Concetti

SnapCenter Software 4.8

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/it-it/snapcenter-48/concept/concept_snapcenter_overview.html on January 18, 2024. Always check docs.netapp.com for the latest.

Sommario

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 o AFF e replicati nei sistemi secondari ONTAP FAS o AFF
  - Dati sui sistemi primari ONTAP Select
  - Dati su sistemi primari e secondari ONTAP FAS o AFF e protetti dallo storage a oggetti StorageGRID locale (utilizzando l'integrazione del backup cloud NetApp BlueXP)
- On-premise in un cloud ibrido per proteggere:
  - Dati presenti nei sistemi primari ONTAP FAS o AFF e replicati in Cloud Volumes ONTAP
  - Dati che si trovano su sistemi primari e secondari ONTAP FAS o AFF e protetti per lo storage di oggetti e archivi nel cloud (utilizzando l'integrazione di NetApp BlueXP Cloud Backup)
- 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

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.

"Storage Automation Store di NetApp"

- Backup basati su policy

  I backup basati su policy sfruttano la tecnologia di copia Snapshot di NetApp per creare backup rapidi, efficienti in termini di spazio, coerenti con le applicazioni 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.

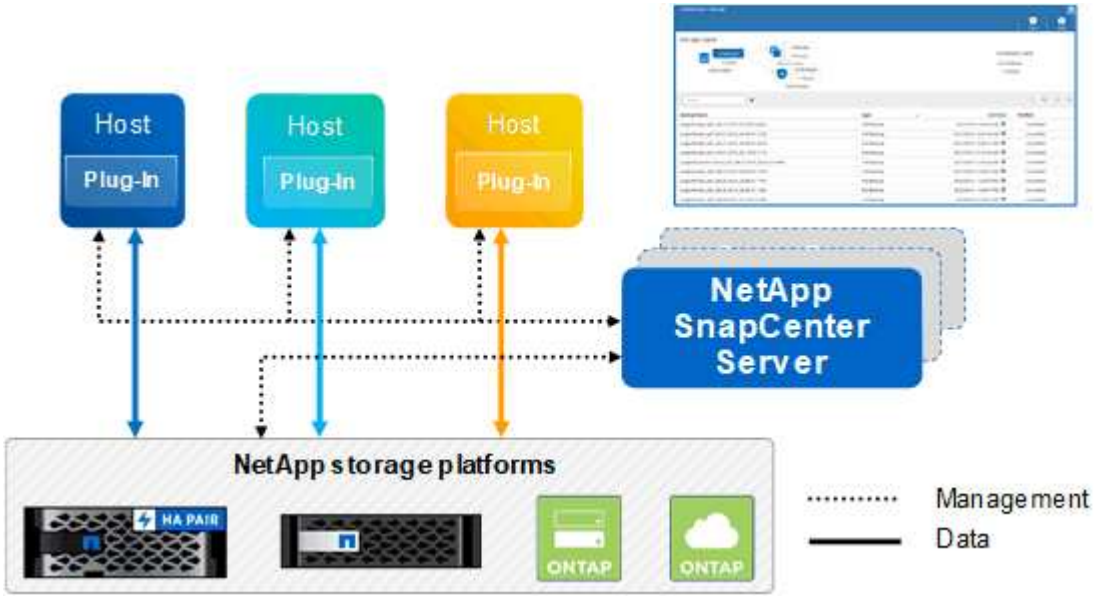
- Disaster Recovery (DR)

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

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 UNIX

> Il plug-in SnapCenter per UNIX non è un plug-in standalone e non può essere installato in modo indipendente. Questo plug-in viene installato automaticamente quando si installa il plug-in SnapCenter per database Oracle o il plug-in SnapCenter per database SAP HANA.

- Pacchetto plug-in SnapCenter per AIX, che include i seguenti plug-in:
  - Plug-in SnapCenter per database Oracle
  - Plug-in SnapCenter per UNIX

> Il plug-in SnapCenter per UNIX non è un plug-in standalone e non può essere installato in modo indipendente. Questo plug-in viene installato automaticamente quando si installa il plug-in SnapCenter per database Oracle.

- Plug-in personalizzati di SnapCenter

  I plug-in personalizzati sono supportati dalla community e possono essere scaricati da "Storage Automation Store di NetApp".

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.

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
Plug-in personalizzati	"Storage Automation Store di NetApp"	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, il "Plug-in SnapCenter per la documentazione di VMware vSphere" Contiene informazioni sulla protezione di database e file system virtualizzati utilizzando il plug-in SnapCenter basato su Linux per l'appliance virtuale VMware vSphere (formato appliance virtuale aperta).

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 delle copie Snapshot e recupero dello spazio per gli 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.

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.

Gli esempi di plug-in personalizzati MySQL, DB2 e MongoDB per il software SnapCenter possono essere scaricati da "Storage Automation Store di NetApp".

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 versione successiva supporta la comunicazione TLS (Transport Layer Security) 1.2 con ONTAP. È inoltre possibile utilizzare la comunicazione TLS 1.2 tra client e server.
- 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".

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".

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 copia 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. Se si desidera eseguire operazioni di copia Snapshot e protezione dei dati in un ambiente di file system Windows sullo storage ONTAP, il ruolo di amministratore di 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 ulteriori 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 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

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
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
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
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
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.

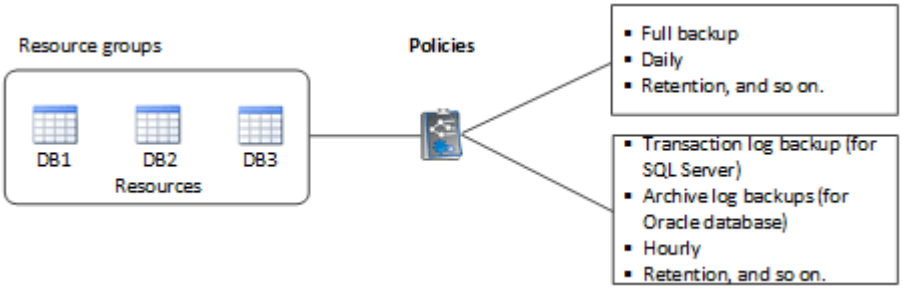
- **Policy** specifica la frequenza di backup, la conservazione delle copie, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  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.

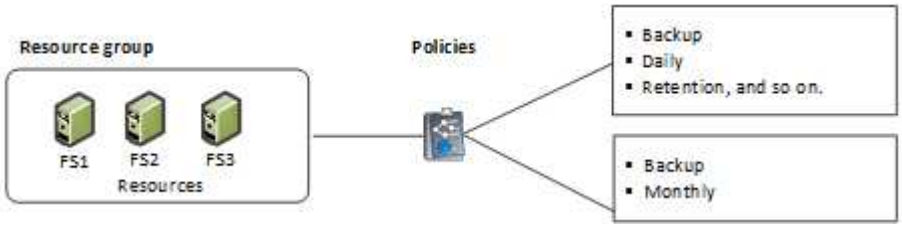
Un gruppo di risorse definisce *cosa* si desidera proteggere e quando si desidera proteggerlo in termini di giorno e ora. Pensa a una policy come a definire *come* la vuoi proteggere. Ad esempio, se si esegue il backup di tutti i database o di tutti i file system di un host, è possibile creare un gruppo 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 di SnapCenter, vedere "Panoramica delle API REST"

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

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.