Inizia subito

SnapCenter software

NetApp
February 20, 2026

Sommario

Inizia subito

Scopri di più sul software SnapCenter

Panoramica di SnapCenter

Il SnapCenter software è una piattaforma semplice, centralizzata e scalabile per la protezione dei dati coerente con le applicazioni. Protegge applicazioni, database, file system host e VM sui sistemi ONTAP nel cloud ibrido.

SnapCenter utilizza le tecnologie NetApp Snapshot, SnapRestore, FlexClone, SnapMirror e SnapVault per fornire:

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

SnapCenter include SnapCenter Server e plug-in leggeri. È possibile automatizzare la distribuzione dei plug-in su host di applicazioni remote, pianificare operazioni di backup, verifica e clonazione e monitorare le operazioni di protezione dei dati.

Per proteggere i dati, puoi installare SnapCenter in locale o su un cloud pubblico.

- In sede per proteggere quanto segue:
  - I dati che sono sui sistemi primari ONTAP FAS, AFF o ASA e replicati sui 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
  - I dati che sono sui sistemi primari e secondari ONTAP ASA R2
- In locale in un cloud ibrido per proteggere quanto segue:
  - Dati presenti nei sistemi primari ONTAP FAS, AFF o ASA e replicati in Cloud Volumes ONTAP
  - Dati presenti sui sistemi primari e secondari ONTAP FAS, AFF o ASA e protetti su storage di oggetti e archivi nel cloud tramite l'integrazione di backup e ripristino NetApp
- 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)

Funzionalità principali

SnapCenter offre le seguenti funzionalità principali:

- Data Protection di diverse applicazioni centralizzata e coerente con l'applicazione

  La data Protection è supportata per Microsoft Exchange Server, Microsoft SQL Server, database Oracle su

Linux o AIX, database SAP HANA, IBM DB2, PostgreSQL, MySQL e Windows host filesystem in esecuzione su sistemi ONTAP. SnapCenter supporta anche la protezione di applicazioni quali MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Backup basati su policy

  I backup basati su policy sfruttano la tecnologia NetApp Snapshot per creare backup basati su disco rapidi, efficienti in termini di spazio e coerenti con le applicazioni. È anche possibile impostare la protezione automatica di questi backup su un archivio secondario aggiornando le relazioni di protezione esistenti.

- Backup per più risorse

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

- 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 consente una clonazione rapida, efficiente in termini di spazio e coerente con l'applicazione. È possibile clonare su qualsiasi destinazione nel cloud ibrido.

- Interfaccia utente grafica per la gestione di un singolo utente

  SnapCenter fornisce un'unica interfaccia per gestire backup e cloni in qualsiasi destinazione Hybrid Cloud.

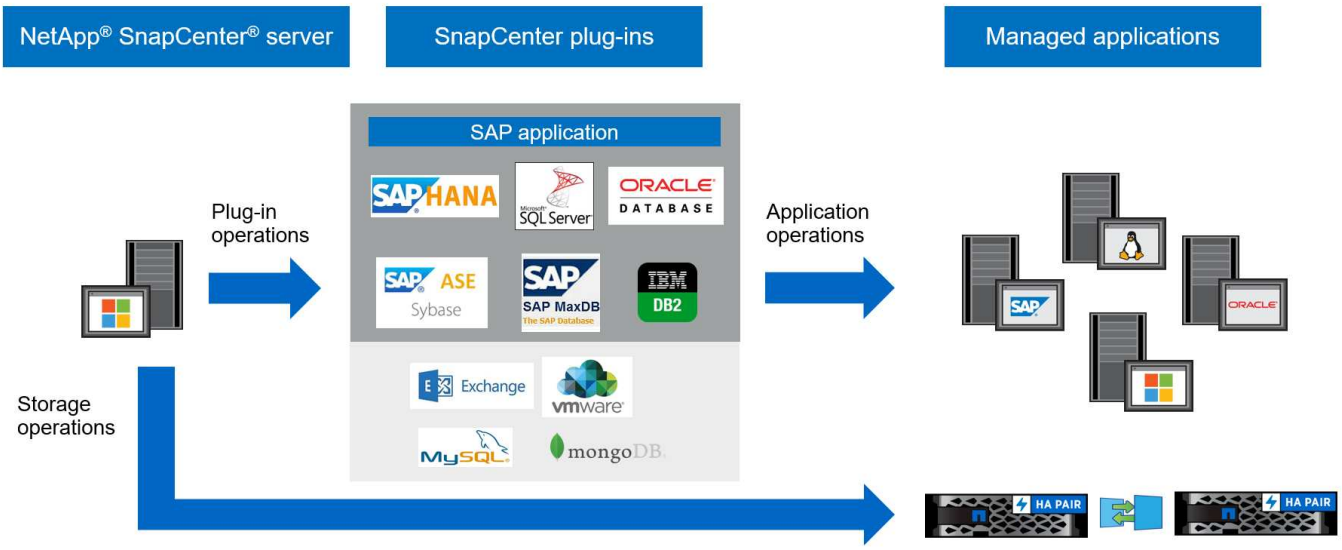
- API REST, cmdlet Windows, comandi UNIX

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

- Dashboard e reporting centralizzati sulla protezione dei dati
- Role-based Access Control (RBAC) per sicurezza e delega
- Un database di repository integrato ad alta disponibilità per la memorizzazione di tutti i metadati di backup
- Installazione push automatica dei plug-in
- Alta disponibilità
- Disaster Recovery (DR)
- SnapLock "Scopri di più"
- SnapMirror Active Sync (inizialmente rilasciato come SnapMirror Business Continuity [SM-BC])
- Mirroring sincrono "Scopri di più"

Architettura e componenti di SnapCenter

SnapCenter utilizza un design a strati con un server di gestione centrale e host plug-in. Il server e gli host dei plug-in possono trovarsi in posizioni diverse.



SnapCenter include il server SnapCenter, il pacchetto plug-in SnapCenter per Windows e il pacchetto plug-in SnapCenter per Linux. Ogni pacchetto contiene plug-in per varie applicazioni e componenti dell'infrastruttura.

Server SnapCenter

Il server SnapCenter supporta i sistemi operativi Microsoft Windows e Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). Il server SnapCenter comprende un server web, un'interfaccia utente centralizzata basata su HTML5, i cmdlet PowerShell, le API REST e il repository SnapCenter.

SnapCenter memorizza le informazioni sulle sue operazioni nel repository SnapCenter .

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 SnapCenter per Microsoft SQL Server	Pacchetto plug-in per Windows	Plug-in per Windows	Host di SQL Server	Windows
Plug-in SnapCenter per Windows	Pacchetto plug-in per Windows		Host Windows	Windows
Plug-in SnapCenter per Microsoft Exchange Server	Pacchetto plug-in per Windows	Plug-in per Windows	Host di Exchange Server	Windows
Plug-in SnapCentre per Oracle Database	Pacchetto plug-in per Linux e pacchetto plug-in per AIX	Plug-in per UNIX	Host Oracle	Linux o AIX

Nome del plug-in	Incluso nel pacchetto di installazione	Richiede altri plug-in	Installato sull'host	Piattaforma supportata
Plug-in SnapCenter per database SAP HANA	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
Plug-in SnapCenter per IBM DB2	Pacchetto plug-in per Linux e plug-in pacchetto per Windows	Plug-in per UNIX o plug-in per Windows	Host DB2	Linux, AIX o Windows
Plug-in SnapCenter per PostgreSQL	Pacchetto plug-in per Linux e pacchetto plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host PostgreSQL	Linux o Windows
Plug-in SnaoCenter per MySQL	Pacchetto plug-in per Linux e pacchetto plug-in per Windows	Plug-in per UNIX o Plug-in per Windows	Host MySQL	Linux o Windows
Plug-in SnapCenter per MongoDB	Pacchetto plug-in per Linux e pacchetto plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host MongoDB	Linux o Windows
Plug-in SnapCenter per ORASCPM (applicazioni Oracle)	Pacchetto plug-in per Linux e pacchetto plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host Oracle	Linux o Windows
Plug-in SnapCenter per SAP ASE	Pacchetto plug-in per Linux e pacchetto plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host SAP	Linux o Windows
Plug-in SnapCenter per SAP MaxDB	Pacchetto plug-in per Linux e pacchetto plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host SAP MaxDB	Linux o Windows
Plug-in SnapCenter per lo storage	Pacchetto plug-in per Linux e pacchetto plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host di storage	Linux o Windows

Il SnapCenter Plug-in for VMware vSphere supporta operazioni di backup e ripristino coerenti con gli arresti

anomali e con le VM per macchine virtuali (VM), datastore e dischi di macchine virtuali (VMDK). Supporta inoltre operazioni di backup e ripristino coerenti con l'applicazione per database e file system virtualizzati.

Per proteggere database, file system, VM o datastore su VM, distribuire il SnapCenter Plug-in for VMware vSphere . Per informazioni, fare riferimento "Plug-in SnapCenter per la documentazione di VMware vSphere" .

Repository SnapCenter

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

L'installazione SnapCenter Server installa per impostazione predefinita il database del repository MySQL Server. Se hai già installato MySQL Server e vuoi eseguire una nuova installazione di SnapCenter Server, devi disinstallare MySQL Server.

SnapCenter supporta MySQL Server 8.0.37 o versioni successive come database del repository SnapCenter . Se si utilizza una versione precedente di MySQL Server con una release precedente di SnapCenter, il processo di aggiornamento di SnapCenter aggiorna MySQL Server alla versione 8.0.37 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

Funzioni di protezione di SnapCenter

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).
- Supporta algoritmi di sicurezza conformi al Federal Information Processing Standard (FIPS).
- Supporta l'utilizzo dei certificati CA autorizzati forniti dal cliente.
- Supporta Transport Layer Security (TLS) 1,3 per la comunicazione con ONTAP. È inoltre possibile utilizzare TLS 1,2 per le comunicazioni tra client e server.
- Supporta un determinato set di suite di crittografia SSL per garantire la protezione della comunicazione di rete. "Scopri di più".
- 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 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'attivazione dell'MFA, vedere "Abilitare l'autenticazione a più fattori".

Role-based access control in SnapCenter

Il controllo degli accessi basato sui ruoli (RBAC) SnapCenter e le autorizzazioni ONTAP consentono agli amministratori SnapCenter di assegnare l'accesso alle risorse a utenti o gruppi. Questo accesso gestito centralmente consente agli amministratori delle applicazioni di lavorare in modo sicuro all'interno di ambienti designati.

Dovresti creare o modificare i ruoli e aggiungere l'accesso alle risorse agli utenti. Quando si configura SnapCenter per la prima volta, aggiungere utenti o gruppi di Active Directory ai ruoli e assegnare risorse a tali utenti o gruppi.

SnapCenter non crea account utente o di gruppo. Creare account utente o di gruppo nell'Active Directory del sistema operativo o del database.

Tipi di RBAC in SnapCenter

SnapCenter supporta i seguenti tipi di controllo degli accessi basato sui ruoli:

- SnapCenter RBAC
- RBAC a livello applicativo
- Plug-in SnapCenter per VMware vSphere RBAC
- Permessi ONTAP

SnapCenter RBAC

SnapCenter ha ruoli predefiniti ed è possibile assegnare utenti o gruppi a questi ruoli.

- 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 assegna un ruolo a un utente, SnapCenter visualizza i lavori pertinenti per quell'utente nella pagina Lavori, a meno che l'utente non abbia il ruolo SnapCenterAdmin.

È inoltre possibile creare nuovi ruoli e gestire autorizzazioni e utenti. È possibile assegnare autorizzazioni a utenti o gruppi per accedere a oggetti SnapCenter come host, connessioni di storage e gruppi di risorse.

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.

Quando crei un ruolo personalizzato, assicurati che includa tutte le autorizzazioni del ruolo SnapCenterAdmin. Se si copiano solo alcune autorizzazioni, SnapCenter impedisce di eseguire tutte le operazioni.

Gli utenti devono autenticarsi quando accedono tramite l'interfaccia utente o i cmdlet di PowerShell. Se gli utenti hanno più ruoli, ne selezionano uno dopo aver effettuato l'accesso. L'autenticazione è richiesta anche 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, per eseguire operazioni di protezione dei dati in un ambiente SQL Server, impostare le credenziali Windows o SQL corrette. Se si desidera eseguire operazioni di protezione dei dati in un ambiente file system Windows su un archivio ONTAP , il ruolo di amministratore SnapCenter deve disporre di 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 (SO) è disabilitata sull'host del database, è necessario impostare le credenziali con il database Oracle o con le credenziali Oracle ASM. Il server SnapCenter autentica le credenziali impostate 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 SnapCenter VMware supporta sia vCenter Server RBAC che ONTAP RBAC. "Scopri di più"

NOTA: NetApp consiglia di creare un ruolo ONTAP per il SnapCenter Plug-in for VMware vSphere e di assegnargli tutti i privilegi richiesti.

Permessi ONTAP

È necessario creare un account vsadmin con le autorizzazioni necessarie per accedere al sistema di archiviazione."Scopri di più"

Autorizzazioni assegnate ai ruoli SnapCenter predefiniti

Quando si aggiunge un utente a un ruolo, assegnare l'autorizzazione StorageConnection per abilitare la comunicazione con la macchina virtuale di archiviazione (SVM) oppure assegnare una SVM all'utente per concedere l'autorizzazione a utilizzare la SVM. L'autorizzazione Connessione di archiviazione consente agli utenti di creare connessioni SVM.

Ad esempio, un amministratore SnapCenter può creare connessioni SVM e assegnarle agli utenti App Backup e Clone Admin, che non possono creare o modificare connessioni SVM. Senza una connessione SVM, gli utenti non possono eseguire operazioni 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
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
SecondaryProtection	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 di Visualizzatore backup e clonazione ha la visualizzazione di sola lettura di tutte le autorizzazioni. Questo ruolo dispone anche di autorizzazioni abilitate per la scoperta, la creazione di report e l'accesso alla 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
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
SecondaryProtection	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
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
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

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Ripristino completo del volume	No	No	Non applicabile	Non applicabile	Non applicabile
SecondaryProtection	No	No	Non applicabile	Non applicabile	Non applicabile
Monitoraggio del processo	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Disaster recovery in SnapCenter

La funzionalità di disaster recovery (DR) di SnapCenter consente di eseguire il ripristino in caso di disastri come il danneggiamento delle risorse o un crash del server. Consente di ripristinare l'archivio di SnapCenter, le pianificazioni dei server, i componenti di configurazione e il plug-in SnapCenter per SQL Server e il relativo storage.

La presente sezione descrive i due tipi di 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 multifattore (MFA), durante il DR del server SnapCenter, chiudere tutte le schede del browser e riaprire un browser per accedere nuovamente. 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 le API REST per eseguire 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 né nel server DR dopo l'operazione di ripristino. Ripetere manualmente le impostazioni del registro di controllo.

Plug-in SnapCenter e DR storage

DR è disponibile solo per il plug-in SnapCenter per SQL Server. Se il plug-in non è attivo, passare a un altro host SQL e ripristinare i dati seguendo alcuni passaggi. Vedere "Disaster recovery del plug-in SnapCenter per SQL Server".

SnapCenter utilizza ONTAP SnapMirror per replicare i dati, che possono essere utilizzati per il DR mantenendo i dati sincronizzati su un sito secondario. Per avviare il failover, interrompere la replica SnapMirror. Durante il fallback, eseguire la sincronizzazione in modo inverso per replicare i dati dal sito DR nella posizione primaria.

Licenze richieste da 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, ASA La licenza standard SnapCenter è una licenza basata su controller ed è inclusa nell'ambito di NetApp ONTAP One. 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 FAS, AFF o ASA, è possibile ottenere una licenza di valutazione di NetApp ONTAP ONE contattando il rappresentante di vendita. Per informazioni sulle licenze incluse in NetApp ONTAP One, fare riferimento alla sezione "Licenze incluse con NetApp ONTAP ONE". 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.
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.
Licenze dei 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.

Licenza	Dove richiesto
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.

Le licenze servizi file NAS SnapCenter e SnapCenter sono obsolete e non sono più disponibili. La licenza standard e la licenza basata sulla capacità non sono più richieste per Amazon FSX per NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP e Azure NetApp Files.

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

Sincronizzazione attiva di SnapMirror in SnapCenter

SnapMirror Active Sync consente ai servizi di business di continuare a funzionare anche in caso di guasto completo del sito, supportando le applicazioni per il failover in modo trasparente con una copia secondaria. Non sono richiesti interventi manuali o script aggiuntivi per attivare un failover con la sincronizzazione attiva di SnapMirror.

Per ulteriori informazioni sulla sincronizzazione attiva di SnapMirror, fare riferimento a "Panoramica su SnapMirror Active Sync".

Per la sincronizzazione attiva di SnapMirror, assicurati di aver soddisfatto i vari requisiti di configurazione di hardware, software e sistema. Per informazioni, fare riferimento a. "Prerequisiti"

I plug-in supportati per questa funzionalità sono plug-in SnapCenter per SQL Server, plug-in SnapCenter per Windows, plug-in SnapCenter per database Oracle, plug-in SnapCenter per database SAP HANA, plug-in SnapCenter per Microsoft Exchange Server e plug-in SnapCenter per Unix.

Dopo aver installato SnapCenter Server e i plug-in, è necessario abilitare l'API REST affinché SnapCenter rilevi le relazioni di sincronizzazione attiva SnapMirror .

- Sull'host del server SnapCenter , modificare il file *C:\Program Files\ NetApp\SMCore\SMCoreServiceHost.dll.config* per modificare il valore del parametro *IsRestEnabledForStorageConnection* su *true*, quindi riavviare il servizio SnapCenter SMCore.
- Sugli host plug-in di Windows:
  - Modificare il file *C:\Programmi\ NetApp\ SnapCenter\SMCore\SMCoreServiceHost.dll.config* per modificare il valore del parametro *IsRestEnabledForStorageConnection* su *true*.
  - Modificare il file *C:\Program Files\ NetApp\ SnapCenter\SMCore\SnapDriveService.dll.config* per modificare il valore del parametro *IsRestEnabledForStorageConnection* su *true*.
  - Riavviare il servizio SnapCenter SMCore.

Per supportare la prossimità dell'iniziatore host in SnapCenter, è necessario impostare il valore, origine o destinazione in ONTAP.

I casi di utilizzo non supportati in SnapCenter:

- Se converti i workload di sincronizzazione attiva SnapMirror asimmetrici esistenti in modo simmetrico modificando la policy sulle relazioni di sincronizzazione attive di SnapMirror da *automatedfailover* a *automatedfailloverduplex* in ONTAP, lo stesso non è supportato in SnapCenter.
- Se sono presenti dei backup di un gruppo di risorse (già protetti in SnapCenter) e quindi la policy di storage viene modificata nelle relazioni di sincronizzazione attive di SnapMirror da *automatedfailover* a *automatedfailloverduplex* in ONTAP, lo stesso non è supportato in SnapCenter.

Concetti chiave relativi alla protezione dei dati

Prima di utilizzare SnapCenter, comprendi i concetti chiave relativi al backup, al cloning e al ripristino.

Risorse

Le risorse includono database, file system Windows o condivisioni di file di cui è stato eseguito il backup o il cloning con SnapCenter. A seconda dell'ambiente in uso, le risorse possono essere anche istanze di database, gruppi di disponibilità di SQL Server, database Oracle, database RAC o gruppi di applicazioni personalizzate.

Gruppo di risorse

Un gruppo di risorse è una raccolta di risorse su un host o cluster, potenzialmente provenienti da più host e cluster. Le operazioni eseguite su un gruppo di risorse si applicano a tutte le risorse in base alla pianificazione specificata. È possibile eseguire backup su richiesta o pianificati per singole risorse o gruppi.

Se un host di un gruppo di risorse condiviso entra in modalità di manutenzione, tutte le operazioni pianificate per tale gruppo verranno sospese in tutti gli host.

Utilizza plug-in pertinenti per eseguire il backup di risorse specifiche: Plug-in per database, plug-in per file system e plug-in SnapCenter per VMware vSphere per macchine virtuali e datastore.

Policy

Le policy specificano la frequenza del backup, la conservazione delle copie, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

È possibile selezionare uno o più criteri durante la creazione di un gruppo di risorse o l'esecuzione di un backup su richiesta.

Un gruppo di risorse definisce ciò che deve essere protetto e quando deve essere protetto in termini di giorno e ora. Una politica descrive come verrà effettuata la protezione. Ad esempio, se è necessario eseguire il backup di tutti i database o file system di un host, potrebbe essere creato un gruppo di risorse che include tutti i database o i file system nell'host. Al gruppo di risorse potrebbero quindi essere associati due criteri: Una politica giornaliera e una politica oraria.

Quando si crea il gruppo di risorse e si allegano i criteri, è possibile configurarlo per eseguire un backup completo ogni giorno e un'altra pianificazione per i backup dei log ogni ora.

È possibile utilizzare post-script e prescrizioni personalizzate per le operazioni di protezione dei dati. Questi script consentono l'automazione prima o dopo il processo di protezione dei dati. Ad esempio, uno script potrebbe notificare automaticamente gli errori o gli avvisi relativi al processo di protezione dei dati. La comprensione dei requisiti per la creazione di questi script è fondamentale prima di impostare prescritti e postscript.

Gruppo di coerenza (CG)

Un gruppo di coerenza è una raccolta di volumi gestiti come un'unica unità. I CG vengono sincronizzati per garantire la coerenza dei dati tra unità di archiviazione e volumi. In ONTAP, forniscono una gestione semplice e una garanzia di protezione per un carico di lavoro applicativo che si estende su più volumi. Scopri di più su "gruppi di coerenza" .

Utilizzo di prescrittori e postscript

Prescrittori e postscript personalizzati possono automatizzare le attività di protezione dei dati prima o dopo l'intervento. Ad esempio, è possibile aggiungere uno script per notificare errori o avvisi di processo. Prima di impostarli, assicurarsi di aver compreso i requisiti 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

Tutti i prescritti e postscript eseguiti come parte delle operazioni SnapCenter su sistemi di 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. All'avvio di 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.

Applicazioni e sistemi storage supportati da SnapCenter

Dovresti conoscere i sistemi storage, le applicazioni e i database supportati da SnapCenter.

Sistemi storage supportati

- NetApp ONTAP 9.12.1 e versioni successive
- Azure NetApp Files
- Amazon FSX per NetApp ONTAP

  Amazon FSx for NetApp ONTAP supporta la memoria non volatile express (NVMe) tramite Transport Control Protocol (TCP).

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

- Sistemi NetApp ASA r2 che eseguono NetApp ONTAP 9.16.1 e versioni successive

Se si utilizzano SnapCenter Server 6.2 e i plug-in SnapCenter 6.2, è necessario utilizzare ONTAP 9.17.1.

Applicazioni e database supportati

SnapCenter supporta la protezione di diverse applicazioni e database.

SnapCenter 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). "Scopri di più".

Metodi di autenticazione per le credenziali SnapCenter

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 per le operazioni di protezione 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 aggiungere host, installare pacchetti di plug-in e pianificare processi.

Autenticazione di dominio non attendibile

SnapCenter consente agli utenti e ai gruppi appartenenti a domini non attendibili di creare credenziali Windows. 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 durante la creazione delle credenziali di Windows, ma viene rinviata 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 quali 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 sysdba Privileges.

Autenticazione Oracle ASM

Il metodo di autenticazione Oracle ASM esegue l'autenticazione con un'istanza di Oracle Automatic Storage Management (ASM). L'autenticazione di Oracle ASM è necessaria se è necessario accedere a un'istanza di Oracle ASM e l'autenticazione del sistema operativo è disattivata sull'host del database. Prima di aggiungere una credenziale Oracle ASM, creare un utente Oracle con Privileges di sistema nell'istanza 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.

Operazioni SnapCenter supportate per sistemi ASA r2

I sistemi di archiviazione ASA r2 sono supportati a partire da SnapCenter 6.1. "Scopri di più sui sistemi ASA R2" .

SnapCenter supporta sia la protezione primaria che quella secondaria delle applicazioni in esecuzione su sistemi fisici e su Virtual Machine File System (VMFS). SnapCenter utilizza le API REST per tutte le operazioni sui sistemi ASA r2. I sistemi ASA r2 non supportano le ZAPI.

Operazioni supportate da SnapCenter per sistemi ASA r2

- Creazione di backup primari delle applicazioni
- Spostamento degli snapshot del gruppo di coerenza gerarchica sul sistema di archiviazione secondario
- Ripristino dei backup dai sistemi di archiviazione primari e secondari all'host originale o alternativo
  - Ripristino sul posto da sistemi di storage primari e secondari utilizzando VMware vMotion
  - Connetti e copia il ripristino dai sistemi di archiviazione primari e secondari
- Clonazione dei backup sull'host originale o sull'host alternativo
- RDM (Raw Device Mapping)
- Protezione dei volumi applicativi per Oracle
- Protezione di SAP HANA NDV
- LockVault
- Provisioning secondario della directory di registro dell'host del plug-in SQL

SnapCenter scopre o crea gruppi di coerenza ONTAP . Imposta relazioni SnapMirror sul cluster di destinazione per la protezione secondaria. "Scopri di più sui gruppi di coerenza ONTAP" .

Dopo l'aggiornamento a SnapCenter 6.2 (server e plug-in) e ONTAP 9.17.1, SnapCenter modifica i gruppi di coerenza semplici in gruppi di coerenza gerarchici durante il primo backup pianificato.

Per informazioni su come abilitare la protezione secondaria sui sistemi ASA r2 per la tua applicazione, consulta:

- "Abilita la protezione secondaria per le risorse di Microsoft SQL Server"
- "Abilita la protezione secondaria per le risorse SAP HANA"
- "Abilita la protezione secondaria per le risorse Oracle"
- "Abilita la protezione secondaria per i file system di Windows"
- "Abilita la protezione secondaria per le risorse IBM Db2"
- "Abilita la protezione secondaria per le risorse PostgreSQL"
- "Abilita la protezione secondaria per le risorse MySQL"
- "Abilita la protezione secondaria per i file system Unix"

Operazioni non supportate da SnapCenter per i sistemi ASA r2

- Snapshot a prova di manomissione
- Volumi FlexGroup
- Migrazione dai sistemi di storage ASA, AFF o FAS ai sistemi di storage ASA r2
- Protezione dei database con un mix di risorse ASA, AFF o FAS e risorse ASA r2
- Ridenominazione degli snapshot
- Provisioning delle risorse di Windows
- Protezione secondaria in caso di failover di sincronizzazione attiva SnapMirror
- Protocollo NVMe (Nonvolatile Memory Express) se è abilitata la sincronizzazione attiva SnapMirror
- Protezione delle applicazioni in esecuzione su AIX
- Tech refresh
- Ripristino di emergenza delle risorse Microsoft SQL

Avvio rapido del software SnapCenter

La guida di avvio rapido descrive i passaggi di base per l'installazione e la configurazione del software SnapCenter.

1 **Preparazione per l'installazione del server SnapCenter**

È necessario assicurarsi che tutti i requisiti per l'installazione del server SnapCenter siano soddisfatti.

- "Requisiti"

- "Effettuare la registrazione per accedere al software SnapCenter"
- "Abilitare l'autenticazione a più fattori"

Installare il server SnapCenter

Il server SnapCenter può essere installato su host Windows o Linux. Scaricare il pacchetto di installazione del server SnapCenter dal "Sito di supporto NetApp" ed eseguire il programma di installazione.

- "Installare il server SnapCenter su Windows"
- "Installare il server SnapCenter su Linux"

Configure SnapCenter Server (Configura server PPTP)

Una volta installato il server SnapCenter, è necessario configurarlo in base all'ambiente in uso.

Installare il plug-in per l'applicazione

Assicurarsi che tutti i requisiti per l'installazione del plug-in specifico dell'applicazione siano soddisfatti in base all'applicazione in uso, quindi procedere con l'installazione del plug-in corrispondente.

Proteggere l'applicazione

Dopo aver installato correttamente il server SnapCenter e i plug-in necessari, è possibile avviare la creazione dei backup delle applicazioni. Questi backup possono essere utilizzati successivamente a scopi di ripristino e cloning, quando necessario.