linux

È necessario gestire la password del keystore SPL e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio di trust SPL e configurare la coppia di chiavi firmate CA per l'archivio di trust SPL con il servizio caricatore plug-in SnapCenter per attivare il certificato digitale installato.

> SPL utilizza il file 'keystore.jks', che si trova in '/var/opt/snapcenter/spl/etc' sia come Trust-store che come keystore.

Gestire la password per l'archivio chiavi SPL e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore SPL dal file di proprietà SPL.

È il valore corrispondente alla chiave 'SOL_KEYSTORE_PASS'.

2. Modificare la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle chiavi private nel
keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS nel file spl.properties.

3. Riavviare il servizio dopo aver modificato la password.

La password per l'archivio chiavi SPL e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust SPL

È necessario configurare i certificati root o intermedi senza la chiave privata in SPL trust-store.

Fasi

1. Accedere alla cartella contenente il keystore SPL: */var/opt/snapcenter/spl/etc*.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungere un certificato root o intermedio:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Riavviare il servizio dopo aver configurato i certificati root o
intermedi in SPL trust-store.
```

Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi con firma CA nell'archivio di trust SPL

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di fiducia SPL.

Fasi

1. Accedere alla cartella contenente il keystore /var/opt/snapcenter/spl/ecc. della SPL
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungere il certificato CA con chiave pubblica e privata.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Elencare i certificati aggiunti nel keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verificare che il keystore contenga l'alias corrispondente al nuovo
certificato CA aggiunto al keystore.
. Modificare la password della chiave privata aggiunta per il
certificato CA in password archivio chiavi.
```

Default SPL keystore password è il valore della chiave SPL_KEYSTORE_PASS nel file spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias con un nome
semplice:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configurare il nome alias dal keystore che si trova nel file
spl.properties.
```

Aggiornare questo valore con la chiave SPL_CERTIFICATE_ALIAS.

4. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA in SPL trust-store.

Configurare l'elenco CRL (Certificate Revocation List) per SPL

Configurare il CRL per SPL

A proposito di questa attività

- SPL ricerca i file CRL in una directory preconfigurata.

- La directory predefinita per i file CRL per SPL è */var/opt/snapcenter/spl/etc/crl*.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file spl.properties in base alla chiave SPL_CRL_PATH.
2. È possibile inserire più file CRL in questa directory.

   I certificati in entrata verranno verificati per ciascun CRL.

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.
5. Selezionare **attiva convalida certificato**.

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- * * Indica che il certificato CA non è né abilitato né assegnato all'host del plug-in.
- * * Indica che il certificato CA è stato convalidato correttamente.
- * * Indica che il certificato CA non può essere convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Installare il plug-in SnapCenter per VMware vSphere

Se il database o il file system sono memorizzati su macchine virtuali (VM), o se si

desidera proteggere macchine virtuali e datastore, è necessario implementare il plug-in SnapCenter per l'appliance virtuale VMware vSphere.

Per informazioni sulla distribuzione, vedere "Panoramica sull'implementazione".

Implementare il certificato CA

Per configurare il certificato CA con il plug-in SnapCenter per VMware vSphere, vedere "Creare o importare un certificato SSL".

Configurare il file CRL

Il plug-in SnapCenter per VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il plug-in SnapCenter per VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Prepararsi per la protezione dei file system Unix

Prima di eseguire qualsiasi operazione di protezione dei dati, ad esempio operazioni di backup, cloning o ripristino, occorre configurare l'ambiente. È inoltre possibile configurare il server SnapCenter in modo che utilizzi le tecnologie SnapMirror e SnapVault.

Per sfruttare i vantaggi delle tecnologie SnapVault e SnapMirror, è necessario configurare e inizializzare una relazione di protezione dei dati tra i volumi di origine e di destinazione sul dispositivo di storage. È possibile utilizzare NetAppSystem Manager oppure la riga di comando della console di storage per eseguire queste attività.

Prima di utilizzare il plug-in per i file system Unix, l'amministratore di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività dei prerequisiti.

- Installare e configurare il server SnapCenter. "Scopri di più"
- Configurare l'ambiente SnapCenter aggiungendo le connessioni del sistema storage. "Scopri di più"

> SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM registrato con SnapCenter utilizzando la registrazione SVM o la registrazione del cluster deve essere univoco.

- Aggiungi host, installa i plug-in e scopri le risorse.
- Se si utilizza SnapCenter Server per proteggere i file system Unix che risiedono su LUN RDM VMware o VMDK, è necessario implementare il plug-in SnapCenter per VMware vSphere e registrare il plug-in con SnapCenter.
- Installare Java sull'host Linux.
- Configurare SnapMirror e SnapVault su ONTAP, se si desidera una replica di backup.

Eseguire il backup dei file system Unix

Individuare i file system UNIX disponibili per il backup

Dopo aver installato il plug-in, tutti i file system su quell'host vengono automaticamente rilevati e visualizzati nella pagina risorse. È possibile aggiungere questi file system ai gruppi di risorse per eseguire operazioni di protezione dei dati.

Prima di iniziare

- Sono necessarie attività quali l'installazione del server SnapCenter, l'aggiunta di host e la creazione di connessioni al sistema di storage.
- Se i file system risiedono su un disco della macchina virtuale (VMDK) o su una mappatura di dispositivi raw (RDM), è necessario implementare il plug-in SnapCenter per VMware vSphere e registrare il plug-in con SnapCenter.

  Per ulteriori informazioni, vedere "Implementare il plug-in SnapCenter per VMware vSphere".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **percorso** dall'elenco Visualizza.
3. Fare clic su **Aggiorna risorse**.

   I file system vengono visualizzati insieme a informazioni quali tipo, nome host, gruppi e criteri di risorse associati e stato.

Creare criteri di backup per i file system Unix

Prima di utilizzare SnapCenter per eseguire il backup dei file system Unix, è necessario creare un criterio di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Un criterio di backup è un insieme di regole che regolano la gestione, la pianificazione e la conservazione dei backup. È inoltre possibile specificare le impostazioni di replica, script e tipo di backup. La creazione di una policy consente di risparmiare tempo quando si desidera riutilizzare la policy su un'altra risorsa o gruppo di risorse.

Prima di iniziare

- Devi essere pronto per la protezione dei dati completando attività come l'installazione di SnapCenter, l'aggiunta di host, il rilevamento dei file system e la creazione di connessioni al sistema di storage.
- Se si stanno replicando Snapshot in uno storage secondario mirror o vault, l'amministratore di SnapCenter deve aver assegnato le SVM per i volumi di origine e di destinazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare **Unix file Systems** dall'elenco a discesa.
4. Fare clic su **nuovo**.
5. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.

6. Specificare la frequenza del programma selezionando **on demand**, **Hourly**, **Daily**, **Weekly** o **Monthly**.
7. Nella pagina conservazione, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina tipo di backup:

Se si desidera…	Quindi…
Mantenere un certo numero di istantanee	Selezionare **totale copie snapshot da conservare**, quindi specificare il numero di istantanee che si desidera conservare. Se il numero di istantanee supera il numero specificato, le istantanee vengono eliminate con le copie meno recenti eliminate per prime. Il valore massimo di conservazione è 1018 per le risorse su ONTAP 9.4 o versioni successive e 254 per le risorse su ONTAP 9.3 o versioni precedenti. I backup non avranno esito positivo se la conservazione viene impostata su un valore superiore a quello supportato dalla versione di ONTAP sottostante. Se si intende attivare la replica SnapVault, è necessario impostare il numero di conservazione su 2 o superiore. Se si imposta il conteggio della conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è il Snapshot di riferimento per la relazione SnapVault fino a quando una snapshot più recente non viene replicata nella destinazione.
Conservare le istantanee per un determinato numero di giorni	Selezionare **Mantieni copie snapshot per**, quindi specificare il numero di giorni per i quali si desidera conservare le istantanee prima di eliminarle.

È possibile conservare i backup dei log di archiviazione solo se sono stati selezionati i file di log di archiviazione come parte del backup.

8. Nella pagina Replication, specificare le impostazioni di replica:

Per questo campo…	Eseguire questa operazione…
Aggiornare SnapMirror dopo aver creato una copia Snapshot locale	Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror).
Aggiornare SnapVault dopo aver creato una copia Snapshot locale	Selezionare questa opzione per eseguire la replica del backup disk-to-disk (backup SnapVault).
Etichetta del criterio secondario	Selezionare un'etichetta Snapshot. A seconda dell'etichetta Snapshot selezionata, ONTAP applica la politica di conservazione Snapshot secondaria corrispondente all'etichetta. Se è stato selezionato **Update SnapMirror dopo la creazione di una copia Snapshot locale**, è possibile specificare l'etichetta del criterio secondario. Tuttavia, se è stato selezionato **Aggiorna SnapVault dopo la creazione di una copia Snapshot locale**, è necessario specificare l'etichetta del criterio secondario.
Numero tentativi di errore	Immettere il numero massimo di tentativi di replica consentiti prima dell'interruzione dell'operazione.

È necessario configurare il criterio di conservazione SnapMirror in ONTAP per lo storage secondario, in modo da evitare di raggiungere il limite massimo di Snapshot sullo storage secondario.

9. Nella pagina script, immettere il percorso e gli argomenti del prespt o del postscript che si desidera eseguire rispettivamente prima o dopo l'operazione di backup.

   Controllare se i comandi sono presenti nell'elenco dei comandi disponibili sull'host plug-in dal percorso */opt/NetApp/snapcenter/scc/etc/allowed_command.config*.

   È inoltre possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

10. Esaminare il riepilogo, quindi fare clic su **fine**.

Creare gruppi di risorse e allegare criteri per i file system Unix

Un gruppo di risorse è un container in cui vengono aggiunte le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire il backup di tutti i dati associati ai file system.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), fare clic su **New Resource Group** (nuovo gruppo di risorse).
3. Nella pagina Name (Nome), eseguire le seguenti operazioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserire una o più etichette nel campo Tag per facilitare la ricerca del gruppo di risorse in un secondo momento.

      Ad esempio, se si aggiunge HR come tag a più gruppi di risorse, è possibile trovare in seguito tutti i gruppi di risorse associati al tag HR.

   c. Selezionare la casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea.

      Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

4. Nella pagina risorse, selezionare un nome host di file system Unix dall'elenco a discesa **host**.

   Le risorse vengono elencate nella sezione risorse disponibili solo se la risorsa viene rilevata correttamente. Le risorse aggiunte di recente vengono visualizzate nell'elenco delle risorse disponibili solo dopo l'aggiornamento dell'elenco delle risorse.

5. Selezionare le risorse dalla sezione risorse disponibili e spostarle nella sezione risorse selezionate.
6. Nella pagina Impostazioni applicazione, effettuare le seguenti operazioni:
   - Selezionare la freccia Scripts (script) e immettere i comandi pre e post per le operazioni quiescenza, istantanea e inquiescenza. In caso di errore, è anche possibile inserire i pre-comandi da eseguire prima di uscire.
   - Selezionare una delle opzioni di coerenza del backup:
     - Selezionare **file System coerenti** se si desidera assicurarsi che i dati memorizzati nella cache dei file system vengano scaricati prima di creare il backup e che non siano consentite operazioni di input o output sul file system durante la creazione del backup.

       Se coerenti con il file system, verranno create snapshot del gruppo di coerenza per i LUN coinvolti nel gruppo di volumi.

     - Selezionare **Crash coerente** se si desidera assicurarsi che i dati memorizzati nella cache dei file system vengano eliminati prima di creare il backup.

       Se sono stati aggiunti file system diversi nel gruppo di risorse, tutti i volumi di file system diversi nel gruppo di risorse verranno inseriti in un gruppo di coerenza.

7. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.

È inoltre possibile creare un criterio facendo clic su + .

Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

b. Fare clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.

Dove *policy_name* è il nome del criterio selezionato.

Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup di SnapCenter.

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report**.

Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

9. Esaminare il riepilogo, quindi fare clic su **fine**.

Eseguire il backup dei file system Unix

Se una risorsa non fa parte di un gruppo di risorse, è possibile eseguarne il backup dalla pagina risorse.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **percorso** dall'elenco Visualizza.
3. Fare clic su , quindi selezionare il nome host e il file system Unix per filtrare le risorse.
4. Selezionare il file system di cui si desidera eseguire il backup.
5. Nella pagina Resources (risorse), è possibile effettuare le seguenti operazioni:

a. Selezionare la casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea.

Ad esempio, `customtext_policy_hostname` o `resource_hostname`. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.

6. Nella pagina Impostazioni applicazione, effettuare le seguenti operazioni:

◦ Selezionare la freccia Scripts (script) e immettere i comandi pre e post per le operazioni quiescenza, istantanea e inquiescenza. In caso di errore, è anche possibile inserire i pre-comandi da eseguire

prima di uscire.

- Selezionare una delle opzioni di coerenza del backup:
  - Selezionare **file System coerenti** se si desidera assicurarsi che i dati memorizzati nella cache dei file system vengano scaricati prima di creare il backup e che non vengano eseguite operazioni sul file system durante la creazione del backup.
  - Selezionare **Crash coerente** se si desidera assicurarsi che i dati memorizzati nella cache dei file system vengano eliminati prima di creare il backup.

7. Nella pagina Criteri, attenersi alla seguente procedura:

   a. Selezionare uno o più criteri dall'elenco a discesa.

   È possibile creare un criterio facendo clic su + .

   Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

   b. Fare clic su + nella colonna Configura pianificazioni per configurare una pianificazione per il criterio desiderato.

   c. Nella finestra Aggiungi pianificazioni per policy *nome_policy* , configurare la pianificazione, quindi selezionare `OK`.

   policy_name è il nome del criterio selezionato.

   Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

8. Nella pagina Notification (notifica), selezionare gli scenari in cui si desidera inviare i messaggi di posta elettronica dall'elenco a discesa **Email preference** (Preferenze email).

   Specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto del messaggio. Se si desidera allegare il report dell'operazione di backup eseguita sulla risorsa, selezionare **Attach Job Report**.

   Per la notifica e-mail, è necessario specificare i dettagli del server SMTP utilizzando il comando GUI o PowerShell `Set-SmSmtpServer`.

9. Esaminare il riepilogo, quindi fare clic su **fine**.

   Viene visualizzata la pagina topologia.

10. Fare clic su **Esegui backup ora**.
11. Nella pagina Backup, attenersi alla seguente procedura:

    a. Se sono stati applicati più criteri alla risorsa, dall'elenco a discesa Policy (criterio), selezionare il criterio da utilizzare per il backup.

    Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Fare clic su **Backup**.

12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Eseguire il backup dei gruppi di risorse dei file system Unix

È possibile eseguire il backup dei file system Unix definiti nel gruppo di risorse. È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina risorse. Se un gruppo di risorse dispone di un criterio allegato e di una pianificazione configurata, i backup vengono creati in base alla pianificazione.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).
3. Immettere il nome del gruppo di risorse nella casella di ricerca o fare clic su , quindi selezionare il tag.

   Fare clic su per chiudere il riquadro del filtro.
4. Nella pagina Resource Group (Gruppo di risorse), selezionare il gruppo di risorse di cui eseguire il backup.
5. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se al gruppo di risorse sono associati più criteri, selezionare il criterio di backup che si desidera utilizzare dall'elenco a discesa **Policy**.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **Backup**.
6. Monitorare l'avanzamento selezionando **Monitor > processi**.

Monitorare il backup dei file system Unix

Scopri come monitorare l'avanzamento delle operazioni di backup e protezione dei dati.

Monitorare le operazioni di backup dei file system Unix

È possibile monitorare l'avanzamento di diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere necessario controllare i progressi per determinare quando sono stati completati o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze

- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Status** (Stato), selezionare lo stato del backup.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene venga visualizzato lo stato del processo di backup , quando si fa clic sui dettagli del processo, è possibile che alcune delle attività secondarie dell'operazione di backup siano ancora in corso o contrassegnate da segnali di avviso.

5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Monitorare le operazioni di protezione dei dati nel riquadro attività

Il riquadro Activity (attività) visualizza le cinque operazioni più recenti eseguite. Il riquadro Activity (attività) visualizza anche il momento in cui l'operazione è stata avviata e lo stato dell'operazione.

Il riquadro Activity (attività) visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli commessa**.

Ripristinare e ripristinare i file system Unix

Ripristinare i file system Unix

In caso di perdita di dati, è possibile utilizzare SnapCenter per ripristinare i file system Unix.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **percorso** o **Gruppo risorse** dall'elenco **Visualizza**.
3. Selezionare il file system dalla vista dettagli o dalla vista dettagli gruppo di risorse.

   Viene visualizzata la pagina topologia.
4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dal sistema di storage primario o secondario (mirrorato o replicato).
5. Selezionare il backup dalla tabella, quindi fare clic su * *  .
6. Nella pagina ambito di ripristino:
   - Per i file system NFS, per impostazione predefinita è selezionato il ripristino **Connect and Copy**. È inoltre possibile selezionare **Ripristino volume** o **Ripristino rapido**.
   - Per i file system non NFS, l'ambito di ripristino viene selezionato in base al layout.

     I nuovi file creati dopo il backup potrebbero non essere disponibili dopo il ripristino a seconda del tipo e del layout del file system.
7. Nella pagina PreOps, immettere i comandi di pre-ripristino da eseguire prima di eseguire un processo di ripristino.
8. Nella pagina PostOps, immettere i comandi di ripristino post da eseguire dopo aver eseguito un processo di ripristino.

   Controllare se i comandi sono presenti nell'elenco dei comandi disponibili sull'host plug-in dal percorso */opt/NetApp/snapcenter/scc/etc/allowed_command.config*.
9. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare le notifiche email.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di ripristino eseguita, selezionare **Allega report**.

   Per la notifica via email, è necessario specificare i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.
10. Esaminare il riepilogo, quindi fare clic su **fine**.

    Se l'operazione di ripristino non riesce, il rollback non è supportato.

    In caso di ripristino di un filesystem residente sul gruppo di volumi, i vecchi contenuti del filesystem non vengono cancellati. Solo il contenuto del filesystem clonato verrà copiato nel filesystem di origine. Ciò è applicabile in presenza di più file system sul gruppo di volumi e ripristini del file system NFS predefiniti.
11. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Monitorare le operazioni di ripristino dei file system Unix

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

gli stati di post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi altra azione di ripristino che è possibile eseguire.

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Ripristina**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato di ripristino.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Clona file system Unix

Clona il backup del file system Unix

Si può usare SnapCenter per clonare il file system Unix usando il backup del filesystem.

Prima di iniziare

- Puoi saltare l'aggiornamento del file fstab impostando il valore di *SKIP_FSTAB_UPDATE* su **true** nel file *agent.properties* situato in */opt/NetApp/snapcenter/scc/etc*.

- È possibile avere un nome di volume clone statico e un percorso di giunzione impostando il valore di *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* su **true** nel file *agent.properties* che si trova in */opt/NetApp/snapcenter/scc/etc*. Dopo aver aggiornato il file, è necessario riavviare SnapCenter per il servizio plug-in personalizzato eseguendo il comando: `/opt/NetApp/snapcenter/scc/bin/scc restart`.

  Esempio: Senza questa proprietà il nome del volume clone e il percorso della giunzione saranno simili a <Source_volume_name>_Clone_<Timestamp>, ma ora saranno <Source_volume_name>_Clone_<Clone_Name>

  Questo mantiene costante il nome in modo da poter mantenere manualmente aggiornato il file fstab se non si preferisce aggiornare il fstab di SnapCenter.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **percorso** o **Gruppo risorse** dall'elenco **Visualizza**.
3. Selezionare il file system dalla vista dettagli o dalla vista dettagli gruppo di risorse.

   Viene visualizzata la pagina topologia.

4. Dalla vista Manage Copies (Gestisci copie), selezionare i backup da Local Copies (copie locali) (primarie), Mirror Copies (copie mirror) (secondarie) o Vault Copies (copie vault) (secondarie).
5. Selezionare il backup dalla tabella, quindi fare clic su * * .
6. Nella pagina Location (posizione), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Server clone	Per impostazione predefinita, l'host di origine viene popolato.
Clona punto di montaggio	Specificare il percorso in cui verrà montato il file system.

7. Nella pagina script, attenersi alla seguente procedura:
   a. Immettere i comandi per pre-clone o post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clone.

   È necessario controllare se i comandi sono presenti nell'elenco dei comandi disponibili sull'host del plug-in dal percorso */opt/NetApp/snapcenter/scc/allowed_Commands.config*.

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report**.

Per la notifica via email, è necessario aver specificato i dettagli del server SMTP utilizzando la GUI o il comando PowerShell Set-SmtpServer.

9. Esaminare il riepilogo, quindi fare clic su **fine**.
10. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Separare un clone

È possibile utilizzare SnapCenter per separare una risorsa clonata dalla risorsa principale. Il clone diviso diventa indipendente dalla risorsa padre.

A proposito di questa attività

- Non è possibile eseguire l'operazione di suddivisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato il clone1 da un backup del database, è possibile creare un backup del clone1 e clonare il backup (clone2). Dopo aver creato il clone2, il clone1 è un clone intermedio e non è possibile eseguire l'operazione di suddivisione del clone sul clone1. Tuttavia, è possibile eseguire l'operazione di suddivisione dei cloni sul clone2.

  Dopo aver diviso il clone2, è possibile eseguire l'operazione di divisione del clone sul clone1, poiché il clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i lavori di clonazione del clone vengono eliminati.
- Per informazioni sulle limitazioni delle operazioni di suddivisione clone, vedere "Guida alla gestione dello storage logico di ONTAP 9".
- Assicurarsi che il volume o l'aggregato sul sistema di storage sia online.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **risorse**, selezionare l'opzione appropriata dall'elenco Visualizza:

Opzione	Descrizione
Per applicazioni di database	Selezionare **Database** dall'elenco View (Visualizza).
Per file system	Selezionare **Path** dall'elenco View (Visualizza).

3. Selezionare la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Nella vista **Gestisci copie**, selezionare la risorsa clonata (ad esempio, il database o il LUN), quindi fare clic su * *  .
5. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
6. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Se il servizio SMCore viene riavviato, l'operazione di split clone smette di rispondere. Eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione di suddivisione del clone.

Se si desidera un tempo di polling più lungo o più breve per controllare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo in cui SMCore deve eseguire il polling per lo stato dell'operazione di suddivisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

Ad esempio:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'operazione di avvio del clone split non riesce se sono in corso operazioni di backup, ripristino o altro clone split. È necessario riavviare l'operazione di suddivisione dei cloni solo al termine delle operazioni in esecuzione.

Informazioni correlate

"Il clone o la verifica di SnapCenter non riesce e l'aggregato non esiste"

Monitorare le operazioni di clonazione dei file system Unix

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e di fine.

c. Dall’elenco a discesa **tipo**, selezionare **Clone**.
d. Dall’elenco a discesa **Status** (Stato), selezionare lo stato del clone.
e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.

4. Selezionare il lavoro clone, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

Proteggi le applicazioni in esecuzione su Azure NetApp Files

Installare SnapCenter e creare le credenziali

Installare SnapCenter sulla macchina virtuale Azure

È possibile scaricare il software SnapCenter dal sito di supporto NetApp e installare il software sulla macchina virtuale Azure.

Prima di iniziare

Assicurarsi che la macchina virtuale Azure Windows soddisfi i requisiti per l'installazione del server SnapCenter. Per informazioni, vedere "Preparazione per l'installazione del server SnapCenter".

Fasi

1. Scaricare il pacchetto di installazione del server SnapCenter da "Sito di supporto NetApp".
2. Avviare l'installazione del server SnapCenter facendo doppio clic sul file .exe scaricato.

   Dopo aver avviato l'installazione, vengono eseguiti tutti i controlli preliminari e, se i requisiti minimi non sono soddisfatti, vengono visualizzati i messaggi di errore o di avvertenza appropriati. È possibile ignorare i messaggi di avviso e procedere con l'installazione; tuttavia, gli errori dovrebbero essere corretti.

3. Esaminare i valori precompilati richiesti per l'installazione del server SnapCenter e modificarli, se necessario.

   Non è necessario specificare la password per il database del repository MySQL Server. Durante l'installazione del server SnapCenter, la password viene generata automaticamente.

   > Il carattere speciale "%" non è supportato nel percorso personalizzato del database del repository. Se si include "%" nel percorso, l'installazione non riesce.

4. Fare clic su **Installa ora**.

   Se sono stati specificati valori non validi, vengono visualizzati i messaggi di errore appropriati. Immettere nuovamente i valori, quindi avviare l'installazione.

   > Se si fa clic sul pulsante **Annulla**, la fase in corso di esecuzione viene completata e quindi viene avviata l'operazione di rollback. Il server SnapCenter verrà completamente rimosso dall'host.

   Tuttavia, se si fa clic su **Annulla** durante l'esecuzione delle operazioni "riavvio del server SnapCenter" o "in attesa dell'avvio del server SnapCenter", l'installazione proseguirà senza annullare l'operazione.

Creare la credenziale Azure in SnapCenter

È necessario creare la credenziale Azure in SnapCenter per accedere all'account Azure NetApp.

Prima di creare la credenziale Azure, assicurarsi di aver creato l'entità del servizio in Azure. L'ID tenant, l'ID

client e la chiave segreta associati all'identità del servizio saranno necessari per creare la credenziale Azure.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.
4. Nella pagina credenziali, specificare le seguenti informazioni necessarie per creare la credenziale.

Per questo campo…	Eseguire questa operazione…
Nome credenziale	Immettere un nome per la credenziale.
Modalità di autenticazione	Selezionare **Azure Credential** dall'elenco a discesa.
ID tenant	Immettere l'ID tenant.
ID client	Immettere l'ID client.
Chiave segreta client	Immettere la chiave segreta client.

5. Fare clic su **OK**.

Configurare l'account di storage Azure

È necessario configurare l'account di archiviazione Azure in SnapCenter.

L'account di storage Azure contiene dettagli sull'ID della sottoscrizione, la credenziale Azure e l'account Azure NetApp.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Systems**.
2. Nella pagina sistemi di archiviazione, selezionare **Azure NetApp Files** e fare clic su **nuovo**.
3. Selezionare la credenziale, l'ID della sottoscrizione e l'account NetApp dai rispettivi elenchi a discesa.
4. Fare clic su **Invia**.

Creare la credenziale per aggiungere l'host del plug-in

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter.

È necessario creare credenziali per l'installazione dei plug-in di SnapCenter e credenziali aggiuntive per l'esecuzione delle operazioni di protezione dei dati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.

4. Nella pagina credenziali, specificare le seguenti informazioni necessarie per creare la credenziale.

Per questo campo…	Eseguire questa operazione…
Nome credenziale	Immettere un nome per la credenziale.
Modalità di autenticazione	Selezionare la modalità di autenticazione dall'elenco a discesa.
Tipo di autenticazione	Selezionare **basato su password** o **basato su chiave SSH** (solo per host Linux).
Nome utente	Specificare il nome utente.
Password	Se è stata selezionata l'autenticazione basata su password, specificare la password.
Chiave privata SSH	Se è stata selezionata l'autenticazione basata su chiave SSH, specificare la chiave privata.
Utilizzare i privilegi sudo	Selezionare la casella di controllo Usa privilegi sudo se si stanno creando credenziali per un utente non root. Applicabile solo agli utenti Linux.

5. Fare clic su **OK**.

Proteggere i database SAP HANA

Aggiungi host e installa il plug-in SnapCenter per il database SAP HANA

Utilizzare la pagina Aggiungi host di SnapCenter per aggiungere host e installare i pacchetti dei plug-in. I plug-in vengono installati automaticamente sugli host remoti.

Prima di iniziare

- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.
- Se si sta installando sull'host centralizzato, assicurarsi che il software client SAP HANA sia installato su quell'host e aprire le porte richieste sull'host del database SAP HANA per eseguire le query HDB SQL in remoto.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.

2. Verificare che la scheda **Managed hosts** sia selezionata.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, eseguire le seguenti operazioni:
   a. Nel campo host Type (tipo host), selezionare il tipo di host.
   b. Nel campo host name (Nome host), immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.
   c. Nel campo credenziali, immettere la credenziale creata.
5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare i plug-in da installare.
6. (Facoltativo) fate clic su **altre opzioni** e specificate i dettagli.
7. Fare clic su **Invia**.
8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi fare clic su **Confirm and Submit** (Conferma e invia).

   In una configurazione del cluster, verificare l'impronta digitale di ciascuno dei nodi del cluster.
9. Monitorare l'avanzamento dell'installazione.

Aggiunta del database SAP HANA

Dovresti aggiungere il database SAP HANA manualmente.

A proposito di questa attività

Le risorse devono essere aggiunte manualmente se il plug-in è installato su un server centralizzato. Se il plug-in SAP HANA è installato sull'host del database HANA, il sistema HANA viene rilevato automaticamente.

> Il rilevamento automatico non è supportato per la configurazione HANA multi-host, ma deve essere aggiunto solo tramite plug-in centralizzato.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare il plug-in SnapCenter per il database SAP HANA dall'elenco a discesa, quindi fare clic su **risorse**.
2. Nella pagina Resources (risorse), fare clic su **Add SAP HANA Database** (Aggiungi database SAP HANA).
3. Nella pagina fornire dettagli sulle risorse, eseguire le seguenti operazioni:
   a. Immettere il tipo di risorsa come contenitore singolo, contenitore database multitenant o Volume non dati.
   b. Inserire il nome del sistema SAP HANA.
   c. Inserire l'ID di sistema (SID).
   d. Selezionare l'host del plug-in.
   e. Inserire la chiave per connettersi al sistema SAP HANA.
   f. Immettere il nome utente per il quale è configurata la chiave di memorizzazione utente protetta HDB.
4. Nella pagina Area di archiviazione, selezionare **Azure NetApp Files** come tipo di archiviazione.
   a. Seleziona l'account Azure NetApp.
   b. Selezionare il pool di capacità e i volumi associati.

c. Fare clic su **Save** (Salva).

5. Esaminare il riepilogo, quindi fare clic su **fine**.

Creare policy di backup per i database SAP HANA

Prima di utilizzare SnapCenter per eseguire il backup delle risorse di database SAP HANA, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **nuovo**.
4. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
5. Nella pagina Impostazioni, attenersi alla seguente procedura:
   a. Selezionare il tipo di backup.
      i. Selezionare **Backup basato su file** se si desidera eseguire un controllo di integrità del database.
      ii. Selezionare **basato su snapshot** se si desidera creare un backup utilizzando la tecnologia Snapshot.
   b. Specificare il tipo di pianificazione.
6. Nella pagina di conservazione, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionato.

   La replica su storage secondario non è supportata.

7. Esaminare il riepilogo e fare clic su **fine**.

Creare gruppi di risorse e collegare le policy di backup per SAP HANA

Un gruppo di risorse è il container al quale è necessario aggiungere risorse di cui si desidera eseguire il backup e la protezione.

Un gruppo di risorse consente di eseguire contemporaneamente il backup di tutti i dati associati a una determinata applicazione. Per qualsiasi lavoro di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario associare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), fare clic su **New Resource Group** (nuovo gruppo di risorse).
3. Nella pagina Name (Nome), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere un nome per il gruppo di risorse.
Tag	Inserire una o più etichette per facilitare la ricerca del gruppo di risorse in un secondo momento.
USA il formato nome personalizzato per la copia Snapshot	Selezionare questa casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea.

4. Nella pagina risorse, selezionare un nome host dall'elenco a discesa **host** e il tipo di risorsa dall'elenco a discesa **tipo di risorsa**.
5. Selezionare le risorse dalla sezione **risorse disponibili**, quindi fare clic sulla freccia destra per spostarle nella sezione **risorse selezionate**.
6. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.
   b. Nella colonna Configura pianificazioni, fare clic su * * per il criterio che si desidera configurare.
   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.
7. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
8. Esaminare il riepilogo, quindi fare clic su **fine**.

Eseguire il backup dei database SAP HANA in esecuzione su Azure NetApp Files

Se una risorsa non fa ancora parte di un gruppo di risorse, è possibile eseguire il backup della risorsa dalla pagina risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resource, filtrare le risorse dall'elenco a discesa **View** in base al tipo di risorsa.
3. Selezionare la risorsa di cui si desidera eseguire il backup.
4. Nella pagina risorsa, selezionare **Usa formato nome personalizzato per copia istantanea**, quindi immettere un formato nome personalizzato che si desidera utilizzare per il nome istantanea.
5. Nella pagina Impostazioni applicazione, effettuare le seguenti operazioni:
   a. Selezionare la freccia **backup** per impostare opzioni di backup aggiuntive.
   b. Selezionare la freccia **Scripts** per eseguire i comandi pre e post per le operazioni quiescenza, istantanea e inquiescenza.
   c. Selezionare la freccia **configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i lavori che utilizzano questa risorsa.
   d. Selezionare **Snapshot Copy Tool > SnapCenter Without file System Consistency** per creare istantanee.

L'opzione **coerenza file system** è applicabile solo alle applicazioni in esecuzione su host Windows.

6. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.
   b. Selezionare * * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi selezionare **OK**.

      policy_name è il nome del criterio selezionato.
7. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. SMTP deve essere configurato anche in **Impostazioni** > **Impostazioni globali**.
8. Esaminare il riepilogo, quindi selezionare **fine**.
9. Selezionare **Esegui backup ora**.
10. Nella pagina Backup, attenersi alla seguente procedura:
    a. Se alla risorsa sono associati più criteri, nell'elenco a discesa **criterio** selezionare il criterio che si desidera utilizzare per il backup.

       Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.
11. Selezionare **Backup**.
12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Eseguire il backup dei gruppi di risorse SAP HANA

Un gruppo di risorse è un insieme di risorse su un host. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).
3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi selezionare **Esegui backup ora**.
4. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se al gruppo di risorse sono associati più criteri, nell'elenco a discesa **criterio** selezionare il criterio che si desidera utilizzare per il backup.

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di

pianificazione.

b. Selezionare **Backup**.

5. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Ripristino e ripristino dei database SAP HANA

È possibile ripristinare i dati dai backup.

A proposito di questa attività

Per i sistemi HANA rilevati automaticamente, se è selezionata l'opzione **complete Resource**, il ripristino viene eseguito utilizzando la tecnologia di ripristino snapshot a file singolo. Se la casella di controllo **Ripristino rapido** è selezionata, viene utilizzata la tecnologia di indirizzamento del volume.

Per le risorse aggiunte manualmente, viene sempre utilizzata la tecnologia Volume Revert.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, filtrare le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.
3. Selezionare la risorsa o un gruppo di risorse, quindi selezionare una risorsa in tale gruppo.
4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primario o secondario (mirrorati o vault).
5. Nella tabella Backup primari, selezionare il backup da cui si desidera eseguire il ripristino, quindi fare clic su * *  .
6. Nella pagina Ripristina ambito, selezionare **completa risorsa**.

   Tutti i volumi di dati configurati del database SAP HANA vengono ripristinati.

7. Per i sistemi HANA rilevati automaticamente, nella pagina ambito ripristino, eseguire le seguenti azioni:
   a. Selezionare **Recupera allo stato più recente** se si desidera ripristinare il più vicino possibile all'ora corrente.
   b. Selezionare **Recover to point in time** se si desidera ripristinare il punto temporale specificato.
   c. Selezionare **Recupera al backup dei dati specificato** se si desidera ripristinare un backup dei dati specifico.
   d. Selezionare **Nessun recupero** se non si desidera eseguire il ripristino ora.
   e. Specificare le posizioni di backup del registro.
   f. Specificare la posizione del catalogo di backup.
8. Nella pagina Pre Ops (operazioni preliminari), immettere i comandi di pre-ripristino e disinstallazione da eseguire prima di eseguire un processo di ripristino.
9. Nella pagina Post Ops (operazioni post), immettere i comandi di montaggio e post ripristino da eseguire dopo l'esecuzione di un processo di ripristino.
10. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

    È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail.

SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

11. Esaminare il riepilogo, quindi fare clic su **fine**.
12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Clona il backup del database SAP HANA

È possibile utilizzare SnapCenter per clonare un backup.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, filtrare le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.
3. Selezionare la risorsa o il gruppo di risorse.
4. Nella vista Gestione copie, selezionare **backup** dal sistema di archiviazione primario.
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su  .
6. Nella pagina Location (posizione), eseguire le seguenti operazioni:
   a. Selezionare l'host in cui è installato il plug-in SAP HANA per la gestione del sistema HANA clonato.

      Può essere un plug-in host centralizzato o un host di sistema HANA.

   b. Inserisci il SID SAP HANA da clonare dai backup esistenti.
   c. Inserire gli indirizzi IP o i nomi host su cui esportare i volumi clonati.
   d. Se i volumi ANF del database SAP HANA sono configurati in un pool di capacità QOS manuale, specificare la QOS per i volumi clonati.

      Se non viene specificata la QOS per i volumi clonati, verrà utilizzata la QOS del volume di origine. Se viene utilizzato il pool di capacità QOS automatico, il valore QOS specificato verrà ignorato.

7. Nella pagina script, attenersi alla seguente procedura:
   a. Immettere i comandi per pre-clone o post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clone.
   b. Immettere il comando mount per montare un file system su un host.

      Se il sistema HANA di origine viene rilevato automaticamente e il plug-in dell'host di destinazione clone è installato sull'host SAP HANA, SnapCenter dismonta automaticamente i volumi di dati HANA esistenti sull'host di destinazione clone e monta i volumi di dati HANA appena clonati.

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
9. Esaminare il riepilogo, quindi fare clic su **fine**.
10. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Clone split è disattivato per i cloni ANF perché il clone ANF è già un volume indipendente creato dall'istantanea selezionata.

Proteggere i database Microsoft SQL Server

Aggiungere host e installare il plug-in SnapCenter per il database SQL Server

SnapCenter supporta la data Protection delle istanze SQL sulle condivisioni SMB su Azure NetApp Files. Sono supportate le configurazioni standalone e gruppo di disponibilità (AG, Availability Group).

È necessario utilizzare la pagina Aggiungi host di SnapCenter per aggiungere host, quindi installare il pacchetto dei plug-in. I plug-in vengono installati automaticamente sugli host remoti.

Prima di iniziare

- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata nella parte superiore.
3. Selezionare **Aggiungi**.
4. Nella pagina hosts:
   a. Nel campo host Type (tipo host), selezionare il tipo di host.
   b. Nel campo host name (Nome host), immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.
   c. Nel campo credenziali, immettere la credenziale creata.
5. Nella sezione **Seleziona plug-in da installare**, selezionare i plug-in da installare.
6. (Facoltativo) fate clic su **altre opzioni** e specificate i dettagli.
7. Selezionare **Invia**.
8. Selezionare **Configure log directory** e nella pagina Configure host log directory, immettere il percorso SMB della directory del log host, quindi fare clic su **Save**.
9. Fare clic su **Invia** e controllare l'avanzamento dell'installazione.

Creare criteri di backup per i database di SQL Server

È possibile creare un criterio di backup per la risorsa o il gruppo di risorse prima di utilizzare SnapCenter per eseguire il backup delle risorse di SQL Server oppure creare un criterio di backup al momento della creazione di un gruppo di risorse o del backup di una singola risorsa.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **nuovo**.

4. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
5. Nella pagina Impostazioni, attenersi alla seguente procedura:
   a. Selezionare il tipo di backup.
      i. Selezionare **Backup completo e Backup registro** se si desidera eseguire il backup dei file di database e dei registri delle transazioni.
      ii. Selezionare **Backup completo** se si desidera eseguire il backup solo dei file di database.
      iii. Selezionare **Log Backup** se si desidera eseguire il backup solo dei registri delle transazioni.
      iv. Selezionare **Copia solo backup** se si desidera eseguire il backup delle risorse utilizzando un'altra applicazione.
   b. Nella sezione Availability Group Settings (Impostazioni gruppo di disponibilità), eseguire le seguenti operazioni:
      i. Selezionare Backup sulla replica di backup preferita se si desidera eseguire il backup solo sulla replica.
      ii. Selezionare la replica AG primaria o la replica AG secondaria per il backup.
      iii. Selezionare la priorità di backup.
   c. Specificare il tipo di pianificazione.
6. Nella pagina di conservazione, in base al tipo di backup selezionato, specificare le impostazioni di conservazione.

   La replica su storage secondario non è supportata.

7. Nella pagina verifica, attenersi alla seguente procedura:
   a. Nella sezione Esegui verifica per le seguenti pianificazioni di backup, selezionare la frequenza di pianificazione.
   b. Nella sezione Opzioni di verifica della coerenza del database, eseguire le seguenti operazioni:
      i. Selezionare **Limit the Integrity Structure to Physical Structure of the database (PHYSICAL_ONLY)** (limita la struttura di integrità alla struttura fisica del database) per limitare il controllo dell'integrità alla struttura fisica del database e rilevare pagine lacerate, errori di checksum e guasti hardware comuni che influiscono sul database.
      ii. Selezionare **Sospendi tutti i messaggi informativi (NO_INFOMSGS)** per eliminare tutti i messaggi informativi.

      Selezionato per impostazione predefinita.

      iii. Selezionare **Visualizza tutti i messaggi di errore riportati per oggetto (ALL_ERRORMSGS)** per visualizzare tutti gli errori segnalati per oggetto.
      iv. Selezionare **non selezionare gli indici non cluster (NOINDEX)** se non si desidera controllare gli indici non cluster.

      Il database SQL Server utilizza Microsoft SQL Server Database Consistency Checker (DBCC) per verificare l'integrità fisica e logica degli oggetti nel database.

      v. Selezionare **limita i controlli e ottenere i blocchi invece di utilizzare una copia snapshot del database interno (TABLOCK)** per limitare i controlli e ottenere i blocchi invece di utilizzare un'istantanea del database interna.
   c. Nella sezione **Log Backup**, selezionare **Verify log backup upon completed** (verifica backup registro

al completamento) per verificare il backup del registro al completamento.

d. Nella sezione **Verification script settings** (Impostazioni script di verifica), immettere il percorso e gli argomenti del prescrittt o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di verifica.

8. Esaminare il riepilogo e fare clic su **fine**.

Creare gruppi di risorse e allegare criteri di backup SQL

Un gruppo di risorse è il container al quale è necessario aggiungere risorse di cui si desidera eseguire il backup e la protezione.

Un gruppo di risorse consente di eseguire contemporaneamente il backup di tutti i dati associati a una determinata applicazione. Per qualsiasi lavoro di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario associare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), fare clic su **New Resource Group** (nuovo gruppo di risorse).
3. Nella pagina Name (Nome), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere un nome per il gruppo di risorse.
Tag	Inserire una o più etichette per facilitare la ricerca del gruppo di risorse in un secondo momento.
USA il formato nome personalizzato per la copia Snapshot	Selezionare questa casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea.

4. Nella pagina risorse, selezionare un nome host dall'elenco a discesa **host** e il tipo di risorsa dall'elenco a discesa **tipo di risorsa**.
5. Selezionare le risorse dalla sezione **risorse disponibili**, quindi fare clic sulla freccia destra per spostarle nella sezione **risorse selezionate**.
6. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.
   b. Nella colonna Configura pianificazioni, fare clic su * * per il criterio che si desidera configurare.
   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.
   d. Selezionare lo scheduler di Microsoft SQL Server.
7. Nella pagina verifica, attenersi alla seguente procedura:
   a. Selezionare il server di verifica.

b. Selezionare il criterio per cui si desidera configurare la pianificazione della verifica, quindi fare clic su * * .

c. Selezionare **Esegui verifica dopo il backup** o **Esegui verifica pianificata**.

d. Fare clic su **OK**.

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
9. Esaminare il riepilogo, quindi fare clic su **fine**.

Eseguire il backup dei database SQL Server in esecuzione su Azure NetApp Files

Se una risorsa non fa ancora parte di un gruppo di risorse, è possibile eseguire il backup della risorsa dalla pagina risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorsa, selezionare **Database**, **istanza** o **Gruppo disponibilità** dall'elenco a discesa Visualizza.
3. Nella pagina risorsa, selezionare **Usa formato nome personalizzato per copia istantanea**, quindi immettere un formato nome personalizzato che si desidera utilizzare per il nome istantanea.
4. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.
   b. Selezionare * * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi selezionare **OK**.

      policy_name è il nome del criterio selezionato.

   d. Selezionare **Usa Utilità di pianificazione Microsoft SQL Server**, quindi selezionare l'istanza dell'utilità di pianificazione dall'elenco a discesa **istanza dell'utilità di pianificazione** associato al criterio di pianificazione.
5. Nella pagina verifica, attenersi alla seguente procedura:
   a. Selezionare il server di verifica.
   b. Selezionare il criterio per cui si desidera configurare la pianificazione della verifica, quindi fare clic su * * .
   c. Selezionare **Esegui verifica dopo il backup** o **Esegui verifica pianificata**.
   d. Fare clic su OK.
6. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
7. Esaminare il riepilogo, quindi fare clic su **fine**.
8. Selezionare **Esegui backup ora**.

9. Nella pagina Backup, attenersi alla seguente procedura:
    a. Se alla risorsa sono associati più criteri, nell'elenco a discesa **criterio** selezionare il criterio che si desidera utilizzare per il backup.
    b. Selezionare **verifica dopo il backup**.
    c. Selezionare **Backup**.
10. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Eseguire il backup dei gruppi di risorse di SQL Server

È possibile eseguire il backup dei gruppi di risorse composti da più risorse. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).
3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi selezionare **Esegui backup ora**.
4. Nella pagina Backup, attenersi alla seguente procedura:
    a. Se al gruppo di risorse sono associati più criteri, nell'elenco a discesa **criterio** selezionare il criterio che si desidera utilizzare per il backup.
    b. Dopo il backup, selezionare **verify** (verifica) per verificare il backup on-demand.
    c. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Ripristinare e ripristinare i database SQL Server

È possibile utilizzare SnapCenter per ripristinare i database di SQL Server di cui è stato eseguito il backup. Il ripristino del database è un processo multifase che copia tutti i dati e le pagine di registro da un backup SQL Server specificato in un database specificato.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **Database** o **Gruppo risorse** dall'elenco Visualizza.
3. Selezionare il database o il gruppo di risorse dall'elenco.
4. Nella vista Gestione copie, selezionare **backup** dal sistema di archiviazione.
5. Selezionare il backup dalla tabella, quindi fare clic sull'  icona.
6. Nella pagina Restore Scope (ambito ripristino), selezionare una delle seguenti opzioni:
    a. Selezionare **Ripristina il database nello stesso host in cui è stato creato il backup** se si desidera ripristinare il database nello stesso server SQL in cui vengono eseguiti i backup.

b. Selezionare **Ripristina il database in un host alternativo** se si desidera che il database venga ripristinato in un server SQL diverso nello stesso host o in un host diverso in cui vengono eseguiti i backup.

7. Nella pagina Recovery Scope (ambito ripristino), selezionare una delle seguenti opzioni:
   a. Selezionare **None** (Nessuno) se si desidera ripristinare solo il backup completo senza alcun registro.
   b. Selezionare **tutti i backup dei registri** operazione di ripristino di backup fino al minuto per ripristinare tutti i backup dei registri disponibili dopo il backup completo.
   c. Selezionare **by log backups** per eseguire un'operazione di ripristino point-in-time, che ripristina il database in base ai log di backup fino al log di backup con la data selezionata.
   d. Selezionare **per data specifica fino a** per specificare la data e l'ora dopo le quali i registri delle transazioni non vengono applicati al database ripristinato.
   e. Se è stato selezionato **All log backups**, **by log backups** o **by specifiche date until** e i log si trovano in una posizione personalizzata, selezionare **Use custom log directory**, quindi specificare la posizione del log.
8. Nella pagina Pre-Ops e Post Ops, specificare i dettagli richiesti.
9. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
10. Esaminare il riepilogo, quindi fare clic su **fine**.
11. Monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

Clona il backup del database SQL Server

È possibile utilizzare SnapCenter per clonare un backup del database SQL Server. Se si desidera accedere o ripristinare una versione precedente dei dati, è possibile clonare i backup del database su richiesta.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database o il gruppo di risorse.
4. Nella pagina di visualizzazione **Gestisci copie**, selezionare il backup dal sistema di archiviazione primario.
5. Selezionare il backup, quindi  .
6. Nella pagina **Clone Options** (Opzioni di clonazione), fornire tutti i dettagli richiesti.
7. Nella pagina Location (posizione), selezionare una posizione di storage per creare un clone.

   Se i volumi ANF del database SQL Server sono configurati in un pool di capacità QOS manuale, specificare la QOS per i volumi clonati.

   Se non viene specificata la QOS per i volumi clonati, verrà utilizzata la QOS del volume di origine. Se viene utilizzato il pool di capacità QOS automatico, il valore QOS specificato verrà ignorato.

8. Nella pagina registri, selezionare una delle seguenti opzioni:
   a. Selezionare **Nessuno** se si desidera clonare solo il backup completo senza alcun registro.

b. Selezionare **tutti i backup dei log** se si desidera clonare tutti i backup dei log disponibili datati dopo il backup completo.

c. Selezionare **per backup del registro fino a** se si desidera clonare il database in base ai registri di backup creati fino al log di backup con la data selezionata.

d. Selezionare **per data specifica fino a** se non si desidera applicare i registri delle transazioni dopo la data e l'ora specificate.

9. Nella pagina **script**, immettere il timeout dello script, il percorso e gli argomenti del prescrittt o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di clone.
10. Nella pagina **Notification**, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
11. Esaminare il riepilogo, quindi selezionare **fine**.
12. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Eseguire il ciclo di vita del clone

Utilizzando SnapCenter, è possibile creare cloni da un gruppo di risorse o da un database. È possibile eseguire cloni on-demand o pianificare operazioni ricorrenti di cloni di un gruppo di risorse o di un database. Se si clonano periodicamente un backup, è possibile utilizzare il clone per sviluppare applicazioni, popolare i dati o ripristinare i dati.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** o **Resource Group** dall'elenco **View** (Visualizza).
3. Selezionare il database o il gruppo di risorse.
4. Nella pagina di visualizzazione **Gestisci copie**, selezionare il backup dal sistema di archiviazione primario.
5. Selezionare il backup, quindi  .
6. Nella pagina **Clone Options** (Opzioni di clonazione), fornire tutti i dettagli richiesti.
7. Nella pagina Location (posizione), selezionare una posizione di storage per creare un clone.

   Se i volumi ANF del database SQL Server sono configurati in un pool di capacità QOS manuale, specificare la QOS per i volumi clonati.

   Se non viene specificata la QOS per i volumi clonati, verrà utilizzata la QOS del volume di origine. Se viene utilizzato il pool di capacità QOS automatico, il valore QOS specificato verrà ignorato.

8. Nella pagina **script**, immettere il timeout dello script, il percorso e gli argomenti del prescrittt o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di clone.
9. Nella pagina Schedule (Pianificazione), eseguire una delle seguenti operazioni:
   - Selezionare **Esegui ora** se si desidera eseguire il processo di clonazione immediatamente.
   - Selezionare **Configure Schedule** (Configura pianificazione) quando si desidera determinare con quale frequenza deve avvenire l'operazione di clonazione, quando deve iniziare la pianificazione di clonazione, in quale giorno deve avvenire l'operazione di clonazione, quando deve scadere la pianificazione e se i cloni devono essere eliminati dopo la scadenza della pianificazione.
10. Nella pagina **Notification**, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

11. Esaminare il riepilogo, quindi selezionare **fine**.
12. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Proteggere i database Oracle

Aggiunta di host e installazione del plug-in SnapCenter per database Oracle

È possibile utilizzare la pagina Aggiungi host per aggiungere host, quindi installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX. I plug-in vengono installati automaticamente sugli host remoti.

È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster. Se stai installando il plug-in su un cluster (Oracle RAC), il plug-in viene installato su tutti i nodi del cluster. Per Oracle RAC One Node, è necessario installare il plug-in su entrambi i nodi attivi e passivi.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, eseguire le seguenti operazioni:
   a. Nel campo host Type (tipo host), selezionare il tipo di host.
   b. Nel campo host name (Nome host), immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.
   c. Nel campo credenziali, immettere la credenziale creata.
5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare i plug-in da installare.
6. (Facoltativo) fate clic su **altre opzioni** e specificate i dettagli.
7. Fare clic su **Invia**.
8. Verificare l'impronta digitale, quindi fare clic su **Confirm and Submit** (Conferma e invia).

   In una configurazione del cluster, verificare l'impronta digitale di ciascuno dei nodi del cluster.

9. Monitorare l'avanzamento dell'installazione.

Creare policy di backup per i database Oracle

Prima di utilizzare SnapCenter per eseguire il backup delle risorse di database Oracle, è necessario creare un criterio di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare Oracle Database dall'elenco a discesa.
4. Fare clic su **nuovo**.

5. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
6. Nella pagina Backup Type (tipo di backup), attenersi alla seguente procedura:
   a. Selezionare il tipo di backup come backup in linea o non in linea.
   b. Specificare la frequenza di pianificazione.
   c. Se si desidera catalogare il backup utilizzando Oracle Recovery Manager (RMAN), selezionare **Catalog backup with Oracle Recovery Manager (RMAN)**.
   d. Se si desidera ridurre i registri di archiviazione dopo il backup, selezionare **Prune archive logs after backup** (Sintonizzare i registri di archiviazione dopo il backup).
   e. Specificare le impostazioni di eliminazione del registro archivio.
7. Nella pagina di conservazione, specificare le impostazioni di conservazione.
8. Nella pagina script, immettere il percorso e gli argomenti del prespt o del postscript che si desidera eseguire rispettivamente prima o dopo l'operazione di backup.
9. Nella pagina verifica, selezionare la pianificazione di backup per la quale si desidera eseguire l'operazione di verifica e immettere il percorso e gli argomenti del postscript o del file di prescrizione che si desidera eseguire prima o dopo l'operazione di verifica, rispettivamente.
10. Esaminare il riepilogo e fare clic su **fine**.

Creare gruppi di risorse e allegare criteri di backup Oracle

Un gruppo di risorse è il container al quale è necessario aggiungere risorse di cui si desidera eseguire il backup e la protezione.

Un gruppo di risorse consente di eseguire contemporaneamente il backup di tutti i dati associati a una determinata applicazione. Per qualsiasi lavoro di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario associare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), fare clic su **New Resource Group** (nuovo gruppo di risorse).
3. Nella pagina Name (Nome), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere un nome per il gruppo di risorse.
Tag	Inserire una o più etichette per facilitare la ricerca del gruppo di risorse in un secondo momento.
USA il formato nome personalizzato per la copia Snapshot	Selezionare questa casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea.
Destinazione del file di registro di archivio	Specificare le destinazioni dei file di registro dell'archivio.

4. Nella pagina risorse, selezionare un nome host dall'elenco a discesa **host** e il tipo di risorsa dall'elenco a discesa **tipo di risorsa**.
5. Selezionare le risorse dalla sezione **risorse disponibili**, quindi fare clic sulla freccia destra per spostarle nella sezione **risorse selezionate**.
6. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.
   b. Nella colonna Configura pianificazioni, fare clic su * * per il criterio che si desidera configurare.
   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.
7. Nella pagina verifica, attenersi alla seguente procedura:
   a. Selezionare il server di verifica.
   b. Selezionare il criterio per il quale si desidera configurare la pianificazione della verifica, quindi fare clic su * .
   c. Selezionare **Esegui verifica dopo il backup** o **Esegui verifica pianificata**.
   d. Fare clic su **OK**.
8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
9. Esaminare il riepilogo, quindi fare clic su **fine**.

Eseguire il backup dei database Oracle in esecuzione su Azure NetApp Files

Se una risorsa non fa ancora parte di un gruppo di risorse, è possibile eseguire il backup della risorsa dalla pagina risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorsa, selezionare **Database** dall'elenco a discesa Visualizza.
3. Nella pagina risorsa, selezionare **Usa formato nome personalizzato per copia istantanea**, quindi immettere un formato nome personalizzato che si desidera utilizzare per il nome istantanea.
4. Nella pagina Criteri, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.
   b. Selezionare * * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi selezionare **OK**.
5. Nella pagina verifica, attenersi alla seguente procedura:
   a. Selezionare il server di verifica.
   b. Selezionare il criterio per cui si desidera configurare la pianificazione della verifica, quindi fare clic su * * .

c. Selezionare **Esegui verifica dopo il backup** o **Esegui verifica pianificata**.

d. Fare clic su OK.

6. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
7. Esaminare il riepilogo, quindi fare clic su **fine**.
8. Selezionare **Esegui backup ora**.
9. Nella pagina Backup, attenersi alla seguente procedura:

a. Se alla risorsa sono associati più criteri, nell'elenco a discesa **criterio** selezionare il criterio che si desidera utilizzare per il backup.

b. Fare clic su **Backup**.

10. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Eseguire il backup dei gruppi di risorse Oracle

È possibile eseguire il backup dei gruppi di risorse composti da più risorse. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).
3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi selezionare **Esegui backup ora**.
4. Nella pagina Backup, attenersi alla seguente procedura:

a. Se al gruppo di risorse sono associati più criteri, nell'elenco a discesa **criterio** selezionare il criterio che si desidera utilizzare per il backup.

b. Selezionare **Backup**.

5. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Ripristinare e ripristinare i database Oracle

In caso di perdita di dati, è possibile utilizzare SnapCenter per ripristinare i dati da uno o più backup nel file system attivo e quindi ripristinare il database.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **Database** o **Gruppo risorse** dall'elenco Visualizza.
3. Selezionare il database o il gruppo di risorse dall'elenco.
4. Nella vista Gestione copie, selezionare **backup** dal sistema di archiviazione primario.
5. Selezionare il backup dalla tabella, quindi fare clic su * *  .

6. Nella pagina Restore Scope (ambito ripristino), eseguire le seguenti operazioni:
    a. Selezionare RAC se è stato selezionato un backup di un database in ambiente RAC.
    b. Eseguire le seguenti operazioni:
        i. Selezionare **tutti i file di dati** se si desidera ripristinare solo i file di database.
        ii. Selezionare **tablespace** se si desidera ripristinare solo gli spazi di tabella.
        iii. Selezionare **Ripristina file di registro** se si desidera ripristinare i file di registro di ripristino dei database di standby di Data Guard o di standby di Active Data Guard.
        iv. Selezionare **Database collegabili** e specificare i PDB che si desidera ripristinare.
        v. Selezionare **tablespace del database Pluggable (PDB)**, quindi specificare il PDB e gli spazi delle tabelle del PDB che si desidera ripristinare.
        vi. Selezionare **Ripristina il database nello stesso host in cui è stato creato il backup** se si desidera ripristinare il database nello stesso server SQL in cui vengono eseguiti i backup.
        vii. Selezionare **Ripristina il database in un host alternativo** se si desidera che il database venga ripristinato in un server SQL diverso nello stesso host o in un host diverso in cui vengono eseguiti i backup.
        viii. Selezionare **Cambia stato del database se necessario per il ripristino e il ripristino** per impostare lo stato del database sullo stato richiesto per eseguire le operazioni di ripristino e ripristino.
        ix. Selezionare **Imponi ripristino** se si desidera eseguire il ripristino in-place negli scenari in cui vengono aggiunti nuovi file di dati dopo il backup o quando i LUN vengono aggiunti, cancellati o ricreati in un gruppo di dischi LVM.
7. Nella pagina Recovery Scope (ambito ripristino), selezionare una delle seguenti opzioni:
    a. Selezionare **All Logs** (tutti i registri) se si desidera ripristinare l'ultima transazione.
    b. Selezionare **fino a SCN (System Change Number)** se si desidera ripristinare un SCN specifico.
    c. Selezionare **Data e ora** se si desidera ripristinare una data e un'ora specifiche.
    d. Selezionare **No recovery** se non si desidera eseguire il ripristino.
    e. Selezionare **specifica ubicazioni log archivio esterno** se si desidera specificare la posizione dei file log archivio esterno.
8. Nella pagina Pre-Ops e Post Ops, specificare i dettagli richiesti.
9. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
10. Esaminare il riepilogo, quindi fare clic su **fine**.
11. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Ripristinare e ripristinare gli spazi delle tabelle utilizzando il ripristino point-in-time

È possibile ripristinare un sottoinsieme di tablespace che sono state danneggiate o rilasciate senza influire sugli altri tablespace nel database. SnapCenter utilizza RMAN per eseguire il recovery point-in-time (PITR) dei tablespace.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **Database** o **Gruppo risorse** dall'elenco Visualizza.

3. Selezionare il database di tipo istanza singola (multitenant).
4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dal sistema di storage.

   Se il backup non è catalogato, selezionare il backup e fare clic su **Catalog** (Catalogo).

5. Selezionare il backup catalogato, quindi fare clic su * *  .
6. Nella pagina Restore Scope (ambito ripristino), eseguire le seguenti operazioni:
   a. Selezionare **RAC** se è stato selezionato un backup di un database in ambiente RAC.
   b. Selezionare **tablespace** se si desidera ripristinare solo gli spazi di tabella.
   c. Selezionare **Cambia stato del database se necessario per il ripristino e il ripristino** per impostare lo stato del database sullo stato richiesto per eseguire le operazioni di ripristino e ripristino.
7. Nella pagina Recovery Scope (ambito ripristino), selezionare una delle seguenti opzioni:
   a. Selezionare **fino a SCN (System Change Number)** se si desidera ripristinare un SCN specifico.
   b. Selezionare **Data e ora** se si desidera ripristinare una data e un'ora specifiche.
8. Nella pagina Pre-Ops e Post Ops, specificare i dettagli richiesti.
9. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
10. Esaminare il riepilogo, quindi fare clic su **fine**.
11. Monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

Ripristino e ripristino di database collegabili mediante ripristino point-in-time

È possibile ripristinare e ripristinare un database collegabile (PDB) che è stato danneggiato o interrotto senza influire sulle altre PDB nel database container (CDB). SnapCenter utilizza RMAN per eseguire il recovery point-in-time (PITR) del PDB.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **Database** o **Gruppo risorse** dall'elenco Visualizza.
3. Selezionare il database di tipo istanza singola (multitenant).
4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dal sistema di storage.

   Se il backup non è catalogato, selezionare il backup e fare clic su **Catalog** (Catalogo).

5. Selezionare il backup catalogato, quindi fare clic su * *  .
6. Nella pagina Restore Scope (ambito ripristino), eseguire le seguenti operazioni:
   a. Selezionare **RAC** se è stato selezionato un backup di un database in ambiente RAC.
   b. A seconda che si desideri ripristinare la PDB o gli spazi delle tabelle in una PDB, eseguire una delle seguenti operazioni:
      - Selezionare **Pluggable Databases (PDB)** se si desidera ripristinare un PDB.
      - Selezionare **spazi di tabella del database Pluggable (PDB)** se si desidera ripristinare spazi di tabella in un PDB.

7. Nella pagina Recovery Scope (ambito ripristino), selezionare una delle seguenti opzioni:
   a. Selezionare **fino a SCN (System Change Number)** se si desidera ripristinare un SCN specifico.
   b. Selezionare **Data e ora** se si desidera ripristinare una data e un'ora specifiche.
8. Nella pagina Pre-Ops e Post Ops, specificare i dettagli richiesti.
9. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
10. Esaminare il riepilogo, quindi fare clic su **fine**.
11. Monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

Clona il backup del database Oracle

È possibile utilizzare SnapCenter per clonare un database Oracle utilizzando il backup del database.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **Database** o **Gruppo risorse** dall'elenco Visualizza.
3. Selezionare il database.
4. Dalla pagina di visualizzazione Gestisci copie, selezionare il backup dal sistema di storage primario.
5. Selezionare il backup dei dati, quindi fare clic su * *  .
6. Nella pagina Name (Nome), selezionare se si desidera clonare un database (CDB o non CDB) o clonare un database inseribile (PDB).
7. Nella pagina posizioni, specificare i dettagli richiesti.

   Se i volumi ANF del database Oracle sono configurati in un pool di capacità QOS manuale, specificare la QOS per i volumi clonati.

   Se non viene specificata la QOS per i volumi clonati, verrà utilizzata la QOS del volume di origine. Se viene utilizzato il pool di capacità QOS automatico, il valore QOS specificato verrà ignorato.

8. Nella pagina credenziali, eseguire una delle seguenti operazioni:
   a. Per Nome credenziale per l'utente sys, selezionare la credenziale da utilizzare per definire la password utente sys del database clone.
   b. Per Nome credenziale istanza ASM, selezionare **Nessuno** se l'autenticazione del sistema operativo è attivata per la connessione all'istanza ASM sull'host clone.

      In caso contrario, selezionare la credenziale Oracle ASM configurata con un utente "sys" o con un utente che dispone del privilegio "sysasm" applicabile all'host clone.

9. Nella pagina Pre-Ops specificare il percorso e gli argomenti dei prescrittori e nella sezione Database Parameter settings (Impostazioni parametri database), modificare i valori dei parametri del database prepopolati utilizzati per inizializzare il database.
10. Nella pagina Post-Ops, per impostazione predefinita sono selezionati **Recupera database** e **fino a Annulla** per eseguire il ripristino del database clonato.

a. Se si seleziona **fino a Annulla**, SnapCenter esegue il ripristino montando l'ultimo backup del registro con la sequenza non interrotta dei registri di archivio dopo il backup dei dati selezionato per la clonazione.

b. Se si seleziona **Data e ora**, SnapCenter ripristina il database fino a una data e a un'ora specificate.

c. Se si seleziona **fino a SCN**, SnapCenter ripristina il database fino a un SCN specificato.

d. Se si seleziona **specifica ubicazioni registro archivio esterno**, SnapCenter identifica e monta il numero ottimale di backup registro in base alla SCN specificata o alla data e all'ora selezionate.

e. Per impostazione predefinita, la casella di controllo **Crea nuovo DBID** è selezionata per generare un numero univoco (DBID) per il database clonato che lo differenzia dal database di origine.

   Deselezionare la casella di controllo se si desidera assegnare il DBID del database di origine al database clonato. In questo scenario, se si desidera registrare il database clonato con il catalogo RMAN esterno in cui il database di origine è già registrato, l'operazione non riesce.

f. Selezionare la casella di controllo **Create tempfile for temporary tablespace** (Crea file tempper tablespace temporanea) se si desidera creare un file temporary tablespace predefinito del database clonato.

g. In **Inserisci voci sql da applicare quando viene creato il clone**, aggiungere le voci sql che si desidera applicare al momento della creazione del clone.

h. In **immettere gli script da eseguire dopo l'operazione di clonazione**, specificare il percorso e gli argomenti del postscript che si desidera eseguire dopo l'operazione di clonazione.

11. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
12. Esaminare il riepilogo, quindi selezionare **fine**.
13. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Clonare un database collegabile

È possibile clonare un database collegabile (PDB) su un CDB di destinazione diverso o uguale sullo stesso host o su un host alternativo. È inoltre possibile ripristinare il PDB clonato a un SCN desiderato o a una data e un'ora.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare **Database** o **Gruppo risorse** dall'elenco Visualizza.
3. Selezionare il database di tipo istanza singola (multitenant).
4. Dalla pagina di visualizzazione Gestisci copie, selezionare il backup dal sistema di storage primario.
5. Selezionare il backup, quindi fare clic su * *  .
6. Nella pagina Nome, selezionare **clone PDB** e specificare gli altri dettagli.
7. Nella pagina posizioni, specificare i dettagli richiesti.
8. Nella pagina Pre-Ops specificare il percorso e gli argomenti dei prescrittori e nella sezione Database Parameter settings (Impostazioni parametri database), modificare i valori dei parametri del database prepopolati utilizzati per inizializzare il database.
9. Nella pagina Post-Ops, per impostazione predefinita è selezionato **Until Cancel** (fino a cancellazione) per eseguire il ripristino del database clonato.

a. Se si seleziona **fino a Annulla**, SnapCenter esegue il ripristino montando l'ultimo backup del registro con la sequenza non interrotta dei registri di archivio dopo il backup dei dati selezionato per la clonazione.

b. Se si seleziona **Data e ora**, SnapCenter ripristina il database fino a una data e a un'ora specificate.

c. Se si seleziona **specifica ubicazioni registro archivio esterno**, SnapCenter identifica e monta il numero ottimale di backup registro in base alla SCN specificata o alla data e all'ora selezionate.

d. Per impostazione predefinita, la casella di controllo **Crea nuovo DBID** è selezionata per generare un numero univoco (DBID) per il database clonato che lo differenzia dal database di origine.

   Deselezionare la casella di controllo se si desidera assegnare il DBID del database di origine al database clonato. In questo scenario, se si desidera registrare il database clonato con il catalogo RMAN esterno in cui il database di origine è già registrato, l'operazione non riesce.

e. Selezionare la casella di controllo **Create tempfile for temporary tablespace** (Crea file tempper tablespace temporanea) se si desidera creare un file temporary tablespace predefinito del database clonato.

f. In **Inserisci voci sql da applicare quando viene creato il clone**, aggiungere le voci sql che si desidera applicare al momento della creazione del clone.

g. In **immettere gli script da eseguire dopo l'operazione di clonazione**, specificare il percorso e gli argomenti del postscript che si desidera eseguire dopo l'operazione di clonazione.

10. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.
11. Esaminare il riepilogo, quindi selezionare **fine**.
12. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Suddividi un clone di un database Oracle

È possibile utilizzare SnapCenter per separare una risorsa clonata dalla risorsa principale. Il clone diviso diventa indipendente dalla risorsa padre.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Database** dall'elenco View (Visualizza).
3. Selezionare la risorsa clonata, ad esempio il database o il LUN, quindi fare clic su * *  .
4. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
5. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Clone separato di un database collegabile

È possibile utilizzare SnapCenter per suddividere un database clonato collegabile (PDB).

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Selezionare il database dei container di origine (CDB) dalla vista delle risorse o dei gruppi di risorse.

3. Nella vista Gestione copie, selezionare **cloni** dai sistemi di archiviazione primari.
4. Selezionare il clone PDB (targetCDB:PDBClone), quindi fare clic su * *  .
5. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
6. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Gestire il server e i plug-in SnapCenter

Visualizza dashboard

Panoramica della dashboard

Dal riquadro di navigazione a sinistra di SnapCenter, la dashboard offre una prima panoramica dello stato del sistema, tra cui attività di lavoro recenti, avvisi, riepilogo della protezione, efficienza e utilizzo dello storage, stato dei processi SnapCenter (backup, clonazione, ripristino), stato della configurazione per host standalone e cluster Windows, Numero di macchine virtuali di storage (SVM) gestite da SnapCenter e capacità di licenza.

Le informazioni visualizzate nella vista Dashboard dipendono dal ruolo assegnato all'utente che ha attualmente effettuato l'accesso a SnapCenter. Alcuni contenuti potrebbero non essere visualizzati se l'utente non dispone dell'autorizzazione per visualizzare tali informazioni.

In molti casi, è possibile visualizzare ulteriori informazioni su un display passando il mouse su **i**. In alcuni casi, le informazioni contenute nella dashboard vengono collegate alle informazioni dettagliate sulla fonte nelle pagine della GUI di SnapCenter, ad esempio risorse, Monitor e Report.

Attività lavorative recenti

Il riquadro attività recenti visualizza l'ultima attività di processo da qualsiasi processo di backup, ripristino e clonazione a cui si dispone dell'accesso. I job in questa schermata presentano uno dei seguenti stati: Completato, Avviso, non riuscito, in esecuzione, in coda, E annullato.

Passando il mouse su un lavoro si ottiene una maggiore quantità di informazioni. È possibile visualizzare ulteriori informazioni sul lavoro facendo clic su un numero di lavoro specifico, che reindirizza l'utente alla pagina Monitor. Da qui, è possibile ottenere dettagli sul lavoro o informazioni di log e generare un report specifico per quel lavoro.

Fare clic su **Visualizza tutto** per visualizzare la cronologia di tutti i job SnapCenter.

Avvisi

Il riquadro Avvisi visualizza gli ultimi avvisi critici e di avviso non risolti per gli host e il server SnapCenter.

Il numero totale di avvisi critici e di categoria di avviso viene visualizzato nella parte superiore del display. Facendo clic sui totali critici o di avviso, viene visualizzata nuovamente la pagina Avvisi con il filtro specifico applicato nella pagina Avvisi.

Facendo clic su un avviso specifico, viene visualizzata nuovamente la pagina Avvisi per ulteriori informazioni sull'avviso. Facendo clic su **Visualizza tutto** nella parte inferiore del display, si viene reindirizzati alla pagina Avvisi per un elenco di tutti gli avvisi.

Riepilogo della protezione più recente

La sezione Riepilogo protezione più recente fornisce lo stato di protezione per tutte le entità a cui si ha accesso. Per impostazione predefinita, il display fornisce lo stato di tutti i plug-in. Vengono fornite informazioni sullo stato delle risorse di cui è stato eseguito il backup sullo storage primario come Snapshot e sullo storage secondario mediante le tecnologie SnapMirror e SnapVault. La disponibilità delle informazioni sullo stato di

protezione per lo storage secondario si basa sul tipo di plug-in selezionato.

Se si utilizza un criterio di protezione del vault mirror, i contatori del riepilogo della protezione vengono visualizzati nel grafico di riepilogo di SnapVault e non nel grafico di SnapMirror.

Lo stato di protezione dei singoli plug-in è disponibile selezionando un plug-in dal menu a discesa. Un grafico a ciambelle mostra la percentuale di risorse protette per il plug-in selezionato. Facendo clic su una sezione ciambella si torna alla pagina **rapporti** > **Plug-in**, che fornisce un report dettagliato di tutte le attività di storage primarie e secondarie per il plug-in specificato.

I report sullo storage secondario sono validi solo per SnapVault; i report SnapMirror non sono supportati.

SAP HANA fornisce informazioni sullo stato di protezione per lo storage primario e secondario per le Snapshot. Per i backup basati su file è disponibile solo lo stato di protezione dello storage primario.

Stato di protezione	Storage primario	Storage secondario
Non riuscito	Numero di entità che fanno parte di un gruppo di risorse, in cui il gruppo di risorse ha eseguito un backup, ma il backup non è riuscito.	Numero di entità con backup che non sono riusciti a trasferire a una destinazione secondaria.
Riuscito	Numero di entità in un gruppo di risorse, in cui è stato eseguito correttamente il backup del gruppo di risorse.	Numero di entità con backup che sono stati trasferiti correttamente a una destinazione secondaria.
Non configurato	Numero di entità che non fanno parte di alcun gruppo di risorse e che non sono state sottoposte a backup.	Numero di entità che fanno parte di uno o più gruppi di risorse non configurati per i backup da trasferire a una destinazione secondaria.
Non avviato	Numero di entità che fanno parte di un gruppo di risorse, ma non è stato eseguito alcun backup.	Non applicabile.

Se si utilizza SnapCenter Server 4.2 e una versione precedente del plug-in (precedente alla 4.2) per creare i backup, la sezione **Riepilogo protezione più recente** non visualizza lo stato di protezione di questi backup.

Lavori

La sezione lavori fornisce un riepilogo dei processi di backup, ripristino e clonazione a cui si ha accesso. È possibile personalizzare l'intervallo di tempo per qualsiasi report utilizzando il menu a discesa. Le opzioni relative all'intervallo di tempo sono fisse alle ultime 24 ore, agli ultimi 7 giorni e agli ultimi 30 giorni. Il report predefinito mostra i processi di protezione dei dati eseguiti negli ultimi 7 giorni.

Le informazioni sul processo di backup, ripristino e clonazione vengono visualizzate nei grafici a nastro. Facendo clic su una sezione ciambella si viene reindirizzati alla pagina Monitor con i filtri dei job pre-applicati alla selezione.

Stato del lavoro	Descrizione
Non riuscito	Numero di lavori non riusciti.
Attenzione	Numero di lavori che hanno riscontrato un errore.
Riuscito	Numero di lavori completati correttamente.
In esecuzione	Numero di processi attualmente in esecuzione.

Storage

Il riquadro Storage visualizza lo storage primario e secondario consumato dai processi di protezione in un periodo di 90 giorni, illustra graficamente le tendenze di consumo e calcola i risparmi dello storage primario. Le informazioni sullo storage vengono aggiornate ogni 24 ore alle 12

Il consumo totale giornaliero, che comprende il numero totale di backup disponibili in SnapCenter e le dimensioni occupate da questi backup, viene visualizzato nella parte superiore del display. A un backup possono essere associati più snapshot, il conteggio rifletterà lo stesso. Ciò è applicabile agli snapshot primari e secondari. Ad esempio, sono stati creati 10 backup, di cui 2 eliminati a causa della conservazione dei backup basata su policy e 1 eliminato esplicitamente dall'utente. In questo modo, viene visualizzato il numero di 7 backup insieme alle dimensioni occupate da questi 7 backup.

Il fattore di risparmio dello storage per lo storage primario è il rapporto tra la capacità logica (risparmi di cloni e Snapshot, più lo storage consumato) e la capacità fisica dello storage primario. Un grafico a barre illustra i risparmi in termini di storage.

Il grafico a linee traccia separatamente il consumo di storage primario e secondario su base giornaliera in un periodo di 90 giorni. Passando il mouse sui grafici si ottengono risultati dettagliati, giorno per giorno.

Se si utilizza SnapCenter Server 4.2 e una versione precedente del plug-in (precedente alla 4.2) per creare i backup, il riquadro **Storage** non visualizza il numero di backup, lo storage utilizzato da questi backup, i risparmi Snapshot, i risparmi sui cloni e le dimensioni di Snapshot.

Configurazione

Il riquadro Configurazione fornisce informazioni consolidate sullo stato di tutti gli host cluster Windows e standalone attivi gestiti da SnapCenter e a cui si dispone dell'accesso. Sono incluse le informazioni sullo stato del plug-in associato a tali host.

Facendo clic sul numero accanto agli host, si viene reindirizzati alla sezione Managed hosts della pagina hosts. Da qui, è possibile ottenere informazioni dettagliate per un host selezionato.

Inoltre, questa schermata mostra la somma delle SVM standalone di ONTAP e delle SVM di Cluster ONTAP gestite da SnapCenter e a cui si dispone dell'accesso. Facendo clic sul numero accanto a SVM si accede nuovamente alla pagina Storage Systems (sistemi storage). Da qui, è possibile ottenere informazioni dettagliate per una SVM selezionata.

Lo stato di configurazione dell'host viene visualizzato come rosso (critico), giallo (avviso) e verde (attivo), insieme al numero di host in ogni stato. I messaggi di stato vengono forniti per ogni stato.

Stato della configurazione	Descrizione
Aggiornamento obbligatorio	Numero di host che eseguono plug-in non supportati e che necessitano di un aggiornamento. Un plug-in non supportato non è compatibile con questa versione di SnapCenter.
Migrazione obbligatoria	Numero di host che eseguono plug-in non supportati e che necessitano di migrazione. Un plug-in non supportato non è compatibile con questa versione di SnapCenter.
Nessun plug-in installato	Numero di host aggiunti correttamente, ma i plug-in devono essere installati o l'installazione dei plug-in non è riuscita.
Sospeso	Numero di host le cui pianificazioni sono sospese e in manutenzione.
Interrotto	Numero di host attivi, ma i servizi plug-in non sono in esecuzione.
Host inattivo	Numero di host non disponibili o non raggiungibili.
Aggiornamento disponibile (opzionale)	Numero di host in cui è disponibile una versione più recente del pacchetto plug-in per l'aggiornamento.
Migrazione disponibile (opzionale)	Numero di host in cui è disponibile una versione più recente del plug-in per la migrazione.
Configurare la directory del registro	Numero di host in cui è necessario configurare la directory di log per consentire a SCSQL di eseguire il backup del log delle transazioni.
Configurare i plug-in VMware	Numero di host in cui è necessario aggiungere il plug-in SnapCenter per VMware vSphere.
Sconosciuto	Numero di host che sono stati registrati ma l'installazione non è stata ancora attivata.
In esecuzione	Numero di host attivi e plug-in in esecuzione. Inoltre, nel caso dei plug-in SCSQL, vengono configurate directory di log e hypervisor.
Installazione/disinstallazione dei plug-in	Numero di host in cui è in corso l'installazione o la disinstallazione del plug-in.

Capacità concessa in licenza

Il riquadro capacità concessa in licenza visualizza informazioni sulla capacità totale concessa in licenza, sulla capacità utilizzata, sugli avvisi di soglia della capacità e sugli avvisi di scadenza della licenza per le licenze basate sulla capacità standard di SnapCenter.

Questa schermata viene visualizzata solo se si utilizzano licenze basate sulla capacità standard di SnapCenter su piattaforme Cloud Volumes ONTAP o ONTAP Select. Per le piattaforme FAS, AFF o All SAN Array (ASA), la licenza SnapCenter è basata su controller e concessa in licenza per capacità illimitata e non è richiesta alcuna licenza per capacità.

Stato della licenza	Descrizione
In uso	Quantità di capacità attualmente in uso.
Notifica	Soglia di capacità alla quale vengono visualizzate le notifiche sul Dashboard e, se configurata, all'invio delle notifiche via email.
Concesso in licenza	Quantità di capacità concessa in licenza.
Finito	Quantità di capacità che ha superato la capacità concessa in licenza.

Come visualizzare le informazioni sulla dashboard

Dal riquadro di navigazione sinistro di SnapCenter, è possibile visualizzare vari riquadri o display del dashboard, insieme ai dettagli del sistema associati. Il numero di display disponibili nella dashboard è fisso e non può essere modificato. Il contenuto fornito all'interno di ogni display dipende dal RBAC (role-based access control).

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Dashboard**.
2. Fare clic sulle aree attive su ciascun display per ottenere ulteriori informazioni.

   Ad esempio, facendo clic su un grafico in **Jobs**, si reindirizza alla pagina Monitor per ulteriori informazioni sulla selezione. Facendo clic su un grafico in **Riepilogo protezione**, si accede nuovamente alla pagina Report, che fornisce ulteriori informazioni sulla selezione.

Richiedere i report di stato dei lavori dalla dashboard

È possibile richiedere report sui processi di backup, ripristino e clonazione dalla pagina Dashboard. Questa opzione è utile se si desidera identificare il numero totale di processi riusciti o non riusciti nell'ambiente SnapCenter.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Dashboard**

2. Individuare il riquadro lavori nella dashboard, quindi selezionare **Backup**, **Ripristina** o **Clone**.
3. Dal menu a discesa, selezionare l'intervallo di tempo per il quale si desidera specificare le informazioni relative ai lavori: 24 ore, 7 giorni o 30 giorni.

   I sistemi visualizzano un grafico a ciambelle che copre i dati.

4. Fare clic sulla sezione che rappresenta le informazioni sul lavoro per cui si desidera creare un report.

   Facendo clic sul grafico a ciambelle, si viene reindirizzati dalla pagina Dashboard alla pagina Monitor. La pagina Monitor visualizza i lavori con lo stato selezionato dal grafico a ciambelle.

5. Dall'elenco della pagina Monitor, fare clic su un job specifico per selezionarlo.
6. Nella parte superiore della pagina Monitor, fare clic su **Report**.

Risultato

Il report visualizza le informazioni solo per il lavoro selezionato. È possibile rivedere il report o scaricarlo sul sistema locale.

Richiedere report sullo stato della protezione dalla dashboard

È possibile richiedere dettagli di protezione per le risorse gestite da plug-in specifici utilizzando la dashboard. Solo i backup dei dati vengono presi in considerazione per il riepilogo della protezione dei dati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Dashboard**.
2. Individuare la sezione Riepilogo protezione più recente nel dashboard e utilizzare il menu a discesa per selezionare un plug-in.

   La dashboard visualizza un grafico delle risorse di cui è stato eseguito il backup sullo storage primario e, se applicabile al plug-in, un grafico delle risorse di cui è stato eseguito il backup sullo storage secondario.

   I report sulla protezione dei dati sono disponibili solo per tipi di plug-in specifici. Specificare **tutti i plug-in** non è supportato.

3. Fare clic sulla sezione che rappresenta lo stato per il quale si desidera creare un report.

   Facendo clic sul grafico DONUT, si viene reindirizzati dalla pagina Dashboard ai report e quindi alla pagina Plug-in. Il report visualizza solo lo stato del plug-in selezionato. È possibile rivedere il report o scaricarlo sul sistema locale.

   Il reindirizzamento alla pagina Report per il diagramma di controllo di SnapMirror e il backup SAP HANA basato su file non è supportato.

Manage RBAC (Gestisci SNMP)

SnapCenter consente di modificare ruoli, utenti e gruppi.

Modificare un ruolo

È possibile modificare un ruolo SnapCenter per rimuovere utenti o gruppi e modificare le autorizzazioni associate al ruolo. È particolarmente utile modificare i ruoli quando si desidera modificare o eliminare le autorizzazioni utilizzate da un intero ruolo.

Prima di iniziare

È necessario aver effettuato l'accesso come ruolo "SnapCenterAdmin".

Non è possibile modificare o rimuovere le autorizzazioni per il ruolo SnapCenterAdmin.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **ruoli**.
3. Nel campo role name (Nome ruolo), fare clic sul ruolo che si desidera modificare.
4. Nella pagina Role Details (Dettagli ruolo) modificare le autorizzazioni o annullare l'assegnazione dei membri in base alle necessità.
5. Selezionare **tutti i membri di questo ruolo possono visualizzare gli oggetti degli altri membri** per consentire agli altri membri del ruolo di visualizzare risorse come volumi e host dopo l'aggiornamento dell'elenco delle risorse.

   Deselezionare questa opzione se non si desidera che i membri di questo ruolo vedano gli oggetti a cui sono assegnati altri membri.

   Quando questa opzione è attivata, l'assegnazione dell'accesso degli utenti agli oggetti o alle risorse non è necessaria se gli utenti appartengono allo stesso ruolo dell'utente che ha creato gli oggetti o le risorse.

6. Fare clic su **Invia**.

Modificare utenti e gruppi

È possibile modificare gli utenti o i gruppi di SnapCenter per modificarne i ruoli e le risorse.

Prima di iniziare

Devi essere connesso come amministratore di SnapCenter.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **utenti e accesso**.
3. Dall'elenco Nome utente o gruppo, fare clic sull'utente o sul gruppo che si desidera modificare.
4. Nella pagina User (utente) o Group Details (Dettagli gruppo), modificare ruoli e risorse.
5. Fare clic su **Invia**.

Gestire gli host

È possibile aggiungere host e installare pacchetti di plug-in SnapCenter, aggiungere un server di verifica, rimuovere host, migrare processi di backup e aggiornare host per aggiornare pacchetti di plug-in o aggiungere nuovi pacchetti di plug-in. A seconda del plug-in utilizzato, è possibile eseguire il provisioning dei dischi, gestire le condivisioni SMB, gestire i gruppi di iniziatori (igroups), gestire le sessioni iSCSI e migrare i dati.

È possibile eseguire queste attività…	**Per Microsoft Exchange Server**	**Per Microsoft SQL Server**	**Per Microsoft Windows**	**Per database Oracle**	**Per SAP HANA Database**	**Per plug-in personalizzati**
Aggiungere host e installare il pacchetto plug-in	Sì	Sì	Sì	Sì	Sì	Sì
Aggiornare le informazioni ESXi per un host	No	Sì	No	No	No	No
Sospendere le pianificazioni e mettere gli host in modalità di manutenzione	Sì	Sì	Sì	Sì	Sì	Sì
Modificare gli host aggiungendo, aggiornando o rimuovendo i plug-in	Sì	Sì	Sì	Sì	Sì	Sì
Rimuovere gli host da SnapCenter	Sì	Sì	Sì	Sì	Sì	Sì
Avviare i servizi plug-in	Sì	Sì	Sì	Sì	Sì	Sì
Eseguire il provisioning dei dischi	No	No	Sì	No	No	No

È possibile eseguire queste attività…	Per Microsoft Exchange Server	Per Microsoft SQL Server	Per Microsoft Windows	Per database Oracle	Per SAP HANA Database	Per plug-in personalizzati
Gestire le condivisioni SMB	No	No	Sì	No	No	No
Gestire iGroups	No	No	Sì	No	No	No
Gestire le sessioni iSCSI	No	No	Sì	No	No	

Aggiorna le informazioni della macchina virtuale

È necessario aggiornare le informazioni della macchina virtuale quando si modificano le credenziali di VMware vCenter o si riavvia l'host del database o del file system. L'aggiornamento delle informazioni della macchina virtuale in SnapCenter avvia la comunicazione con VMware vSphere vCenter e ottiene le credenziali vCenter.

I dischi basati su RDM sono gestiti dal plug-in SnapCenter per Microsoft Windows, installato sull'host del database. Per gestire gli RDM, il plug-in SnapCenter per Microsoft Windows comunica con il server vCenter che gestisce l'host del database.

Fasi

1. Nel riquadro di navigazione sinistro di SnapCenter, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Nella pagina Managed hosts (host gestiti), selezionare l'host che si desidera aggiornare.
4. Fare clic su **Aggiorna VM**.

Modificare gli host dei plug-in

Dopo aver installato un plug-in, è possibile modificare i dettagli degli host del plug-in, se necessario. È possibile modificare le credenziali, il percorso di installazione, i plug-in, i dettagli della directory di log per il plug-in SnapCenter per Microsoft SQL Server, l'account di servizio gestito di gruppo (gMSA) e la porta del plug-in.

Assicurarsi che la versione del plug-in sia la stessa della versione del server SnapCenter.

A proposito di questa attività

- È possibile modificare una porta del plug-in solo dopo l'installazione del plug-in.

  Non è possibile modificare la porta del plug-in durante le operazioni di aggiornamento.

- Durante la modifica di una porta plug-in, è necessario conoscere i seguenti scenari di rollback delle porte:
  - In un'installazione standalone, se SnapCenter non riesce a modificare la porta di uno dei componenti, l'operazione non riesce e la vecchia porta viene conservata per tutti i componenti.

Se la porta è stata modificata per tutti i componenti ma uno dei componenti non inizia con la nuova porta, la vecchia porta viene conservata per tutti i componenti. Ad esempio, se si desidera modificare la porta per due plug-in sull'host standalone e SnapCenter non applica la nuova porta a uno dei plug-in, l'operazione non riesce (con un messaggio di errore appropriato) e la vecchia porta viene conservata per entrambi i plug-in.

- In un'installazione in cluster, se SnapCenter non riesce a modificare la porta del plug-in installato su uno dei nodi, l'operazione non riesce e la vecchia porta viene conservata per tutti i nodi.

  Ad esempio, se il plug-in viene installato su quattro nodi in un'installazione in cluster e se la porta non viene modificata per uno dei nodi, la vecchia porta viene mantenuta per tutti i nodi.

Quando i plug-in vengono installati con gMSA, è possibile modificarli nelle finestre **altre opzioni**. Quando i plug-in vengono installati senza gMSA, è possibile specificare l'account gMSA da utilizzare come account del servizio plug-in.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Verificare che l'opzione **Managed hosts** sia selezionata nella parte superiore.
3. Selezionare l'host per il quale si desidera modificare e modificare un campo qualsiasi.

   È possibile modificare un solo campo alla volta.
4. Fare clic su **Invia**.

Risultato

L'host viene validato e aggiunto al server SnapCenter.

Avviare o riavviare i servizi plug-in

L'avvio dei servizi plug-in di SnapCenter consente di avviare i servizi se non sono in esecuzione o di riavviarli se sono in esecuzione. Potrebbe essere necessario riavviare i servizi dopo aver eseguito la manutenzione.

Al riavvio dei servizi, assicurarsi che non siano in esecuzione processi.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Nella pagina Managed hosts (host gestiti), selezionare l'host che si desidera avviare.
4. Fare clic  sull'icona e fare clic su **Avvia servizio** o **Riavvia servizio**.

   È possibile avviare o riavviare il servizio di più host contemporaneamente.

Sospendere le pianificazioni per la manutenzione dell'host

Se si desidera impedire all'host di eseguire qualsiasi processo pianificato SnapCenter, è possibile impostare l'host in modalità di manutenzione. Questa operazione deve essere eseguita prima di aggiornare i plug-in o se si eseguono attività di manutenzione sugli host.

Non è possibile sospendere le pianificazioni su un host inattivo perché SnapCenter non è in grado di comunicare con tale host.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Nella pagina Managed hosts (host gestiti), selezionare l'host che si desidera sospendere.
4. Fare clic sull' icona, quindi fare clic su **Sospendi pianificazione** per impostare l'host per il plug-in in modalità di manutenzione.

   È possibile sospendere la pianificazione di più host contemporaneamente.

   Non è necessario interrompere prima il servizio plug-in. Il servizio plug-in può essere in esecuzione o arrestato.

Risultato

Dopo aver sospeso le pianificazioni sull'host, la pagina Managed hosts (host gestiti) mostra **Suspended** nel campo di stato generale dell'host.

Una volta completata la manutenzione dell'host, è possibile disattivare la modalità di manutenzione dell'host facendo clic su **Activate Schedule** (attiva pianificazione). È possibile attivare la pianificazione di più host contemporaneamente.

Operazioni supportate dalla pagina risorse

È possibile individuare le risorse ed eseguire operazioni di protezione dei dati dalla pagina risorse. Le operazioni che è possibile eseguire variano in base al plug-in utilizzato per gestire le risorse.

Dalla pagina risorse, è possibile eseguire le seguenti operazioni:

È possibile eseguire queste attività…	Per Microsoft Exchange Server	Per Microsoft SQL Server	Per Microsoft Windows	Per database Oracle	Per SAP HANA Database	Per plug-in personalizzati
Determinare se le risorse sono disponibili per il backup	Sì	Sì	Sì	Sì	Sì	Sì
Eseguire il backup on-demand di una risorsa	Sì	Sì	Sì	Sì	Sì	Sì

È possibile eseguire queste attività…	Per Microsoft Exchange Server	Per Microsoft SQL Server	Per Microsoft Windows	Per database Oracle	Per SAP HANA Database	Per plug-in personalizzati
Ripristinare dai backup	Sì	Sì	Sì	Sì	Sì	Sì
Clonare i backup	No	Sì	Sì	Sì	Sì	Sì
Gestire i backup	Sì	Sì	Sì	Sì	Sì	Sì
Gestire i cloni	No	Sì	Sì	Sì	Sì	Sì
Gestire le policy	Sì	Sì	Sì	Sì	Sì	Sì
Gestire le connessioni storage	Sì	Sì	Sì	Sì	Sì	Sì
Montare i backup	No	No	No	Sì	No	No
Smontare i backup	No	No	No	Sì	No	No
Visualizza i dettagli	Sì	Sì	Sì	Sì	Sì	Sì

Gestire le policy

È possibile scollegare i criteri da una risorsa o da un gruppo di risorse, modificarli, eliminarli, visualizzarli e copiarli.

Modificare i criteri

È possibile modificare le opzioni di replica, le impostazioni di conservazione di Snapshot, il conteggio dei tentativi di errore o le informazioni sugli script mentre un criterio è collegato a una risorsa o a un gruppo di risorse. È possibile modificare il tipo di pianificazione (frequenza) solo dopo aver disaccoppiato un criterio.

A proposito di questa attività

La modifica del tipo di pianificazione in un criterio richiede operazioni aggiuntive, in quanto il server SnapCenter registra il tipo di pianificazione solo nel momento in cui il criterio viene associato a una risorsa o a un gruppo di risorse.

Se si desidera…	Quindi…
Aggiungere un tipo di pianificazione aggiuntivo	Creare una nuova policy e allegarla alle risorse o ai gruppi di risorse necessari. Ad esempio, se un criterio del gruppo di risorse specifica solo i backup orari e si desidera aggiungere anche i backup giornalieri, è possibile creare un criterio con un tipo di pianificazione giornaliera e aggiungerlo al gruppo di risorse. Il gruppo di risorse avrebbe quindi due criteri: orario e giornaliero.
Rimuovere o modificare un tipo di pianificazione	Effettuare le seguenti operazioni: 1. Scollegare la policy da ogni risorsa e gruppo di risorse che utilizza tale policy. 2. Modificare il tipo di pianificazione. 3. Associare nuovamente il criterio a tutte le risorse e a tutti i gruppi di risorse. Ad esempio, se un criterio specifica i backup orari e si desidera modificarli in backup giornalieri, è necessario prima scollegare il criterio.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare il criterio, quindi fare clic su **Modify** (Modifica).
4. Modificare le informazioni, quindi fare clic su **fine**.

Scollegare le policy

È possibile scollegare le policy da una risorsa o da un gruppo di risorse ogni volta che non si desidera più che tali policy regolino la protezione dei dati per le risorse. È necessario scollegare un criterio prima di poterlo eliminare o prima di modificare il tipo di pianificazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).
3. Selezionare il gruppo di risorse, quindi fare clic su **Modify Resource Group** (Modifica gruppo di risorse).
4. Nella pagina Criteri della procedura guidata Modifica gruppo di risorse, dall'elenco a discesa, deselezionare il segno di spunta accanto ai criteri che si desidera scollegare.
5. Apportare eventuali modifiche aggiuntive al gruppo di risorse nel resto della procedura guidata, quindi fare clic su **fine**.

Eliminare i criteri

Se non sono più necessarie policy, è possibile eliminarle.

Prima di iniziare

Se il criterio è associato a qualsiasi risorsa o gruppo di risorse, è necessario scollegarlo dai gruppi di risorse o risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare il criterio, quindi fare clic su **Delete** (Elimina).
4. Fare clic su **Sì**.

Gestire i gruppi di risorse

È possibile eseguire varie operazioni sui gruppi di risorse.

È possibile eseguire le seguenti attività relative ai gruppi di risorse:

- Modificare un gruppo di risorse selezionando il gruppo di risorse e facendo clic su **Modify Resource Group** (Modifica gruppo di risorse) per modificare le informazioni fornite durante la creazione del gruppo di risorse.

  È possibile modificare la pianificazione durante la modifica del gruppo di risorse. Tuttavia, per modificare il tipo di pianificazione è necessario modificare il criterio.

  Se si rimuovono risorse da un gruppo di risorse, le impostazioni di conservazione del backup definite nei criteri attualmente associati al gruppo di risorse continueranno ad essere applicate alle risorse rimosse.

- Creare un backup di un gruppo di risorse.
- Creare un clone di un backup.

  È possibile clonare dai backup esistenti di SQL, Oracle, file system Windows, applicazioni personalizzate e risorse di database SAP HANA o gruppi di risorse.

- Creare un clone di un gruppo di risorse.

  Questa operazione è supportata solo per i gruppi di risorse SQL (che contengono solo database). È possibile configurare una pianificazione per la clonazione di un gruppo di risorse (ciclo di vita dei cloni).

- Impedire l'avvio delle operazioni pianificate sui gruppi di risorse.
- Eliminare un gruppo di risorse.

Interrompere e riprendere le operazioni sui gruppi di risorse

È possibile disattivare temporaneamente l'avvio delle operazioni pianificate su un gruppo di risorse. In un secondo momento, è possibile attivare tali operazioni.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).
3. Selezionare il gruppo di risorse e fare clic su **manutenzione**.
4. Fare clic su **OK**.

Se si desidera riprendere le operazioni sul gruppo di risorse attivato in modalità di manutenzione, selezionare il gruppo di risorse e fare clic su **produzione**.

Eliminare i gruppi di risorse

È possibile eliminare un gruppo di risorse se non è più necessario proteggere le risorse del gruppo di risorse. Prima di rimuovere i plug-in da SnapCenter, è necessario assicurarsi che i gruppi di risorse vengano eliminati.

A proposito di questa attività

È necessario eliminare manualmente tutti i cloni creati per qualsiasi risorsa del gruppo di risorse. È possibile facoltativamente forzare l'eliminazione di tutti i backup, i metadati, le policy e gli Snapshot associati al gruppo di risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).
3. Selezionare il gruppo di risorse, quindi fare clic su **Elimina**.
4. Facoltativo: Selezionare la casella di controllo **Elimina backup e scollega criteri associati a questo gruppo di risorse** per rimuovere tutti i backup, i metadati, i criteri e le istantanee associati al gruppo di risorse.
5. Fare clic su **OK**.

Gestire i backup

È possibile rinominare ed eliminare i backup. È inoltre possibile eliminare più backup contemporaneamente.

Rinominare i backup

È possibile rinominare i backup se si desidera fornire un nome migliore per migliorare la ricerca.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.

3. Selezionare la risorsa o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina della topologia di risorse o gruppi di risorse. Se la risorsa o il gruppo di risorse non è configurato per la protezione dei dati, viene visualizzata la procedura guidata di protezione invece della pagina della topologia.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primari.

   Non è possibile rinominare i backup presenti nel sistema di storage secondario.

   Se i backup dei database Oracle sono stati catalogati utilizzando Oracle Recovery Manager (RMAN), non è possibile rinominare i backup catalogati.

5. Selezionare il backup, quindi fare clic su  .
6. Nel campo **Rinomina backup come**, immettere un nuovo nome e fare clic su **OK**.

Eliminare i backup

È possibile eliminare i backup se non è più necessario eseguire il backup per altre operazioni di protezione dei dati.

Prima di iniziare

È necessario eliminare i cloni associati prima di eliminare un backup.

Se un backup è associato a una risorsa clonata, non è possibile eliminarlo.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina della topologia di risorse o gruppi di risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primari.

   Non è possibile eliminare i backup presenti nel sistema di storage secondario.

5. Selezionare il backup, quindi fare clic su  .

   Se si elimina un backup del database SAP HANA, vengono eliminati anche i cataloghi SAP HANA associati al backup.

   Se l'ultimo backup rimanente viene eliminato, le voci del catalogo HANA associate non possono essere eliminate.

6. Fare clic su **OK**.

Se si dispone di backup di database obsoleti in SnapCenter che non dispongono di backup corrispondenti sul sistema di storage, è necessario utilizzare il comando remove-smbackup per ripulire queste voci di backup obsolete. Se i backup obsoleti sono stati catalogati, verranno discatalogati dal database del catalogo di ripristino.

Rimuovere la protezione

Rimuovi protezione elimina tutti i backup e scollega tutti i criteri. Prima di rimuovere la protezione, è necessario assicurarsi che i backup non siano montati e che nessun clone sia associato al backup.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina della topologia di risorse o gruppi di risorse.

4. Selezionare il backup e fare clic su **Rimuovi protezione**.

Eliminare i cloni

È possibile eliminare i cloni se non sono più necessari.

A proposito di questa attività

Non è possibile eliminare cloni che agiscono come origine per altri cloni.

Ad esempio, se il database di produzione è db1, il clono1 del database viene clonato dal backup di db1 e successivamente il clono1 viene protetto. Il clone2 del database viene clonato dal backup del clone1. Se si decide di eliminare il clone1, è necessario prima eliminare il clone2, quindi eliminarlo.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **cloni** dai sistemi di storage primario o secondario (mirrorati o replicati).
5. Selezionare il clone, quindi fare clic su  .

   Se si stanno eliminando i cloni del database SAP HANA, nella pagina Delete Clone (Elimina clone), eseguire le seguenti operazioni:

   a. Nel campo **Pre clone delete**, immettere i comandi da eseguire prima di eliminare il clone.

b. Nel campo **Unmount**, immettere il comando per smontare il clone prima di eliminarlo.

6. Fare clic su **OK**.

Al termine

A volte i file system non vengono cancellati. È necessario aumentare il valore del parametro CLONE_DELETE_DELAY eseguendo il seguente comando: `./sccli Set-SmConfigSettings`

> Il parametro CLONE_DELETE_DELAY specifica il numero di secondi di attesa dopo il completamento dell'eliminazione del clone dell'applicazione e prima di iniziare l'eliminazione del file system.

Dopo aver modificato il valore del parametro, riavviare il servizio caricatore plug-in (SPL) di SnapCenter.

Monitoraggio di processi, pianificazioni, eventi e registri

È possibile monitorare l'avanzamento dei lavori, ottenere informazioni sui lavori pianificati e rivedere eventi e registri dalla pagina Monitor.

Monitorare i lavori

È possibile visualizzare informazioni sui processi di backup, clonazione, ripristino e verifica di SnapCenter. È possibile filtrare questa visualizzazione in base alla data di inizio e di fine, al tipo di processo, al gruppo di risorse, alla policy o al plug-in SnapCenter. È inoltre possibile ottenere ulteriori dettagli e file di registro per i lavori specificati.

È inoltre possibile monitorare i lavori relativi alle operazioni di SnapMirror e SnapVault.

> È possibile monitorare solo i lavori creati e rilevanti per l'utente, a meno che non venga assegnato un ruolo di amministratore SnapCenter o un altro ruolo di super utente.

È possibile eseguire le seguenti attività relative ai lavori di monitoraggio:

- Monitorare le operazioni di backup, clonazione, ripristino e verifica.
- Visualizzare i dettagli e i report relativi al lavoro.
- Interrompere un processo pianificato.

Monitorare le pianificazioni

È possibile visualizzare le pianificazioni correnti per determinare quando l'operazione viene avviata, quando è stata eseguita l'ultima volta e quando viene eseguita successivamente. È inoltre possibile determinare l'host su cui viene eseguita l'operazione, insieme alle informazioni sul gruppo di risorse e sui criteri dell'operazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Schedules**.
3. Selezionare il gruppo di risorse e il tipo di pianificazione.
4. Visualizzare l'elenco delle operazioni pianificate.

Monitorare gli eventi

È possibile visualizzare un elenco di eventi SnapCenter nel sistema, ad esempio quando un utente crea un gruppo di risorse o quando il sistema avvia attività, ad esempio la creazione di un backup pianificato. È possibile visualizzare gli eventi per determinare se è in corso un'operazione come un'operazione di backup o ripristino.

A proposito di questa attività

Tutte le informazioni sul lavoro vengono visualizzate nella pagina Eventi. Ad esempio, all'avvio di un processo di backup, viene visualizzato un evento "backup start". Al termine del backup, viene visualizzato un evento "backup complete".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Eventi**.
3. (Facoltativo) nella casella Filter (filtro), inserire la data di inizio o di fine, la categoria dell'evento (ad esempio backup, gruppo di risorse o policy) e il livello di severità, quindi fare clic su **Apply** (Applica). In alternativa, inserire i caratteri nella casella Cerca.
4. Visualizzare l'elenco degli eventi.

Registri di monitoraggio

È possibile visualizzare e scaricare i log del server SnapCenter, i log dell'agente host SnapCenter e i log dei plug-in. È possibile visualizzare i registri per agevolare la risoluzione dei problemi.

A proposito di questa attività

È possibile filtrare i registri in modo da visualizzare solo un livello di severità del registro specifico:

- Debug
- Info
- Attenzione
- Errore
- Fatale

È inoltre possibile ottenere registri dei livelli di lavoro, ad esempio registri che consentono di risolvere i problemi relativi al motivo di un errore del processo di backup. Per i registri dei livelli di lavoro, utilizzare l'opzione **Monitor** > **Jobs**.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina lavori, selezionare un lavoro e fare clic su Scarica registri.

   La cartella zippata scaricata contiene i log dei lavori e i log comuni. Il nome della cartella zippata contiene l'id lavoro e il tipo di lavoro selezionato.

3. Nella pagina Monitor, fare clic su **Logs**.
4. Selezionare il tipo di log, l'host e l'istanza.

Se si seleziona il tipo di registro come **plugin**, è possibile selezionare un host o un plug-in SnapCenter. Non è possibile eseguire questa operazione se il tipo di registro è **server**.

5. Per filtrare i registri in base a un'origine, messaggio o livello di registro specifico, fare clic sull'icona del filtro nella parte superiore dell'intestazione della colonna.

   Per visualizzare tutti i registri, scegliere **maggiore di o uguale a** come `Debug` livello.

6. Fare clic su **Aggiorna**.
7. Visualizzare l'elenco dei registri.
8. Fare clic su **Download** per scaricare i registri.

   La cartella zippata scaricata contiene i log dei lavori e i log comuni. Il nome della cartella zippata contiene l'id lavoro e il tipo di lavoro selezionato.

Nelle configurazioni di grandi dimensioni per ottenere prestazioni ottimali, è necessario impostare le impostazioni di log per SnapCenter su un livello minimo utilizzando il cmdlet PowerShell.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```

Per accedere alle informazioni di integrità o configurazione al termine di un processo di failover, eseguire il cmdlet `Get-SmRepositoryConfig`.

Rimuovere job e log da SnapCenter

È possibile rimuovere i log e i processi di backup, ripristino, clonazione e verifica da SnapCenter. SnapCenter memorizza i log dei processi riusciti e non riusciti a tempo indeterminato, a meno che non vengano rimossi. Potrebbe essere necessario rimuoverli per riempire lo storage.

A proposito di questa attività

Non devono essere presenti lavori attualmente in funzione. È possibile rimuovere un lavoro specifico fornendo un ID lavoro oppure rimuovere i lavori entro un periodo specificato.

Non è necessario impostare l'host in modalità di manutenzione per rimuovere i lavori.

Fasi

1. Avviare PowerShell.
2. Dal prompt dei comandi, immettere: `Open-SMConnection`
3. Dal prompt dei comandi, immettere: `Remove-SmJobs`
4. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
5. Nella pagina Monitor, fare clic su **Jobs**.
6. Nella pagina lavori, controllare lo stato del lavoro.

Informazioni correlate

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Panoramica delle funzionalità di reporting di SnapCenter

SnapCenter offre una vasta gamma di opzioni di reporting che consentono di monitorare e gestire lo stato di salute del sistema e il successo delle operazioni.

Tipo di report	Descrizione
Report di backup	Il report di backup fornisce dati generali sui trend di backup per l'ambiente SnapCenter, sulla percentuale di successo del backup e alcune informazioni su ciascun backup eseguito durante il tempo specificato. Se un backup viene eliminato, il report non visualizza alcuna informazione di stato per il backup cancellato. Il report dettagliato del backup fornisce informazioni dettagliate su un processo di backup specificato ed elenca le risorse di cui è stato eseguito il backup e le eventuali risorse non riuscite.
Clona report	Il report sui cloni fornisce dati generali sulle tendenze dei cloni per l'ambiente SnapCenter, sulla percentuale di successo dei cloni e alcune informazioni su ciascun processo di cloni eseguito durante il tempo specificato. Se un clone viene cancellato, il report non visualizza alcuna informazione di stato per il clone cancellato. Il Clone Detail Report fornisce informazioni dettagliate sullo stato delle attività del clone, dell'host clone e del processo clone specificati. Se un'attività non riesce, il Report dettagli clone visualizza le informazioni relative all'errore.
Ripristina report	Il rapporto di ripristino fornisce informazioni generali sui processi di ripristino. Il report dei dettagli di ripristino fornisce dettagli su un processo di ripristino specificato, tra cui nome host, nome del backup, inizio e durata del processo e stato delle singole attività del processo. Se un'attività non riesce, il report dei dettagli di ripristino visualizza le informazioni relative all'errore.
Report sulla protezione	Questi report forniscono dettagli di protezione per le risorse gestite da tutte le istanze di plug-in SnapCenter. Questo report fornisce dettagli sulla protezione per le risorse gestite da tutte le istanze di plug-in. È possibile visualizzare una panoramica, i dettagli delle risorse non protette, le risorse di cui non è stato eseguito il backup al momento della generazione del report, le risorse di un gruppo di risorse per cui le operazioni di backup non sono riuscite e lo stato di SnapVault.

Tipo di report	Descrizione
Report pianificato	Questi report sono pianificati per essere eseguiti periodicamente, ad esempio ogni giorno, ogni settimana o ogni mese. I report vengono generati automaticamente in base alla data e all'ora specificate e vengono inviati alle rispettive persone tramite e-mail È possibile attivare, disattivare, modificare o eliminare le pianificazioni. La pianificazione abilitata può essere eseguita su richiesta facendo clic sul pulsante **Esegui ora**. L'amministratore può eseguire qualsiasi pianificazione, ma il report generato conterrà i dati in base all'autorizzazione fornita dall'utente che ha creato la pianificazione. Qualsiasi altro utente diverso da Administrator potrà visualizzare o modificare la pianificazione in base alla propria autorizzazione. Se tutti i membri di questo ruolo possono vedere gli oggetti degli altri membri è selezionata nella pagina Aggiungi ruolo, gli altri membri del ruolo potranno vedere e modificare.

Accesso ai report

È possibile utilizzare la dashboard di SnapCenter per ottenere una rapida panoramica dello stato di salute del sistema. Dalla dashboard è possibile analizzare più dettagli. In alternativa, è possibile accedere direttamente ai report dettagliati.

È possibile accedere ai report utilizzando uno dei seguenti metodi:

- Nel riquadro di spostamento di sinistra, fare clic su **Dashboard**, quindi fare clic sul grafico a torta **Last Protection Summary** per visualizzare ulteriori dettagli nella pagina Report.
- Nel riquadro di spostamento di sinistra, fare clic su **Report**.

Filtrare il report

È possibile filtrare i dati del report in base a una serie di parametri, a seconda del livello di dettaglio e dell'intervallo di tempo delle informazioni richieste.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Report**.
2. Se la vista dei parametri non viene visualizzata, fare clic sull'icona **Alterna area parametri** nella barra degli strumenti del report.
3. Specificare l'intervallo di tempo per il quale si desidera eseguire il report. + se si omette la data di fine, si recuperano tutte le informazioni disponibili.
4. Filtrare le informazioni del report in base a uno dei seguenti criteri:
    - Gruppo di risorse
    - Host

- Policy
- Risorsa
- Stato
- Nome plug-in

5. Fare clic su **Apply** (Applica).

Esportare o stampare i report

L'esportazione dei report SnapCenter consente di visualizzare il report in diversi formati alternativi. È inoltre possibile stampare i report.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Report**.
2. Dalla barra degli strumenti dei report, eseguire una delle seguenti operazioni:
   - Fare clic sull'icona **Alterna anteprima di stampa** per visualizzare in anteprima un report stampabile.
   - Selezionare un formato dall'elenco a discesa dell'icona **Esporta** per esportare un report in un formato alternativo.
3. Per stampare un report, fare clic sull'icona **Stampa**.
4. Per visualizzare un riepilogo specifico del report, selezionare la sezione appropriata del report.

Impostare il server SMTP per le notifiche e-mail

È possibile specificare il server SMTP da utilizzare per l'invio dei report dei processi di protezione dei dati a se stessi o ad altri. È inoltre possibile inviare un'e-mail di prova per verificare la configurazione. Le impostazioni vengono applicate a livello globale per qualsiasi processo SnapCenter per il quale si configura la notifica via email.

Questa opzione consente di configurare il server SMTP per l'invio di tutti i report dei processi di protezione dei dati. Tuttavia, se si desidera che i processi di protezione dei dati SnapCenter vengano aggiornati regolarmente per una determinata risorsa, in modo da poter monitorare lo stato di tali aggiornamenti, è possibile configurare l'opzione per inviare tramite email i report SnapCenter quando si crea un gruppo di risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.
3. Immettere il server SMTP e fare clic su **Save** (Salva).
4. Per inviare un'e-mail di prova, immettere l'indirizzo e-mail da e a cui si desidera inviare l'e-mail, immettere l'oggetto e fare clic su **Invia**.

Configurare l'opzione per inviare i report via email

Se si desidera che i normali aggiornamenti dei processi di protezione dei dati di SnapCenter vengano inviati a se stessi o ad altri utenti in modo da poter monitorare lo stato di tali aggiornamenti, è possibile configurare l'opzione per inviare tramite email i report di SnapCenter quando si crea un gruppo di risorse.

Prima di iniziare

È necessario aver configurato il server SMTP nella pagina Global Settings (Impostazioni globali) in Settings (Impostazioni).

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Selezionare il tipo di risorsa che si desidera visualizzare e fare clic su **nuovo gruppo di risorse** oppure selezionare un gruppo di risorse esistente e fare clic su **Modifica** per configurare i report di posta elettronica per un gruppo di risorse esistente.
3. Nel pannello Notification (notifica) della procedura guidata New Resource Group (nuovo gruppo di risorse), selezionare dal menu a discesa se si desidera ricevere i report sempre, in caso di guasto o in caso di errore o avviso.
4. Inserire l'indirizzo da cui viene inviato il messaggio e-mail, l'indirizzo a cui viene inviato il messaggio e l'oggetto del messaggio.

Gestire il repository del server SnapCenter

Le informazioni relative alle varie operazioni eseguite da SnapCenter vengono memorizzate nel repository del database del server SnapCenter. È necessario creare backup del repository per proteggere il server SnapCenter dalla perdita di dati.

Il repository del server SnapCenter viene talvolta definito database NSM.

Prerequisiti per la protezione del repository SnapCenter

L'ambiente deve soddisfare determinati prerequisiti per proteggere il repository SnapCenter.

- Gestione delle connessioni SVM (Storage Virtual Machine)

  È necessario configurare le credenziali dello storage.

- Provisioning degli host

  Almeno un disco di storage NetApp deve essere presente sull'host del repository SnapCenter. Se un disco NetApp non è presente sull'host del repository SnapCenter, è necessario crearne uno.

  Per ulteriori informazioni sull'aggiunta di host, la configurazione delle connessioni SVM e il provisioning degli host, consultare le istruzioni di installazione.

- Provisioning del LUN iSCSI o VMDK

  Per la configurazione ad alta disponibilità (ha), è possibile eseguire il provisioning di un LUN iSCSI o di un VMDK in uno dei server SnapCenter.

Eseguire il backup del repository SnapCenter

Il backup del repository del server SnapCenter consente di proteggerlo dalla perdita di dati. È possibile eseguire il backup del repository eseguendo il cmdlet *Protect-SmRepository*.

A proposito di questa attività

Il cmdlet *Protect-SmRepository* esegue le seguenti attività:

- Crea un gruppo di risorse e una policy
- Crea una pianificazione di backup per il repository SnapCenter

Fasi

1. Avviare PowerShell.
2. Sull'host del server SnapCenter, stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
3. Eseguire il backup del repository utilizzando il cmdlet *Protect-SmRepository* e i parametri richiesti.

Visualizzare i backup del repository SnapCenter

È possibile visualizzare un elenco dei backup del repository di database del server SnapCenter eseguendo il cmdlet *Get-SmRepositoryBackups*.

I backup del repository vengono creati in base alla pianificazione specificata nel cmdlet *Protect-SmRepository*.

Fasi

1. Avviare PowerShell.
2. Dal prompt dei comandi, immettere il seguente cmdlet, quindi fornire le credenziali per la connessione al server SnapCenter: *Open-SMConnection*
3. Elencare tutti i backup dei database SnapCenter disponibili utilizzando il cmdlet *Get-SmRepositoryBackups*.

Ripristinare il repository del database SnapCenter

È possibile ripristinare il repository SnapCenter eseguendo il cmdlet *Restore-SmRepositoryBackup*.

Durante il ripristino del repository SnapCenter, le altre operazioni SnapCenter in esecuzione saranno interessate dal fatto che durante l'operazione di ripristino il database del repository non è accessibile.

Fasi

1. Avviare PowerShell.
2. Dal prompt dei comandi, immettere il seguente cmdlet, quindi fornire le credenziali per la connessione al server SnapCenter: *Open-SMConnection*
3. Ripristinare il backup del repository utilizzando il cmdlet *Restore-SmRepositoryBackup*.

   Il seguente cmdlet ripristina il repository del database MySQL di SnapCenter dai backup esistenti su LUN iSCSI o VMDK:

   ```
   C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
   ```

   Il seguente cmdlet ripristina il database MySQL di SnapCenter quando i file di backup vengono cancellati accidentalmente nel LUN iSCSI. Per VMDK ripristinare manualmente il backup da Snapshot ONTAP.

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```

Il backup utilizzato per eseguire l'operazione di ripristino del repository non viene elencato quando vengono recuperati i backup del repository dopo aver eseguito l'operazione di ripristino.

Migrare il repository SnapCenter

È possibile migrare il repository del database del server SnapCenter dalla posizione predefinita a un altro disco. È possibile migrare il repository quando si desidera spostarlo su un disco con più spazio.

Fasi

1. Arrestare il servizio MYSQL57 in Windows.
2. Individuare la directory dei dati MySQL.

   La directory dei dati si trova generalmente all'indirizzo C: ProgramData MySQL Server 5.7 Data.
3. Copiare la directory dei dati MySQL nella nuova posizione, ad esempio e:
4. Fare clic con il pulsante destro del mouse sulla nuova directory, quindi selezionare **Proprietà** > **sicurezza** per aggiungere l'account del server locale del servizio di rete alla nuova directory, quindi assegnare il controllo completo dell'account.
5. Rinominare la directory del database originale, ad esempio nsm_copy.
6. Dal prompt dei comandi di Windows, creare un link simbolico alla directory utilizzando il comando *mklink*.

   ```
   "mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
   ```
7. Avviare il servizio MYSQL57 in Windows.
8. Verificare che la modifica della posizione del database abbia esito positivo effettuando l'accesso a SnapCenter e controllando le voci del repository oppure effettuando l'accesso all'utility MySQL e connettendosi al nuovo repository.
9. Eliminare la directory del repository del database originale, rinominata (nsm_copy).

Reimpostare la password del repository SnapCenter

La password del database del repository MySQL Server viene generata automaticamente durante l'installazione del server SnapCenter da SnapCenter 4.2. Questa password generata automaticamente non è nota all'utente SnapCenter in nessun momento. Se si desidera accedere al database del repository, è necessario reimpostare la password.

Prima di iniziare

Per reimpostare la password, è necessario disporre dei privilegi di amministratore di SnapCenter.

Fasi

1. Avviare PowerShell.
2. Dal prompt dei comandi, immettere il seguente comando, quindi fornire le credenziali per la connessione al server SnapCenter: *Open-SMConnection*

3. Reimpostare la password del repository: *Set-SmRepositoryPassword*

   Il seguente comando reimposta la password del repository:

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: ********
ConfirmPassword: ********
Successfully updated the MySQL server password.
```

Informazioni correlate

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Gestire le risorse di domini non attendibili

Oltre a gestire gli host nei domini attendibili di Active Directory (ad), SnapCenter gestisce anche gli host in più domini ad non attendibili. I domini ad non attendibili devono essere registrati con il server SnapCenter. SnapCenter supporta utenti e gruppi di più domini ad non attendibili.

È possibile installare il server SnapCenter su un computer che si trova in un dominio o in un gruppo di lavoro. Per installare il server SnapCenter, specificare le credenziali di dominio se il computer si trova in un dominio o le credenziali di amministratore locale se il computer si trova in un gruppo di lavoro.

I gruppi Active Directory (ad) che appartengono a domini non registrati con il server SnapCenter non sono supportati. Sebbene sia possibile creare ruoli SnapCenter con questi gruppi ad, l'accesso al server SnapCenter non riesce e viene visualizzato il seguente messaggio di errore: L'utente che si sta tentando di accedere non appartiene ad alcun ruolo. Contattare l'amministratore.

Modificare i domini non attendibili

È possibile modificare un dominio non attendibile quando si desidera aggiornare gli indirizzi IP del controller di dominio o il nome di dominio completo (FQDN).

A proposito di questa attività

Dopo aver modificato l'FQDN, le risorse associate (host, utenti e gruppi) potrebbero non funzionare come previsto.

Per modificare un dominio non attendibile, è possibile utilizzare l'interfaccia utente di SnapCenter o i cmdlet PowerShell.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.
3. Nella pagina Global Settings (Impostazioni globali), fare clic su **Domain Settings** (Impostazioni dominio).

4. Fare clic su  , quindi fornire i seguenti dettagli:

Per questo campo…	Eseguire questa operazione…
FQDN del dominio	Specificare l'FQDN e fare clic su **Resolve** (Risolvi).
Indirizzi IP dei controller di dominio	Se l'FQDN del dominio non è risolvibile, specificare uno o più indirizzi IP del controller di dominio.

5. Fare clic su **OK**.

Annullare la registrazione dei domini Active Directory non attendibili

È possibile annullare la registrazione di un dominio Active Directory non attendibile se non si desidera utilizzare le risorse associate a tale dominio.

Prima di iniziare

Gli host, gli utenti, i gruppi e le credenziali associati al dominio non attendibile dovrebbero essere stati rimossi.

A proposito di questa attività

- Una volta che il dominio viene disregistrato dal server SnapCenter, gli utenti di tale dominio non possono accedere al server SnapCenter.
- Se sono presenti risorse associate (host, utenti e gruppi), dopo aver disregistrato il dominio, le risorse non saranno operative.
- Per annullare la registrazione di un dominio non attendibile, è possibile utilizzare l'interfaccia utente di SnapCenter o i cmdlet PowerShell.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.
3. Nella pagina Global Settings (Impostazioni globali), fare clic su **Domain Settings** (Impostazioni dominio).
4. Dall'elenco dei domini, selezionare il dominio che si desidera annullare la registrazione.
5. Fare clic su , quindi su **OK**.

Gestire il sistema storage

Dopo aver aggiunto il sistema di storage, è possibile modificare la configurazione e le connessioni del sistema di storage o eliminarlo.

Modificare la configurazione del sistema storage

È possibile utilizzare SnapCenter per modificare la configurazione del sistema di storage se si desidera modificare il nome utente, la password, la piattaforma, la porta, il protocollo, Periodo di timeout, indirizzo IP preferito o opzioni di messaggistica.

A proposito di questa attività

È possibile modificare le connessioni di storage per un singolo utente o per un gruppo. Se si appartiene a uno o più gruppi con autorizzazione per lo stesso sistema di storage, il nome della connessione di storage viene visualizzato più volte nell'elenco delle connessioni di storage, una volta per ogni gruppo con autorizzazione per il sistema di storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Systems**.
2. Nella pagina Storage Systems (sistemi storage), dal menu a discesa **Type** (tipo), eseguire una delle seguenti operazioni:

Selezionare…	Fasi…
SVM ONTAP	Per visualizzare tutte le macchine virtuali di storage (SVM) aggiunte e modificare la configurazione SVM richiesta. a. Nella pagina Storage Connections (connessioni storage), fare clic sul nome SVM appropriato. b. Eseguire una delle seguenti operazioni: ◦ Se la SVM non fa parte di alcun cluster, nella pagina Modifica sistema di storage, modificare le configurazioni come nome utente, password, impostazioni EMS e AutoSupport, piattaforma, protocollo, porta, timeout, E IP preferito. ◦ Se la SVM fa parte di un cluster, nella pagina Modifica sistema storage, selezionare **Gestisci SVM in modo indipendente** e modificare le configurazioni come nome utente, password, impostazioni EMS e AutoSupport, piattaforma, protocollo, porta, timeout, E IP preferito. Dopo aver modificato la SVM in modo da gestirla in modo indipendente, se si decide di gestirla attraverso il cluster, eliminare la SVM e fare clic su **riscopri**. La SVM verrà aggiunta al cluster ONTAP. Quando una password del sistema di storage viene aggiornata sull'interfaccia grafica di SnapCenter, è necessario riavviare i servizi SMCore del rispettivo plug-in o dell'host del server perché la password aggiornata non si riflette in SMCore e i processi di backup non vengono eseguiti correttamente con un errore di credenziale errato.

Selezionare…	Fasi…
Cluster ONTAP	Per visualizzare tutti i cluster aggiunti e modificare la configurazione del cluster richiesta. a. Nella pagina Storage Connections (connessioni storage), fare clic sul nome del cluster. b. Nella pagina Modify Storage System (Modifica sistema storage), fare clic sull'icona di modifica accanto a Username (Nome utente) e modificare il nome utente e la password. c. Selezionare o deselezionare le impostazioni EMS e AutoSupport. d. Fare clic su **altre opzioni** e modificare altre configurazioni come piattaforma, protocollo, porta, timeout e IP preferito.

3. Fare clic su **Invia**.

Eliminare il sistema di storage

È possibile utilizzare SnapCenter per eliminare qualsiasi sistema di storage inutilizzato.

A proposito di questa attività

È possibile eliminare le connessioni di storage per un singolo utente o per un gruppo. Se si appartiene a uno o più gruppi con autorizzazione per lo stesso sistema di storage, il nome del sistema di storage viene visualizzato più volte nell'elenco delle connessioni di storage, una volta per ogni gruppo con autorizzazione per il sistema di storage.

Quando si elimina un sistema di storage, tutte le operazioni eseguite su tale sistema di storage avranno esito negativo.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Systems**.
2. Nella pagina sistemi storage, dal menu a discesa **tipo**, selezionare **SVM ONTAP** o **Clusters ONTAP**.
3. Nella pagina Storage Connections (connessioni storage), selezionare la casella di controllo accanto a SVM o il cluster che si desidera eliminare.

   Non è possibile selezionare la SVM che fa parte di un cluster.

4. Fare clic su **Delete** (Elimina).
5. Nella pagina Delete Storage System Connection Settings (Elimina impostazioni di connessione del sistema di storage), fare clic su **OK**.

   Se una SVM viene eliminata dal cluster ONTAP utilizzando l'interfaccia grafica di ONTAP, nella GUI di SnapCenter fare clic su **riscopri** per aggiornare l'elenco SVM.

Gestire la raccolta di dati EMS

È possibile pianificare e gestire la raccolta di dati EMS (Event Management System) utilizzando i cmdlet PowerShell. La raccolta di dati EMS comprende la raccolta di dettagli sul server SnapCenter, sui pacchetti plug-in SnapCenter installati, sugli host e informazioni simili, quindi l'invio a una specifica macchina virtuale di storage ONTAP (SVM).

L'utilizzo della CPU del sistema è elevato quando è in corso l'attività di raccolta dei dati. L'utilizzo della CPU rimane elevato fino a quando l'operazione è in corso indipendentemente dalle dimensioni dei dati.

Interrompere la raccolta dei dati EMS

Per impostazione predefinita, la raccolta dei dati EMS viene attivata e viene eseguita ogni sette giorni dopo la data di installazione. È possibile disattivare la raccolta dati in qualsiasi momento utilizzando il cmdlet PowerShell *Disable-SmDataCollectionEMS*.

Fasi

1. Da una riga di comando PowerShell, stabilire una sessione con SnapCenter immettendo *Open-SmConnection*.
2. Disattivare la raccolta dati EMS immettendo *Disable-SmDataCollectionEms*.

Avviare la raccolta dati EMS

La raccolta dei dati EMS è attivata per impostazione predefinita ed è pianificata per l'esecuzione ogni sette giorni dalla data di installazione. Se è stata disattivata, è possibile avviare nuovamente la raccolta dati EMS utilizzando il cmdlet *Enable-SmDataCollectionEMS*.

L'autorizzazione generate-autosupport-log dell'evento Data ONTAP è stata concessa all'utente della macchina virtuale di storage (SVM).

Fasi

1. Da una riga di comando PowerShell, stabilire una sessione con SnapCenter immettendo *Open-SmConnection*.
2. Abilitare la raccolta dati EMS immettendo *Enable-SmDataCollectionEMS*.

Modificare il programma di raccolta dei dati EMS e la SVM di destinazione

È possibile utilizzare i cmdlet PowerShell per modificare la pianificazione della raccolta dati EMS o la SVM (Storage Virtual Machine) di destinazione.

Fasi

1. Dalla riga di comando di PowerShell, per stabilire una sessione con SnapCenter, immettere il cmdlet *Open-SmConnection*.
2. Per modificare la destinazione della raccolta dati EMS, immettere il cmdlet *set-SmDataCollectionEmsTarget*.

3. Per modificare la pianificazione della raccolta dati EMS, immettere il cmdlet *set-SmDataCollectionEmsSchedule*.

Monitorare lo stato di raccolta dei dati EMS

È possibile monitorare lo stato della raccolta dati EMS utilizzando diversi cmdlet PowerShell. È possibile ottenere informazioni su pianificazione, destinazione della macchina virtuale di storage (SVM) e stato.

Fasi

1. Da una riga di comando PowerShell, stabilire una sessione con SnapCenter immettendo *Open-SmConnection*.
2. Recuperare le informazioni sulla pianificazione della raccolta dati EMS immettendo *Get-SmDataCollectionEmsSchedule*.
3. Recuperare le informazioni sullo stato della raccolta dati EMS immettendo *Get-SmDataCollectionEmsStatus*.
4. Recuperare le informazioni sulla destinazione di raccolta dati EMS immettendo *Get-SmDataCollectionEmsTarget*.

Informazioni correlate

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Aggiornare il server e i plug-in SnapCenter

Configurare SnapCenter per verificare la disponibilità di aggiornamenti

SnapCenter comunica periodicamente con il sito di supporto NetApp per notificare gli aggiornamenti software disponibili. È inoltre possibile creare una pianificazione per specificare l'intervallo in cui si desidera ricevere informazioni sugli aggiornamenti disponibili.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina **Impostazioni**, fare clic su **Software**.

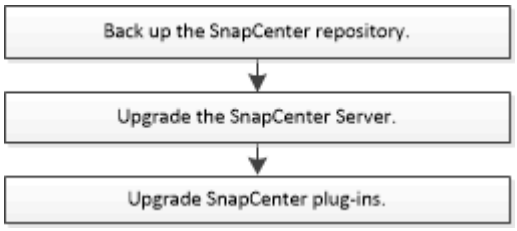
   La pagina Software disponibile visualizza i pacchetti plug-in disponibili, le versioni disponibili e il relativo stato di installazione.

3. Fare clic su **Controlla aggiornamenti** per verificare se sono disponibili versioni più recenti dei pacchetti plug-in.
4. Fare clic su **Schedule Updates** (Pianifica aggiornamenti) per creare una pianificazione in cui specificare l'intervallo in cui si desidera ricevere informazioni sugli aggiornamenti disponibili:
   a. Selezionare l'intervallo in **Controlla aggiornamenti**.
   b. Selezionare la credenziale di amministrazione del server SnapCenter e fare clic su **OK**.

Workflow di upgrade

Ogni release di SnapCenter contiene un pacchetto di plug-in e server SnapCenter aggiornati. Gli aggiornamenti dei pacchetti plug-in vengono distribuiti con il programma di installazione di SnapCenter. È possibile configurare SnapCenter per verificare la disponibilità di aggiornamenti.

Il flusso di lavoro mostra le diverse attività richieste per aggiornare il server SnapCenter e i pacchetti plug-in.



Percorsi di upgrade supportati

Se si utilizza la versione del server SnapCenter…	È possibile aggiornare direttamente il server SnapCenter a…	Versioni plug-in supportate
4,7	4,8	• 4,7 • 4,8
	4,9	• 4,9
4,8	4,9	• 4,8 • 4,9
	5,0	• 5,0
4,9	5,0	• 4,9 • 5,0

Ad esempio, se si utilizza SnapCenter versione 4,7 e si desidera eseguire l'aggiornamento alla versione 5,0, è necessario prima eseguire l'aggiornamento alla versione 4,8 e poi eseguire un aggiornamento alla versione 5,0.

Per informazioni sull'aggiornamento del plug-in SnapCenter per VMware vSphere, vedere "Upgrade del plug-in SnapCenter per VMware vSphere".

Aggiornare il server SnapCenter

È possibile utilizzare il file eseguibile del programma di installazione del server SnapCenter per aggiornare il server SnapCenter.

Prima di iniziare

- L'host del server SnapCenter deve essere aggiornato con gli aggiornamenti di Windows, senza riavvii del sistema in sospeso.
- Prima di iniziare l'operazione di aggiornamento, assicurarsi che non siano in esecuzione altre operazioni.
- È necessario eseguire il backup del database del repository SnapCenter (MySQL) dopo aver eseguito tutti i processi. Si consiglia di eseguire l'aggiornamento del server SnapCenter e del plug-in Exchange.

  Per informazioni, vedere "Eseguire il backup del repository SnapCenter".

- Eseguire il backup di tutti i file di configurazione SnapCenter modificati sull'host del server SnapCenter o sul plug-in host.

  Esempi di file di configurazione di SnapCenter: SnapDriveService.exe.config, SMCoreServiceHost.exe.config e così via.

A proposito di questa attività

- Durante l'aggiornamento, l'host viene automaticamente messo in modalità di manutenzione che impedisce all'host di eseguire qualsiasi processo pianificato. Dopo l'aggiornamento, l'host viene automaticamente

disattivato dalla modalità di manutenzione.

- Durante l'aggiornamento, viene eseguito uno script SQL per aggiornare i dati di Exchange nel database NSM, che converte il DAG e il shortname host in FQDN. Questa opzione è applicabile solo se si utilizza il server SnapCenter con il plug-in Exchange.
- Prima di iniziare l'operazione di aggiornamento, se l'host è stato impostato manualmente in modalità di manutenzione, dopo l'aggiornamento è necessario disattivare manualmente la modalità di manutenzione dell'host facendo clic su **host** > **attiva pianificazione**.
- Per il plug-in SnapCenter per Microsoft SQL Server, il plug-in SnapCenter per Microsoft Exchange Server e il plug-in SnapCenter per Microsoft Windows, si consiglia di aggiornare sia il server che gli host dei plug-in alla versione 4.7 affinché IL PERCORSO SCRIPT venga eseguito.

  Per le pianificazioni di backup e verifica esistenti con prescritture e postscript attivati nel criterio, le operazioni di backup continueranno a funzionare dopo l'aggiornamento.

  Nella pagina **Dettagli lavoro**, un messaggio di avviso consiglia al cliente di copiare gli script nel PERCORSO_SCRIPT e modificare il criterio per fornire un percorso relativo al PERCORSO_SCRIPT. Per il lavoro del ciclo di vita clone, il messaggio di avviso viene visualizzato a livello di lavoro secondario.

Fasi

1. Scaricare il pacchetto di installazione del server SnapCenter dal sito del supporto NetApp.

   https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab

2. Creare una copia del file web.config che si trova in C: File di programma NetApp SnapCenter WebApp.
3. Esportare le pianificazioni SnapCenter relative all'host plug-in dalla pianificazione delle attività di Windows in modo da poterle utilizzare per ripristinare le pianificazioni in caso di errore nell'aggiornamento.

   ```
   md d:\\SCBackup``schtasks /query /xml /TN taskname >>
   "D:\SCBackup\taskname.xml"
   ```

4. Creare il dump del database MySQL SnapCenter se il backup del repository non è configurato.

   ```
   md d:\\SCBackup``mysqldump --all-databases --single-transaction --add-drop
   -database --triggers --routines --events -u root -p >
   D:\SCBackup\SCRepoBackup.dmp
   ```

   Quando richiesto, inserire la password.

5. Avviare l'aggiornamento del server SnapCenter facendo doppio clic sul file .exe scaricato.

   Una volta avviato l'aggiornamento, vengono eseguiti tutti i controlli preliminari e, se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati. È possibile ignorare i messaggi di avviso e procedere con l'installazione. Tuttavia, gli errori devono essere corretti.

   SnapCenter continuerà a utilizzare la password esistente del database del repository MySQL Server fornita durante l'installazione della versione precedente del server SnapCenter.

6. Fare clic su **Upgrade** (Aggiorna).

   In qualsiasi momento, facendo clic sul pulsante **Annulla**, il flusso di lavoro di aggiornamento viene annullato. Non ripristinerà lo stato precedente del server SnapCenter.

Procedura consigliata: per accedere all'interfaccia grafica di SnapCenter, è necessario disconnettersi e accedere a SnapCenter oppure chiudere e aprire un nuovo browser.

Al termine

- Se il plug-in viene installato utilizzando un utente sudo, copiare le chiavi sha224 disponibili in *C:\ProgramData\NetApp\SnapCenter\Package Repository\oracle_checksum.txt* per aggiornare il file */etc/sudoers*.
- È necessario eseguire un nuovo rilevamento delle risorse sugli host.

  Se lo stato dell'host viene visualizzato come interrotto, è possibile attendere qualche istante ed eseguire una nuova ricerca. È inoltre possibile modificare il valore del parametro **HostRefreshInterval** (il valore predefinito è 3600 secondi) su un valore superiore a 10 minuti.
- Se l'aggiornamento non riesce, è necessario eliminare l'installazione non riuscita, reinstallare la versione precedente di SnapCenter e ripristinare il database NSM allo stato precedente.
- Dopo aver aggiornato l'host del server SnapCenter, è necessario aggiornare i plug-in prima di aggiungere qualsiasi sistema di storage.

Aggiorna i pacchetti plug-in

I pacchetti plug-in vengono distribuiti come parte dell'aggiornamento di SnapCenter.

La procedura di aggiornamento posiziona l'host Windows, Linux o AIX in modalità "maintenance", impedendo all'host di eseguire qualsiasi processo pianificato.

Prima di iniziare

- Se si è utenti non root con accesso alle macchine Linux, aggiornare il file */etc/sudoers* con i valori checksum più recenti prima di eseguire l'operazione di aggiornamento.
- Per impostazione predefinita, SnapCenter rileva JAVA_HOME dall'ambiente. Se si desidera utilizzare UNA JAVA_HOME fissa e si stanno aggiornando i plug-in su un host Linux, aggiungere manualmente IL parametro SKIP_JAVAHOME_UPDATE nel file *spl.properties* che si trova in */var/opt/snapcenter/spl/etc/* e impostare il valore su TRUE.

  Il valore DI JAVA_HOME viene aggiornato quando il plug-in viene aggiornato o quando il servizio caricatore di plug-in (SPL) di SnapCenter viene riavviato. Prima di aggiornare o riavviare SPL, se si aggiunge IL parametro SKIP_JAVAHOME_UPDATE e si imposta il valore su TRUE, IL valore DI JAVA_HOME non viene aggiornato.
- È necessario aver eseguito il backup di tutti i file di configurazione SnapCenter modificati sull'host del server SnapCenter o sul plug-in host.

  Esempi di file di configurazione di SnapCenter: SnapDriveService.exe.config, SMCoreServiceHost.exe.config e così via.

A proposito di questa attività

- La procedura di aggiornamento posiziona l'host Windows, Linux o AIX in modalità "maintenance", impedendo all'host di eseguire qualsiasi processo pianificato.
- Per il plug-in SnapCenter per Microsoft SQL Server, il plug-in SnapCenter per Microsoft Exchange Server e il plug-in SnapCenter per Microsoft Windows, si consiglia di aggiornare sia il server che gli host plug-in alla versione più recente per l'esecuzione DI SCRIPTS_PATH.

Per le pianificazioni di backup e verifica esistenti con prescritture e postscript attivati nel criterio, le operazioni di backup continueranno a funzionare dopo l'aggiornamento.

Nella pagina **Dettagli lavoro**, un messaggio di avviso consiglia al cliente di copiare gli script nel PERCORSO_SCRIPT e modificare il criterio per fornire un percorso relativo al PERCORSO_SCRIPT. Per il lavoro del ciclo di vita clone, il messaggio di avviso viene visualizzato a livello di lavoro secondario.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **hosts** > **Managed hosts**.
2. Aggiornare gli host eseguendo una delle seguenti operazioni:
   - Se la colonna Overall Status (Stato generale) visualizza "Upgrade Available" (aggiornamento disponibile) per uno degli host, fare clic sul nome host ed eseguire le seguenti operazioni:
     i. Fare clic su **altre opzioni**.
     ii. Selezionare **Ignora precheck** se non si desidera verificare se l'host soddisfa i requisiti per l'aggiornamento del plug-in.
     iii. Fare clic su **Upgrade** (Aggiorna).
   - Se si desidera aggiornare più host, selezionare tutti gli host, fare clic su , quindi fare clic su **Upgrade** > **OK**.

     Tutti i servizi correlati vengono riavviati durante l'aggiornamento del plug-in.

     Tutti i plug-in del pacchetto vengono selezionati, ma solo i plug-in installati con la versione precedente di SnapCenter vengono aggiornati e i plug-in rimanenti non vengono installati. Per installare qualsiasi nuovo plug-in, utilizzare l'opzione **Aggiungi plug-in**.

     Se non è stata selezionata la casella di controllo **Ignora controlli preliminari**, l'host viene convalidato per verificare se soddisfa i requisiti di installazione del plug-in. Se i requisiti minimi non sono soddisfatti, vengono visualizzati messaggi di errore o di avvertenza appropriati. Dopo aver risolto il problema, fare clic su **Upgrade** (Aggiorna).

     Se l'errore riguarda lo spazio su disco o la RAM, è possibile aggiornare il file web.config che si trova in C: File di programma NetApp SnapCenter WebApp o i file di configurazione PowerShell che si trovano in C: Windows System 32, WindowsPowerShell v1.0, moduli SnapCenter per modificare i valori predefiniti. Se l'errore riguarda i parametri rimanenti, è necessario risolvere il problema e convalidare nuovamente i requisiti.

Tech refresh

Aggiornamento tecnico dell'host server SnapCenter

Quando l'host del server SnapCenter richiede l'aggiornamento, è possibile installare la stessa versione del server SnapCenter sul nuovo host e quindi eseguire le API per eseguire il backup di SnapCenter dal vecchio server e ripristinarlo sul nuovo server.

Fasi

1. Distribuire il nuovo host ed eseguire le seguenti operazioni:
   a. Installare la stessa versione del server SnapCenter.
   b. (Facoltativo) configurare i certificati CA e abilitare SSL bidirezionale. Per ulteriori informazioni, fare riferimento a "Configurare il certificato CA" e "Configurare e abilitare SSL bidirezionale".
   c. (Opzionale) configurare l'autenticazione a più fattori. Per ulteriori informazioni, fare riferimento a "Abilitare l'autenticazione a più fattori".
2. Accedere come utente amministratore SnapCenter.
3. Creare un backup del server SnapCenter sul vecchio host utilizzando l'API: O il cmdlet: `/5.0/server/backup` *New-SmServerBackup*.

   Prima di eseguire il backup, sospendere tutti i processi pianificati e assicurarsi che non siano in esecuzione.

   Se si desidera ripristinare il backup sul server SnapCenter in esecuzione su un nuovo dominio, prima di eseguire un backup è necessario aggiungere il nuovo utente di dominio nel vecchio host SnapCenter e assegnare il ruolo di amministratore SnapCenter.

4. Copiare il backup dal vecchio host al nuovo host.
5. Ripristinare il backup del server SnapCenter sul nuovo host utilizzando l'API: O il cmdlet: `/5.0/server/restore` *Restore-SmServerBackup*.

   Per impostazione predefinita, Restore aggiornerà il nuovo URL del server SnapCenter in tutti gli host. Se si desidera ignorare l'aggiornamento, utilizzare l'attributo *-SkipSMSURLInHosts* e aggiornare separatamente l'URL del server eseguendo l'API: O il cmdlet: `/5.0/server/configureurl` *Set-SmServerConfig*.

   Se l'host del plug-in non è in grado di risolvere il nome host del server, accedere a ciascun host del plug-in e aggiungere la voce *etc/host* per il nuovo IP nel formato <New IP> SC_Server_Name.

   Le voci del server *etc/host* non verranno ripristinate. È possibile ripristinarlo manualmente dal vecchio server.

   Se il backup viene ripristinato sul server SnpCenter in esecuzione su un nuovo dominio e si desidera continuare a utilizzare i vecchi utenti di dominio, è necessario registrare il vecchio dominio nel nuovo server SnapCenter.

Se il file web.config è stato aggiornato manualmente nel vecchio host SnapCenter, gli aggiornamenti non verranno copiati nel nuovo host. È necessario apportare manualmente le stesse modifiche nel file web.config del nuovo host.

6. Se è stato saltato l'aggiornamento dell'URL del server SnapCenter o uno qualsiasi degli host è rimasto inattivo durante il processo di ripristino, aggiornare il nuovo nome del server in tutti gli host o host specificati gestiti da SnapCenter utilizzando l'API: `/5.0/server/configureurl` O il cmdlet: *Set-SmServerConfig*.
7. Attivare i processi pianificati su tutti gli host dal nuovo server SnapCenter.

Tech refresh di un nodo nel cluster F5

Puoi fare un tech refresh di qualsiasi nodo nel cluster F5 rimuovendo il nodo e aggiungendo il nuovo nodo. Se il nodo da aggiornare è attivo, rendere attivo un altro nodo del cluster e quindi rimuovere il nodo.

Per informazioni su come aggiungere un nodo al cluster F5, fare riferimento a "Configurare i server SnapCenter per l'alta disponibilità utilizzando F5".

Se l'URL del cluster F5 cambia, l'URL può essere aggiornato in tutti gli host utilizzando l'API: O il cmdlet: `/5.0/server/configureurl` *Set-SmServerConfig*.

Smantellamento del vecchio host del server SnapCenter

È possibile rimuovere il vecchio host del server SnapCenter dopo aver verificato che il nuovo server SnapCenter sia attivo e funzionante e che tutti gli host dei plug-in siano in grado di comunicare con il nuovo host del server SnapCenter.

Eseguire il rollback dell'host del server SnapCenter precedente

In caso di problemi, è possibile ripristinare il vecchio host del server SnapCenter aggiornando l'URL del server SnapCenter in tutti gli host utilizzando l'API: O il cmdlet: `/5.0/server/configureurl` *Set-SmServerConfig*.

Disaster recovery

Disaster recovery dell'host SnapCenter standalone

È possibile eseguire il ripristino di emergenza ripristinando il backup del server nel nuovo host.

Prima di iniziare

Assicurarsi di disporre di un backup del vecchio server SnapCenter.

Fasi

1. Distribuire il nuovo host ed eseguire le seguenti operazioni:
   a. Installare la stessa versione del server SnapCenter.
   b. Configurare i certificati CA e abilitare SSL bidirezionale. Per ulteriori informazioni, fare riferimento a "Configurare il certificato CA" e "Configurare e abilitare SSL bidirezionale".
2. Copiare il vecchio backup del server SnapCenter nel nuovo host.
3. Accedere come utente amministratore SnapCenter.
4. Ripristinare il backup del server SnapCenter sul nuovo host utilizzando l'API: O il cmdlet:

`/5.0/server/restore` *Restore-SmServerBackup*.

Per impostazione predefinita, Restore aggiornerà il nuovo URL del server SnapCenter in tutti gli host. Se si desidera ignorare l'aggiornamento, utilizzare l'attributo *-SkipSMSURLInHosts* e aggiornare separatamente l'URL del server utilizzando l'API: O il cmdlet: `/5.0/server/configureurl` *Set-SmServerConfig*.

Se l'host del plug-in non è in grado di risolvere il nome host del server, accedere a ciascun host del plug-in e aggiungere la voce *etc/host* per il nuovo IP nel formato <New IP> SC_Server_Name.

Le voci del server *etc/host* non verranno ripristinate. È possibile ripristinarlo manualmente dal vecchio server.

5. Se è stato saltato l'aggiornamento dell'URL o uno qualsiasi degli host è stato inattivo durante il processo di ripristino, aggiornare il nuovo nome del server in tutti gli host o host specificati che sono gestiti da SnapCenter utilizzando l'API: `/5.0/server/configureurl` O il cmdlet: *Set-SmServerConfig*.

Disaster recovery del cluster SnapCenter F5

È possibile eseguire il ripristino di emergenza ripristinando il backup del server nel nuovo host e convertendo quindi l'host standalone in un cluster.

Prima di iniziare

Assicurarsi di disporre di un backup del vecchio server SnapCenter.

Fasi

1. Distribuire il nuovo host ed eseguire le seguenti operazioni:
   a. Installare la stessa versione del server SnapCenter.
   b. Configurare i certificati CA e abilitare SSL bidirezionale. Per ulteriori informazioni, fare riferimento a "Configurare il certificato CA" e "Configurare e abilitare SSL bidirezionale".
2. Copiare il vecchio backup del server SnapCenter nel nuovo host.
3. Accedere come utente amministratore SnapCenter.
4. Ripristinare il backup del server SnapCenter sul nuovo host utilizzando l'API: O il cmdlet: `/5.0/server/restore` *Restore-SmServerBackup*.

   Per impostazione predefinita, Restore aggiornerà il nuovo URL del server SnapCenter in tutti gli host. Se si desidera ignorare l'aggiornamento, utilizzare l'attributo *-SkipSMSURLInHosts* e aggiornare separatamente l'URL del server utilizzando l'API: O il cmdlet: `/5.0/server/configureurl` *Set-SmServerConfig*.

   Se l'host del plug-in non è in grado di risolvere il nome host del server, accedere a ciascun host del plug-in e aggiungere la voce *etc/host* per il nuovo IP nel formato <New IP> SC_Server_Name.

   Le voci del server *etc/host* non verranno ripristinate. È possibile ripristinarlo manualmente dal vecchio server.

5. Se è stato saltato l'aggiornamento dell'URL o uno qualsiasi degli host è stato inattivo durante il processo di ripristino, aggiornare il nuovo nome del server in tutti gli host o host specificati che sono gestiti da SnapCenter utilizzando l'API: `/5.0/server/configureurl` O il cmdlet: *Set-SmServerConfig*.

6. Conversione dell'host standalone in cluster F5.

   Per informazioni sulla configurazione di F5, fare riferimento alla "Configurare i server SnapCenter per l'alta disponibilità utilizzando F5".

Informazioni correlate

Per informazioni sulle API, è necessario accedere alla pagina Swagger. "Come accedere alle API REST utilizzando la pagina web delle API di swagger"vedere .

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, è anche possibile fare riferimento a "Guida di riferimento al cmdlet del software SnapCenter".

Tech refresh degli host plug-in SnapCenter

Quando gli host dei plug-in SnapCenter richiedono un aggiornamento, è necessario spostare le risorse dal vecchio host al nuovo host. Quando il nuovo host viene aggiunto a SnapCenter, scoprirà tutte le risorse ma sarà trattato come nuove risorse.

A proposito di questa attività

È necessario eseguire l'API o il cmdlet che prenderà il vecchio nome host e il nuovo nome host come input, confrontare le risorse per nome e ricollegare gli oggetti delle risorse corrispondenti dal vecchio host al nuovo host. Le risorse corrispondenti verranno contrassegnate come protette.

- Il parametro *IsDryRun* è impostato su True per impostazione predefinita e identifica le risorse corrispondenti del vecchio e del nuovo host.

  Dopo aver verificato le risorse corrispondenti, impostare il parametro *IsDryRun* su False per ricollegare gli oggetti delle risorse corrispondenti dal vecchio host al nuovo host.

- Per impostazione predefinita, il parametro *AutoMigrateManuallyAddedResources* è impostato su True e in modo da copiare automaticamente le risorse aggiunte manualmente dal vecchio host al nuovo host.

  Il parametro *AutoMigrateManuallyAddedResources* è applicabile solo alle risorse Oracle e SAP HANA.

- Il parametro *SQLInstanceMapping* deve essere utilizzato se il nome dell'istanza è diverso tra il vecchio host e il nuovo host. Se si tratta di un'istanza predefinita, utilizzare *default_instance* come nome dell'istanza.

Il tech refresh è supportato per i seguenti plug-in SnapCenter:

- Plug-in SnapCenter per Microsoft SQL Server
  - Se i database SQL sono protetti a livello di istanza e come parte dell'aggiornamento tecnico dell'host vengono spostate solo le risorse parziali nel nuovo host, la protezione a livello di istanza esistente verrà convertita nella protezione del gruppo di risorse e le istanze di entrambi gli host verranno aggiunte al gruppo di risorse.
  - Se si utilizza un host SQL (ad esempio host1) come scheduler o come server di verifica per le risorse di un altro host (ad esempio Host2), durante l'esecuzione dell'aggiornamento tecnico su host1, i dettagli della pianificazione o della verifica non verranno migrati e continueranno a essere eseguiti su host1. Se dovete modificare, allora dovreste cambiarlo manualmente nei rispettivi host.
  - Se si utilizza il setup delle istanze del cluster di failover SQL (FCI), è possibile eseguire

l'aggiornamento tecnico aggiungendo il nuovo nodo al cluster FCI e aggiornando l'host del plug-in in SnapCenter.

    - Se si utilizza la configurazione di SQL Availability Group (AG), l'aggiornamento tecnico non è necessario. È possibile aggiungere il nuovo nodo ad AG e aggiornare l'host in SnapCenter.

- Plug-in SnapCenter per Windows
- Plug-in SnapCenter per database Oracle

  Se si utilizza il setup di Oracle Real Application Cluster (RAC), è possibile eseguire l'aggiornamento tecnico aggiungendo il nuovo nodo al cluster RAC e aggiornando l'host plug-in in SnapCenter.

- Plug-in SnapCenter per database SAP HANA

I casi d'utilizzo supportati sono:

- Migrazione delle risorse da un host a un altro host.
- Migrazione delle risorse da più host a uno o meno host.
- Migrazione delle risorse da un host a più host.

Gli scenari supportati sono:

- Il nuovo host ha un nome diverso dal vecchio host
- L'host esistente è stato rinominato

Prima di iniziare

Poiché questo workflow modifica i dati nel repository SnapCenter, si consiglia di eseguire il backup del repository SnapCenter. In caso di problemi con i dati, il repository SnapCenter può essere riportato allo stato precedente utilizzando il backup.

Per ulteriori informazioni, fare riferimento a "Eseguire il backup del repository SnapCenter".

Fasi

1. Distribuire il nuovo host e installare l'applicazione.
2. Sospendere le pianificazioni del vecchio host.
3. Spostare le risorse necessarie dal vecchio host al nuovo host.
    a. Acquisizione dei database richiesti nel nuovo host dallo stesso storage.
        - Assicurarsi che lo spazio di archiviazione sia mappato sulla stessa unità o sullo stesso percorso di montaggio del vecchio host. Se l'archiviazione non è mappata correttamente, i backup creati nel vecchio host non possono essere utilizzati per il ripristino.

          Per impostazione predefinita, Windows assegna automaticamente la successiva unità disponibile.

        - Se il DR di archiviazione è abilitato, il relativo storage deve essere montato nel nuovo host.
    b. Verificare la compatibilità in caso di modifica della versione dell'applicazione.
    c. Solo per l'host del plug-in Oracle, assicurarsi che gli UID e i GID di Oracle e degli utenti del gruppo siano identici a quelli del vecchio host.

       Per informazioni, fare riferimento a:

- "Come eseguire la migrazione del database SQL dal vecchio host al nuovo host"
- "Come migrare il database Oracle dal vecchio host al nuovo host"
- "Come attivare il database SAP HANA nel nuovo host"

4. Aggiungere il nuovo host a SnapCenter.
5. Verificare se tutte le risorse sono state rilevate.
6. Eseguire l'API di aggiornamento dell'host: O il cmdlet: `/5.0/techrefresh/host` *Invoke-SmTechRefreshHost*.

   La seriografia a secco è attivata per impostazione predefinita e vengono identificate le risorse corrispondenti da ricollegare. È possibile verificare le risorse eseguendo l'API: '/Jobs/{jobid}' o il cmdlet *get-SmJobSummaryReport*.

   Se le risorse sono state migrate da più host, è necessario eseguire l'API o il cmdlet per tutti gli host. Se l'unità o il percorso di montaggio nel nuovo host non è lo stesso del vecchio host, le seguenti operazioni di ripristino non avranno esito positivo:

   - Il ripristino SQL sul posto non avrà esito positivo. Tuttavia, la funzione RTAL può essere sfruttata.
   - Il ripristino dei database Oracle e SAP HANA non avrà esito positivo.

     Se si desidera migrare a più host, è necessario eseguire tutti i passaggi dal punto 1 per tutti gli host.

   È possibile eseguire più volte l'API o il cmdlet sullo stesso host, che verrà ricollegato solo se è stata identificata una nuova risorsa.

7. (Facoltativo) rimuovere il vecchio host o gli host da SnapCenter.

Informazioni correlate

Per informazioni sulle API , è necessario accedere alla pagina Swagger . "Come accedere alle API REST utilizzando la pagina web delle API di swagger"vedere .

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, è anche possibile fare riferimento a "Guida di riferimento al cmdlet del software SnapCenter".

Tech refresh del sistema storage

Quando lo storage viene tech refresh, i dati vengono migrati al nuovo storage e gli host delle applicazioni vengono montati con nuovo storage. Il workflow di backup di SnapCenter identifica il nuovo storage e crea la snapshot se il nuovo storage viene registrato in SnapCenter.

Puoi eseguire il ripristino, il montaggio e il cloning sui nuovi backup creati in seguito all'aggiornamento dello storage. Tuttavia, queste operazioni non avranno esito positivo quando vengono eseguite sui backup creati prima dell'aggiornamento dello storage, in quanto i backup contengono i dettagli dello storage precedente. È necessario eseguire l'API di refresh della tecnologia storage o il cmdlet per aggiornare i vecchi backup in SnapCenter con i nuovi dettagli storage.

Il tech refresh è supportato per i seguenti plug-in SnapCenter:

- Plug-in SnapCenter per Microsoft SQL Server
- Plug-in SnapCenter per Windows
- Plug-in SnapCenter per database Oracle
- Plug-in SnapCenter per database SAP HANA
- Plug-in SnapCenter per server Microsoft Exchange

I casi d'utilizzo supportati sono:

- Refresh dello storage primario

  L'aggiornamento tecnologico dello storage è supportato per sostituire lo storage primario con il nuovo storage. Non è possibile convertire lo storage secondario esistente in uno storage primario.

- Refresh dello storage secondario

Gli altri scenari supportati sono:

- Modifica del nome della SVM
- Modifica del nome del volume

Aggiornare i backup dello storage primario

Quando lo storage viene tech refresh, è necessario eseguire l'API o il cmdlet per l'aggiornamento dei vecchi backup in SnapCenter con i nuovi dettagli dello storage.

Prima di iniziare

Poiché questo workflow modifica i dati nel repository SnapCenter, si consiglia di eseguire il backup del repository SnapCenter. In caso di problemi con i dati, il repository SnapCenter può essere riportato allo stato precedente utilizzando il backup.

Per ulteriori informazioni, fare riferimento a "Eseguire il backup del repository SnapCenter".

Fasi

1. Migrazione dei dati dal vecchio storage al nuovo storage.

   Per informazioni su come eseguire la migrazione, fare riferimento a:

   - "Come migrare i dati in un nuovo storage"
   - "Come si copia un volume e come si conservano tutte le copie Snapshot?"
2. Impostare l'host sulla modalità di manutenzione.
3. Montare il nuovo storage nei rispettivi host e visualizzare i database.

   Il nuovo dispositivo di archiviazione deve essere collegato all'host come in precedenza. Ad esempio, se fosse connessa come SAN, deve essere connessa come SAN.

   Il nuovo storage deve essere montato sulla stessa unità o percorso del vecchio storage.

4. Verificare che tutte le risorse siano attive e in funzione.
5. Aggiungi il nuovo storage in SnapCenter.

Assicurati di avere un nome SVM univoco tra i cluster in SnapCenter. Se stai utilizzando lo stesso nome SVM nel nuovo storage e se è possibile migrare tutti i volumi della SVM prima di eseguire il refresh dello storage, si consiglia quindi di eliminare la SVM nel vecchio cluster e riscoprire il vecchio cluster in SnapCenter, in modo da rimuovere la SVM dalla cache.

6. Impostare l'host in modalità di produzione.
7. In SnapCenter, creare un backup delle risorse di cui viene eseguita la migrazione dello storage. È necessario un nuovo backup affinché SnapCenter possa identificare l'impatto più recente dello storage, che verrà utilizzato per aggiornare i metadati dei vecchi backup esistenti.

> Ogni volta che un nuovo LUN viene collegato all'host, avrà un nuovo numero di serie. Durante il rilevamento del file system di Windows, SnapCenter tratterà ogni numero seriale univoco come nuova risorsa. Durante l'aggiornamento tecnico dello storage, quando il LUN del nuovo storage viene collegato all'host con la stessa lettera o percorso dell'unità, il rilevamento del file system di Windows in SnapCenter contrassegnerà la risorsa esistente come eliminata anche se è montata con la stessa lettera o percorso di unità e visualizzerà il nuovo LUN come nuova risorsa. Poiché la risorsa viene contrassegnata come eliminata, non verrà presa in considerazione per il tech refresh dello storage in SnapCenter e tutti i backup della risorsa precedente andranno persi. In caso di aggiornamento dello storage, per le risorse del file system Windows, il rilevamento delle risorse non deve essere eseguito prima di eseguire l'API di refresh dello storage o il cmdlet.

8. Eseguire l'API di aggiornamento dello storage: O il cmdlet: `/5.0/techrefresh/primarystorage` *Invoke-SmTechRefreshPrimaryStorage*.

> Se la risorsa è configurata con un criterio abilitato per la replica, il backup più recente dopo l'aggiornamento dello storage dovrebbe contenere i dettagli dello storage secondario.

   a. Se si utilizza il setup delle istanze del cluster di failover SQL (FCI), i backup vengono mantenuti a livello di cluster. Fornire il nome del cluster come input per l'aggiornamento della tecnologia di storage.
   b. Se si utilizza l'installazione di SQL Availability Group (AG), i backup vengono mantenuti a livello di nodo. Fornire il nome del nodo come input per l'aggiornamento tecnologico dello storage.
   c. Se si utilizza l'installazione di Oracle Real Application Clusters (RAC), è possibile eseguire l'aggiornamento tecnico dello storage su qualsiasi nodo.

      L'attributo *IsDryRun* è impostato su True per impostazione predefinita. Consente di identificare le risorse per le quali viene aggiornato lo storage. È possibile visualizzare la risorsa e i dettagli di archiviazione modificati eseguendo l'API: "5,0/Jobs/{jobid}" o il cmdlet *get-SmJobSummaryReport*.

9. Dopo aver verificato i dettagli dello storage, impostare l'attributo *IsDryRun* su False ed eseguire l'API di aggiornamento dello storage: O il cmdlet: `/5.0/techrefresh/primarystorage` *Invoke-SmTechRefreshPrimaryStorage*.

   In questo modo verranno aggiornati i dettagli di archiviazione nei backup precedenti.

   È possibile eseguire più volte l'API o il cmdlet sullo stesso host; i dettagli dello storage nei backup meno recenti verranno aggiornati solo se lo storage viene aggiornato.

> Non è possibile migrare la gerarchia di cloni in ONTAP. Se lo storage da migrare contiene metadati cloni in SnapCenter, la risorsa clonata verrà contrassegnata come risorsa indipendente. I cloni dei metadati dei cloni verranno rimossi in modo ricorsivo.

10. (Facoltativo) se tutti gli snapshot non vengono spostati dal vecchio storage primario al nuovo storage primario, eseguire la seguente API: `/5.0/hosts/primarybackupsexistencecheck` O il cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

    In questo modo verrà eseguito il controllo dell'esistenza dello snapshot sul nuovo storage primario e verranno contrassegnati i rispettivi backup non disponibili per alcuna operazione in SnapCenter.

Aggiornare i backup dello storage secondario

Quando lo storage viene tech refresh, è necessario eseguire l'API o il cmdlet per l'aggiornamento dei vecchi backup in SnapCenter con i nuovi dettagli dello storage.

Prima di iniziare

Poiché questo workflow modifica i dati nel repository SnapCenter, si consiglia di eseguire il backup del repository SnapCenter. In caso di problemi con i dati, il repository SnapCenter può essere riportato allo stato precedente utilizzando il backup.

Per ulteriori informazioni, fare riferimento a "Eseguire il backup del repository SnapCenter".

Fasi

1. Migrazione dei dati dal vecchio storage al nuovo storage.

    Per informazioni su come eseguire la migrazione, fare riferimento a:

    - "Come migrare i dati in un nuovo storage"
    - "Come si copia un volume e come si conservano tutte le copie Snapshot?"
2. Stabilire la relazione SnapMirror tra lo storage primario e il nuovo storage secondario e verificare che lo stato della relazione sia integro.
3. In SnapCenter, creare un backup delle risorse di cui viene eseguita la migrazione dello storage.

    È necessario un nuovo backup affinché SnapCenter identifichi l'impatto più recente dello storage e venga utilizzato per aggiornare i metadati dei vecchi backup esistenti.

    > Attendere il completamento di questa operazione. Se si passa alla fase successiva prima del completamento, SnapCenter perderà completamente i metadati dello snapshot secondario precedente.

4. Dopo aver creato correttamente il backup di tutte le risorse in un host, eseguire l'API di aggiornamento dello storage secondario: O il cmdlet: `/5.0/techrefresh/secondarystorage` *Invoke-SmTechRefreshSecondaryStorage*.

    In questo modo verranno aggiornati i dettagli dello storage secondario dei backup precedenti nell'host specificato.

    Se si desidera eseguire questa operazione a livello di risorsa, fare clic su **Aggiorna** per ogni risorsa per aggiornare i metadati di archiviazione secondari.

5. Dopo aver aggiornato con successo i backup meno recenti, è possibile interrompere la vecchia relazione tra lo storage secondario e lo storage primario.

Disinstallare il server SnapCenter e i plug-in

Disinstallare i pacchetti di plug-in di SnapCenter

Prerequisiti per la rimozione di un host

È possibile rimuovere gli host e disinstallare singoli plug-in o pacchetti di plug-in utilizzando l'interfaccia grafica di SnapCenter. È inoltre possibile disinstallare singoli plug-in o pacchetti di plug-in su host remoti utilizzando l'interfaccia della riga di comando (CLI) sull'host del server SnapCenter o utilizzando l'opzione Windows **Disinstalla un programma** localmente su qualsiasi host.

Prima di rimuovere un host dal server SnapCenter, è necessario completare i prerequisiti.

- Devi effettuare l'accesso come amministratore.
- Se si utilizzano plug-in personalizzati di SnapCenter, è necessario eliminare tutti i cloni da SnapCenter associati all'host.
- Assicurarsi che i processi di rilevamento non siano in esecuzione sull'host.
- È necessario assegnare un ruolo con le autorizzazioni necessarie per rimuovere tutti gli oggetti associati all'host. In caso contrario, l'operazione di rimozione non riesce.
- Se la chiave SSH è stata modificata dopo aver aggiunto l'host a SnapCenter, confermare l'impronta digitale.
- Confermare l'impronta digitale se l'host SnapCenter viene aggiornato a una versione successiva di SnapCenter ma l'host del plug-in esegue ancora una versione precedente del plug-in.

Prerequisiti per rimuovere un host utilizzando il controllo degli accessi basato sui ruoli

- Si dovrebbe aver effettuato l'accesso utilizzando un ruolo RBAC che dispone delle autorizzazioni di lettura, eliminazione dell'host, installazione, disinstallazione del plug-in ed eliminazione degli oggetti.

  Gli oggetti possono essere cloni, backup, gruppo di risorse, sistema di storage e così via.

- L'utente RBAC dovrebbe essere stato aggiunto al ruolo RBAC.
- Assegnare l'utente RBAC all'host, al plug-in, alle credenziali, ai gruppi di risorse e al sistema di storage (per cloni) che si desidera eliminare.
- Dovresti aver effettuato l'accesso a SnapCenter come utente RBAC.

Prerequisiti per rimuovere un host con cloni creati dall'operazione di ciclo di vita dei cloni

- I lavori cloni dovrebbero essere stati creati utilizzando la gestione del ciclo di vita dei cloni per i database SQL.
- Si dovrebbe aver creato un ruolo RBAC con le autorizzazioni di lettura ed eliminazione dei cloni, lettura ed eliminazione delle risorse, lettura ed eliminazione dei gruppi di risorse, lettura ed eliminazione dello storage, provisioning delle autorizzazioni di lettura ed eliminazione, montaggio, disinstallazione, installazione e disinstallazione dei plug-in, lettura ed eliminazione degli host.
- L'utente RBAC dovrebbe essere stato assegnato al ruolo RBAC.
- L'utente RBAC deve essere stato assegnato all'host, al plug-in SnapCenter per Microsoft SQL Server, alle

credenziali, al gruppo di risorse del ciclo di vita dei cloni e al sistema di storage.

- Dovresti aver effettuato l'accesso a SnapCenter come utente RBAC.

Per informazioni sulla disinstallazione del plug-in SnapCenter per VMware vSphere, vedere Rimuovi plug-in SnapCenter per vmware vsphere.

Rimuovere un host

Quando il server SnapCenter rimuove un host, rimuove prima il backup, i cloni, i processi di clonazione, i gruppi di risorse e le risorse elencati per tale host nella pagina risorse SnapCenter, quindi disinstalla i pacchetti plug-in sull'host.

A proposito di questa attività

- Se si elimina un host, vengono eliminati anche i backup, i cloni e i gruppi di risorse associati all'host.
- Quando si rimuovono i gruppi di risorse, vengono rimosse anche tutte le pianificazioni associate.
- Se l'host dispone di un gruppo di risorse condiviso con un altro host ed è stato eliminato l'host, anche il gruppo di risorse viene eliminato.
- Utilizzare il cmdlet *Remove-SmHost* per rimuovere gli host plug-in decommissionati o irraggiungibili.

  Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche alla "Guida di riferimento al cmdlet del software SnapCenter"

- Il tempo necessario per rimuovere un host dipende dal numero di backup e dalle impostazioni di conservazione. Ciò avviene perché le Snapshot vengono eliminate da ciascun controller e i metadati vengono ripuliti.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina **hosts**, fare clic su **Managed hosts**.
3. Selezionare l'host che si desidera rimuovere, quindi fare clic su **Remove** (Rimuovi).
4. Per i cluster Oracle RAC, per rimuovere il software SnapCenter da tutti gli host del cluster, selezionare **include all the hosts of cluster** (Includi tutti gli host del cluster).

   È anche possibile rimuovere un nodo di un cluster e in questo modo rimuovere tutti i nodi uno alla volta.

5. Fare clic su **OK**.

> Quando si disinstallano e reinstallano i plug-in host su un cluster, le risorse del cluster non vengono rilevate automaticamente. Selezionare il nome host del cluster, quindi fare clic su **Refresh Resources** (Aggiorna risorse) per rilevare automaticamente le risorse del cluster.

Disinstallare i plug-in utilizzando l'interfaccia grafica di SnapCenter

Quando si decide di non richiedere più un singolo plug-in o un pacchetto plug-in, è possibile disinstallarlo utilizzando l'interfaccia di SnapCenter.

Prima di iniziare

- Dovrebbero essere stati rimossi i gruppi di risorse per il pacchetto plug-in che si sta disinstallando.
- I criteri associati ai gruppi di risorse per il pacchetto plug-in che si sta disinstallando dovrebbero essere stati scollegati.

A proposito di questa attività

È possibile disinstallare un singolo plug-in. Ad esempio, potrebbe essere necessario disinstallare il plug-in SnapCenter per Microsoft SQL Server perché un host sta esaurendo le risorse e si desidera spostare il plug-in in in un host più potente. È inoltre possibile disinstallare un intero pacchetto plug-in. Ad esempio, potrebbe essere necessario disinstallare il pacchetto di plug-in SnapCenter per Linux, che include il plug-in SnapCenter per database Oracle e il plug-in SnapCenter per UNIX.

- La rimozione di un host include la disinstallazione di tutti i plug-in.

  Quando si rimuove un host da SnapCenter, SnapCenter disinstalla tutti i pacchetti plug-in sull'host prima di rimuoverlo.

- L'interfaccia grafica di SnapCenter rimuove i plug-in da un host alla volta.

  Quando si utilizza l'interfaccia grafica di SnapCenter, è possibile disinstallare i plug-in su un solo host alla volta. Tuttavia, è possibile eseguire diverse operazioni di disinstallazione contemporaneamente.

  È inoltre possibile disinstallare un plug-in da più host utilizzando il cmdlet *Uninstall-SmHostPackage* e i parametri richiesti. Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

> La disinstallazione del pacchetto di plug-in SnapCenter per Windows da un host su cui è installato il server SnapCenter danneggerà l'installazione del server SnapCenter. Non disinstallare il pacchetto di plug-in SnapCenter per Windows, a meno che non si sia certi di non aver più bisogno del server SnapCenter.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Nella pagina host gestiti, selezionare l'host dal quale si desidera disinstallare il pacchetto plug-in o plug-in.
4. Accanto al plug-in che si desidera rimuovere, fare clic su **Rimuovi** > **Invia**.

Al termine

Attendere 5 minuti prima di reinstallare il plug-in su tale host. Questo periodo di tempo è sufficiente per l'aggiornamento dello stato dell'host gestito da parte dell'interfaccia grafica utente di SnapCenter. L'installazione non riesce se si reinstalla immediatamente il plug-in.

Se si disinstalla il pacchetto di plug-in SnapCenter per Linux, i file di log specifici per la disinstallazione sono disponibili all'indirizzo: */custom_location/snapcenter/log*.

Disinstallare i plug-in di Windows utilizzando il cmdlet PowerShell

È possibile disinstallare singoli plug-in o disinstallare pacchetti di plug-in da uno o più host utilizzando il cmdlet *Uninstall-SmHostPackage* nell'interfaccia della riga di comando dell'host server SnapCenter.

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera disinstallare i plug-in.

Fasi

1. Avviare PowerShell.
2. Nell'host del server SnapCenter, immettere il comando https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME_ _Open-SMConnection -SMSbaseUrl, quindi immettere le credenziali.
3. Disinstallare i plug-in di Windows utilizzando il cmdlet *Uninstall-SmHostPackage* e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, è anche possibile fare riferimento a "Guida di riferimento al cmdlet del software SnapCenter".

Disinstallare i plug-in localmente su un host

È possibile disinstallare i plug-in SnapCenter localmente su un host se non è possibile raggiungere l'host dal server SnapCenter.

A proposito di questa attività

La procedura consigliata per disinstallare singoli plug-in o pacchetti plug-in consiste nell'utilizzare la GUI di SnapCenter o il cmdlet Uninstall-SmHostPackage sull'interfaccia della riga di comando dell'host server SnapCenter. Queste procedure consentono al server SnapCenter di rimanere aggiornato su eventuali modifiche.

Tuttavia, potrebbe essere raro disinstallare i plug-in localmente. Ad esempio, è possibile che sia stato eseguito un processo di disinstallazione dal server SnapCenter ma il processo non è riuscito oppure che il server SnapCenter e i plug-in orfani siano stati disinstallati su un host.

La disinstallazione locale di un pacchetto plug-in su un host non elimina i dati associati all'host, ad esempio i processi pianificati e i metadati di backup.

Non tentare di disinstallare il pacchetto di plug-in SnapCenter per Windows localmente dal pannello di controllo. È necessario utilizzare l'interfaccia grafica di SnapCenter per assicurarsi che il plug-in SnapCenter per Microsoft Windows sia stato disinstallato correttamente.

Fasi

1. Sul sistema host, accedere al pannello di controllo e fare clic su **Disinstalla un programma**.
2. Nell'elenco dei programmi, selezionare il plug-in o il pacchetto plug-in SnapCenter che si desidera disinstallare e fare clic su **Disinstalla**.

   Windows disinstalla tutti i plug-in del pacchetto selezionato.

Disinstallare il pacchetto plug-in per Linux o AIX utilizzando CLI

È possibile disinstallare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX utilizzando l'interfaccia della riga di comando.

Prima di iniziare

- Assicurarsi di aver eliminato i processi pianificati
- Assicurarsi che tutti i lavori in esecuzione siano stati completati.

Fase

Eseguire */custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall* per disinstallare.

Disinstallare il server SnapCenter

Se non si desidera più utilizzare il server SnapCenter per gestire i processi di protezione dei dati, è possibile disinstallare il server SnapCenter utilizzando il pannello di controllo programmi e funzionalità dell'host del server SnapCenter. La disinstallazione del server SnapCenter rimuove tutti i suoi componenti.

Prima di iniziare

- Assicurarsi di disporre di almeno 2 GB di spazio libero sul disco in cui è installato il server SnapCenter.
- Assicurarsi che il dominio in cui è installato il server SnapCenter non sia stato rimosso.

  Se si rimuove il dominio in cui è stato installato il server SnapCenter e si tenta di eseguire la disinstallazione, l'operazione non riesce.

- Il backup del database del repository dovrebbe essere stato eseguito perché il database del repository verrà pulito e disinstallato.

Fasi

1. Sull'host del server SnapCenter, accedere al pannello di controllo.
2. Assicurarsi di essere nella vista **Categoria**.
3. In programmi, fare clic su **Disinstalla un programma**.

   Viene visualizzata la finestra programmi e funzionalità.

4. Selezionare il server NetApp SnapCenter, quindi fare clic su **Disinstalla**.

   Da SnapCenter 4.2, quando disinstalli il server SnapCenter, tutti i suoi componenti, incluso il database del repository MySQL Server, vengono disinstallati.

   - La rimozione del nodo NLB da un cluster NLB richiede il riavvio dell'host del server SnapCenter. Se non si riavvia l'host, potrebbe verificarsi un errore se si tenta di reinstallare il server SnapCenter.
   - È necessario disinstallare manualmente .NET Framework che non viene rimosso durante la disinstallazione.

Automatizzare utilizzando le API REST

Panoramica delle API REST

Le API REST possono essere utilizzate per eseguire diverse operazioni di gestione SnapCenter. Le API REST sono esposte attraverso la pagina web di Swagger.

È possibile accedere alla pagina Web Swagger disponibile all'indirizzo _ https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/_ per visualizzare la documentazione dell'API REST e per effettuare manualmente una chiamata API.

I plug-in che supportano le API REST sono:

- Plug-in per Microsoft SQL Server
- Plug-in per SAP HANA Database
- Plug-in personalizzati
- Plug-in per Oracle Database

Come accedere all'API REST di SnapCenter in modo nativo

È possibile accedere direttamente all'API REST di SnapCenter utilizzando qualsiasi linguaggio di programmazione che supporti un client REST. Le lingue più diffuse includono Python, PowerShell e Java.

Base REST per i web Services

Representational state Transfer (REST) è uno stile per la creazione di applicazioni web distribuite. Quando viene applicato alla progettazione di un'API di servizi Web, stabilisce un insieme di tecnologie e Best practice per esporre le risorse basate su server e gestirne gli stati. Utilizza protocolli e standard mainstream per fornire una base flessibile per la gestione di SnapCenter.

Risorse e rappresentazione dello stato

Le risorse sono i componenti di base di un sistema basato su web. Quando si crea un'applicazione di servizi Web REST, le attività di progettazione iniziali includono:

Identificazione delle risorse di sistema o basate su server

Ogni sistema utilizza e gestisce le risorse. Una risorsa può essere un file, una transazione di business, un processo o un'entità amministrativa. Una delle prime attività nella progettazione di un'applicazione basata sui servizi web REST è quella di identificare le risorse.

Definizione degli stati delle risorse e delle operazioni di stato associate

Le risorse si trovano sempre in un numero limitato di stati. Gli stati, così come le operazioni associate utilizzate per influenzare i cambiamenti di stato, devono essere chiaramente definiti.

Endpoint URI

Ogni risorsa REST deve essere definita e resa disponibile utilizzando uno schema di indirizzamento ben definito. Gli endpoint in cui sono situate e identificate le risorse utilizzano un URI (Uniform Resource Identifier).

L'URI fornisce un framework generale per la creazione di un nome univoco per ogni risorsa nella rete. L'URL (Uniform Resource Locator) è un tipo di URI utilizzato con i servizi Web per identificare e accedere alle risorse. Le risorse sono in genere esposte in una struttura gerarchica simile a una directory di file.

Messaggi HTTP

HTTP (Hypertext Transfer Protocol) è il protocollo utilizzato dal client e dal server dei servizi Web per scambiare messaggi di richiesta e risposta relativi alle risorse.

Durante la progettazione di un'applicazione di servizi Web, i metodi HTTP vengono mappati alle risorse e alle azioni di gestione dello stato corrispondenti. HTTP è stateless. Pertanto, per associare un insieme di richieste e risposte correlate come parte di una transazione, è necessario includere informazioni aggiuntive nelle intestazioni HTTP portate con i flussi di dati di richiesta e risposta.

Formattazione JSON

Sebbene le informazioni possano essere strutturate e trasferite tra un client e un server di servizi Web in diversi modi, l'opzione più diffusa è JavaScript Object Notation (JSON).

JSON è uno standard di settore per la rappresentazione di semplici strutture di dati in testo normale e viene utilizzato per trasferire informazioni di stato che descrivono le risorse. L'API REST di SnapCenter utilizza JSON per formattare i dati trasportati nel corpo di ogni richiesta e risposta HTTP.

Caratteristiche operative di base

Mentre REST stabilisce un insieme comune di tecnologie e Best practice, i dettagli di ciascuna API possono variare in base alle scelte di progettazione.

Transazione API di richiesta e risposta

Ogni chiamata API REST viene eseguita come richiesta HTTP al sistema del server SnapCenter che genera una risposta associata al client. Questa coppia di richieste e risposte è considerata una transazione API.

Prima di utilizzare l'API, è necessario conoscere le variabili di input disponibili per controllare una richiesta e il contenuto dell'output della risposta.

Supporto per le operazioni CRUD

Si accede a ciascuna delle risorse disponibili tramite l'API REST SnapCenter in base al modello CRUD:

- Creare
- Leggi
- Aggiornare
- Eliminare

Per alcune delle risorse, è supportato solo un sottoinsieme delle operazioni.

Identificatori di oggetti

A ogni istanza o oggetto di risorsa viene assegnato un identificatore univoco al momento della creazione. Nella maggior parte dei casi, l'identificatore è un UUID a 128 bit. Questi identificatori sono univoci a livello globale all'interno di uno specifico server SnapCenter.

Dopo aver eseguito una chiamata API che crea una nuova istanza di oggetto, un URL con l'ID associato viene restituito al chiamante nell'intestazione di posizione della risposta HTTP. È possibile estrarre l'identificatore e utilizzarlo nelle chiamate successive quando si fa riferimento all'istanza della risorsa.

Il contenuto e la struttura interna degli identificatori di oggetti possono cambiare in qualsiasi momento. È necessario utilizzare gli identificatori delle chiamate API applicabili solo se necessario quando si fa riferimento agli oggetti associati.

Istanze e raccolte di oggetti

A seconda del percorso di risorsa e del metodo HTTP, una chiamata API può essere applicata a un'istanza di oggetto specifica o a un insieme di oggetti.

Operazioni sincrone e asincrone

SnapCenter esegue una richiesta HTTP ricevuta da un client in modo sincrono o asincrono.

Elaborazione sincrona

SnapCenter esegue immediatamente la richiesta e risponde con un codice di stato HTTP 200 o 201 se l'operazione ha esito positivo.

Ogni richiesta che utilizza il metodo GET viene sempre eseguita in modo sincrono. Inoltre, le richieste che utilizzano IL POST sono progettate per essere eseguite in modo sincrono se si prevede che vengano completate in meno di due secondi.

Elaborazione asincrona

Se una richiesta asincrona è valida, SnapCenter crea un'attività in background per elaborare la richiesta e un oggetto di lavoro per ancorare l'attività. Il codice di stato HTTP 202 viene restituito al chiamante insieme all'oggetto lavoro. È necessario recuperare lo stato del lavoro per determinare il successo o l'errore.

Le richieste che utilizzano i metodi POST e DELETE sono progettate per essere eseguite in modo asincrono se il completamento richiede più di due secondi.

Sicurezza

La sicurezza fornita con L'API REST si basa principalmente sulle funzionalità di sicurezza esistenti disponibili con SnapCenter. L'API utilizza la seguente protezione:

Transport Layer Security

Tutto il traffico inviato in rete tra il server SnapCenter e il client viene in genere crittografato utilizzando TLS, in base alle impostazioni di configurazione di SnapCenter.

Autenticazione HTTP

A livello HTTP, per le transazioni API viene utilizzata l'autenticazione di base. A ogni richiesta viene aggiunta un'intestazione HTTP con nome utente e password in una stringa base64.

Variabili di input che controllano una richiesta API

È possibile controllare la modalità di elaborazione di una chiamata API attraverso parametri e variabili impostati nella richiesta HTTP.

Metodi HTTP

I metodi HTTP supportati dall'API REST di SnapCenter sono illustrati nella seguente tabella.

Non tutti i metodi HTTP sono disponibili in ogni endpoint REST.

Metodo HTTP	Descrizione
OTTIENI	Recupera le proprietà dell'oggetto su un'istanza o una raccolta di risorse.
POST	Crea una nuova istanza di risorsa in base all'input fornito.
ELIMINARE	Elimina un'istanza di risorsa esistente.
IN PRIMO PIANO	Modifica un'istanza di risorsa esistente.

Intestazioni delle richieste

È necessario includere diverse intestazioni nella richiesta HTTP.

Tipo di contenuto

Se il corpo della richiesta include JSON, questa intestazione deve essere impostata su *application/json*.

Accettare

Questa intestazione deve essere impostata su *application/json*.

Autorizzazione

L'autenticazione di base deve essere impostata con il nome utente e la password codificati come stringa base64.

Corpo della richiesta

Il contenuto del corpo della richiesta varia in base alla chiamata specifica. Il corpo della richiesta HTTP è costituito da uno dei seguenti elementi:

- Oggetto JSON con variabili di input
- Vuoto

Filtraggio degli oggetti

Quando si esegue una chiamata API che utilizza GET, è possibile limitare o filtrare gli oggetti restituiti in base a qualsiasi attributo. Ad esempio, è possibile specificare un valore esatto da associare:

```
<field>=<query value>
```

Oltre a una corrispondenza esatta, sono disponibili altri operatori per restituire un set di oggetti su un intervallo di valori. L'API REST di SnapCenter supporta gli operatori di filtraggio mostrati nella tabella seguente.

Operatore	Descrizione
=	Uguale a.
<	Inferiore a.
>	Maggiore di
⇐	Minore o uguale a.
>=	Maggiore o uguale a.
AGGIORNARE	Oppure
!	Non uguale a.
*	Goloso carattere jolly

È inoltre possibile restituire un insieme di oggetti in base all'impostazione o meno di un campo specifico utilizzando la parola chiave **null** o la relativa negazione **!null** come parte della query.

Tutti i campi non impostati sono generalmente esclusi dalle query corrispondenti.

Richiesta di campi oggetto specifici

Per impostazione predefinita, l'emissione di una chiamata API utilizzando GET restituisce solo gli attributi che identificano in modo univoco lo o gli oggetti. Questo insieme minimo di campi funge da chiave per ciascun oggetto e varia in base al tipo di oggetto. È possibile selezionare ulteriori proprietà dell'oggetto utilizzando il `fields` parametro di query nei seguenti modi:

Campi comuni o standard

Specificare **fields=*** per recuperare i campi oggetto più comunemente utilizzati. Questi campi vengono generalmente mantenuti nella memoria del server locale o richiedono un'elaborazione ridotta per l'accesso. Si tratta delle stesse proprietà restituite per un oggetto dopo l'utilizzo DI GET con una chiave UUID (URL PATH Key).

Tutti i campi

Specificare **fields=**** per recuperare tutti i campi oggetto, inclusi quelli che richiedono un'ulteriore elaborazione del server per l'accesso.

Selezione di campi personalizzati

Utilizzare **fields=<field_name>** per specificare il campo desiderato. Quando si richiedono più campi, i valori devono essere separati utilizzando virgole senza spazi.

Come Best practice, devi sempre identificare i campi specifici che desideri. Recuperare solo il set di campi comuni o tutti i campi quando necessario. I campi classificati come comuni e restituiti utilizzando *fields*=*, vengono determinati da NetApp in base all'analisi interna delle performance. La classificazione di un campo potrebbe cambiare nelle release future.

Ordinamento degli oggetti nel set di output

I record di una raccolta di risorse vengono restituiti nell'ordine predefinito definito dall'oggetto. È possibile modificare l'ordine utilizzando il `order_by` parametro query con il nome del campo e la direzione di ordinamento come segue:

```
order_by=<field name> asc|desc
```

Ad esempio, è possibile ordinare il campo tipo in ordine decrescente seguito da id in ordine crescente:

```
order_by=type desc, id asc
```

- Se si specifica un campo di ordinamento ma non si fornisce una direzione, i valori vengono ordinati in ordine crescente.
- Quando si includono più parametri, è necessario separare i campi con una virgola.

Impaginazione durante il recupero di oggetti in una raccolta

Quando si esegue una chiamata API utilizzando GET per accedere a un insieme di oggetti dello stesso tipo, SnapCenter tenta di restituire il maggior numero possibile di oggetti in base a due vincoli. È possibile controllare ciascuno di questi vincoli utilizzando parametri di query aggiuntivi sulla richiesta. Il primo vincolo raggiunto per una richiesta GET specifica termina la richiesta e limita quindi il numero di record restituiti.

Se una richiesta termina prima di scorrere tutti gli oggetti, la risposta contiene il collegamento necessario per recuperare il batch successivo di record.

Limitazione del numero di oggetti

Per impostazione predefinita, SnapCenter restituisce un massimo di 10,000 oggetti per una richiesta GET. È possibile modificare questo limite utilizzando il parametro di query *max_records*. Ad esempio:

```
max_records=20
```

Il numero di oggetti effettivamente restituiti può essere inferiore al massimo effettivo, in base al relativo vincolo temporale e al numero totale di oggetti nel sistema.

Limitare il tempo impiegato per recuperare gli oggetti

Per impostazione predefinita, SnapCenter restituisce il maggior numero di oggetti possibile entro il tempo consentito per la richiesta GET. Il timeout predefinito è 15 secondi. È possibile modificare questo limite utilizzando il parametro di query *return_timeout*. Ad esempio:

```
return_timeout=5
```

Il numero di oggetti effettivamente restituiti può essere inferiore al massimo effettivo, in base al vincolo relativo al numero di oggetti e al numero totale di oggetti nel sistema.

Restringimento del set di risultati

Se necessario, è possibile combinare questi due parametri con altri parametri di query per restringere il set di risultati. Ad esempio, quanto segue restituisce fino a 10 eventi EMS generati dopo il tempo specificato:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

È possibile inviare più richieste per scorrere gli oggetti. Ogni successiva chiamata API deve utilizzare un nuovo valore temporale basato sull'ultimo evento dell'ultimo set di risultati.

Proprietà delle dimensioni

I valori di input utilizzati con alcune chiamate API e alcuni parametri di query sono numerici. Invece di fornire un numero intero in byte, è possibile utilizzare un suffisso come mostrato nella tabella seguente.

Suffisso	Descrizione
KB	KB kilobyte (1024 byte) o kibyte
MB	MB Megabyte (KB x 1024 byte) o megibyte
GB	GB Gigabyte (MB x 1024 byte) o gibibyte
TB	TB terabyte (GB x 1024 byte) o tebibyte
PB	PB petabyte (TB x 1024 byes) o pebibyte

Interpretazione di una risposta API

Ogni richiesta API genera una risposta al client. È necessario esaminare la risposta per determinare se è stata eseguita correttamente e recuperare dati aggiuntivi in base alle necessità.

Codice di stato HTTP

I codici di stato HTTP utilizzati dall'API REST SnapCenter sono descritti di seguito.

Codice	Descrizione
200	OK indica che le chiamate che non creano un nuovo oggetto sono riuscite.
201	Creazione di un oggetto completata. L'intestazione della posizione nella risposta include l'identificatore univoco dell'oggetto.
202	Accettato Un lavoro in background è stato avviato per eseguire la richiesta, ma non è stato ancora completato.
400	Richiesta errata l'input della richiesta non è riconosciuto o non è appropriato.
401	Autenticazione utente non autorizzata non riuscita.

Codice	Descrizione
403	Accesso non consentito negato a causa di un errore di autorizzazione (RBAC).
404	Non trovato la risorsa a cui si fa riferimento nella richiesta non esiste.
405	Metodo non consentito il metodo HTTP nella richiesta non è supportato per la risorsa.
409	Conflitto un tentativo di creazione di un oggetto non è riuscito perché è necessario creare prima un oggetto diverso oppure l'oggetto richiesto esiste già.
500	Errore interno Si è verificato Un errore interno generale nel server.

Intestazioni delle risposte

Nella risposta HTTP generata da SnapCenter sono incluse diverse intestazioni.

Posizione

Quando viene creato un oggetto, l'intestazione di posizione include l'URL completo del nuovo oggetto, incluso l'identificatore univoco assegnato all'oggetto.

Tipo di contenuto

Questo sarà normalmente `application/json`.

Corpo di risposta

Il contenuto del corpo di risposta risultante da una richiesta API varia in base all'oggetto, al tipo di elaborazione e al successo o all'errore della richiesta. Il rendering della risposta viene sempre eseguito in JSON.

Oggetto singolo

È possibile restituire un singolo oggetto con un set di campi in base alla richiesta. AD esempio, È possibile utilizzare GET per recuperare le proprietà selezionate di un cluster utilizzando l'identificatore univoco.

Oggetti multipli

È possibile restituire più oggetti di una raccolta di risorse. In tutti i casi, viene utilizzato un formato coerente, con `num_records` l'indicazione del numero di record e record contenenti una matrice delle istanze dell'oggetto. Ad esempio, è possibile recuperare i nodi definiti in un cluster specifico.

Oggetto lavoro

Se una chiamata API viene elaborata in modo asincrono, viene restituito un oggetto Job che ancora l'attività in background. Ad esempio, la richiesta DI PATCH utilizzata per aggiornare la configurazione del cluster viene elaborata in modo asincrono e restituisce un oggetto Job.

Oggetto di errore

Se si verifica un errore, viene sempre restituito un oggetto Error. Ad esempio, si riceve un errore quando si tenta di modificare un campo non definito per un cluster.

Vuoto

In alcuni casi, non viene restituito alcun dato e il corpo della risposta include un oggetto JSON vuoto.

Errori

Se si verifica un errore, viene restituito un oggetto di errore nel corpo della risposta.

Formato

Un oggetto di errore ha il seguente formato:

```
"error": {
"message": "<string>",
"code": <integer>[,
"target": "<string>"]
}
```

È possibile utilizzare il valore del codice per determinare il tipo o la categoria di errore generale e il messaggio per determinare l'errore specifico. Se disponibile, il campo di destinazione include l'input utente specifico associato all'errore.

Codici di errore comuni

I codici di errore più comuni sono descritti nella seguente tabella. Le chiamate API specifiche possono includere codici di errore aggiuntivi.

Codice	Descrizione
409	Esiste già un oggetto con lo stesso identificatore.
400	Il valore di un campo ha un valore non valido o manca oppure è stato fornito un campo aggiuntivo.
400	L'operazione non è supportata.
405	Impossibile trovare un oggetto con l'identificatore specificato.
403	L'autorizzazione per eseguire la richiesta viene negata.
409	La risorsa è in uso.

API REST supportate per il server e i plug-in SnapCenter

Le risorse disponibili tramite l'API REST di SnapCenter sono organizzate in categorie, come mostrato nella pagina di documentazione dell'API di SnapCenter. Di seguito viene

presentata una breve descrizione di ciascuna delle risorse con i percorsi delle risorse di base, insieme a ulteriori considerazioni sull'utilizzo, se del caso.

Auth

È possibile utilizzare questa API per accedere al server SnapCenter. Questa API restituisce un token di autorizzazione utente utilizzato per autenticare le richieste successive.

Domini

È possibile utilizzare le API per eseguire diverse operazioni.

- Recuperare tutti i domini in SnapCenter
- recuperare i dettagli di un dominio specifico
- registrare o annullare la registrazione di un dominio
- modificare un dominio

Lavori

È possibile utilizzare le API per eseguire diverse operazioni.

- Recuperare tutti i lavori in SnapCenter
- recuperare lo stato di un lavoro
- annullare o interrompere un lavoro

Impostazioni

È possibile utilizzare le API per eseguire diverse operazioni.

- registrare, modificare o rimuovere una credenziale
- Visualizza le informazioni sulle credenziali registrate nel server SnapCenter
- configurare le impostazioni di notifica
- Recupera le informazioni sul server SMTP attualmente configurato per l'invio di notifiche e-mail e visualizza il nome del server SMTP, il nome dei destinatari e il nome del mittente
- Visualizza la configurazione di autenticazione a più fattori (MFA) dell'accesso al server SnapCenter
- Attivare o disattivare e configurare MFA per l'accesso al server SnapCenter
- Creare il file di configurazione richiesto per configurare MFA

Host

È possibile utilizzare le API per eseguire diverse operazioni.

- Eseguire query su tutti gli host SnapCenter
- Rimuovere uno o più host da SnapCenter
- recuperare un host in base al nome
- recuperare tutte le risorse su un host

- Recuperare una risorsa utilizzando l'ID risorsa
- recuperare i dettagli di configurazione del plug-in
- configurare l'host del plug-in
- Recuperare tutte le risorse del plug-in per l'host Microsoft SQL Server
- Recuperare tutte le risorse del plug-in per l'host del database Oracle
- recuperare tutte le risorse del plug-in per l'host dell'applicazione personalizzato
- Recuperare tutte le risorse del plug-in per l'host SAP HANA
- recuperare i plug-in installati
- installare i plug-in su un host esistente
- pacchetto host di upgrade
- rimuovere i plug-in da un host esistente
- aggiungere il plug-in su un host
- aggiungere o modificare l'host
- Ottenere la firma dell'host Linux
- Registrare la firma dell'host Linux
- impostare l'host in modalità di manutenzione o produzione
- avviare o riavviare i servizi plug-in sull'host
- rinominare un host

Risorse

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare tutte le risorse
- Recuperare una risorsa utilizzando l'ID risorsa
- Recuperare tutte le risorse del plug-in per l'host Microsoft SQL Server
- Recuperare tutte le risorse del plug-in per l'host del database Oracle
- recuperare tutte le risorse del plug-in per l'host dell'applicazione personalizzato
- Recuperare tutte le risorse del plug-in per l'host SAP HANA
- Recuperare una risorsa Microsoft SQL Server utilizzando una chiave
- recuperare una risorsa personalizzata utilizzando una chiave
- modificare una risorsa del plug-in per l'host dell'applicazione personalizzato
- rimuovere una risorsa del plug-in per l'host dell'applicazione personalizzato utilizzando una chiave
- Recuperare una risorsa SAP HANA utilizzando una chiave
- Modificare una risorsa del plug-in per l'host SAP HANA
- Rimuovere una risorsa del plug-in per l'host SAP HANA utilizzando una chiave
- Recuperare una risorsa Oracle utilizzando una chiave
- Creare una risorsa di volume per applicazioni Oracle
- Modificare una risorsa di volume dell'applicazione Oracle

- Rimuovere una risorsa di volume dell'applicazione Oracle utilizzando una chiave
- Recuperare i dettagli secondari della risorsa Oracle
- Eseguire il backup della risorsa Microsoft SQL Server utilizzando il plug-in per Microsoft SQL Server
- Eseguire il backup della risorsa Oracle utilizzando il plug-in per il database Oracle
- eseguire il backup della risorsa personalizzata utilizzando il plug-in per l'applicazione personalizzata
- Configurare il database SAP HANA
- Configurare il database Oracle
- Ripristinare un backup del database SQL
- Ripristinare un backup del database Oracle
- ripristinare un backup personalizzato dell'applicazione
- creare una risorsa plug-in personalizzata
- Creare una risorsa SAP HANA
- proteggere una risorsa personalizzata utilizzando il plug-in per l'applicazione personalizzata
- Proteggere una risorsa Microsoft SQL Server utilizzando il plug-in per Microsoft SQL Server
- Modificare una risorsa Microsoft SQL Server protetta
- Rimuovere la protezione per la risorsa Microsoft SQL Server
- Proteggere una risorsa Oracle utilizzando il plug-in per il database Oracle
- Modificare una risorsa Oracle protetta
- Rimuovere la protezione dalla risorsa Oracle
- clonare una risorsa dal backup utilizzando il plug-in per l'applicazione personalizzata
- Clonare un volume applicativo Oracle dal backup utilizzando il plug-in per il database Oracle
- Clonare una risorsa Microsoft SQL Server dal backup utilizzando il plug-in per Microsoft SQL Server
- Creare un ciclo di vita clone di una risorsa Microsoft SQL Server
- Modificare il ciclo di vita dei cloni di una risorsa Microsoft SQL Server
- Eliminare il ciclo di vita di un clone di una risorsa Microsoft SQL Server
- Spostare un database Microsoft SQL Server esistente da un disco locale a un LUN NetApp
- Creare un file di specifica clone per un database Oracle
- Avviare un processo di refresh dei cloni on-demand di una risorsa Oracle
- Creare una risorsa Oracle dal backup utilizzando il file di specifica del clone
- ripristina il database nella replica secondaria e lo ricongiunge al gruppo di disponibilità
- Creare una risorsa di volume per applicazioni Oracle

Backup

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i dettagli del backup in base al nome, al tipo, al plug-in, alla risorsa o alla data del backup
- recuperare tutti i backup
- recuperare i dettagli del backup

- rinominare o eliminare i backup
- Montare un backup Oracle
- Smontare un backup Oracle
- cataloga un backup Oracle
- Discatalogare un backup Oracle
- ottieni tutti i backup necessari per eseguire il recovery point-in-time

Cloni

È possibile utilizzare le API per eseguire diverse operazioni.

- Creare, visualizzare, modificare ed eliminare il file delle specifiche dei cloni del database Oracle
- Visualizzare la gerarchia di cloni del database Oracle
- recuperare i dettagli dei cloni
- recuperare tutti i cloni
- eliminare i cloni
- Recuperare i dettagli del clone per ID
- Avviare un processo di refresh dei cloni on-demand di una risorsa Oracle
- Clonare una risorsa Oracle dal backup utilizzando il file di specifica del clone

Suddivisione dei cloni

È possibile utilizzare le API per eseguire diverse operazioni.

- stima dell'operazione di suddivisione del clone della risorsa clonata
- recuperare lo stato di un'operazione di suddivisione dei cloni
- avviare o arrestare un'operazione di suddivisione dei cloni

Gruppi di risorse

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i dettagli di tutti i gruppi di risorse
- recuperare il gruppo di risorse in base al nome
- creare un gruppo di risorse per il plug-in per l'applicazione personalizzata
- Creare un gruppo di risorse per il plug-in per Microsoft SQL Server
- Creare un gruppo di risorse per il plug-in per il database Oracle
- modificare un gruppo di risorse per il plug-in per l'applicazione personalizzata
- Modificare un gruppo di risorse per il plug-in per Microsoft SQL Server
- Modificare un gruppo di risorse per il plug-in per il database Oracle
- Creare, modificare o eliminare il ciclo di vita dei cloni di un gruppo di risorse per il plug-in per Microsoft SQL Server
- eseguire il backup di un gruppo di risorse

- impostare il gruppo di risorse in modalità di manutenzione o produzione
- rimuovere un gruppo di risorse

Policy

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i dettagli della policy
- recuperare i dettagli della policy per nome
- eliminare una policy
- creare una copia di un criterio esistente
- creare o modificare il criterio per il plug-in per l'applicazione personalizzata
- Creare o modificare i criteri per il plug-in per Microsoft SQL Server
- Creare o modificare il criterio per il plug-in per il database Oracle
- Creare o modificare i criteri per il plug-in per il database SAP HANA

Storage

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare tutte le condivisioni
- recuperare una condivisione in base al nome
- creare o eliminare una condivisione
- recuperare i dettagli dello storage
- recuperare i dettagli dello storage per nome
- creare, modificare o eliminare uno storage
- scopri le risorse su un cluster di storage
- recuperare le risorse su un cluster di storage

Condividere

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i dettagli di una condivisione
- recuperare i dettagli di tutte le condivisioni
- creare o eliminare una condivisione sullo storage
- recuperare una condivisione in base al nome

Plug-in

È possibile utilizzare le API per eseguire diverse operazioni.

- elencare tutti i plug-in per un host
- Recuperare una risorsa Microsoft SQL Server utilizzando una chiave

- modificare una risorsa personalizzata utilizzando una chiave
- rimuovere una risorsa personalizzata utilizzando una chiave
- Recuperare una risorsa SAP HANA utilizzando una chiave
- Modificare una risorsa SAP HANA utilizzando una chiave
- Rimuovere una risorsa SAP HANA utilizzando una chiave
- Recuperare una risorsa Oracle utilizzando una chiave
- Modificare una risorsa di volume di un'applicazione Oracle utilizzando una chiave
- Rimuovere una risorsa di volume dell'applicazione Oracle utilizzando una chiave
- Eseguire il backup della risorsa Microsoft SQL Server utilizzando il plug-in per Microsoft SQL Server e una chiave
- Eseguire il backup della risorsa Oracle utilizzando un plug-in per il database Oracle e una chiave
- eseguire il backup della risorsa applicativa personalizzata utilizzando il plug-in per l'applicazione personalizzata e una chiave
- Configurare il database SAP HANA utilizzando una chiave
- Configurare il database Oracle utilizzando una chiave
- ripristinare un backup personalizzato dell'applicazione utilizzando una chiave
- creare una risorsa plug-in personalizzata
- Creare una risorsa SAP HANA
- Creare una risorsa di volume per applicazioni Oracle
- proteggere una risorsa personalizzata utilizzando il plug-in per l'applicazione personalizzata
- Proteggere una risorsa Microsoft SQL Server utilizzando il plug-in per Microsoft SQL Server
- Modificare una risorsa Microsoft SQL Server protetta
- Rimuovere la protezione per la risorsa Microsoft SQL Server
- Proteggere una risorsa Oracle utilizzando il plug-in per il database Oracle
- Modificare una risorsa Oracle protetta
- Rimuovere la protezione dalla risorsa Oracle
- clonare una risorsa dal backup utilizzando il plug-in per l'applicazione personalizzata
- Clonare un volume applicativo Oracle dal backup utilizzando il plug-in per il database Oracle
- Clonare una risorsa Microsoft SQL Server dal backup utilizzando il plug-in per Microsoft SQL Server
- Creare un ciclo di vita clone di una risorsa Microsoft SQL Server
- Modificare il ciclo di vita dei cloni di una risorsa Microsoft SQL Server
- Eliminare il ciclo di vita di un clone di una risorsa Microsoft SQL Server
- Creare un file di specifica clone per un database Oracle
- Avviare un ciclo di vita dei cloni on-demand di una risorsa Oracle
- Clonare una risorsa Oracle dal backup utilizzando il file di specifica del clone

Report

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i report delle operazioni di backup, ripristino e clonazione per i rispettivi plug-in
- aggiungere, eseguire, eliminare o modificare le pianificazioni
- recuperare i dati per i report pianificati

Avvisi

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare tutti gli avvisi
- Recuperare gli avvisi in base agli ID
- Consente di eliminare più avvisi o un avviso per ID

RBAC

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i dettagli di utenti, gruppi e ruoli
- aggiungere o eliminare utenti
- assegnare l'utente al ruolo
- annullare l'assegnazione dell'utente dal ruolo
- creare, modificare o eliminare ruoli
- assegnare un gruppo a un ruolo
- annullare l'assegnazione di un gruppo da un ruolo
- aggiungere o eliminare gruppi
- creare una copia di un ruolo esistente
- assegnare o annullare l'assegnazione delle risorse all'utente o al gruppo

Configurazione

È possibile utilizzare le API per eseguire diverse operazioni.

- visualizzare le impostazioni di configurazione
- modificare le impostazioni di configurazione

CertificateSettings (Impostazioni certificazione)

È possibile utilizzare le API per eseguire diverse operazioni.

- Visualizzare lo stato del certificato per il server SnapCenter o l'host del plug-in
- Modificare le impostazioni del certificato per il server SnapCenter o l'host del plug-in

Repository

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i backup del repository

- visualizzare le informazioni di configurazione relative al repository
- Proteggere e ripristinare il repository SnapCenter
- Annullare la protezione del repository SnapCenter
- ricostruire e eseguire il failover del repository

Versione

È possibile utilizzare questa API per visualizzare la versione di SnapCenter.

Come accedere alle API REST utilizzando la pagina Web API di Swagger

Le API REST sono esposte attraverso la pagina web di Swagger. È possibile accedere alla pagina Web Swagger per visualizzare le API REST del server SnapCenter e per eseguire manualmente una chiamata API. È possibile utilizzare le API REST per gestire il server SnapCenter o per eseguire operazioni di protezione dei dati.

È necessario conoscere l'indirizzo IP di gestione o il nome di dominio del server SnapCenter su cui si desidera eseguire le API REST.

Non sono necessarie autorizzazioni speciali per eseguire il client API REST. Qualsiasi utente può accedere alla pagina Web di Swagger. Le rispettive autorizzazioni sugli oggetti a cui si accede tramite l'API REST si basano sull'utente che genera il token per accedere all'API REST.

Fasi

1. Da un browser, immettere l'URL per accedere alla pagina Web Swagger nel formato _ https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/_.

   Assicurarsi che l'URL API REST non contenga i seguenti caratteri: +, ., % e &.

2. Nel campo **Swagger Explore**, se la documentazione dell'API Swagger non viene visualizzata automaticamente, digitare: *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Content/swagger/SnapCenter.yaml*
3. Fare clic su **Esplora**.

   Viene visualizzato un elenco di tipi o categorie di risorse API.

4. Fare clic su un tipo di risorsa API per visualizzare le API in quel tipo di risorsa.

Se si verificano comportamenti imprevisti durante l'esecuzione delle API REST di SnapCenter, è possibile utilizzare i file di log per identificare la causa e risolvere il problema. È possibile scaricare i file di log dall'interfaccia utente di SnapCenter facendo clic su **Monitor** > **Log** > **Download**.

Inizia con L'API REST

È possibile iniziare rapidamente a utilizzare l'API REST di SnapCenter. L'accesso all'API offre una prospettiva prima di iniziare a utilizzarla con i processi di workflow più complessi in un setup live.

Ciao mondo

È possibile eseguire un semplice comando sul sistema per iniziare a utilizzare l'API REST di SnapCenter e verificarne la disponibilità.

Prima di iniziare

- Assicurarsi che l'utility Curl sia disponibile sul sistema.
- Indirizzo IP o nome host del server SnapCenter
- Nome utente e password di un account autorizzato ad accedere all'API REST di SnapCenter.

> Se le credenziali includono caratteri speciali, è necessario formattarle in modo accettabile per Curl in base alla shell in uso. Ad esempio, è possibile inserire una barra rovesciata prima di ogni carattere speciale o racchiudere l'intera stringa tra virgolette `username:password` singole.

Fase

Nell'interfaccia della riga di comando, eseguire quanto segue per recuperare le informazioni del plug-in:

```
curl -X GET -u username:password -k
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

Esempio:

```
curl -X GET -u admin:password -k
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

"Avviso per SnapCenter 5,0"

Informazioni sul copyright

Informazioni sul marchio commerciale