Iniziare

SnapCenter software

NetApp
November 06, 2025

Sommario

Iniziare

Scopri di più sul SnapCenter software

Panoramica 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 basati su disco rapidi, efficienti in termini di spazio e coerenti con le applicazioni
- Ripristino rapido e dettagliato e recupero coerente con l'applicazione
- Clonazione rapida e salvaspazio

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:
  - Dati presenti sui sistemi primari ONTAP FAS, AFF o ASA e replicati sui sistemi secondari ONTAP FAS, AFF o ASA
  - Dati presenti sui sistemi primari ONTAP Select
  - Dati presenti sui sistemi primari e secondari ONTAP FAS, AFF o ASA e protetti nell'archiviazione di oggetti StorageGRID locale
  - Dati presenti sui sistemi primari e secondari ONTAP ASA r2
- In locale in un cloud ibrido per proteggere quanto segue:
  - Dati presenti sui sistemi primari ONTAP FAS, AFF o ASA e replicati su 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 quanto segue:
  - Dati presenti sui sistemi primari Cloud Volumes ONTAP (in precedenza ONTAP Cloud)
  - Dati presenti su Amazon FSX per ONTAP
  - Dati presenti nei Azure NetApp Files primari (Oracle, Microsoft SQL e SAP HANA)

Caratteristiche principali

SnapCenter offre le seguenti funzionalità principali:

- Protezione dei dati centralizzata e coerente con le applicazioni di diverse applicazioni

  La protezione dei dati è supportata per Microsoft Exchange Server, Microsoft SQL Server, Oracle

Database su Linux o AIX, database SAP HANA, IBM Db2, PostgreSQL, MySQL e file system host Windows 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 recupero

  SnapCenter fornisce ripristini rapidi e granulari dei backup e ripristini basati sul tempo e coerenti con l'applicazione. È possibile effettuare il ripristino da qualsiasi destinazione nel cloud ibrido.

- Clonazione

  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.

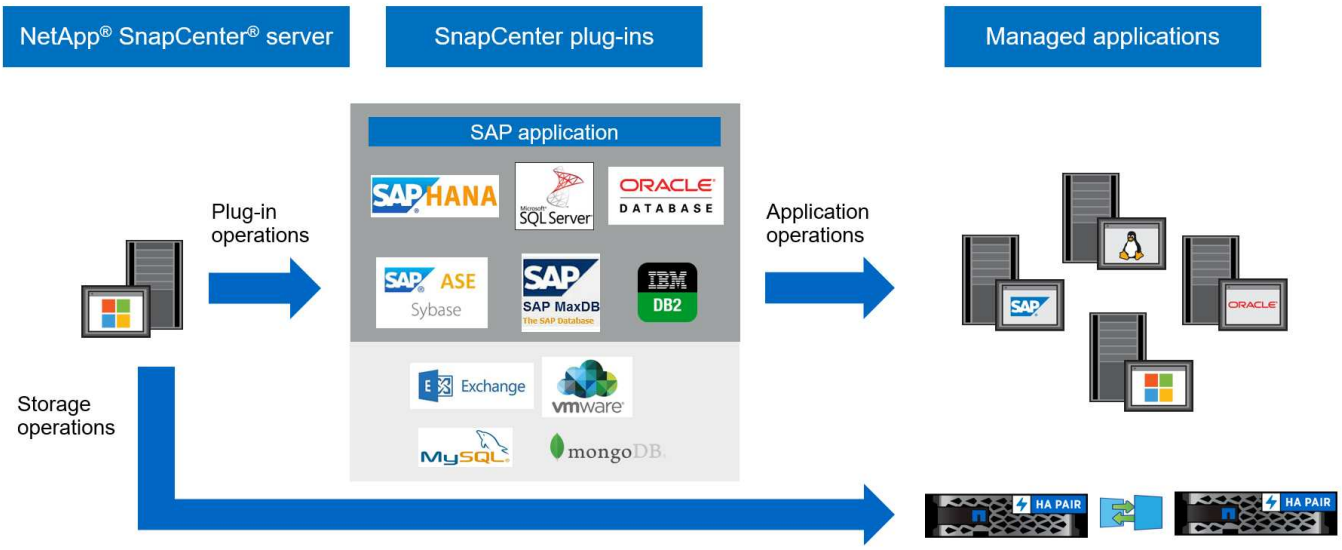
- API REST, cmdlet di Windows, comandi UNIX

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

- Dashboard e reporting centralizzati sulla protezione dei dati
- Controllo degli accessi basato sui ruoli (RBAC) per la sicurezza e la delega
- Un database di repository integrato con elevata disponibilità per archiviare tutti i metadati di backup
- Installazione push automatizzata dei plug-in
- Alta disponibilità
- Ripristino di emergenza (DR)
- SnapLock "Saperne di più"
- Sincronizzazione attiva SnapMirror (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC])
- Mirroring sincrono "Saperne di più"

Architettura e componenti 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 SnapCenter Server, il pacchetto SnapCenter Plug-in per Windows e il pacchetto SnapCenter Plug-in per Linux. Ogni pacchetto contiene plug-in per varie applicazioni e componenti infrastrutturali.

Server SnapCenter

SnapCenter Server supporta i sistemi operativi Microsoft Windows e Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). Il server SnapCenter include un server Web, un'interfaccia utente centralizzata basata su HTML5, cmdlet PowerShell, 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 di plug-in per Windows	Plug-in per Windows	Host di SQL Server	Finestre
Plug-in SnapCenter per Windows	Pacchetto di plug-in per Windows		Host Windows	Finestre
Plug-in SnapCenter per Microsoft Exchange Server	Pacchetto di plug-in per Windows	Plug-in per Windows	Host del server Exchange	Finestre
Plug-in SnapCentre per Oracle Database	Pacchetto di plug-in per Linux e pacchetto di 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 il database SAP HANA	Pacchetto di plug-in per Linux e pacchetto di 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 di plug-in per Linux e pacchetto di plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host DB2	Linux, AIX o Windows
Plug-in SnapCenter per PostgreSQL	Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host PostgreSQL	Linux o Windows
Plug-in SnaoCenter per MySQL	Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows	Plug-in per UNIX o Plug-in per Windows	Host MySQL	Linux o Windows
Plug-in SnapCenter per MongoDB	Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host MongoDB	Linux o Windows
Plug-in SnapCenter per ORASCPM (Oracle Applications)	Pacchetto di plug-in per Linux e pacchetto di 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 di plug-in per Linux e pacchetto di 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 di plug-in per Linux e pacchetto di plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host SAP MaxDB	Linux o Windows
Plug-in SnapCenter per il plug-in di archiviazione	Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows	Plug-in per UNIX o plug-in per Windows	Host di archiviazione	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 "Documentazione SnapCenter Plug-in for VMware vSphere" .

Repository SnapCenter

Il repository SnapCenter , a volte denominato 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:

- Metadati di backup, clonazione, ripristino e verifica
- Informazioni su report, lavori ed eventi
- Informazioni sull'host e sul plug-in
- Dettagli su ruolo, utente e autorizzazione
- Informazioni sulla connessione del sistema di archiviazione

Funzionalità di sicurezza in SnapCenter

SnapCenter utilizza rigorose funzionalità di sicurezza e autenticazione per consentirti di proteggere i tuoi dati.

SnapCenter include le seguenti funzionalità di sicurezza:

- Tutte le comunicazioni con SnapCenter utilizzano HTTP su SSL (HTTPS).
- Tutte le credenziali in SnapCenter sono protette tramite crittografia Advanced Encryption Standard (AES).
- Supporta algoritmi di sicurezza conformi allo standard 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 possibile utilizzare anche TLS 1.2 per la comunicazione tra client e server.
- Supporta un determinato set di suite di crittografia SSL per garantire la sicurezza nelle comunicazioni di rete. "Saperne di più" .
- SnapCenter viene installato all'interno del firewall aziendale per consentire l'accesso a SnapCenter Server e la comunicazione tra SnapCenter Server e i plug-in.
- L'accesso alle API e alle operazioni SnapCenter utilizza token crittografati con crittografia AES, che scadono dopo 24 ore.
- SnapCenter si integra con Windows Active Directory per l'accesso e il controllo degli accessi basato sui ruoli (RBAC) che regolano le autorizzazioni di accesso.

- IPsec è supportato con SnapCenter su ONTAP per macchine host Windows e Linux. "Saperne di più" .
- I cmdlet SnapCenter PowerShell sono protetti dalla sessione.
- Dopo un periodo predefinito di 15 minuti di inattività, SnapCenter ti avvisa che verrai disconnesso entro 5 minuti.

  Dopo 20 minuti di inattività, SnapCenter effettua la disconnessione e sarà necessario effettuare nuovamente l'accesso. È possibile modificare il periodo di disconnessione.

- L'accesso viene temporaneamente disabilitato dopo 5 tentativi di accesso errati.
- Supporta l'autenticazione del certificato CA tra SnapCenter Server e ONTAP. "Saperne di più" .
- Integrity Verifier viene aggiunto a SnapCenter Server e ai plug-in e convalida tutti i file binari forniti durante le operazioni di nuova installazione e aggiornamento.

Panoramica del certificato CA

Il programma di installazione di SnapCenter Server 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 distribuire i certificati CA dopo aver installato SnapCenter Server e i rispettivi plug-in. Per ulteriori informazioni, consultare "Genera file CSR del certificato CA" .

È anche possibile distribuire 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 SnapCenter Server e i plug-in.

Panoramica sull'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 abilitata la funzionalità SSL bidirezionale.

Autenticazione a più fattori (MFA)

MFA utilizza un Identity Provider (IdP) di terze parti tramite Security Assertion Markup Language (SAML) per gestire le sessioni utente. Questa funzionalità migliora la sicurezza dell'autenticazione offrendo la possibilità di utilizzare più fattori, come TOTP, dati biometrici, notifiche push ecc., insieme 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) per tutto il proprio portafoglio.

L'MFA è applicabile solo per l'accesso all'interfaccia utente di SnapCenter Server. Gli accessi vengono autenticati tramite l'IdP Active Directory Federation Services (AD FS). È possibile configurare vari fattori di autenticazione in AD FS. SnapCenter è il fornitore del servizio e dovresti SnapCenter come relying party in AD FS. Per abilitare MFA in SnapCenter, saranno necessari i metadati AD FS.

Per informazioni su come abilitare MFA, vedere"Abilita l'autenticazione a più fattori" .

Controllo degli accessi basato sui ruoli in SnapCenter

Il controllo degli accessi basato sui ruoli (RBAC) SnapCenter e le autorizzazioni ONTAP consentono agli amministratori 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 di ambienti delegati.

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

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

Tipi di RBAC in SnapCenter

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

- SnapCenter RBAC
- RBAC a livello di applicazione
- Plug-in SnapCenter per VMware vSphere RBAC
- Autorizzazioni ONTAP

SnapCenter RBAC

SnapCenter ha ruoli predefiniti ed è possibile assegnare utenti o gruppi di utenti a tali ruoli. I ruoli predefiniti sono:

- Ruolo di amministratore SnapCenter
- Ruolo di amministratore di backup e clonazione delle app
- Ruolo di visualizzatore di backup e clonazione
- Ruolo di amministratore dell'infrastruttura

Quando assegni un ruolo a un utente, nella pagina Lavori saranno visibili solo i lavori pertinenti a quell'utente, a meno che non gli sia stato assegnato il ruolo SnapCenterAdmin.

Puoi anche creare nuovi ruoli e gestire autorizzazioni e utenti. È possibile assegnare autorizzazioni a utenti o gruppi per accedere agli oggetti SnapCenter , quali host, connessioni di archiviazione e gruppi di risorse.

È possibile assegnare 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 in più foreste.

Se si crea un ruolo personalizzato, questo deve contenere tutte le autorizzazioni del ruolo SnapCenterAdmin. Se si copiano solo alcune autorizzazioni, ad esempio Aggiunta host o Rimozione host, non sarà possibile eseguire tali operazioni.

Gli utenti sono tenuti a fornire l'autenticazione durante l'accesso, tramite l'interfaccia utente grafica (GUI) o utilizzando i cmdlet di PowerShell. Se gli utenti sono membri di più di un ruolo, dopo aver immesso le

credenziali di accesso, verrà chiesto loro di specificare il ruolo che desiderano utilizzare. Gli utenti devono inoltre fornire l'autenticazione per eseguire le API.

RBAC a livello di applicazione

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 protezione dei dati in un ambiente SQL Server, è necessario impostare le credenziali con le credenziali Windows o SQL appropriate. Il server SnapCenter autentica le credenziali impostate utilizzando entrambi i metodi. 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 nell'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.

SnapCenter Plug-in for VMware vSphere RBAC

Se si utilizza il plug-in SnapCenter VMware per la protezione dei dati coerente con la VM, vCenter Server fornisce un livello aggiuntivo di RBAC. Il plug-in SnapCenter VMware supporta sia vCenter Server RBAC sia ONTAP RBAC. "Saperne di più"

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

Autorizzazioni ONTAP

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

Autorizzazioni assegnate ai ruoli predefiniti SnapCenter

Quando si aggiunge un utente a un ruolo, è necessario assegnare l'autorizzazione StorageConnection per abilitare la comunicazione con la macchina virtuale di archiviazione (SVM) oppure assegnare una SVM all'utente per abilitare l'autorizzazione a utilizzare la SVM. L'autorizzazione Connessione di archiviazione 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 amministratore di backup e clonazione delle app, che per impostazione predefinita non ha l'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 SnapCenter

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

Ruolo di amministratore di backup e clonazione delle app

Il ruolo di amministratore di backup e clonazione delle app dispone delle autorizzazioni necessarie per eseguire azioni amministrative per i backup delle applicazioni e le attività correlate alla clonazione. Questo ruolo non dispone delle autorizzazioni per la gestione dell'host, il provisioning, la gestione della connessione di

archiviazione o l'installazione remota.

Permessi	Abilitato	Creare	Leggere	Aggiornamento	Eliminare
Gruppo di risorse	Non applicabile	SÌ	SÌ	SÌ	SÌ
Politica	Non applicabile	SÌ	SÌ	SÌ	SÌ
Backup	Non applicabile	SÌ	SÌ	SÌ	SÌ
Ospite	Non applicabile	SÌ	SÌ	SÌ	SÌ
Connessione di archiviazione	Non applicabile	NO	SÌ	NO	NO
Clone	Non applicabile	SÌ	SÌ	SÌ	SÌ
Disposizione	Non applicabile	NO	SÌ	NO	NO
Pannello di controllo	SÌ	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Rapporti	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
Smonta	SÌ	SÌ	Non applicabile	Non applicabile	Non applicabile
Ripristino del volume completo	NO	NO	Non applicabile	Non applicabile	Non applicabile
Protezione secondaria	NO	NO	Non applicabile	Non applicabile	Non applicabile
Monitoraggio del lavoro	SÌ	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Ruolo di visualizzatore di backup e clonazione

Il ruolo di Visualizzatore backup e clonazione ha una 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	Abilitato	Creare	Leggere	Aggiornamento	Eliminare
Gruppo di risorse	Non applicabile	NO	SÌ	NO	NO
Politica	Non applicabile	NO	SÌ	NO	NO
Backup	Non applicabile	NO	SÌ	NO	NO
Ospite	Non applicabile	NO	SÌ	NO	NO
Connessione di archiviazione	Non applicabile	NO	SÌ	NO	NO
Clone	Non applicabile	NO	SÌ	NO	NO
Disposizione	Non applicabile	NO	SÌ	NO	NO
Pannello di controllo	SÌ	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Rapporti	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
Smonta	SÌ	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristino del volume completo	NO	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Protezione secondaria	NO	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Permessi	Abilitato	Creare	Leggere	Aggiornamento	Eliminare
Monitoraggio del lavoro	SÌ	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Ruolo di amministratore dell'infrastruttura

Il ruolo di amministratore dell'infrastruttura dispone di autorizzazioni abilitate per la gestione dell'host, la gestione dell'archiviazione, il provisioning, i gruppi di risorse, i report di installazione remota e l'accesso alla dashboard.

Permessi	Abilitato	Creare	Leggere	Aggiornamento	Eliminare
Gruppo di risorse	Non applicabile	SÌ	SÌ	SÌ	SÌ
Politica	Non applicabile	NO	SÌ	SÌ	SÌ
Backup	Non applicabile	SÌ	SÌ	SÌ	SÌ
Ospite	Non applicabile	SÌ	SÌ	SÌ	SÌ
Connessione di archiviazione	Non applicabile	SÌ	SÌ	SÌ	SÌ
Clone	Non applicabile	NO	SÌ	NO	NO
Disposizione	Non applicabile	SÌ	SÌ	SÌ	SÌ
Pannello di controllo	SÌ	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Rapporti	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
Smonta	NO	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Permessi	Abilitato	Creare	Leggere	Aggiornamento	Eliminare
Ripristino del volume completo	NO	NO	Non applicabile	Non applicabile	Non applicabile
Protezione secondaria	NO	NO	Non applicabile	Non applicabile	Non applicabile
Monitoraggio del lavoro	SÌ	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Ripristino di emergenza in SnapCenter

La funzionalità di ripristino di emergenza (DR) SnapCenter consente di ripristinare i dati in caso di disastri quali danneggiamento delle risorse o arresti anomali del server. Aiuta a ripristinare il repository SnapCenter , le pianificazioni del server, i componenti di configurazione e il plug-in SnapCenter per SQL Server e il relativo archivio.

Questa sezione spiega i due tipi di DR in SnapCenter:

SnapCenter Server DR

- I dati di SnapCenter Server vengono sottoposti a backup e possono essere recuperati senza che sia necessario aggiungere o gestire alcun plug-in da SnapCenter Server.
- 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 ripristino di emergenza di SnapCenter Server, chiudere tutte le schede del browser e riaprire un browser per effettuare nuovamente l'accesso. In questo modo verranno cancellati i cookie di sessione esistenti o attivi e verranno aggiornati i dati di configurazione corretti.
- La funzionalità di ripristino di emergenza SnapCenter utilizza le API REST per eseguire il backup del server SnapCenter . Vedere "Flussi di lavoro API REST per il ripristino di emergenza di SnapCenter Server" .
- Il file di configurazione correlato alle impostazioni di controllo non viene sottoposto a backup nel backup DR né sul server DR dopo l'operazione di ripristino. Dovresti ripetere manualmente le impostazioni del registro di controllo.

Plug-in SnapCenter e Storage DR

DR è disponibile solo per il plug-in SnapCenter per SQL Server. Se il plug-in non funziona, passare a un altro host SQL e recuperare i dati seguendo alcuni passaggi. Vedere "Ripristino di emergenza 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, inverti la sincronizzazione per replicare i dati dal sito DR alla posizione primaria.

Licenze richieste da SnapCenter

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

Licenza	Dove richiesto
Basato su controller SnapCenter Standard	Richiesto per FAS, AFF, ASA La licenza SnapCenter Standard è una licenza basata su controller ed è inclusa come parte di NetApp ONTAP One. Se si dispone della licenza SnapManager Suite, si ottiene anche il diritto alla licenza SnapCenter Standard. Se si desidera installare SnapCenter in prova con storage FAS, AFF o ASA , è possibile ottenere una licenza di valutazione NetApp ONTAP One contattando il rappresentante commerciale. Per informazioni sulle licenze incluse con NetApp ONTAP One, fare riferimento a "Licenze incluse con NetApp ONTAP One" . SnapCenter è offerto anche come parte del pacchetto di protezione dei dati. Se hai acquistato A400 o una versione successiva, dovresti acquistare il pacchetto di protezione dei dati.
SnapMirror o SnapVault	ONTAP Se la replica è abilitata in SnapCenter , è necessaria una licenza SnapMirror o SnapVault .
SnapRestore	Necessario per ripristinare e verificare i backup. Sui sistemi di archiviazione primari • Richiesto sui sistemi di destinazione SnapVault per eseguire la verifica remota e il ripristino da un backup. • Richiesto sui sistemi di destinazione SnapMirror per eseguire la verifica remota.

Licenza	Dove richiesto
FlexClone	Necessario per clonare database e operazioni di verifica. Sui sistemi di storage primari e secondari • Richiesto sui sistemi di destinazione SnapVault per creare cloni dal backup del vault secondario. • Richiesto sui sistemi di destinazione SnapMirror per creare cloni dal backup SnapMirror secondario.
Licenze di protocollo	• Licenza iSCSI o FC per LUN • Licenza CIFS per azioni SMB • Licenza NFS per VMDK di tipo NFS • Licenza iSCSI o FC per VMDK di tipo VMFS Richiesto sui sistemi di destinazione SnapMirror per fornire dati se un volume di origine non è disponibile.
Licenze SnapCenter Standard (facoltative)	Destinazioni secondarie Si consiglia, ma non è obbligatorio, di aggiungere licenze SnapCenter Standard alle destinazioni secondarie. Se le licenze SnapCenter Standard 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, per eseguire operazioni di clonazione e verifica sulle destinazioni secondarie è necessaria una licenza FlexClone .

Licenza	Dove richiesto
Licenze Single Mailbox Recovery (SMBR)	Se si utilizza il plug-in SnapCenter per Exchange per gestire i database di Microsoft Exchange Server e Single Mailbox Recovery (SMBR), sarà necessaria una licenza aggiuntiva per SMBR, che deve essere acquistata separatamente in base alla casella di posta dell'utente. NetApp® Single Mailbox Recovery ha raggiunto la fine della disponibilità (EOA) il 12 maggio 2023. Per maggiori informazioni, fare riferimento"CPC-00507" . NetApp continuerà a supportare i clienti che hanno acquistato capacità di casella di posta, manutenzione e supporto tramite i codici prodotto di marketing introdotti il 24 giugno 2020, per tutta la durata del diritto al supporto. NetApp Single Mailbox Recovery è un prodotto partner fornito da Ontrack. Ontrack PowerControls offre funzionalità simili a quelle di NetApp Single Mailbox Recovery. I clienti possono acquistare nuove licenze software Ontrack PowerControls e rinnovi di manutenzione e supporto Ontrack PowerControls da Ontrack (tramite licensingteam@ontrack.com) per il ripristino granulare delle caselle di posta dopo la data di scadenza del 12 maggio 2023.

Le licenze SnapCenter Advanced e SnapCenter NAS File Services sono obsolete e non sono più disponibili. La licenza standard e la licenza basata sulla capacità non sono più necessarie per Amazon FSx for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP e Azure NetApp Files.

Dovresti installare una o più licenze SnapCenter . Per informazioni su come aggiungere licenze, vedere"Aggiungi licenze basate sul controller SnapCenter Standard" .

Sincronizzazione attiva SnapMirror in SnapCenter

La sincronizzazione attiva SnapMirror consente ai servizi aziendali 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 SnapMirror ActiveSync non è necessario alcun intervento manuale né scripting aggiuntivo.

Per ulteriori informazioni sulla sincronizzazione attiva SnapMirror , fare riferimento "Panoramica della sincronizzazione attiva SnapMirror" .

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

I plug-in supportati per questa funzionalità sono SnapCenter Plug-in per SQL Server, SnapCenter Plug-in per Windows, SnapCenter Plug-in per database Oracle, SnapCenter Plug-in per database SAP HANA,

SnapCenter Plug-in per Microsoft Exchange Server e SnapCenter Plug-in per Unix.

> Per supportare la prossimità dell'iniziatore host in SnapCenter, il suo valore, origine o destinazione, deve essere impostato in ONTAP.

Casi d'uso non supportati in SnapCenter:

- Se si convertono i carichi di lavoro attivi SnapMirror asimmetrici esistenti in simmetrici modificando la policy sulle relazioni di sincronizzazione attiva SnapMirror da *automatedfailover* a *automatedfailoverduplex* in ONTAP, la stessa operazione non è supportata in SnapCenter.
- Se sono presenti backup di un gruppo di risorse (già protetti in SnapCenter) e quindi la policy di archiviazione viene modificata nelle relazioni di sincronizzazione attiva SnapMirror da *automatedfailover* a *automatedfailoverduplex* in ONTAP, la stessa cosa non è supportata in SnapCenter.

Concetti chiave della protezione dei dati

Prima di utilizzare SnapCenter, è necessario comprendere i concetti chiave relativi a backup, clonazione e ripristino.

Risorse

Le risorse includono database, file system Windows o condivisioni di file sottoposti a backup o clonati con SnapCenter. A seconda dell'ambiente, le risorse potrebbero essere anche istanze di database, gruppi di disponibilità di SQL Server, database Oracle, database RAC o gruppi di applicazioni personalizzati.

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 sue risorse in base alla pianificazione specificata. È possibile eseguire backup su richiesta o pianificati per singole risorse o gruppi.

> Se un host in un gruppo di risorse condivise entra in modalità di manutenzione, tutte le operazioni pianificate per quel gruppo verranno sospese su tutti gli host.

Utilizzare i plug-in appropriati per eseguire il backup di risorse specifiche: plug-in di database per i database, plug-in di file system per i file system e SnapCenter Plug-in for VMware vSphere per VM e datastore.

Politiche

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

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

Un gruppo di risorse definisce cosa deve essere protetto e quando deve essere protetto in termini di giorno e ora. Una politica descrive come verrà attuata la protezione. Ad esempio, se è necessario eseguire il backup di tutti i database o file system di un host, è possibile creare un gruppo di risorse che includa tutti i database o file system nell'host. Al gruppo di risorse potrebbero quindi essere associate due policy: una policy giornaliera e una policy oraria.

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

Nelle operazioni di protezione dei dati è possibile utilizzare prescrizioni e post-scrizioni personalizzate. Questi script consentono l'automazione prima o dopo il processo di protezione dei dati. Ad esempio, uno script potrebbe notificare automaticamente errori o avvisi relativi ai processi di protezione dei dati. Prima di impostare prescript e postscript è fondamentale comprendere i requisiti per la creazione di questi script.

Utilizzo di prescrizioni e poscrizioni

Prescrizioni e post-script personalizzati possono automatizzare le attività di protezione dei dati prima o dopo il lavoro. Ad esempio, puoi aggiungere uno script per ricevere notifiche di errori o avvisi nei processi. Prima di configurarli, assicurati di aver compreso i requisiti per questi script.

Tipi di script supportati

Per Windows sono supportati i seguenti tipi di script:

- File batch
- Script di PowerShell
- script Perl

Per UNIX sono supportati i seguenti tipi di script:

- script Perl
- script Python
- Script di shell

> Oltre alla shell bash predefinita, sono supportate anche altre shell come sh-shell, k-shell e c-shell.

Percorso dello script

Tutti i prescript e i postscript eseguiti come parte delle operazioni SnapCenter su sistemi di archiviazione virtualizzati e non virtualizzati vengono eseguiti sull'host plug-in.

- Gli script di Windows dovrebbero trovarsi sull'host del plug-in.

> Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

- Gli script UNIX dovrebbero trovarsi sull'host del plug-in.

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

Dove specificare gli script

Gli script sono specificati nei criteri di backup. Quando viene avviato un processo di backup, il criterio associa automaticamente lo script alle risorse sottoposte a backup. Quando si crea un criterio di backup, è possibile specificare gli argomenti prescript e postscript.

> Non è possibile specificare più script.

Timeout degli script

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

Output dello script

La directory predefinita per i file di output prescript e postscript di Windows è Windows\System32.

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

Sistemi di archiviazione e applicazioni supportati da SnapCenter

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

Sistemi di archiviazione supportati

- NetApp ONTAP 9.12.1 e versioni successive
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

  Supporta la memoria non volatile express (NVMe) tramite Transport Control Protocol (TCP).

  Per informazioni su Amazon FSx for NetApp ONTAP, vedere "Documentazione Amazon FSx for NetApp ONTAP" .

- Sistemi NetApp ASA r2 che eseguono NetApp ONTAP 9.16.1.

Applicazioni e database supportati

SnapCenter supporta la protezione di diverse applicazioni e database. Per informazioni dettagliate sulle applicazioni e sui database supportati, vedere "Strumento matrice di interoperabilità NetApp" .

SnapCenter supporta la protezione dei carichi di lavoro Oracle e Microsoft SQL negli ambienti VMware Cloud su Amazon Web Services (AWS) Software-Defined Data Center (SDDC). "Saperne 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 le operazioni SnapCenter . Dovresti creare un set di credenziali per l'installazione dei plug-in e un altro per le operazioni di protezione dei dati.

Autenticazione di Windows

Il metodo di autenticazione di Windows esegue l'autenticazione tramite Active Directory. Per l'autenticazione di Windows, Active Directory è configurato all'esterno di SnapCenter. SnapCenter esegue l'autenticazione senza alcuna configurazione aggiuntiva. Per aggiungere host, installare pacchetti plug-in e pianificare attività, è necessario disporre delle credenziali Windows.

Autenticazione di dominio non attendibile

SnapCenter consente agli utenti e ai gruppi appartenenti a domini non attendibili di creare credenziali Windows. Per far sì che l'autenticazione vada a buon fine, 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 posticipata finché non vengono eseguite la registrazione dell'host e altre operazioni sull'host.

Autenticazione di SQL Server

Il metodo di autenticazione SQL esegue l'autenticazione su un'istanza di SQL Server. Ciò significa che un'istanza di SQL Server deve essere individuata in SnapCenter. Pertanto, prima di aggiungere una credenziale SQL, è necessario aggiungere un host, installare pacchetti plug-in e aggiornare le risorse. Per eseguire operazioni quali la pianificazione su SQL Server o l'individuazione di risorse è necessaria l'autenticazione di SQL Server.

Autenticazione Linux

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

Autenticazione del database Oracle

Il metodo di autenticazione del database Oracle esegue l'autenticazione su un database Oracle. Per eseguire operazioni sul database Oracle è necessaria l'autenticazione del database Oracle se l'autenticazione del sistema operativo (SO) è disabilitata sull'host del database. Pertanto, prima di aggiungere una credenziale del 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 su un'istanza di Oracle Automatic Storage Management (ASM). L'autenticazione Oracle ASM è obbligatoria se è necessario accedere a un'istanza Oracle ASM e l'autenticazione del sistema operativo è disabilitata sull'host del database. Prima di aggiungere una credenziale Oracle ASM, creare un utente Oracle con privilegi di sistema nell'istanza ASM.

Autenticazione del catalogo RMAN

Il metodo di autenticazione del catalogo RMAN esegue l'autenticazione in base al database del catalogo Oracle Recovery Manager (RMAN). Se hai configurato un meccanismo di catalogo esterno e registrato il tuo database nel database di catalogo, devi 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 sfrutta le API REST per eseguire tutte le operazioni sui sistemi ASA r2, che non supportano le ZAPI.

Operazioni supportate da SnapCenter per sistemi ASA r2

- Creazione di backup primari delle applicazioni su VMDK
- Trasferimento degli snapshot del gruppo di coerenza al sistema di archiviazione secondario
- Ripristino dei backup dai sistemi di archiviazione primari e secondari all'host originale o all'host alternativo
  - Ripristino sul posto da sistemi di archiviazione 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

SnapCenter può scoprire o creare gruppi di coerenza ONTAP . Può anche predisporre e inizializzare le relazioni SnapMirror sul cluster di destinazione per una protezione secondaria.

Per informazioni sull'abilitazione della protezione secondaria sui sistemi ASA r2 per la tua applicazione, fai riferimento a:

- "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

- Mappatura dei dispositivi grezzi (RDM)
- Volumi applicativi per Oracle
- SAP HANA NDV
- LockVault
- Istantanee a prova di manomissione
- Volumi FlexGroup
- Gruppo di coerenza gerarchica
- Migrazione dai sistemi di archiviazione ASA, AFF o FAS ai sistemi di archiviazione ASA r2
- Protezione dei database che hanno un mix di risorse ASA, AFF o FAS e risorse ASA r2
- Ridenominazione degli snapshot

- Provisioning secondario della directory di registro dell'host del plug-in SQL

Avvio rapido del SnapCenter software

La guida rapida descrive i passaggi di base per installare e configurare il SnapCenter software.

1 Prepararsi all'installazione di SnapCenter Server

È necessario assicurarsi che siano soddisfatti tutti i requisiti per l'installazione di SnapCenter Server.

- "Requisiti"
- "Registrati per accedere SnapCenter software"
- "Abilita l'autenticazione a più fattori"

2 Installa SnapCenter Server

SnapCenter Server può essere installato su host Windows o Linux. Scaricare il pacchetto di installazione di SnapCenter Server da "Sito di supporto NetApp" ed eseguire il programma di installazione.

- "Installa il server SnapCenter su Windows"
- "Installa SnapCenter Server su Linux"

3 Configurare SnapCenter Server

Dopo aver installato SnapCenter Server, è necessario configurarlo in base al proprio ambiente.

4 Installa il plug-in per la tua 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 rispettivo plug-in.

5 Proteggi la tua applicazione

Dopo aver installato correttamente SnapCenter Server e i plug-in necessari, è possibile avviare la creazione dei backup dell'applicazione. Questi backup possono essere successivamente utilizzati per scopi di ripristino e clonazione, quando necessario.