Documentazione NetApp Backup and Recovery

NetApp Backup and Recovery

NetApp
February 13, 2026

Sommario

Documentazione NetApp Backup and Recovery

Note di rilascio

Novità di NetApp Backup and Recovery

Scopri le novità di NetApp Backup and Recovery.

09 febbraio 2026

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Carichi di lavoro Microsoft Hyper-V supportati in General Availability (GA)

Il supporto per i carichi di lavoro Microsoft Hyper-V è ora generalmente disponibile (GA) in NetApp Backup and Recovery.

Carichi di lavoro VMware supportati in General Availability (GA)

Il supporto dei carichi di lavoro VMware è ora generalmente disponibile (GA) in NetApp Backup and Recovery.

Miglioramenti dei carichi di lavoro Kubernetes

Questa versione dei carichi di lavoro Kubernetes introduce le seguenti funzionalità migliorate:

- **Supporto del flusso di lavoro CR**: ora è possibile eseguire attività di protezione comuni utilizzando i CR e l'interfaccia utente web di NetApp Backup and Recovery.
- **Migrazione cluster**: ora puoi aggiungere i cluster Kubernetes esistenti protetti con Trident Protect a NetApp Backup and Recovery.
- **Supporto del framework di alerting**: ora puoi ricevere avvisi tramite e-mail e interfaccia utente per determinati eventi del carico di lavoro Kubernetes.
- **Integrazione della scheda Ripristina**: ora puoi accedere alle azioni di ripristino del workload Kubernetes dal menu Ripristina.
- **Supporto per l'architettura di backup fanout 3-2-1**: ora puoi utilizzare un'architettura fanout 3-2-1 nella tua policy di protezione quando proteggi i workload Kubernetes.

Per i dettagli sulla protezione dei carichi di lavoro Kubernetes, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro di Kubernetes" .

Miglioramenti dei carichi di lavoro Oracle Database

Questa versione dei carichi di lavoro Oracle Database introduce le seguenti funzionalità migliorate:

- **Supporto per utenti non root**: Gli utenti non root possono ora eseguire operazioni di backup, ripristino e clonazione, migliorando la sicurezza e la conformità.
- **Supporto clone**: le funzionalità di clonazione sono ora supportate negli ambienti NAS, SAN e ASM primari e secondari utilizzando ASM library v2, consentendo flussi di lavoro di protezione coordinati.
- **Supporto per la suddivisione dei cloni**: ora puoi suddividere gli snapshot scrivibili (cloni) dai volumi padre, liberando spazio di storage e consentendo operazioni indipendenti.
- **Backup e ripristino per archivio di oggetti**: Le funzionalità native di backup e ripristino sono ora supportate per le destinazioni di storage a oggetti compatibili con S3.

- **Clone Lifecycle Management (CLM)**: le operazioni di aggiornamento dei cloni sono supportate sullo storage primario.
- **Clona su host alternativo**: ora puoi clonare i database su un host diverso (a scopo di test o analisi) sia dallo storage primario che dallo storage secondario.
- **Supporto per i gruppi di coerenza ONTAP**: Ora sono supportati i gruppi di coerenza ONTAP, garantendo snapshot coerenti con l'applicazione su più volumi.
- NetApp Backup and Recovery ora supporta le seguenti architetture di policy di protezione per i carichi di lavoro di Oracle Database:
  - Fanout 3-2-1
  - Da disco a disco
  - Da disco a storage a oggetti
  - A cascata
  - Istantanea locale

Per informazioni dettagliate sulla protezione dei carichi di lavoro Oracle Database, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro del database Oracle".

19 gennaio 2026

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Miglioramenti dei carichi di lavoro del volume ONTAP

Questa versione dei carichi di lavoro del volume ONTAP introduce le seguenti funzionalità migliorate:

Supporto per più bucket: (Anteprima privata) A partire da ONTAP 9.17.1 e versioni successive, è possibile proteggere i volumi all'interno di un sistema con un massimo di 6 bucket per sistema su diversi provider cloud.

"Scopri di più sul backup dei dati del volume ONTAP utilizzando NetApp Backup and Recovery".

Miglioramenti dei carichi di lavoro VMware

Questa versione dei carichi di lavoro VMware introduce le seguenti funzionalità avanzate:

- Il supporto dei carichi di lavoro VMware è ora generalmente disponibile (GA) in NetApp Backup and Recovery.
- Ora puoi ripristinare i file e le cartelle del sistema operativo guest.

"Scopri di più sul ripristino di file e cartelle guest".

Miglioramenti dell'anteprima dei carichi di lavoro Hyper-V

Questa versione dei carichi di lavoro Hyper-V introduce le seguenti funzionalità avanzate:

- Ora puoi ripristinare backup e snapshot delle VM Hyper-V in una posizione alternativa. Utilizza questa funzionalità per gestire le versioni delle VM su diversi host Hyper-V.
- NetApp Backup and Recovery ora supporta le macchine virtuali Hyper-V fornite da System Center Virtual Machine Manager (SCVMM) e ospitate su una CIFS share.
- Ora puoi modificare i gruppi di protezione.

Solo in questa versione non è possibile aggiornare i plugin NetApp per Hyper-V o Windows utilizzando l'opzione **Aggiorna** nel menu Azioni. In alternativa, rimuovere ciascun host Hyper-V e aggiungerlo nuovamente per aggiornare i plugin.

"Scopri di più sul ripristino delle VM Hyper-V con NetApp Backup and Recovery".

Miglioramenti dell'anteprima dei carichi di lavoro KVM

L'anteprima dei carichi di lavoro KVM ora protegge gli host KVM e le macchine virtuali gestite da Apache CloudStack.

Per i dettagli sulla protezione dei carichi di lavoro KVM, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro KVM" .

08 dicembre 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Miglioramenti dell'anteprima dei carichi di lavoro VMware

La versione di anteprima dei carichi di lavoro VMware introduce le seguenti funzionalità avanzate:

- Ora puoi ripristinare backup e snapshot in una posizione alternativa. Questa funzionalità è utile se si desidera gestire le versioni di una VM su diverse distribuzioni VMware vCenter, host VMware ESXi o datastore VMware.

"Scopri di più sul ripristino delle VM VMware con NetApp Backup and Recovery".

- Ora è possibile ripristinare specifici dischi virtuali VMware (immagini VMDK) da una posizione primaria o secondaria, consentendo un controllo più granulare sul ripristino dei dati della VM.

"Scopri di più sul ripristino dei dischi virtuali VMware con NetApp Backup and Recovery".

06 ottobre 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Il BlueXP backup and recovery ora sono NetApp Backup and Recovery

Il BlueXP backup and recovery sono stati rinominati NetApp Backup and Recovery.

BlueXP è ora NetApp Console

NetApp Console, basata sulle fondamenta BlueXP migliorate e ristrutturate, offre una gestione centralizzata dello storage NetApp e NetApp Data Services in ambienti on-premise e cloud di livello aziendale, offrendo informazioni in tempo reale, flussi di lavoro più rapidi e un'amministrazione semplificata, altamente sicura e conforme.

Per i dettagli su cosa è cambiato, vedere"Note sulla versione NetApp Console ."

Supporto del carico di lavoro Hyper-V come anteprima privata

Questa versione di NetApp Backup and Recovery introduce il supporto per l'individuazione e la gestione dei carichi di lavoro Hyper-V:

- Backup e ripristino di VM su istanze autonome e istanze di cluster di failover (FCI)
- Proteggere le VM archiviate su condivisioni SMB3
- Protezione in blocco a livello di macchina virtuale
- Backup coerenti con VM e crash
- Ripristinare le VM da storage primario, secondario e di oggetti
- Cerca e ripristina i backup delle VM

Per i dettagli sulla protezione dei carichi di lavoro Hyper-V, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro Hyper-V" .

Supporto del carico di lavoro KVM come anteprima privata

Questa versione di NetApp Backup and Recovery introduce il supporto per l'individuazione e la gestione dei carichi di lavoro KVM:

- Eseguire il backup e il ripristino delle immagini VM qcow2 archiviate su condivisioni NFS
- Backup dei pool di archiviazione
- Protezione in blocco di VM e pool di archiviazione mediante gruppi di protezione
- Backup di VM coerenti con la VM e con gli arresti anomali
- Cerca e ripristina i backup delle VM da storage primario, secondario e di oggetti
- Procedura guidata per il backup e il ripristino di VM basate su KVM e dati di VM

Per i dettagli sulla protezione dei carichi di lavoro KVM, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro KVM" .

Miglioramenti dell'anteprima di Kubernetes

La versione di anteprima dei carichi di lavoro Kubernetes introduce le seguenti funzionalità avanzate:

- Supporto dell'architettura di backup fan-out 3-2-1
- Supporto per ONTAP S3 come destinazione di backup
- Nuova dashboard di Kubernetes per una gestione più semplice
- La configurazione avanzata del controllo degli accessi basato sui ruoli (RBAC) include il supporto per i seguenti ruoli:
  - Super amministratore di backup e ripristino
  - Backup e ripristino amministratore del backup
  - Backup e ripristino ripristino amministratore
  - Visualizzatore di backup e ripristino
- Supporto per la distribuzione Kubernetes di SUSE Rancher
- Supporto multi-bucket: ora puoi proteggere i volumi all'interno di un sistema con più bucket per sistema su diversi provider cloud

Per i dettagli sulla protezione dei carichi di lavoro Kubernetes, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro di Kubernetes" .

Miglioramenti dell'anteprima VMware

La versione di anteprima dei carichi di lavoro VMware introduce le seguenti funzionalità avanzate:

- Supporto per il ripristino da storage di oggetti
- La dashboard NetApp Console ora visualizza le informazioni sullo stato del carico di lavoro VMware
- Supporto per il controllo degli accessi basato sui ruoli (RBAC)
- Supporto per notifiche ed avvisi via e-mail per eventi lavorativi
- Supporto per il backup e il ripristino su storage basato su NVMe
- Modifica gruppi di protezione
- Modifica le policy di protezione

Per i dettagli sulla protezione dei carichi di lavoro VMware, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro VMware" .

Supporto del carico di lavoro di Oracle Database come anteprima privata

Questa versione di NetApp Backup and Recovery introduce il supporto per l'individuazione e la gestione dei carichi di lavoro di Oracle Database:

- Scopri i database Oracle autonomi
- Creare policy di protezione solo per i dati o per i backup di dati e log
- Proteggi i database Oracle con uno schema di backup 3-2-1
- Configurare la conservazione del backup
- Montare e smontare i backup ARCHIVELOG
- Database virtualizzati
- Cerca e ripristina i backup del database
- Supporto dashboard Oracle

Per informazioni dettagliate sulla protezione dei carichi di lavoro Oracle Database, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro del database Oracle".

Miglioramenti del carico di lavoro del volume ONTAP

Questa versione dei carichi di lavoro del volume ONTAP introduce le seguenti funzionalità migliorate:

A partire da ONTAP 9.17.1 e versioni successive, DataLock è ora supportato da Google Cloud Platform. Ciò integra il supporto DataLock esistente con Amazon AWS, Microsoft Azure e NetApp StorageGRID.

25 agosto 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Supporto per la protezione dei carichi di lavoro VMware in anteprima

Questa versione aggiunge il supporto in anteprima per la protezione dei carichi di lavoro VMware. Esegui il backup di VM VMware e datastore dai sistemi ONTAP locali ad Amazon Web Services e StorageGRID.

La documentazione sulla protezione dei carichi di lavoro VMware viene fornita come anteprima tecnologica. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli, i contenuti e la tempistica dell'offerta prima della disponibilità generale.

"Scopri di più sulla protezione dei carichi di lavoro VMware con NetApp Backup and Recovery".

L'indicizzazione ad alte prestazioni per AWS, Azure e GCP è generalmente disponibile

A febbraio 2025 abbiamo annunciato l'anteprima dell'indicizzazione ad alte prestazioni (Indexed Catalog v2) per AWS, Azure e GCP. Questa funzionalità è ora generalmente disponibile (GA). Nel giugno 2025 lo abbiamo fornito di default a tutti i *nuovi* clienti. Con questa versione, il supporto è disponibile per *tutti* i clienti. L'indicizzazione ad alte prestazioni migliora le prestazioni delle operazioni di backup e ripristino per i carichi di lavoro protetti nell'archiviazione di oggetti.

Abilitato per impostazione predefinita:

- Se sei un nuovo cliente, l'indicizzazione ad alte prestazioni è abilitata per impostazione predefinita.
- Se sei un cliente esistente, puoi abilitare la reindicizzazione andando alla sezione Ripristina dell'interfaccia utente.

12 agosto 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

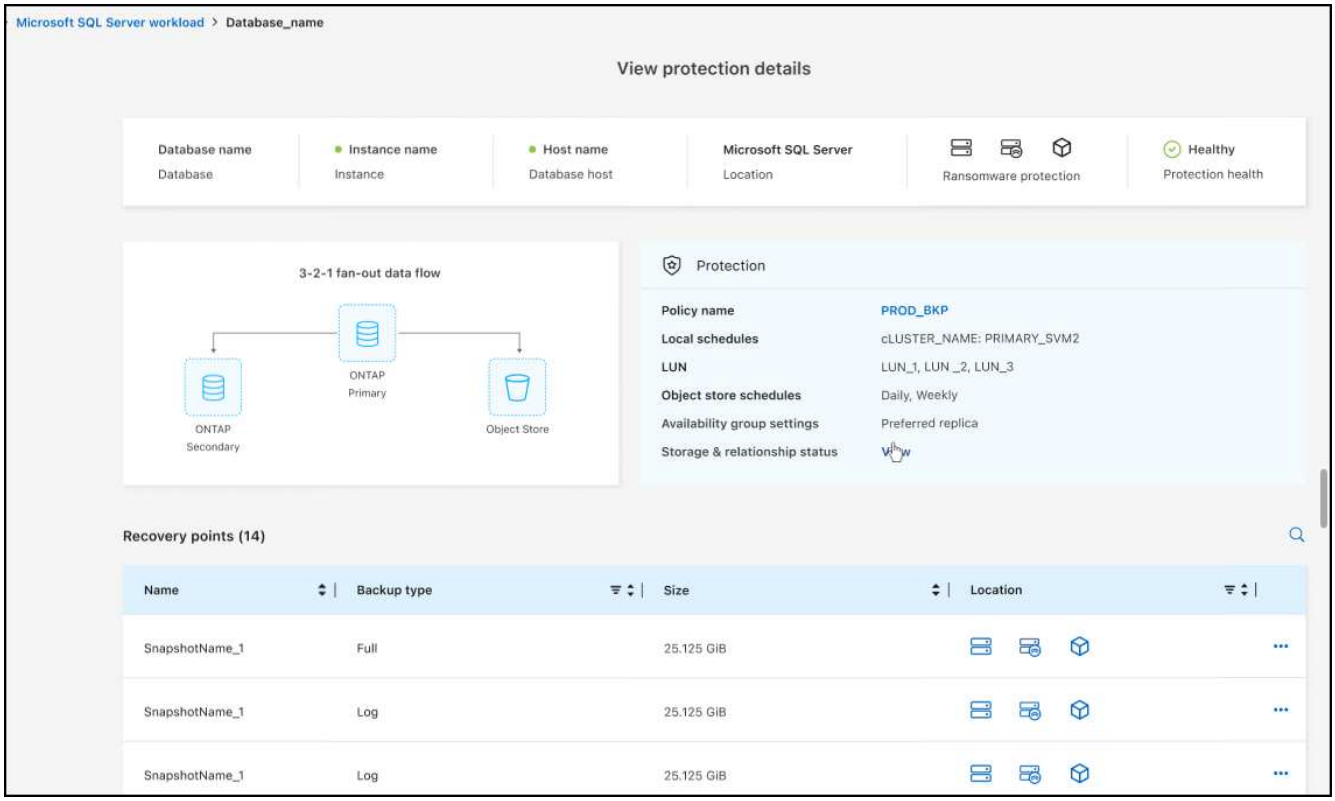
Carico di lavoro di Microsoft SQL Server supportato in disponibilità generale (GA)

Il supporto del carico di lavoro di Microsoft SQL Server è ora generalmente disponibile (GA) in NetApp Backup and Recovery. Le organizzazioni che utilizzano un ambiente MSSQL su ONTAP, Cloud Volumes ONTAP e Amazon FSx for NetApp ONTAP possono ora sfruttare questo nuovo servizio di backup e ripristino per proteggere i propri dati.

Questa versione include i seguenti miglioramenti al supporto del carico di lavoro di Microsoft SQL Server rispetto alla versione di anteprima precedente:

- * Sincronizzazione attiva SnapMirror **: questa versione supporta ora la sincronizzazione attiva SnapMirror (nota anche come SnapMirror Business Continuity [SM-BC]), che 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. NetApp Backup and Recovery supporta ora la protezione dei database Microsoft SQL Server in una configurazione SnapMirror ActiveSync e Metrocluster. Le informazioni vengono visualizzate nella sezione *Stato di archiviazione e relazione** della pagina Dettagli protezione. Le informazioni sulla relazione vengono visualizzate nella sezione aggiornata **Impostazioni secondarie** della pagina Policy.

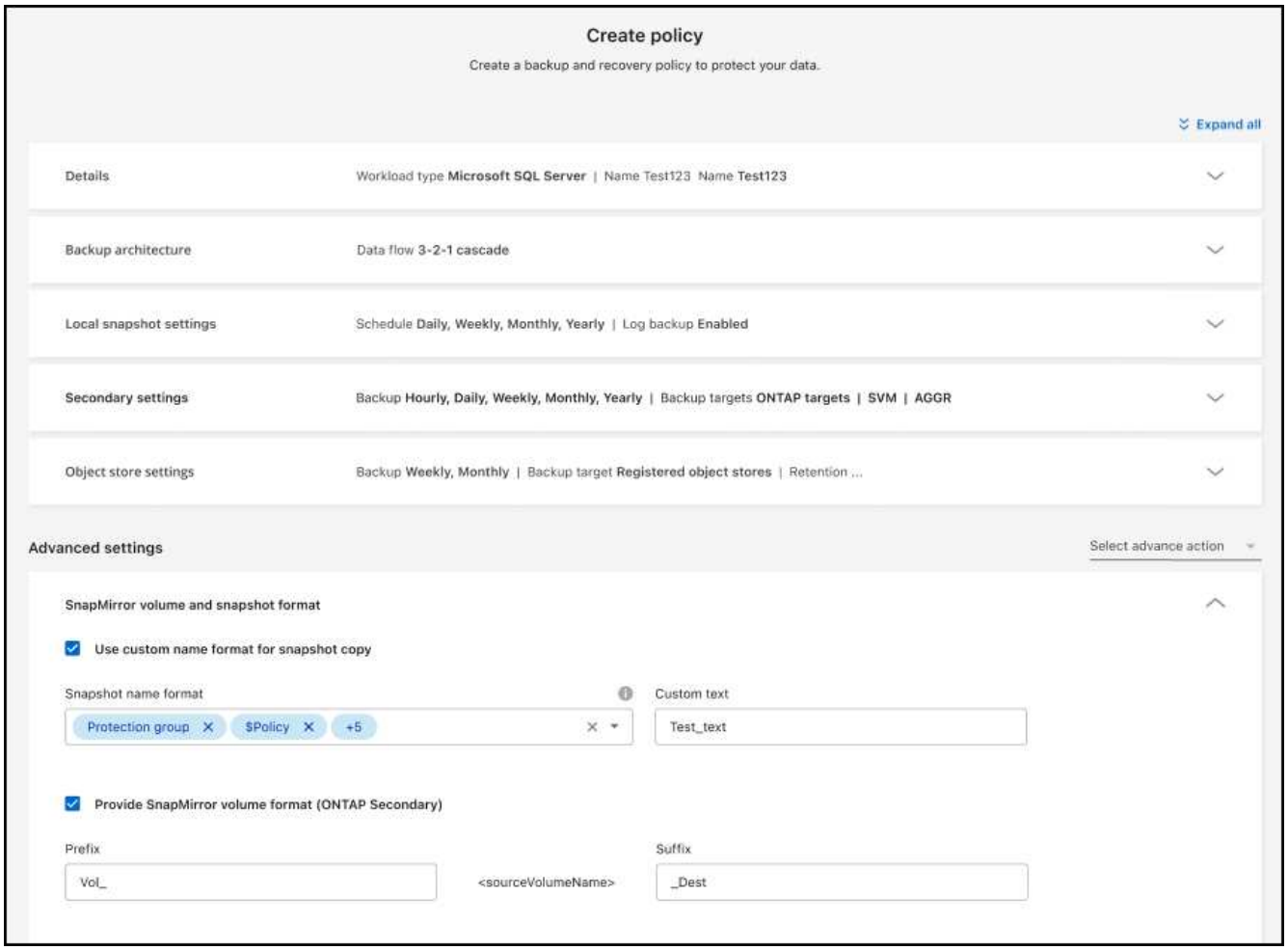
  Fare riferimento a "Utilizza policy per proteggere i tuoi carichi di lavoro" .



- **Supporto multi-bucket**: ora puoi proteggere i volumi all'interno di un ambiente di lavoro con un massimo di 6 bucket per ambiente di lavoro su diversi provider cloud.
- **Aggiornamenti di licenze e versioni di prova gratuite** per carichi di lavoro di SQL Server: ora puoi utilizzare il modello di licenza NetApp Backup and Recovery esistente per proteggere i carichi di lavoro di SQL Server. Non esiste alcun requisito di licenza separato per i carichi di lavoro di SQL Server.

  Per i dettagli, fare riferimento a "Impostare la licenza per NetApp Backup and Recovery" .

- **Nome snapshot personalizzato**: ora puoi utilizzare il nome del tuo snapshot in un criterio che regola i backup per i carichi di lavoro di Microsoft SQL Server. Inserisci queste informazioni nella sezione **Impostazioni avanzate** della pagina Policy.

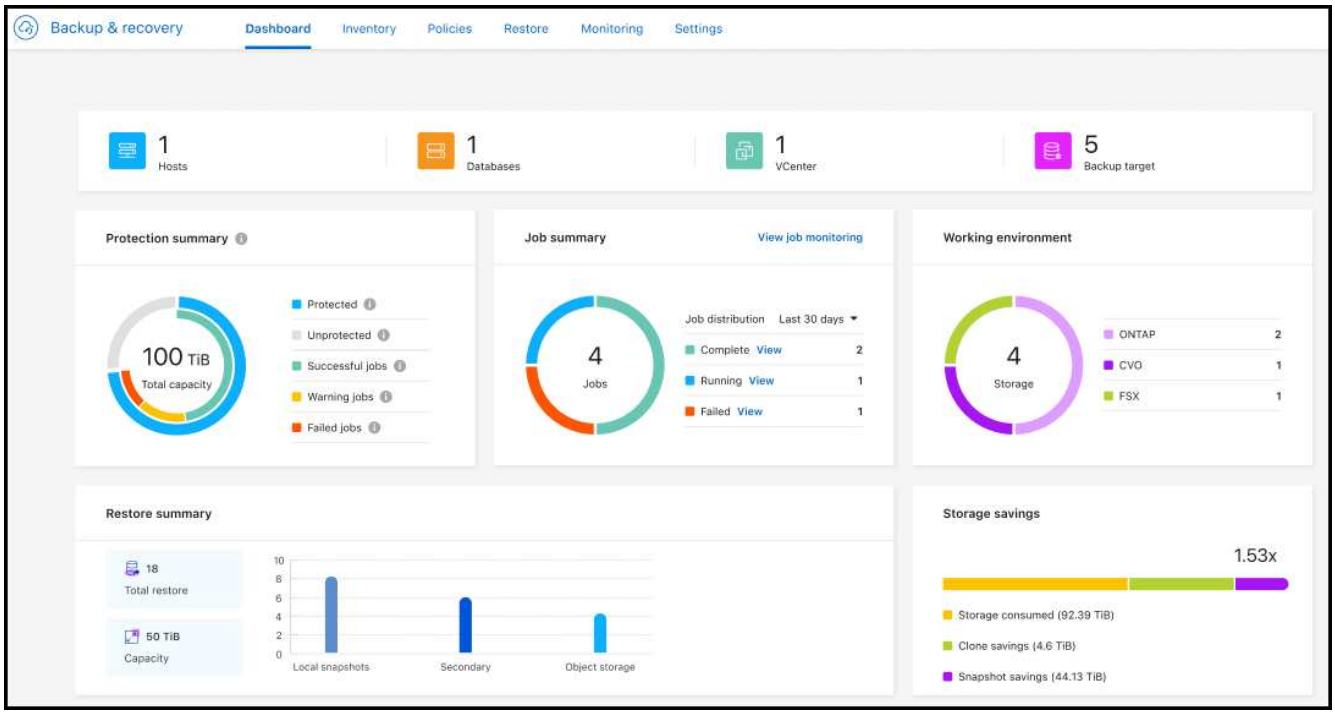


Fare riferimento a "Utilizza policy per proteggere i tuoi carichi di lavoro" .

- **Prefisso e suffisso del volume secondario**: è possibile immettere un prefisso e un suffisso personalizzati nella sezione **Impostazioni avanzate** della pagina Criteri.
- **Identità e accesso**: ora puoi controllare l'accesso degli utenti alle funzionalità.

  Fare riferimento a "Accedi a NetApp Backup and Recovery" E "Accesso alle funzionalità NetApp Backup and Recovery" .

- **Ripristino da un archivio oggetti a un host alternativo**: ora puoi eseguire il ripristino da un archivio oggetti a un host alternativo anche se l'archivio primario è inattivo.
- **Dati di backup del registro**: la pagina dei dettagli sulla protezione del database ora mostra i backup del registro. È possibile visualizzare la colonna Tipo di backup che indica se il backup è un backup completo o un backup del registro.
- **Dashboard migliorata**: la dashboard ora mostra i risparmi di archiviazione e clonazione.



Miglioramenti del carico di lavoro del volume ONTAP

- *Ripristino multi-cartella per volumi ONTAP *: fino ad ora, era possibile ripristinare una cartella o più file alla volta tramite la funzionalità Sfoglia e ripristina. NetApp Backup and Recovery ora offre la possibilità di selezionare più cartelle contemporaneamente utilizzando la funzionalità Sfoglia e ripristina.
- **Visualizzazione e gestione dei backup dei volumi eliminati**: la dashboard NetApp Backup and Recovery ora offre un'opzione per visualizzare e gestire i volumi eliminati da ONTAP. Con questo, è possibile visualizzare ed eliminare i backup dai volumi che non esistono più in ONTAP.
- **Eliminazione forzata dei backup**: in alcuni casi estremi, potresti voler impedire a NetApp Backup and Recovery di accedere più ai backup. Ciò potrebbe accadere, ad esempio, se il servizio non ha più accesso al bucket di backup o se i backup sono protetti da DataLock ma non si desidera più utilizzarli. In precedenza non era possibile eliminarli autonomamente, ma era necessario contattare l'assistenza NetApp . Con questa versione, è possibile utilizzare l'opzione per forzare l'eliminazione dei backup (a livello di volume e di ambiente di lavoro).

> Utilizzare questa opzione con cautela e solo in caso di estrema necessità di pulizia. NetApp Backup and Recovery non avrà più accesso a questi backup, anche se non vengono eliminati dall'archiviazione degli oggetti. Sarà necessario rivolgersi al proprio provider cloud ed eliminare manualmente i backup.

Fare riferimento a "Proteggere i carichi di lavoro ONTAP" .

28 luglio 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Supporto del carico di lavoro Kubernetes in anteprima

Questa versione di NetApp Backup and Recovery introduce il supporto per l'individuazione e la gestione dei carichi di lavoro Kubernetes:

- Scopri i cluster Red Hat OpenShift e Kubernetes open source, supportati da NetApp ONTAP, senza condividere i file kubeconfig.
- Scopri, gestisci e proteggi le applicazioni su più cluster Kubernetes utilizzando un piano di controllo unificato.
- Trasferisci le operazioni di spostamento dei dati per il backup e il ripristino delle applicazioni Kubernetes a NetApp ONTAP.
- Orchestrare i backup delle applicazioni locali e basati su storage di oggetti.
- Esegui il backup e il ripristino di intere applicazioni e singole risorse su qualsiasi cluster Kubernetes.
- Lavora con container e macchine virtuali in esecuzione su Kubernetes.
- Crea backup coerenti con l'applicazione utilizzando modelli e hook di esecuzione.

Per i dettagli sulla protezione dei carichi di lavoro Kubernetes, fare riferimento a "Panoramica sulla protezione dei carichi di lavoro di Kubernetes" .

14 luglio 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Dashboard del volume ONTAP migliorato

Nell'aprile 2025 abbiamo lanciato un'anteprima di una Dashboard del volume ONTAP migliorata, molto più veloce ed efficiente.

Questa dashboard è stata progettata per aiutare i clienti aziendali con un numero elevato di carichi di lavoro. Anche per i clienti con 20.000 volumi, il nuovo dashboard si carica in meno di 10 secondi.

Dopo un'anteprima di successo e un feedback positivo da parte dei clienti, ora la stiamo rendendo l'esperienza predefinita per tutti i nostri clienti. Preparatevi a una dashboard incredibilmente veloce.

Per i dettagli, vedere"Visualizza lo stato di protezione nella Dashboard" .

Supporto del carico di lavoro di Microsoft SQL Server come anteprima tecnologica pubblica

Questa versione di NetApp Backup and Recovery fornisce un'interfaccia utente aggiornata che consente di gestire i carichi di lavoro di Microsoft SQL Server utilizzando una strategia di protezione 3-2-1, nota in NetApp Backup and Recovery. Con questa nuova versione, è possibile eseguire il backup di questi carichi di lavoro sullo storage primario, replicarli sullo storage secondario ed eseguirne il backup sullo storage di oggetti cloud.

Puoi iscriverti all'anteprima completando questo "Anteprima del modulo di registrazione" .

> Questa documentazione sulla protezione dei carichi di lavoro di Microsoft SQL Server viene fornita come anteprima tecnologica. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare dettagli, contenuti e tempistiche prima della disponibilità generale.

Questa versione di NetApp Backup and Recovery include i seguenti aggiornamenti:

- **Funzionalità di backup 3-2-1**: questa versione integra le funzionalità SnapCenter , consentendo di gestire e proteggere le risorse SnapCenter con una strategia di protezione dei dati 3-2-1 dall'interfaccia utente NetApp Backup and Recovery .
- **Importa da SnapCenter**: puoi importare i dati di backup e le policy SnapCenter in NetApp Backup and Recovery.

- **Un'interfaccia utente riprogettata** offre un'esperienza più intuitiva per la gestione delle attività di backup e ripristino.
- **Destinazioni di backup**: puoi aggiungere bucket negli ambienti Amazon Web Services (AWS), Microsoft Azure Blob Storage, StorageGRID e ONTAP S3 da utilizzare come destinazioni di backup per i carichi di lavoro di Microsoft SQL Server.
- **Supporto del carico di lavoro**: questa versione consente di eseguire il backup, il ripristino, la verifica e la clonazione di database e gruppi di disponibilità di Microsoft SQL Server. (Il supporto per altri carichi di lavoro verrà aggiunto nelle versioni future.)
- **Opzioni di ripristino flessibili**: questa versione consente di ripristinare i database sia nelle posizioni originali che in quelle alternative in caso di danneggiamento o perdita accidentale dei dati.
- **Copie di produzione istantanee**: genera copie di produzione salvaspazio per sviluppo, test o analisi in pochi minuti anziché in ore o giorni.
- Questa versione include la possibilità di creare report dettagliati.

Per informazioni dettagliate sulla protezione dei carichi di lavoro di Microsoft SQL Server, vedere"Panoramica sulla protezione dei carichi di lavoro di Microsoft SQL Server" .

09 giugno 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Aggiornamenti del supporto del catalogo indicizzato

Nel febbraio 2025 abbiamo introdotto la funzionalità di indicizzazione aggiornata (Catalogo indicizzato v2) da utilizzare durante il metodo di ricerca e ripristino dei dati. La versione precedente ha migliorato significativamente le prestazioni di indicizzazione dei dati negli ambienti on-premise. Con questa versione, il catalogo di indicizzazione è ora disponibile negli ambienti Amazon Web Services, Microsoft Azure e Google Cloud Platform (GCP).

Se sei un nuovo cliente, il Catalogo indicizzato v2 è abilitato per impostazione predefinita per tutti i nuovi ambienti. Se sei un cliente esistente, puoi reindicizzare il tuo ambiente per sfruttare Indexed Catalog v2.

Come si abilita l'indicizzazione?

Prima di poter utilizzare il metodo Cerca e ripristina per ripristinare i dati, è necessario abilitare "Indicizzazione" su ogni ambiente di lavoro di origine da cui si prevede di ripristinare volumi o file. Selezionare l'opzione **Abilita indicizzazione** quando si esegue una ricerca e un ripristino.

Il catalogo indicizzato può quindi tenere traccia di ogni volume e file di backup, rendendo le ricerche rapide ed efficienti.

Per maggiori informazioni, fare riferimento a "Abilita l'indicizzazione per Ricerca e Ripristino" .

Endpoint di collegamento privato di Azure ed endpoint di servizio

In genere, NetApp Backup and Recovery stabilisce un endpoint privato con il provider cloud per gestire le attività di protezione. Questa versione introduce un'impostazione facoltativa che consente di abilitare o disabilitare la creazione automatica di un endpoint privato da parte NetApp Backup and Recovery . Potrebbe esserti utile se desideri un maggiore controllo sul processo di creazione dell'endpoint privato.

È possibile abilitare o disabilitare questa opzione quando si abilita la protezione o si avvia il processo di ripristino.

Se si disabilita questa impostazione, è necessario creare manualmente l'endpoint privato affinché NetApp Backup and Recovery funzioni correttamente. Senza una connettività adeguata, potresti non essere in grado di eseguire correttamente le attività di backup e ripristino.

Supporto per SnapMirror su Cloud Resync su ONTAP S3

La versione precedente ha introdotto il supporto per SnapMirror su Cloud Resync (SM-C Resync). La funzionalità semplifica la protezione dei dati durante la migrazione dei volumi negli ambienti NetApp . Questa versione aggiunge il supporto per SM-C Resync su ONTAP S3 e altri provider compatibili con S3 come Wasabi e MinIO.

Porta il tuo bucket per StorageGRID

Quando si creano file di backup nell'archiviazione di oggetti per un ambiente di lavoro, per impostazione predefinita NetApp Backup and Recovery crea il contenitore (bucket o account di archiviazione) per i file di backup nell'account di archiviazione di oggetti configurato. In precedenza, era possibile ignorare questa impostazione e specificare un contenitore personalizzato per Amazon S3, Azure Blob Storage e Google Cloud Storage. Con questa versione, ora puoi utilizzare il tuo contenitore di archiviazione oggetti StorageGRID .

Vedere "Crea il tuo contenitore di archiviazione oggetti" .

13 maggio 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

SnapMirror su Cloud Resync per le migrazioni dei volumi

La funzionalità SnapMirror to Cloud Resync semplifica la protezione e la continuità dei dati durante le migrazioni dei volumi negli ambienti NetApp . Quando un volume viene migrato tramite SnapMirror Logical Replication (LRSE) da una distribuzione NetApp locale a un'altra o a una soluzione basata su cloud come Cloud Volumes ONTAP, SnapMirror to Cloud Resync garantisce che i backup cloud esistenti rimangano intatti e operativi.

Questa funzionalità elimina la necessità di un'operazione di reimpostazione della baseline, che richiede molto tempo e risorse, consentendo alle operazioni di backup di continuare anche dopo la migrazione. Questa funzionalità è utile negli scenari di migrazione del carico di lavoro, supportando sia FlexVols che FlexGroups ed è disponibile a partire dalla versione 9.16.1 ONTAP .

Mantenendo la continuità del backup in tutti gli ambienti, SnapMirror to Cloud Resync migliora l'efficienza operativa e riduce la complessità della gestione dei dati ibridi e multi-cloud.

Per i dettagli su come eseguire l'operazione di risincronizzazione, vedere "Migrare i volumi utilizzando SnapMirror su Cloud Resync" .

Supporto per l'archivio oggetti MinIO di terze parti (anteprima)

NetApp Backup and Recovery estende ora il suo supporto agli archivi di oggetti di terze parti, concentrandosi principalmente su MinIO. Questa nuova funzionalità di anteprima consente di sfruttare qualsiasi archivio di oggetti compatibile con S3 per le proprie esigenze di backup e ripristino.

Con questa versione di anteprima, speriamo di garantire una solida integrazione con gli archivi di oggetti di terze parti prima che venga implementata la funzionalità completa. Vi invitiamo a esplorare questa nuova funzionalità e a fornire feedback per contribuire a migliorare il servizio.

Questa funzionalità non dovrebbe essere utilizzata in produzione.

Limitazioni della modalità di anteprima

Sebbene questa funzionalità sia in anteprima, presenta alcune limitazioni:

- La funzione Bring Your Own Bucket (BYOB) non è supportata.
- L'abilitazione di DataLock nel criterio non è supportata.
- L'abilitazione della modalità di archiviazione nel criterio non è supportata.
- Sono supportati solo gli ambienti ONTAP locali.
- MetroCluster non è supportato.
- Le opzioni per abilitare la crittografia a livello di bucket non sono supportate.

Iniziare

Per iniziare a utilizzare questa funzionalità di anteprima, è necessario abilitare un flag sull'agente della console. È quindi possibile immettere i dettagli di connessione dell'archivio oggetti di terze parti MinIO nel flusso di lavoro di protezione selezionando l'archivio oggetti **Compatibile con terze parti** nella sezione di backup.

16 aprile 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Miglioramenti dell'interfaccia utente

Questa versione migliora la tua esperienza semplificando l'interfaccia:

- La rimozione della colonna Aggregate dalle tabelle Volumi, insieme alle colonne Snapshot Policy, Backup Policy e Replication Policy dalla tabella Volume nella Dashboard V2, si traduce in un layout più snello.
- Escludendo gli ambienti di lavoro non attivati dall'elenco a discesa, l'interfaccia diventa meno confusa, la navigazione più efficiente e il caricamento più rapido.
- Anche se l'ordinamento nella colonna Tag è disabilitato, è comunque possibile visualizzare i tag, assicurandosi che le informazioni importanti rimangano facilmente accessibili.
- La rimozione delle etichette sulle icone di protezione contribuisce a un aspetto più pulito e riduce i tempi di caricamento.
- Durante il processo di attivazione dell'ambiente di lavoro, una finestra di dialogo visualizza un'icona di caricamento per fornire feedback fino al completamento del processo di individuazione, migliorando la trasparenza e la fiducia nelle operazioni del sistema.

Dashboard del volume migliorata (anteprima)

La dashboard del volume ora si carica in meno di 10 secondi, offrendo un'interfaccia molto più veloce ed efficiente. Questa versione di anteprima è disponibile per clienti selezionati, offrendo loro un'anteprima di questi miglioramenti.

Supporto per l'archivio oggetti Wasabi di terze parti (anteprima)

NetApp Backup and Recovery estende ora il supporto agli archivi di oggetti di terze parti, concentrandosi principalmente su Wasabi. Questa nuova funzionalità di anteprima consente di sfruttare qualsiasi archivio di

oggetti compatibile con S3 per le proprie esigenze di backup e ripristino.

Come iniziare con Wasabi

Per iniziare a utilizzare un archivio di terze parti come archivio oggetti, è necessario abilitare un flag nell'agente della console. Successivamente, puoi immettere i dettagli di connessione per il tuo archivio oggetti di terze parti e integrarlo nei tuoi flussi di lavoro di backup e ripristino.

Passi

1. Accedi tramite SSH al tuo connettore.
2. Accedere al contenitore del server NetApp Backup and Recovery cbs:

```
docker exec -it cloudmanager_cbs sh
```

3. Apri il `default.json` file all'interno del `config` cartella tramite VIM o qualsiasi altro editor:

```
vi default.json
```

4. Modificare `allow-s3-compatible` : falso a `allow-s3-compatible` : VERO.
5. Salva le modifiche.
6. Uscire dal contenitore.
7. Riavviare il contenitore del server NetApp Backup and Recovery cbs.

Risultato

Dopo aver riattivato il contenitore, aprire l'interfaccia utente NetApp Backup and Recovery . Quando avvii un backup o modifichi una strategia di backup, vedrai elencato il nuovo provider "S3 Compatible" insieme ad altri provider di backup di AWS, Microsoft Azure, Google Cloud, StorageGRID e ONTAP S3.

Limitazioni della modalità di anteprima

Sebbene questa funzionalità sia in anteprima, tieni presente le seguenti limitazioni:

- La funzione Bring Your Own Bucket (BYOB) non è supportata.
- L'abilitazione di DataLock in un criterio non è supportata.
- L'abilitazione della modalità di archiviazione in un criterio non è supportata.
- Sono supportati solo gli ambienti ONTAP locali.
- MetroCluster non è supportato.
- Le opzioni per abilitare la crittografia a livello di bucket non sono supportate.

Durante questa anteprima, ti invitiamo a esplorare questa nuova funzionalità e a fornire feedback sull'integrazione con archivi di oggetti di terze parti prima che la funzionalità completa venga implementata.

17 marzo 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Esplorazione degli snapshot SMB

Questo aggiornamento NetApp Backup and Recovery ha risolto un problema che impediva ai clienti di esplorare gli snapshot locali in un ambiente SMB.

Aggiornamento dell'ambiente AWS GovCloud

Questo aggiornamento NetApp Backup and Recovery ha risolto un problema che impediva all'interfaccia utente di connettersi a un ambiente AWS GovCloud a causa di errori del certificato TLS. Il problema è stato risolto utilizzando il nome host dell'agente della console anziché l'indirizzo IP.

Limiti di conservazione della policy di backup

In precedenza, l'interfaccia utente NetApp Backup and Recovery limitava i backup a 999 copie, mentre la CLI ne consentiva di più. Ora è possibile collegare fino a 4.000 volumi a un criterio di backup e includere 1.018 volumi non collegati a un criterio di backup. Questo aggiornamento include ulteriori convalide che impediscono il superamento di questi limiti.

Risincronizzazione di SnapMirror Cloud

Questo aggiornamento garantisce che la risincronizzazione SnapMirror Cloud non possa essere avviata da NetApp Backup and Recovery per le versioni ONTAP non supportate dopo l'eliminazione di una relazione SnapMirror .

21 febbraio 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Indicizzazione ad alte prestazioni

NetApp Backup and Recovery introduce una funzionalità di indicizzazione aggiornata che rende più efficiente l'indicizzazione dei dati sul sistema di origine. La nuova funzionalità di indicizzazione include aggiornamenti all'interfaccia utente, prestazioni migliorate del metodo Cerca e ripristina per il ripristino dei dati, aggiornamenti alle funzionalità di ricerca globale e una migliore scalabilità.

Ecco una ripartizione dei miglioramenti:

- **Consolidamento delle cartelle**: la versione aggiornata raggruppa le cartelle utilizzando nomi che includono identificatori specifici, rendendo il processo di indicizzazione più fluido.
- **Compattazione dei file Parquet**: la versione aggiornata riduce il numero di file utilizzati per indicizzare ciascun volume, semplificando il processo ed eliminando la necessità di un database aggiuntivo.
- **Scale-out con più sessioni**: la nuova versione aggiunge più sessioni per gestire le attività di indicizzazione, velocizzando il processo.
- **Supporto per più contenitori di indicizzazione**: la nuova versione utilizza più contenitori per gestire e distribuire meglio le attività di indicizzazione.
- **Flusso di lavoro dell'indice diviso**: la nuova versione divide il processo di indicizzazione in due parti, migliorando l'efficienza.
- **Miglioramento della concorrenza**: la nuova versione consente di eliminare o spostare le directory contemporaneamente, velocizzando il processo di indicizzazione.

Chi trae vantaggio da questa funzionalità?

La nuova funzionalità di indicizzazione è disponibile per tutti i nuovi clienti.

Come si abilita l'indicizzazione?

Prima di poter utilizzare il metodo Cerca e ripristina per ripristinare i dati, è necessario abilitare "Indicizzazione" su ciascun sistema di origine da cui si prevede di ripristinare volumi o file. Ciò consente al catalogo indicizzato di tenere traccia di ogni volume e di ogni file di backup, rendendo le ricerche rapide ed efficienti.

Abilitare l'indicizzazione nell'ambiente di lavoro di origine selezionando l'opzione "Abilita indicizzazione" quando si esegue una ricerca e un ripristino.

Per maggiori informazioni, consultare la documentazione "come ripristinare i dati ONTAP utilizzando Cerca e Ripristina" .

Scala supportata

La nuova funzionalità di indicizzazione supporta quanto segue:

- Efficienza di ricerca globale in meno di 3 minuti
- Fino a 5 miliardi di file
- Fino a 5000 volumi per cluster
- Fino a 100.000 snapshot per volume
- Il tempo massimo per l'indicizzazione di base è inferiore a 7 giorni. Il tempo effettivo varierà a seconda dell'ambiente.

Miglioramenti delle prestazioni di ricerca globale

Questa versione include anche miglioramenti alle prestazioni della ricerca globale. Ora vedrai indicatori di avanzamento e risultati di ricerca più dettagliati, tra cui il numero di file e il tempo impiegato per la ricerca. Contenitori dedicati per la ricerca e l'indicizzazione garantiscono che le ricerche globali vengano completate in meno di cinque minuti.

Tieni presente queste considerazioni relative alla ricerca globale:

- Il nuovo indice non viene eseguito sugli snapshot etichettati come orari.
- La nuova funzionalità di indicizzazione funziona solo sugli snapshot su FlexVols e non sugli snapshot su FlexGroups.

13 febbraio 2025

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Versione di anteprima NetApp Backup and Recovery

Questa versione di anteprima di NetApp Backup and Recovery fornisce un'interfaccia utente aggiornata che consente di gestire i carichi di lavoro di Microsoft SQL Server utilizzando una strategia di protezione 3-2-1, nota in NetApp Backup and Recovery. Con questa nuova versione, è possibile eseguire il backup di questi carichi di lavoro sullo storage primario, replicarli sullo storage secondario ed eseguirne il backup sullo storage di oggetti cloud.

> La presente documentazione viene fornita come anteprima tecnologica. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli, i contenuti e la tempistica dell'offerta prima della disponibilità generale.

Questa versione di NetApp Backup and Recovery Preview 2025 include i seguenti aggiornamenti.

- Un’interfaccia utente riprogettata che offre un’esperienza più intuitiva per la gestione delle attività di backup e ripristino.
- La versione di anteprima consente di eseguire il backup e il ripristino dei database Microsoft SQL Server. (Il supporto per altri carichi di lavoro verrà aggiunto nelle versioni future.)
- Questa versione integra le funzionalità SnapCenter , consentendo di gestire e proteggere le risorse SnapCenter con una strategia di protezione dei dati 3-2-1 dall’interfaccia utente NetApp Backup and Recovery .
- Questa versione consente di importare carichi di lavoro SnapCenter in NetApp Backup and Recovery.

22 novembre 2024

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Modalità di protezione SnapLock Compliance e SnapLock Enterprise

NetApp Backup and Recovery ora può eseguire il backup dei volumi locali FlexVol e FlexGroup configurati utilizzando le modalità di protezione SnapLock Compliance o SnapLock Enterprise . Per usufruire di questo supporto, i cluster devono eseguire ONTAP 9.14 o versione successiva. Il backup dei volumi FlexVol mediante la modalità SnapLock Enterprise è supportato a partire dalla versione 9.11.1 ONTAP . Le versioni precedenti ONTAP non forniscono alcun supporto per il backup dei volumi di protezione SnapLock .

Consulta l’elenco completo dei volumi supportati in "Scopri di più su NetApp Backup and Recovery" .

Indicizzazione per il processo di ricerca e ripristino nella pagina Volumi

Prima di poter utilizzare Ricerca e ripristino, è necessario abilitare "Indicizzazione" su ciascun sistema sorgente da cui si desidera ripristinare i dati del volume. Ciò consente al catalogo indicizzato di tenere traccia dei file di backup per ogni volume. La pagina Volumi ora mostra lo stato di indicizzazione:

- Indicizzato: i volumi sono stati indicizzati.
- In corso
- Non indicizzato
- Indicizzazione sospesa
- Errore
- Non abilitato

27 settembre 2024

Questa versione NetApp Backup and Recovery include i seguenti aggiornamenti.

Supporto Podman su RHEL 8 o 9 con Browse e Restore

NetApp Backup and Recovery ora supporta il ripristino di file e cartelle su Red Hat Enterprise Linux (RHEL) versioni 8 e 9 utilizzando il motore Podman. Ciò si applica al metodo Sfoglia e Ripristina NetApp Backup and Recovery .

La versione 3.9.40 dell’agente console supporta determinate versioni di Red Hat Enterprise Linux versioni 8 e 9 per qualsiasi installazione manuale del software dell’agente console su un host RHEL 8 o 9, indipendentemente dalla posizione, oltre ai sistemi operativi menzionati nel "requisiti dell’host" . Queste versioni più recenti di RHEL richiedono il motore Podman anziché il motore Docker. In precedenza, NetApp

Backup and Recovery presentava due limitazioni quando si utilizzava il motore Podman. Queste limitazioni sono state rimosse.

"Scopri di più sul ripristino dei dati ONTAP dai file di backup".

L'indicizzazione più rapida del catalogo migliora la ricerca e il ripristino

Questa versione include un indice del catalogo migliorato che completa l'indicizzazione di base molto più velocemente. Un'indicizzazione più rapida consente di utilizzare più rapidamente la funzione Cerca e Ripristina.

"Scopri di più sul ripristino dei dati ONTAP dai file di backup".

Limitazioni note con NetApp Backup and Recovery per volumi ONTAP

Qui sono elencate le piattaforme, i dispositivi o le funzionalità che non funzionano o non funzionano bene con questa versione. Leggere attentamente queste limitazioni.

- NetApp Backup and Recovery può eseguire il backup Cloud Volumes ONTAP in un archivio oggetti nelle regioni AWS Cina (incluse Pechino e Ningxia); tuttavia, potrebbe essere necessario modificare manualmente prima le policy di identità e di accesso.

  Per i dettagli sulla creazione di un agente Console in AWS, fare riferimento a "Installazione di un agente Console in AWS" .

  Per ulteriori dettagli, fare riferimento al post del blog "Blog sulle funzionalità NetApp Backup and Recovery , maggio 2023" .

- NetApp Backup and Recovery non supporta le regioni Microsoft Azure Cina.

  Per i dettagli sulla creazione di un agente Console in Azure, fare riferimento a "Installazione di un agente console in Azure" .

- NetApp Backup and Recovery non supporta i backup dei volumi FlexCache .

Limitazioni di replica per i volumi ONTAP

- È possibile selezionare un solo volume FlexGroup alla volta per la replica. Sarà necessario attivare i backup separatamente per ogni volume FlexGroup .

  Non vi sono limitazioni per i volumi FlexVol : puoi selezionare tutti i volumi FlexVol nel tuo sistema e assegnare gli stessi criteri di backup.

- La seguente funzionalità è supportata in "NetApp Replication" , ma non quando si utilizza la funzionalità di replica di NetApp Backup and Recovery:
  - Non è supportato alcun tipo di configurazione a cascata in cui la replica avviene dal volume A al volume B e dal volume B al volume C. Il supporto include la replica dal volume A al volume B.
  - Non è disponibile alcun supporto per la replica dei dati da e verso FSx per i sistemi ONTAP .
  - Non è disponibile alcun supporto per la creazione di una replica una tantum di un volume.
- Quando si creano repliche da sistemi ONTAP locali, se la versione ONTAP sul sistema Cloud Volumes

ONTAP di destinazione è 9.8, 9.9 o 9.11, sono consentiti solo criteri mirror-vault.

- NetApp Backup & Recovery non supporta la conversione di un FlexVol volume con una relazione di backup cloud attiva in un volume FlexGroup mantenendo la funzionalità di backup cloud.

Limitazioni del backup su oggetto per i volumi ONTAP

- Durante il backup dei dati, NetApp Backup and Recovery non manterrà la crittografia NetApp Volume Encryption (NVE). Ciò significa che i dati crittografati sul volume NVE verranno decrittografati durante il trasferimento dei dati alla destinazione e la crittografia non verrà mantenuta.

  Per una spiegazione su questi tipi di crittografia, fare riferimento ahttps://docs.netapp.com/us-en/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html["Panoramica sulla configurazione della crittografia del volume NetApp"^] .

- Se gli snapshot di conservazione a lungo termine sono abilitati su un volume di destinazione SnapMirror utilizzando la pianificazione nella policy SnapMirror , gli snapshot vengono creati direttamente sul volume di destinazione. In questo caso, non dovresti eseguire il backup di quei volumi utilizzando NetApp Backup and Recovery perché quegli snapshot non verranno spostati nell'archiviazione degli oggetti.
- Durante il backup dei dati, NetApp Backup and Recovery non manterrà la crittografia NetApp Volume Encryption (NVE). Ciò significa che i dati crittografati sul volume NVE verranno decrittografati durante il trasferimento dei dati alla destinazione e la crittografia non verrà mantenuta.

  Per una spiegazione su questi tipi di crittografia, fare riferimento ahttps://docs.netapp.com/us-en/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html["Panoramica sulla configurazione della crittografia del volume NetApp"^] .

- Se gli snapshot di conservazione a lungo termine sono abilitati su un volume di destinazione SnapMirror utilizzando la pianificazione nella policy SnapMirror , gli snapshot vengono creati direttamente sul volume di destinazione. In questo caso, non dovresti eseguire il backup di quei volumi utilizzando NetApp Backup and Recovery perché quegli snapshot non verranno spostati nell'archiviazione degli oggetti.
- Quando si crea o si modifica un criterio di backup senza che vi siano volumi assegnati, il numero massimo di backup conservati può essere 1018. Dopo aver assegnato i volumi al criterio, è possibile modificarlo per creare fino a 4000 backup.
- Durante il backup dei volumi di protezione dei dati (DP):
  - Relazioni con le etichette SnapMirror `app_consistent` E `all_source_snapshot` non verrà eseguito il backup sul cloud.
  - Se si creano copie locali di Snapshot sul volume di destinazione SnapMirror (indipendentemente dalle etichette SnapMirror utilizzate), tali Snapshot non verranno spostati nel cloud come backup. A questo punto sarà necessario creare una policy Snapshot con le etichette desiderate sul volume DP di origine affinché NetApp Backup and Recovery ne esegua il backup.
- I backup dei volumi FlexGroup non possono essere spostati nell'archiviazione.
- I backup dei volumi FlexGroup possono utilizzare la protezione DataLock e Ransomware se il cluster esegue ONTAP 9.13.1 o versione successiva.
- Il backup del volume SVM-DR è supportato con le seguenti restrizioni:
  - I backup sono supportati solo dal dispositivo secondario ONTAP .
  - La policy Snapshot applicata al volume deve essere una delle policy riconosciute da NetApp Backup and Recovery, tra cui giornaliera, settimanale, mensile, ecc. La policy predefinita "sm_created" (utilizzata per **Mirror All Snapshots**) non viene riconosciuta e il volume DP non verrà visualizzato nell'elenco dei volumi di cui è possibile eseguire il backup.

    - Il backup e il ripristino di SVM-DR e del volume funzionano in modo completamente indipendente quando il backup viene eseguito dall'origine o dalla destinazione. L'unica limitazione è che SVM-DR non replica la relazione cloud SnapMirror . Nello scenario DR, quando l'SVM va online nella posizione secondaria, è necessario aggiornare manualmente la relazione cloud SnapMirror .
- Supporto MetroCluster :
    - Se si utilizza ONTAP 9.12.1 GA o versione successiva, il backup è supportato quando si è connessi al sistema primario. L'intera configurazione del backup viene trasferita al sistema secondario, in modo che i backup sul cloud continuino automaticamente dopo il passaggio. Non è necessario impostare il backup sul sistema secondario (anzi, non è consentito farlo).
    - Quando si utilizza ONTAP 9.12.0 e versioni precedenti, il backup è supportato solo dal sistema secondario ONTAP .
    - A partire da ONTAP 9.18.1, i backup dei volumi FlexGroup sono supportati nelle configurazioni MetroCluster.
- Il backup di volumi ad hoc tramite il pulsante **Esegui backup ora** non è supportato sui volumi di protezione dati.
- Le configurazioni SM-BC non sono supportate.
- ONTAP non supporta il fan-out delle relazioni SnapMirror da un singolo volume a più archivi di oggetti; pertanto, questa configurazione non è supportata da NetApp Backup and Recovery.
- Al momento, la modalità WORM/Compliance su un archivio oggetti è supportata su Amazon S3, Azure e StorageGRID . Questa funzionalità è nota come DataLock e deve essere gestita tramite le impostazioni NetApp Backup and Recovery , non tramite l'interfaccia del provider cloud.

Limitazioni di ripristino per i volumi ONTAP

Queste limitazioni si applicano sia ai metodi Cerca e ripristina che Sfoglia e ripristina per il ripristino di file e cartelle, a meno che non siano espressamente indicate.

- Browse & Restore può ripristinare fino a 100 file singoli alla volta.
- Search & Restore può ripristinare 1 file alla volta.
- Se si utilizza ONTAP 9.13.0 o versione successiva, Browse & Restore e Search & Restore possono ripristinare una cartella insieme a tutti i file e le sottocartelle in essa contenuti.

  Quando si utilizza una versione di ONTAP successiva alla 9.11.1 ma precedente alla 9.13.0, l'operazione di ripristino può ripristinare solo la cartella selezionata e i file in quella cartella; non vengono ripristinate le sottocartelle o i file nelle sottocartelle.

  Se si utilizza una versione di ONTAP precedente alla 9.11.1, il ripristino delle cartelle non è supportato.
- Il ripristino di directory/cartelle è supportato per i dati che risiedono nell'archiviazione solo quando il cluster esegue ONTAP 9.13.1 e versioni successive.
- Il ripristino di directory/cartelle è supportato per i dati protetti tramite DataLock solo quando il cluster esegue ONTAP 9.13.1 e versioni successive.
- Il ripristino di directory/cartelle non è attualmente supportato da repliche e/o snapshot locali.
- Il ripristino da volumi FlexGroup a volumi FlexVol o da volumi FlexVol a volumi FlexGroup non è supportato.
- Il file da ripristinare deve utilizzare la stessa lingua del volume di destinazione. Se le lingue non sono le stesse, verrà visualizzato un messaggio di errore.

- La priorità di ripristino *Alta* non è supportata durante il ripristino dei dati dall'archiviazione di Azure ai sistemi StorageGRID .
- Se si esegue il backup di un volume DP e poi si decide di interrompere la relazione SnapMirror con quel volume, non sarà possibile ripristinare i file su quel volume a meno che non si elimini anche la relazione SnapMirror o si inverta la direzione SnapMirror .
- Limitazioni del ripristino rapido:
  - La posizione di destinazione deve essere un sistema Cloud Volumes ONTAP che utilizza ONTAP 9.13.0 o versione successiva.
  - Non è supportato con i backup memorizzati in un archivio.
  - I volumi FlexGroup sono supportati solo se il sistema di origine da cui è stato creato il backup cloud eseguiva ONTAP 9.12.1 o versione successiva.
  - I volumi SnapLock sono supportati solo se il sistema di origine da cui è stato creato il backup su cloud eseguiva ONTAP 9.11.0 o versione successiva.

Limitazioni note con NetApp Backup and Recovery per carichi di lavoro Microsoft SQL Server

Qui sono elencate le piattaforme, i dispositivi o le funzionalità che non funzionano o non funzionano bene con questa versione. Leggere attentamente queste limitazioni.

Supporto del ciclo di vita dei cloni

- La clonazione da un archivio di oggetti non è supportata.
- Le operazioni di clonazione in blocco non sono supportate per i cloni su richiesta.
- La scelta dei gruppi I non è supportata.
- La scelta delle opzioni QOS (throughput massimo) non è supportata.

Solo modalità di distribuzione standard

Questa versione NetApp Backup and Recovery funziona solo in modalità di distribuzione standard, non in modalità riservata o privata.

Restrizione del nome del cluster Windows

Il nome del cluster Windows non può contenere un carattere di sottolineatura (_).

Problemi di migrazione SnapCenter

La migrazione delle risorse da SnapCenter a NetApp Backup and Recovery presenta le seguenti limitazioni.

Per i dettagli su come i criteri di SnapCenter migrano ai criteri di NetApp Backup and Recovery , vedere"Criteri in SnapCenter confrontati con quelli in NetApp Backup and Recovery" .

Limitazioni del gruppo di risorse

Se tutte le risorse in un gruppo di risorse sono protette e una di queste risorse è protetta anche all'esterno del gruppo di risorse, la migrazione da SnapCenter viene bloccata.

Soluzione alternativa: proteggere la risorsa in un gruppo di risorse o da sola, ma non in entrambi.

Risorse con più policy che utilizzano lo stesso livello di pianificazione non supportate

Non è possibile assegnare più policy che utilizzano lo stesso livello di pianificazione (ad esempio, oraria, giornaliera, settimanale, ecc.) a una risorsa. NetApp Backup and Recovery non importerà tali risorse da SnapCenter.

Soluzione alternativa: associare a una risorsa solo un criterio utilizzando lo stesso livello di pianificazione.

Le politiche orarie devono iniziare all'inizio dell'ora

Se si dispone di una policy SnapCenter che si ripete ogni ora ma non utilizza intervalli all'inizio dell'ora, NetApp Backup and Recovery non importerà la risorsa. Ad esempio, le policy con orari 1:30, 2:30, 3:30, ecc. non sono supportate, mentre sono supportate le policy con orari 1:00, 2:00, 3:00, ecc.

Soluzione alternativa: utilizzare un criterio che si ripete a intervalli di 1 ora a partire dall'inizio dell'ora.

Non sono supportate le policy giornaliere e mensili associate a una risorsa

Se una policy SnapCenter si ripete sia a intervalli giornalieri che mensili, NetApp Backup and Recovery non importerà la policy.

Ad esempio, non è possibile associare una policy giornaliera (con durata inferiore o uguale a 7 giorni o superiore a 7 giorni) a una risorsa e allo stesso tempo associare una policy mensile alla stessa risorsa.

Soluzione alternativa: utilizzare un criterio che preveda un intervallo giornaliero o mensile, ma non entrambi.

Criteri di backup su richiesta non migrati

NetApp Backup and Recovery non importa policy di backup su richiesta da SnapCenter.

Criteri di backup solo log non migrati

NetApp Backup and Recovery non importa i criteri di backup solo log da SnapCenter. Se una policy SnapCenter include backup solo di log, NetApp Backup and Recovery non importerà la risorsa.

Soluzione alternativa: utilizzare un criterio in SnapCenter che utilizzi più dei semplici backup di log.

Mappatura host

SnapCenter non dispone di cluster di archiviazione delle mappe o SVM per le risorse sugli host, mentre NetApp Backup and Recovery sì. Il cluster ONTAP o SVM locale non verrà mappato a un host nelle versioni di anteprima NetApp Backup and Recovery . Inoltre, NetApp Console non supporta le SVM.

Soluzione alternativa: prima di importare risorse da SnapCenter, creare un sistema in NetApp Backup and Recovery per tutti i sistemi di storage ONTAP locali registrati in SnapCenter locali. Quindi, importare le risorse per quel cluster da SnapCenter in NetApp Backup and Recovery.

Orari non a intervalli di 15 minuti

Se si dispone di una pianificazione di policy SnapCenter che inizia a una determinata ora e si ripete a intervalli diversi da 15 minuti, NetApp Backup and Recovery non importerà la pianificazione.

Soluzione alternativa: utilizzare SnapCenter per modificare il criterio in modo che venga ripetuto a intervalli di

15 minuti.

Supporto limitato per il software di gestione della virtualizzazione

Quando si proteggono i carichi di lavoro KVM, NetApp Backup and Recovery non supporta l'individuazione dei carichi di lavoro KVM quando è in uso un software di gestione della virtualizzazione come Apache CloudStack o Red Hat OpenShift Virtualization.

Limitazioni note con NetApp Backup and Recovery per carichi di lavoro VMware

Qui sono elencate le piattaforme, i dispositivi o le funzionalità che non funzionano o non funzionano bene con questa versione. Leggere attentamente queste limitazioni.

Le seguenti azioni non sono supportate nella versione di anteprima dei carichi di lavoro VMware in NetApp Backup and Recovery:

- Montare
- Smonta
- Allega VMDK
- Stacca VMDK
- Supporto vVol
- Supporto NVMe
- Integrazione e-mail
- Modifica la politica
- Modifica gruppo di protezione
- Supporto per il controllo degli accessi basato sui ruoli (RBAC)

Limitazioni note con NetApp Backup and Recovery per carichi di lavoro Hyper-V

Qui sono elencate le piattaforme, i dispositivi o le funzionalità che non funzionano o non funzionano bene con questa versione. Leggere attentamente queste limitazioni.

Azioni non supportate

Le seguenti azioni non sono supportate nella versione di anteprima privata dei carichi di lavoro Hyper-V in NetApp Backup and Recovery:

- Crea gruppi di risorse utilizzando VM da più host Hyper-V
- Ripristinare le VM in una posizione alternativa
- Spanning dei dischi (su più condivisioni CIFS)
- Proteggere le VM su SAN
- Non è possibile ripristinare VM o dati di VM tra sistemi con CPU di fornitori diversi (da Intel ad AMD o viceversa), indipendentemente dall'impostazione "Compatibilità processore" in Hyper-V. Questa

impostazione supporta solo la compatibilità tra generazioni diverse dello stesso fornitore (ad esempio, da Intel a Intel o da AMD ad AMD).

Nella versione del 19 gennaio 2026, non è possibile aggiornare i plugin NetApp per Hyper-V o Windows utilizzando l'opzione **Aggiorna** nel menu Azioni. In alternativa, rimuovere ciascun host Hyper-V e aggiungerlo nuovamente per aggiornare i plugin.

Limitazioni note con NetApp Backup and Recovery per carichi di lavoro KVM

Qui sono elencate le piattaforme, i dispositivi o le funzionalità che non funzionano o non funzionano bene con questa versione. Leggere attentamente queste limitazioni.

Le seguenti azioni e configurazioni non sono supportate nella versione di anteprima privata dei carichi di lavoro KVM in NetApp Backup and Recovery:

Azioni non supportate

Le seguenti azioni non sono supportate nella versione di anteprima privata:

- Clona, monta o smonta le VM
- Ripristinare le VM in una posizione alternativa
- Proteggere le VM archiviate su SAN
- Proteggere le applicazioni
- Modifica gruppi di protezione
- Creare gruppi di protezione utilizzando VM da più host KVM
- Crea backup definiti dall'utente (sono supportati solo i backup avviati dalla NetApp Console)

Configurazioni non supportate

Le seguenti configurazioni non sono supportate:

- Controllo degli accessi basato sui ruoli (RBAC)
- Dischi collegati direttamente all'host KVM
- Dischi distribuiti su più punti di montaggio o condivisioni NFS
- Formato disco RAW
- Tipi di pool di archiviazione diversi da NetFS (è supportato solo NetFS)

Note sulla risoluzione dei problemi

Quando si utilizza l'anteprima privata dei carichi di lavoro KVM con NetApp Backup and Recovery, tenere presente quanto segue:

- Per garantire che i ripristini del carico di lavoro KVM vengano completati correttamente, accertarsi che l'impostazione **Abilita snapshot coerente con la VM** sia attiva nel criterio di protezione utilizzato per i backup KVM.
- Non è possibile eseguire il backup di un pool di archiviazione con host KVM gestiti da Apache CloudStack

a meno che non si aggiungano tutti gli host gestiti a NetApp Backup and Recovery. Come soluzione alternativa, aggiungi ogni host KVM gestito da CloudStack a NetApp Backup and Recovery.

- Non è possibile eseguire il backup di una macchina virtuale arrestata che appartiene a un gruppo di protezione. Come soluzione alternativa, rimuovere la macchina virtuale arrestata dal gruppo di protezione prima di avviare il backup.

Limitazioni note con NetApp Backup e ripristino per carichi di lavoro di Oracle Database

Qui sono elencate le piattaforme, i dispositivi o le funzionalità che non funzionano o non funzionano bene con questa versione. Leggere attentamente queste limitazioni.

La seguente azione non è supportata nella versione di anteprima privata dei carichi di lavoro di Oracle Database in NetApp Backup and Recovery:

- Backup offline

Oracle Database è supportato solo come distribuzione autonoma utilizzando NFS, SAN o ASM SAN nella versione di anteprima privata dei carichi di lavoro di Oracle Database.

Iniziare

Scopri di più su NetApp Backup and Recovery

NetApp Backup and Recovery è un servizio dati che fornisce una protezione dati efficiente, sicura e conveniente per tutti i carichi di lavoro ONTAP , inclusi volumi, database, macchine virtuali e carichi di lavoro Kubernetes.

Il supporto per il backup e il ripristino è già integrato in tutti i sistemi ONTAP , quindi non sono necessari hardware, licenze software o gateway multimediali aggiuntivi. Ciò rende le operazioni di backup semplici ed economiche. NetApp Console semplifica l'implementazione di qualsiasi strategia di backup, inclusa l'intera gamma di varianti di backup 3-2-1, senza la necessità di più gestori di risorse o personale specializzato.

> La documentazione sulla protezione dei carichi di lavoro VMware, KVM, Hyper-V e Kubernetes viene fornita come anteprima tecnologica. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli, i contenuti e la tempistica dell'offerta prima della disponibilità generale.

Cosa puoi fare con NetApp Backup and Recovery

Utilizza NetApp Backup and Recovery per raggiungere i seguenti obiettivi:

- * Carichi di lavoro del volume ONTAP *:
  - Crea snapshot locali, replica su storage secondario ed esegui il backup dei volumi ONTAP dai sistemi ONTAP locali o Cloud Volumes ONTAP su storage di oggetti nel tuo account cloud pubblico o privato.
  - Crea backup incrementali permanenti a livello di blocco, archiviati su un altro cluster ONTAP e nell'archiviazione di oggetti nel cloud.
  - Utilizzare NetApp Backup and Recovery insieme a SnapCenter.
  - Fare riferimento a"Proteggere i volumi ONTAP" .
- **Carichi di lavoro di Microsoft SQL Server**:
  - Esegui il backup di istanze e database di Microsoft SQL Server da ONTAP locale, Cloud Volumes ONTAP o Amazon FSx for NetApp ONTAP.
  - Ripristinare i database di Microsoft SQL Server.
  - Clonare i database Microsoft SQL Server.
  - Utilizzare NetApp Backup and Recovery senza SnapCenter.
  - Fare riferimento a"Proteggere i carichi di lavoro di Microsoft SQL Server" .
- **Carichi di lavoro VMware (anteprima con nuova interfaccia utente senza SnapCenter Plug-in for VMware vSphere)**:
  - Proteggi le tue VM VMware e i tuoi datastore con NetApp Backup and Recovery.
  - Esegui il backup dei carichi di lavoro VMware su Amazon Web Services S3 o StorageGRID (per l'anteprima).
  - Ripristina i dati VMware dal cloud al vCenter locale.
  - È possibile ripristinare la macchina virtuale esattamente nella stessa posizione da cui è stato eseguito il backup oppure in una posizione alternativa.

    - Utilizzare NetApp Backup and Recovery senza il SnapCenter Plug-in for VMware vSphere.
    - Fare riferimento a"Proteggi i carichi di lavoro VMware" .
- **Carichi di lavoro VMware (con SnapCenter Plug-in for VMware vSphere)**:
    - Esegui il backup di VM e datastore su Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform e StorageGRID e ripristina le VM sul SnapCenter Plug-in for VMware vSphere .
    - Ripristina i dati della VM dal cloud al vCenter locale con NetApp Backup and Recovery. È possibile ripristinare la macchina virtuale esattamente nella stessa posizione da cui è stato eseguito il backup oppure in una posizione alternativa.
    - Utilizzare NetApp Backup and Recovery insieme al SnapCenter Plug-in for VMware vSphere.
    - Fare riferimento a"Proteggi i carichi di lavoro VMware" .
- **Carichi di lavoro KVM (anteprima)**:
    - Eseguire il backup e il ripristino delle macchine virtuali
    - Eseguire il backup dei pool di archiviazione KVM
    - Utilizzare gruppi di protezione per gestire le attività di backup
    - Fare riferimento a"Proteggere i carichi di lavoro KVM" .
- **Carichi di lavoro Hyper-V (anteprima)**:
    - Eseguire il backup e il ripristino delle macchine virtuali
    - Utilizzare gruppi di protezione per gestire le attività di backup
    - Fare riferimento a"Proteggere i carichi di lavoro Hyper-V" .
- **Carichi di lavoro Oracle Database (anteprima)**:
    - Eseguire il backup e il ripristino di database e registri
    - Utilizzare gruppi di protezione per gestire le attività di backup
    - Creare policy per gestire i backup del database e del registro
    - Proteggere un database con un'architettura di backup 3-2-1
    - Configurare la conservazione del backup
    - Montare e smontare i backup ARCHIVELOG
    - Fare riferimento a "Proteggi i carichi di lavoro Oracle Database".
- **Carichi di lavoro Kubernetes (anteprima)**:
    - Gestisci e proteggi le tue applicazioni e risorse Kubernetes, tutto in un unico posto.
    - Utilizza criteri di protezione per strutturare i tuoi backup incrementali.
    - Ripristinare applicazioni e risorse negli stessi cluster e namespace o in cluster e namespace diversi.
    - Utilizzare NetApp Backup and Recovery senza SnapCenter.
    - Fare riferimento a"Proteggere i carichi di lavoro di Kubernetes" .

Vantaggi dell'utilizzo di NetApp Backup and Recovery

NetApp Backup and Recovery offre i seguenti vantaggi:

- **Efficiente**: NetApp Backup and Recovery esegue una replica incrementale e continua a livello di blocco, riducendo significativamente la quantità di dati replicati e archiviati. Ciò aiuta a ridurre al minimo il traffico di rete e i costi di archiviazione.

- **Sicuro**: NetApp Backup and Recovery crittografa i dati in transito e inattivi e utilizza protocolli di comunicazione sicuri per proteggere i tuoi dati.
- **Conveniente**: NetApp Backup and Recovery utilizza i livelli di storage più economici disponibili nel tuo account cloud, il che aiuta a ridurre i costi.
- **Automatizzato**: NetApp Backup and Recovery genera automaticamente backup in base a una pianificazione predefinita, il che contribuisce a garantire la protezione dei dati.
- **Flessibile**: NetApp Backup and Recovery consente di ripristinare i dati sullo stesso sistema o su un sistema diverso, garantendo flessibilità nel recupero dei dati.

Costo

NetApp non addebita alcun costo per l'utilizzo della versione di prova. Tuttavia, sei responsabile dei costi associati alle risorse cloud che utilizzi, come ad esempio i costi di archiviazione e di trasferimento dati.

Esistono due tipi di costi associati all'utilizzo della funzionalità di backup su oggetto di NetApp Backup and Recovery con sistemi ONTAP :

- Costi delle risorse
- Spese di servizio

Non vi è alcun costo per la creazione di snapshot o volumi replicati, a parte lo spazio su disco necessario per archiviare gli snapshot e i volumi replicati.

Costi delle risorse

I costi delle risorse vengono pagati al provider cloud per la capacità di archiviazione degli oggetti e per la scrittura e la lettura dei file di backup sul cloud.

- Per il backup su storage di oggetti, paghi al tuo provider cloud i costi di storage di oggetti.

  Poiché NetApp Backup and Recovery preserva l'efficienza di archiviazione del volume di origine, si pagano al provider cloud i costi di archiviazione degli oggetti per i dati *dopo* le efficienze ONTAP (per la quantità minore di dati dopo l'applicazione della deduplicazione e della compressione).

- Per ripristinare i dati tramite Search & Restore, alcune risorse vengono fornite dal tuo provider cloud e vi è un costo per TiB associato alla quantità di dati scansionati dalle tue richieste di ricerca. (Queste risorse non sono necessarie per Sfoglia e ripristina.)
  - In AWS, "Amazzone Atena" E "AWS Glue" le risorse vengono distribuite in un nuovo bucket S3.
  - In Azure, un "Area di lavoro di Azure Synapse" E "Archiviazione di Azure Data Lake" sono predisposti nel tuo account di archiviazione per archiviare e analizzare i tuoi dati.
  - In Google, viene distribuito un nuovo bucket e il "Servizi Google Cloud BigQuery" sono forniti a livello di account/progetto.
- Se si prevede di ripristinare i dati del volume da un file di backup che è stato spostato in un archivio di oggetti, il provider cloud applicherà una tariffa aggiuntiva per il recupero per GiB e una tariffa per richiesta.
- Se intendi analizzare un file di backup alla ricerca di ransomware durante il processo di ripristino dei dati del volume (se hai abilitato DataLock e Ransomware Resilience per i tuoi backup cloud), dovrai sostenere anche costi di uscita aggiuntivi dal tuo provider cloud.

Spese di servizio

Per i carichi di lavoro dei volumi ONTAP , vengono addebitati solo i volumi protetti nell'archiviazione degli

oggetti. I costi si basano sulla capacità logica utilizzata dei volumi ONTAP di origine prima dell'applicazione delle efficienze, nota anche come Front-End Terabyte (FETB).

Per i carichi di lavoro Kubernetes, l'addebito avviene in base alle dimensioni combinate di tutti i volumi persistenti.

Per tutti gli altri carichi di lavoro, ti verranno addebitate le risorse protette su almeno una destinazione di archiviazione secondaria o di oggetti. I costi vengono calcolati in base alla dimensione logica del carico di lavoro di origine. Per i database, questo significa la dimensione del database; per le VM, la dimensione della VM.

Esistono tre modi per pagare Backup e Ripristino:

- La prima opzione è quella di abbonarsi al tuo provider cloud, che ti consente di pagare mensilmente.
- La seconda opzione è quella di acquistare un contratto annuale.
- La terza opzione è quella di acquistare le licenze direttamente da NetApp. Fare riferimento al Licenza sezione per i dettagli.

Licenza

NetApp Backup and Recovery offre una prova gratuita, che consente di utilizzarlo senza una chiave di licenza per un periodo di tempo limitato.

Una licenza di backup è richiesta solo per le operazioni di backup e ripristino che coinvolgono l'archiviazione di oggetti. La creazione di snapshot e volumi replicati non richiede una licenza.

Puoi scegliere tra tre opzioni di licenza:

- **Bring Your Own License (BYOL)**: acquista da NetApp una licenza a termine (1, 2 o 3 anni) e basata sulla capacità (in incrementi di 1 TiB). Per attivare, immettere il numero di serie fornito nella NetApp Console . La licenza copre tutti i sistemi sorgente della tua organizzazione. Il rinnovo è necessario quando si raggiunge il termine o il limite di capienza.
- **Pay As You Go (PAYGO)**: abbonati tramite il marketplace del tuo provider cloud e paga per GiB di dati sottoposti a backup, con fatturazione mensile. Non è richiesto alcun pagamento anticipato. Al momento della prima registrazione è disponibile una prova gratuita di 30 giorni. Per maggiori informazioni, fare riferimento a "utilizzare un abbonamento NetApp Backup and Recovery PAYGO" .
- **Contratto annuale**: disponibile tramite i marketplace AWS e Azure per 1, 2 o 3 anni. Sono disponibili due contratti annuali:
  - **Cloud Backup**: esegue il backup dei dati Cloud Volumes ONTAP e ONTAP in locale.
  - **CVO Professional**: Bundle Cloud Volumes ONTAP e NetApp Backup and Recovery, con backup illimitati per i volumi Cloud Volumes ONTAP (la capacità di backup non viene conteggiata nella licenza).
    - Con il piano CVO Professional sono previsti due tipi di addebiti:
      - **Costi delle risorse**: in base all'utilizzo dello spazio di archiviazione. Per maggiori informazioni, fare riferimento a "licenze per Cloud Volumes ONTAP" .
      - **Costi del servizio**: Costi per NetApp Backup and Recovery. Tuttavia, se il volume di origine si trova in un sistema di archiviazione che utilizza il piano CVO Professional, NetApp Backup and Recovery viene fornito gratuitamente.

Quando utilizzi Google Cloud Platform, richiedi un'offerta privata da NetApp e seleziona il tuo piano durante l'attivazione nel Google Cloud Marketplace.

"Scopri come impostare le licenze".

Carichi di lavoro, sistemi e destinazioni di backup supportati

Carichi di lavoro supportati

NetApp Backup and Recovery protegge i seguenti tipi di carichi di lavoro:

- Volumi ONTAP
- Istanze e database di Microsoft SQL Server archiviati su disco fisico e VMware Virtual Machine Disk (VMDK) su VMFS o NFS
- VM e datastore VMware
- Carichi di lavoro KVM (anteprima)
- Carichi di lavoro Hyper-V (anteprima)
- Carichi di lavoro di Oracle Database (anteprima)
- Carichi di lavoro Kubernetes (anteprima)

Sistemi supportati

- SAN ONTAP on-premise (protocollo iSCSI) e NAS (utilizzando protocolli NFS e CIFS) con ONTAP versione 9.8 o successiva
- Cloud Volumes ONTAP 9.8 o versione successiva per AWS (utilizzando SAN e NAS)
- Cloud Volumes ONTAP 9.8 o versione successiva per Google Cloud Platform (utilizzando i protocolli NFS e CIFS)
- Cloud Volumes ONTAP 9.8 o versione successiva per Microsoft Azure (utilizzando SAN e NAS)
- Amazon FSx for NetApp ONTAP (solo carichi di lavoro Microsoft SQL Server)

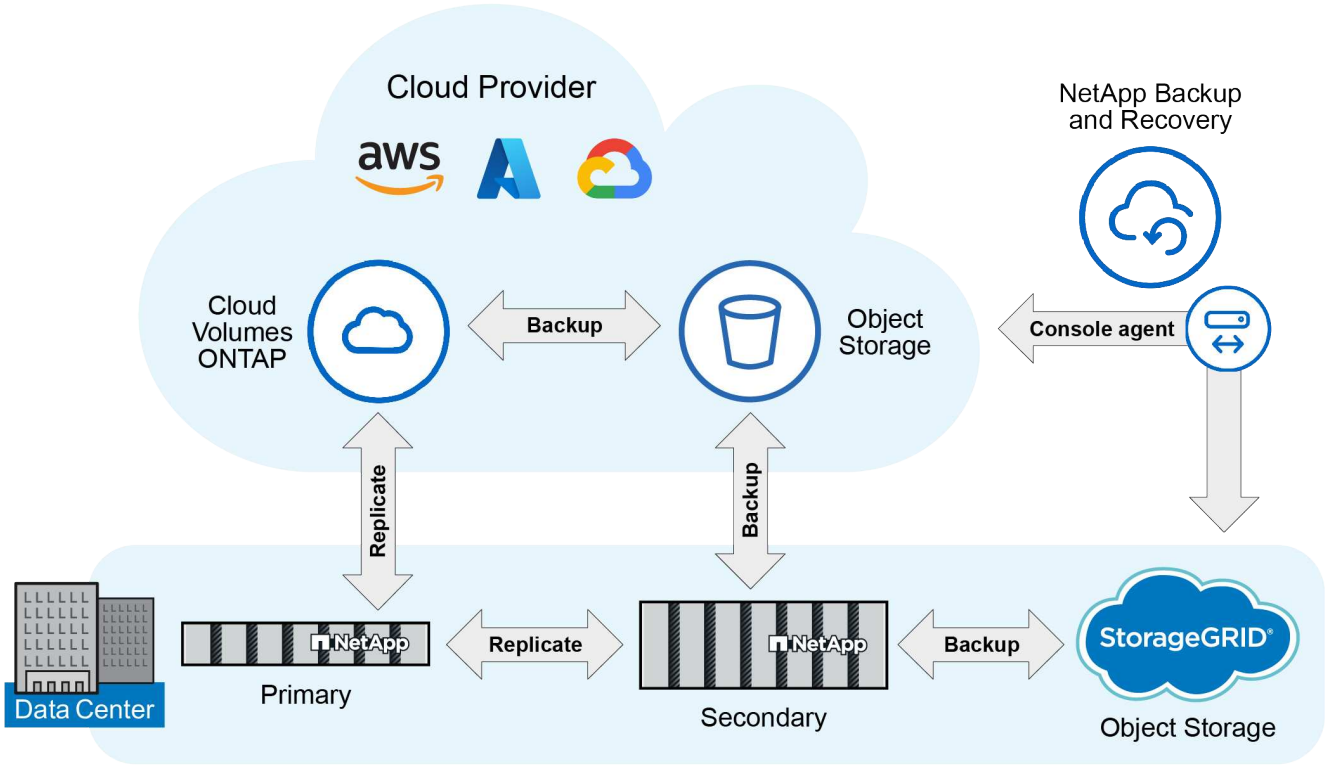
Destinazioni di backup supportate

- Servizi Web Amazon (AWS) S3
- Google Cloud Storage
- Microsoft Azure Blob (non disponibile per i carichi di lavoro VMware in anteprima)
- StorageGRID
- ONTAP S3 (non disponibile per carichi di lavoro VMware in anteprima)

Come funziona NetApp Backup and Recovery

Quando si abilita NetApp Backup and Recovery, il servizio esegue un backup completo dei dati. Dopo il backup iniziale, tutti i backup aggiuntivi sono incrementali. In questo modo il traffico di rete viene ridotto al minimo.

L'immagine seguente mostra la relazione tra i componenti.



È supportato anche lo storage primario verso l'archiviazione di oggetti, non solo quello secondario verso l'archiviazione di oggetti.

Dove risiedono i backup nelle posizioni dell'archivio oggetti

Le copie di backup vengono archiviate in un archivio oggetti creato dalla NetApp Console nel tuo account cloud. Esiste un archivio oggetti per cluster o sistema e la Console assegna a tale archivio il seguente nome: `netapp-backup-clusteruuid` . Assicurarsi di non eliminare questo archivio oggetti.

- In AWS, la NetApp Console consente di "Funzionalità di blocco dell'accesso pubblico di Amazon S3" sul bucket S3.
- In Azure, la NetApp Console utilizza un gruppo di risorse nuovo o esistente con un account di archiviazione per il contenitore BLOB. la console "blocca l'accesso pubblico ai dati del tuo blob" per impostazione predefinita.
- In StorageGRID, la console utilizza un account di archiviazione esistente per il bucket di archiviazione degli oggetti.
- In ONTAP S3, la console utilizza un account utente esistente per il bucket S3.

Le copie di backup sono associate alla tua organizzazione NetApp Console

Le copie di backup sono associate all'organizzazione NetApp Console in cui risiede l'agente Console. "Scopri di più su NetApp Console Identity e accesso" .

Se nella stessa organizzazione NetApp Console sono presenti più agenti Console, ogni agente Console visualizza lo stesso elenco di backup.

Termini che potrebbero aiutarti con NetApp Backup and Recovery

Potrebbe essere utile comprendere un po' di terminologia relativa alla protezione.

- **Protezione**: la protezione in NetApp Backup and Recovery significa garantire che gli snapshot e i backup immutabili vengano eseguiti regolarmente su un dominio di sicurezza diverso utilizzando policy di protezione.
- **Carico di lavoro**: un carico di lavoro in NetApp Backup and Recovery può includere volumi ONTAP , istanze e database di Microsoft SQL Server, VM e datastore VMware o cluster e applicazioni Kubernetes.

Prerequisiti NetApp Backup and Recovery

Inizia a utilizzare NetApp Backup and Recovery verificando la prontezza del tuo ambiente operativo, dell'agente NetApp Console e dell'account NetApp Console . Per utilizzare NetApp Backup and Recovery, sono necessari i seguenti prerequisiti.

Prerequisito per ONTAP 9.8 e versioni successive

È necessario abilitare una licenza ONTAP One sull'istanza ONTAP locale.

Prerequisiti per i backup su storage di oggetti

Per utilizzare l'archiviazione di oggetti come destinazione di backup, è necessario un account con AWS S3, Microsoft Azure Blob, StorageGRID o ONTAP e le autorizzazioni di accesso appropriate configurate.

- "Proteggi i dati del tuo volume ONTAP"

Requisiti per la protezione dei carichi di lavoro di Microsoft SQL Server

Per utilizzare NetApp Backup and Recovery per i carichi di lavoro di Microsoft SQL Server, sono necessari i seguenti prerequisiti relativi a sistema host, spazio e dimensionamento.

Articolo	Requisiti
Sistemi operativi	Microsoft Windows Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .
Versioni di Microsoft SQL Server	Le versioni 2012 e successive sono supportate per VMware Virtual Machine File System (VMFS) e VMware Virtual Machine Disk (VMDK) NFS.
Versione di SnapCenter Server	Per importare i dati esistenti da SnapCenter in NetApp Backup and Recovery è necessario SnapCenter Server versione 5.0 o successiva. Se hai già SnapCenter, verifica innanzitutto di aver soddisfatto i prerequisiti prima di importare da SnapCenter. Vedere"Prerequisiti per l'importazione di risorse da SnapCenter" .

Articolo	Requisiti
RAM minima per il plug-in sull'host SQL Server	1 GB
Spazio minimo di installazione e di registro per il plug-in sull'host SQL Server	5 GB Assegnare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di backup eseguiti e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente, i log per le operazioni non verranno creati.
Pacchetti software richiesti	• ASP.NET Core Runtime 8.0.12 Hosting Bundle (e tutte le patch 8.0.x successive) • PowerShell 7.4.2 Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .

Requisiti per la protezione dei carichi di lavoro VMware

Per individuare e proteggere i carichi di lavoro VMware sono necessari requisiti specifici.

Supporto software

- Sono supportati i datastore NFS e VMFS.
- Versioni NFS supportate: NFS 3 e NFS 4.1
- Versioni di VMware ESXi Server supportate: 7.0U1 e successive
- Versioni di VMware vCenter vSphere supportate: 7.0U1 e successive
- Indirizzi IP: IPv4 e IPv6
- VMware TLS: 1.2, 1.3
- Archiviazione connessa supportata: ONTAP 9.13 o versioni successive

Requisiti di connessione e porta per la protezione dei carichi di lavoro VMware

Tipo di porto	Porta preconfigurata
Porta del server VMware ESXi	443 (HTTPS), bidirezionale. La funzionalità di ripristino dei file guest utilizza questa porta.
Cluster di archiviazione o porta VM di archiviazione	443 (HTTPS), bidirezionale. 80 (HTTP), bidirezionale. Questa porta viene utilizzata per la comunicazione tra l'appliance virtuale e la VM di archiviazione o il cluster contenente la VM di archiviazione.

Requisiti di controllo degli accessi basato sui ruoli (RBAC) per la protezione dei carichi di lavoro VMware

L'account amministratore vCenter deve disporre dei privilegi vCenter richiesti.

Per un elenco dei privilegi vCenter necessari, vedere "SnapCenter Plug-in for VMware vSphere Privilegi vCenter necessari" .

Requisiti per la protezione dei carichi di lavoro KVM

Per individuare e proteggere le macchine virtuali KVM sono necessari requisiti specifici.

- Una moderna distribuzione Linux che esegue la versione del kernel 5.14.0-503.22.1.el9_5.x86_64 (a lungo termine) o successiva
- Gli host KVM e le VM devono essere gestiti da una piattaforma di gestione. NetApp Backup and Recovery supporta le seguenti piattaforme di gestione:
  - Apache CloudStack 4.22.0.0
- Assicurarsi che il traffico di rete in entrata sulla porta 22 sia consentito dall'agente della console all'host KVM
- QEMU Guest Agent versione 9.0.0 o successiva
- libvirt versione 10.5.0 o successiva

Per garantire che i ripristini del carico di lavoro KVM vengano completati correttamente, accertarsi che l'impostazione **Abilita snapshot coerente con la VM** sia attiva nel criterio di protezione utilizzato per i backup KVM.

Per abilitare la protezione delle VM KVM amministrate da utenti non root, attenersi alla seguente procedura:

1. Montare il volume come tipo NFS3 per evitare l'uso del `nobody` utente e gruppo.
2. Utilizzare il seguente comando per aggiungere un utente non root al `qemu` gruppo pur preservando i loro gruppi esistenti:

```
usermod -aG qemu <non-root-user>
```

3. Utilizzare il seguente comando per concedere la proprietà del percorso di montaggio al `qemu` utente e gruppo e modifica i permessi per il percorso di montaggio:

```
chown -R qemu:qemu <kvm_vm_mount_path> & chmod 771
<kvm_vm_mount_path>
```

4. Eliminare la directory NetApp_SnapCenter_Backups esistente, se presente.

Requisiti per la protezione dei carichi di lavoro Oracle Database

Assicurati che il tuo ambiente soddisfi requisiti specifici per scoprire e proteggere le risorse Oracle.

- Database Oracle:
  - Oracle 19C e 21C sono supportati in una distribuzione autonoma.
  - Oracle Database deve essere distribuito nello storage NetApp ONTAP primario o secondario.

    - Supporto del sistema operativo host: Red Hat Enterprise Linux 8 e 9
- Supporto per l'archiviazione di oggetti:
    - Archiviazione oggetti di Azure
    - Amazon AWS
    - NetApp StorageGRID
    - ONTAP S3

Requisiti per la protezione delle applicazioni Kubernetes

Per scoprire le risorse di Kubernetes e proteggere le applicazioni Kubernetes, sono necessari requisiti specifici.

Per i requisiti NetApp Console , fare riferimento aNella NetApp Console .

- Un sistema ONTAP primario (ONTAP 9.16.1 o successivo)
- Un cluster Kubernetes: le distribuzioni e le versioni di Kubernetes supportate includono:
    - Anthos On-Prem (VMware) e Anthos su bare metal 1.16
    - Kubernetes 1.27 - 1.33
    - OpenShift 4.10 - 4.18
    - Motore Kubernetes Rancher 2 (RKE2) v1.26.7+rke2r1, v1.28.5+rke2r1
    - Suse Rancher
- NetApp Trident 24.10 o successivo
- NetApp Trident Protect 25.07 o versioni successive (installato durante la scoperta del carico di lavoro Kubernetes)
- NetApp Trident Protect Connector 25.07 o versioni successive (installato durante la scoperta del carico di lavoro Kubernetes)
    - Assicurarsi che la porta TCP 443 non sia filtrata in direzione outbound tra il cluster Kubernetes, il Trident Protect Connector e il Trident Protect proxy.

Requisiti per la protezione dei carichi di lavoro Hyper-V

Assicurati che la tua istanza Hyper-V soddisfi requisiti specifici per individuare e proteggere le macchine virtuali.

- Requisiti software per l'host Hyper-V Windows Server:
    - Edizioni Microsoft Hyper-V 2019, 2022 e 2025
    - ASP.NET Core Runtime 8.0.12 Hosting Bundle (e tutte le patch 8.0.x successive)
    - PowerShell 7.4.2 o versione successiva
    - Se gli utenti che non fanno parte di un dominio amministratore proteggeranno le VM Hyper-V, assicurarsi che l'utente disponga delle seguenti autorizzazioni:
        - Assicurarsi che l'utente sia membro del gruppo degli amministratori locali.
        - Assicurarsi che l'utente faccia parte della policy di sicurezza locale "Accedi come servizio".
    - Assicurarsi che il traffico HTTPS bidirezionale sia consentito per le seguenti porte nelle impostazioni di Windows Firewall:

        - 8144 (Plugin NetApp per Hyper-V)
        - 8145 (Plugin NetApp per Windows)
- Requisiti hardware per l'host Hyper-V:
    - Sono supportati host autonomi e in cluster FCI
    - Almeno 1 GB di RAM per il plug-in NetApp Hyper-V sull'host Hyper-V
    - Spazio minimo di installazione e registro di 5 GB per il plug-in sull'host Hyper-V

> Assicurarsi di allocare spazio su disco sufficiente sull'host Hyper-V per la cartella dei registri e monitorarne regolarmente l'utilizzo. Lo spazio necessario dipende dalla frequenza con cui si verificano i backup e le operazioni di protezione dei dati. Se lo spazio non è sufficiente, i registri non verranno generati.

- Requisiti di configurazione NetApp ONTAP :
    - Un sistema ONTAP primario (ONTAP 9.14.1 o successivo)
    - Per le distribuzioni Hyper-V che utilizzano condivisioni CIFS per archiviare i dati delle macchine virtuali, assicurarsi che la proprietà di condivisione della disponibilità continua sia abilitata sul sistema ONTAP . Fare riferimento al "Documentazione ONTAP" per istruzioni.

Nella NetApp Console

Assicurarsi che NetApp Console soddisfi i seguenti requisiti.

- Un utente della console deve disporre del ruolo e dei privilegi necessari per eseguire operazioni sui carichi di lavoro Microsoft SQL Server e Kubernetes. Per scoprire le risorse, è necessario disporre del ruolo di Super amministratore di NetApp Backup and Recovery . Vedere"Accesso basato sui ruoli NetApp Backup and Recovery alle funzionalità" per i dettagli sui ruoli e le autorizzazioni necessari per eseguire operazioni in NetApp Backup and Recovery.
- Un'organizzazione Console con almeno un agente Console attivo che si connette ai cluster ONTAP locali o a Cloud Volumes ONTAP.
- Almeno un sistema Console con un cluster NetApp ONTAP on-premise o Cloud Volumes ONTAP .
- Un agente della console

  Fare riferimento a "Scopri come configurare un agente Console" E "requisiti standard NetApp Console" .

    - La versione di anteprima richiede il sistema operativo Ubuntu 22.04 LTS per l'agente Console.

Configurare la NetApp Console

Il passaggio successivo consiste nell'impostare la console e NetApp Backup and Recovery.

Revisione "requisiti standard NetApp Console" .

Creare un agente Console

Dovresti contattare il tuo team di prodotto NetApp per provare Backup e ripristino. Quindi, quando si utilizza l'agente Console, questo includerà le funzionalità appropriate per il servizio.

Per creare un agente Console nella NetApp Console prima di utilizzare il servizio, fare riferimento alla documentazione della Console che descrive "come creare un agente Console" .

Dove installare l'agente Console

Per completare un'operazione di ripristino, l'agente Console può essere installato nei seguenti percorsi:

- Per Amazon S3, l'agente della console può essere distribuito in sede.
- Per Azure Blob, l'agente Console può essere distribuito in locale.
- Per StorageGRID, l'agente Console deve essere distribuito presso la tua sede, con o senza accesso a Internet.
- Per ONTAP S3, l'agente della console può essere distribuito presso la tua sede (con o senza accesso a Internet) o in un ambiente di provider cloud

I riferimenti ai "sistemi ONTAP locali" includono i sistemi FAS e AFF .

Impostare la licenza per NetApp Backup and Recovery

Puoi ottenere la licenza NetApp Backup and Recovery acquistando un abbonamento annuale o pay-as-you-go (PAYGO) a * NetApp Intelligent Services* dal tuo provider cloud oppure acquistando una licenza bring-your-own (BYOL) da NetApp. Per attivare NetApp Backup and Recovery su un sistema, creare backup dei dati di produzione e ripristinare i dati di backup su un sistema di produzione è necessaria una licenza valida.

Alcune note prima di proseguire nella lettura:

- Se hai già sottoscritto un abbonamento pay-as-you-go (PAYGO) nel marketplace del tuo provider cloud per un sistema Cloud Volumes ONTAP , sarai automaticamente abbonato anche a NetApp Backup and Recovery . Non sarà necessario abbonarsi nuovamente.
- La licenza BYOL (Bring Your Own License) NetApp Backup and Recovery è una licenza mobile che puoi utilizzare su tutti i sistemi associati alla tua organizzazione o al tuo account NetApp Console . Pertanto, se si dispone di una capacità di backup sufficiente da una licenza BYOL esistente, non sarà necessario acquistare un'altra licenza BYOL.
- Se si utilizza una licenza BYOL, si consiglia di sottoscrivere anche un abbonamento PAYGO. Se esegui il backup di più dati di quelli consentiti dalla tua licenza BYOL o se scade il termine della tua licenza, il backup continua tramite l'abbonamento a consumo, senza alcuna interruzione del servizio.
- Quando si esegue il backup dei dati ONTAP on-premise su StorageGRID, è necessaria una licenza BYOL, ma non vi sono costi per lo spazio di archiviazione del provider cloud.

"Scopri di più sui costi associati all'utilizzo di NetApp Backup and Recovery."

Prova gratuita di 30 giorni

È disponibile una prova gratuita di 30 giorni NetApp Backup and Recovery se sottoscrivi un abbonamento pay-as-you-go nel marketplace del tuo provider cloud a * NetApp Intelligent Services*. La prova gratuita inizia nel momento in cui ti iscrivi all'elenco del marketplace. Tieni presente che se paghi l'abbonamento al marketplace quando distribuisci un sistema Cloud Volumes ONTAP e poi avvii la prova gratuita NetApp Backup and Recovery 10 giorni dopo, avrai 20 giorni rimanenti per utilizzare la prova gratuita.

Al termine del periodo di prova gratuito, passerai automaticamente all'abbonamento PAYGO senza interruzioni. Se decidi di non continuare a utilizzare NetApp Backup and Recovery,"annullare la registrazione NetApp Backup and Recovery dal sistema" prima della fine del periodo di prova e non ti verrà addebitato alcun costo.

Termina la prova gratuita

Se desideri continuare a utilizzare NetApp Backup and Recovery dopo la scadenza del periodo di prova gratuito, devi sottoscrivere un abbonamento a pagamento. Puoi farlo dall'interfaccia della NetApp Console andando alla sezione fatturazione e selezionando un piano di abbonamento adatto alle tue esigenze. Se non desideri continuare a utilizzare NetApp Backup and Recovery, puoi interrompere la prova gratuita.

Se termini il periodo di prova gratuito senza sottoscrivere un piano a pagamento, i tuoi dati verranno automaticamente eliminati 60 giorni dopo la fine del periodo di prova gratuito. Facoltativamente, puoi fare in modo che il sistema elimini immediatamente i tuoi dati.

Passi

1. Dalla pagina di destinazione NetApp Backup and Recovery , seleziona **Visualizza prova gratuita**.
2. Seleziona **Termina prova gratuita**.
3. Seleziona **Elimina i dati subito dopo aver terminato la prova gratuita** per eliminare immediatamente i tuoi dati.
4. Digitare **fine prova** nella casella.
5. Selezionare **Fine** per confermare.

Utilizzare un abbonamento NetApp Backup and Recovery PAYGO

Con il pagamento in base al consumo, pagherai al tuo provider cloud i costi di archiviazione degli oggetti e i costi di licenza del backup NetApp su base oraria in un unico abbonamento. Dovresti abbonarti a * NetApp Intelligent Services* nel Marketplace anche se hai una prova gratuita o se porti la tua licenza (BYOL):

- L'abbonamento garantisce che non vi saranno interruzioni del servizio al termine del periodo di prova gratuito. Al termine del periodo di prova, ti verrà addebitato un costo orario in base alla quantità di dati sottoposti a backup.
- Se esegui il backup di più dati di quelli consentiti dalla tua licenza BYOL, le operazioni di backup e ripristino dei dati continueranno tramite l'abbonamento a consumo. Ad esempio, se si dispone di una licenza BYOL da 10 TiB, tutta la capacità oltre i 10 TiB verrà addebitata tramite l'abbonamento PAYGO.

Non ti verrà addebitato alcun costo sul tuo abbonamento a consumo durante il periodo di prova gratuito o se non hai superato la durata della tua licenza BYOL.

Esistono alcuni piani PAYGO per NetApp Backup and Recovery:

- Un pacchetto "Cloud Backup" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP locali.
- Un pacchetto "CVO Professional" che consente di raggruppare Cloud Volumes ONTAP e NetApp Backup and Recovery. Ciò include backup illimitati per il sistema Cloud Volumes ONTAP utilizzando la licenza (la capacità di backup non viene conteggiata nella capacità concessa in licenza). Questa opzione non consente di eseguire il backup dei dati ONTAP locali.

  Si noti che questa opzione richiede anche un abbonamento PAYGO per backup e ripristino, ma non verranno addebitati costi per i sistemi Cloud Volumes ONTAP idonei.

"Scopri di più su questi pacchetti di licenze basati sulla capacità".

Utilizza questi link per abbonarti a NetApp Backup and Recovery dal marketplace del tuo provider cloud:

- AWS: "Per i dettagli sui prezzi, vai all'offerta Marketplace per NetApp Intelligent Services" .
- Azzurro: "Per i dettagli sui prezzi, vai all'offerta Marketplace per NetApp Intelligent Services" .
- Google Cloud: "Per i dettagli sui prezzi, vai all'offerta Marketplace per NetApp Intelligent Services" .

Utilizzare un contratto annuale

Paga annualmente NetApp Backup and Recovery acquistando un contratto annuale. Sono disponibili con durata di 1, 2 o 3 anni.

Se hai un contratto annuale da un marketplace, tutto il consumo NetApp Backup and Recovery verrà addebitato su quel contratto. Non è possibile combinare un contratto annuale di mercato con un contratto BYOL.

Quando si utilizza AWS, sono disponibili due contratti annuali da "Pagina AWS Marketplace" per i sistemi Cloud Volumes ONTAP e ONTAP on-premise:

- Un piano "Cloud Backup" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP locali.

  Se vuoi utilizzare questa opzione, configura il tuo abbonamento dalla pagina Marketplace e poi "associa l'abbonamento alle tue credenziali AWS" . Tieni presente che dovrai pagare anche i tuoi sistemi Cloud Volumes ONTAP utilizzando questo abbonamento contrattuale annuale, poiché puoi assegnare un solo abbonamento attivo alle tue credenziali AWS nella Console.

- Un piano "CVO Professional" che consente di raggruppare Cloud Volumes ONTAP e NetApp Backup and Recovery. Ciò include backup illimitati per il sistema Cloud Volumes ONTAP utilizzando la licenza (la capacità di backup non viene conteggiata nella capacità concessa in licenza). Questa opzione non consente di eseguire il backup dei dati ONTAP locali.

  Vedi il "Argomento sulla licenza Cloud Volumes ONTAP" per saperne di più su questa opzione di licenza.

  Se desideri utilizzare questa opzione, puoi impostare il contratto annuale quando crei un sistema Cloud Volumes ONTAP e la Console ti chiederà di iscriverti ad AWS Marketplace.

Quando si utilizza Azure, sono disponibili due contratti annuali da "Pagina di Azure Marketplace" per i sistemi Cloud Volumes ONTAP e ONTAP on-premise:

- Un piano "Cloud Backup" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP locali.

  Se vuoi utilizzare questa opzione, configura il tuo abbonamento dalla pagina Marketplace e poi "associare la sottoscrizione alle credenziali di Azure" . Tieni presente che dovrai pagare anche i tuoi sistemi Cloud Volumes ONTAP utilizzando questo abbonamento contrattuale annuale, poiché puoi assegnare un solo abbonamento attivo alle tue credenziali Azure nella Console.

- Un piano "CVO Professional" che consente di raggruppare Cloud Volumes ONTAP e NetApp Backup and Recovery. Ciò include backup illimitati per il sistema Cloud Volumes ONTAP utilizzando la licenza (la capacità di backup non viene conteggiata nella capacità concessa in licenza). Questa opzione non consente di eseguire il backup dei dati ONTAP locali.

  Vedi il "Argomento sulla licenza Cloud Volumes ONTAP" per saperne di più su questa opzione di licenza.

  Se si desidera utilizzare questa opzione, è possibile impostare il contratto annuale quando si crea un sistema Cloud Volumes ONTAP e la Console richiede di sottoscrivere l'abbonamento ad Azure

Marketplace.

Se utilizzi GCP, contatta il tuo rappresentante commerciale NetApp per acquistare un contratto annuale. Il contratto è disponibile come offerta privata su Google Cloud Marketplace.

Dopo che NetApp avrà condiviso con te l'offerta privata, potrai selezionare il piano annuale quando ti iscrivi da Google Cloud Marketplace durante l'attivazione NetApp Backup and Recovery .

Utilizzare una licenza BYOL NetApp Backup and Recovery

Le licenze Bring-your-own di NetApp sono disponibili con durata di 1, 2 o 3 anni. Si paga solo per i dati che si proteggono, calcolati in base alla capacità logica utilizzata (prima di qualsiasi efficienza) dei volumi ONTAP di origine sottoposti a backup. Questa capacità è nota anche come Front-End Terabyte (FETB).

La licenza BYOL NetApp Backup and Recovery è una licenza mobile in cui la capacità totale è condivisa tra tutti i sistemi associati all'organizzazione o all'account NetApp Console . Per i sistemi ONTAP , è possibile ottenere una stima approssimativa della capacità necessaria eseguendo il comando CLI `volume show -fields logical-used-by-afs` per i volumi di cui si intende eseguire il backup.

Se non si dispone di una licenza BYOL NetApp Backup and Recovery , fare clic sull'icona della chat in basso a destra della Console per acquistarne una.

Facoltativamente, se disponi di una licenza basata su nodi non assegnata per Cloud Volumes ONTAP che non utilizzerai, puoi convertirla in una licenza NetApp Backup and Recovery con lo stesso equivalente in dollari e la stessa data di scadenza. "Vai qui per i dettagli" .

Per gestire le licenze BYOL è possibile utilizzare la NetApp Console . È possibile aggiungere nuove licenze, aggiornare quelle esistenti e visualizzare lo stato delle licenze dalla Console.

"Scopri come aggiungere licenze".

Superamento della capacità della licenza

Il superamento della capacità concessa dalla licenza attiva le tariffe PAYGO; senza un abbonamento PAYGO, non è possibile creare nuovi backup, anche se i backup esistenti rimangono ripristinabili senza garanzia di servizio. Assicurati di rinnovare la licenza prima che scada; una licenza scaduta impedisce la creazione di nuovi backup e interrompe il servizio.

Impostare i certificati di sicurezza per StorageGRID e ONTAP in NetApp Backup and Recovery

Creare un certificato di sicurezza per abilitare la comunicazione tra NetApp Backup and Recovery e StorageGRID o ONTAP.

Creare un certificato di sicurezza per StorageGRID

Se la comunicazione tra i contenitori NetApp Backup and Recovery e StorageGRID deve verificare il certificato StorageGRID , completare i seguenti passaggi.

Il certificato generato deve avere CN e Subject Alternative Name come nome fornito in NetApp Backup and Recovery al momento dell'attivazione del backup.

Passi

1. Per creare il certificato StorageGRID , seguire i passaggi indicati nella documentazione di StorageGRID .

   "Informazioni StorageGRID sulla configurazione dei certificati"

2. Aggiorna StorageGRID con il certificato se non lo hai già fatto.
3. Accedi all'agente Console come utente root. Correre:

   ```
   sudo su
   ```

4. Ottieni il volume Docker NetApp Backup and Recovery (Cloud Backup Service). Correre:

   ```
   docker volume ls | grep cbs
   ```

   Esempio di output:

   ```
   local service-manager-2_cloudmanager_cbs_volume"
   ```

   Il nome del volume varia tra le modalità di distribuzione Standard, Privata e Limitata. In questo esempio viene utilizzata la modalità Standard. Fare riferimento a "Modalità di distribuzione NetApp Console" .

5. Trova il punto di montaggio del volume NetApp Backup and Recovery . Correre:

   ```
   docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
   Mountpoint
   ```

   Esempio di output:

   ```
   "Mountpoint": "/var/lib/docker/volumes/service-manager-
   2_cloudmanager_cbs_volume/_data"
   ```

   Il punto di montaggio varia tra le modalità di distribuzione Standard, Privata e Limitata. Questo esempio mostra una distribuzione cloud standard. Fare riferimento a "Modalità di distribuzione NetApp Console" .

6. Passare alla directory MountPoint. Correre:

   ```
   cd /var/lib/docker/volumes/service-manager-
   2_cloudmanager_cbs_volume/_data
   ```

7. Se il certificato di StorageGRID è firmato dalla CA radice e da una CA intermedia, aggiungere `pem` file di

entrambi in un unico file denominato `sgws.crt` nella posizione attuale. Non aggiungere il certificato foglia a questo file.

Passaggi per il contenitore cloudmanager_cbs

Sarà necessario abilitare la verifica del certificato del server StorageGRID in NetApp Backup and Recovery (Cloud Backup Service).

1. Passare alle directory del volume Docker ottenuto nei passaggi precedenti.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Cambiare directory e passare alla directory config.

```
cd cbs_config
```

3. Crea e salva un file di configurazione come mostrato di seguito con uno dei seguenti nomi in base all'ambiente di distribuzione:

   - `production-customer.json`Utilizzato per le distribuzioni in modalità Standard e in modalità Ristretta.
   - `darksite-customer.json`Utilizzato per le distribuzioni in modalità privata.

   Fare riferimento a "Modalità di distribuzione NetApp Console" .

   File di configurazione

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Uscire dal contenitore. Correre:

```
exit
```

5. Ricomincia `cloudmanager_cbs` . Correre:

```
docker restart cloudmanager_cbs
```

Passaggi per il contenitore cloudmanager_cbs_catalog

Successivamente, sarà necessario abilitare la verifica del certificato del server StorageGRID per il servizio di catalogazione.

1. Cambiare directory nel volume Docker:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Configura il catalogo. Correre:

```
cd cbs_catalog_config
```

3. Crea un file di configurazione come mostrato di seguito con uno dei seguenti nomi in base al tuo ambiente di distribuzione:

   - `production-customer.json`Utilizzato per le distribuzioni in modalità Standard e in modalità Ristretta.
   - `darksite-customer.json`Utilizzato per le distribuzioni in modalità privata.

   Fare riferimento a "Modalità di distribuzione NetApp Console" .

   File di configurazione del catalogo

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Riavvia il catalogo. Correre:

```
docker restart cloudmanager_cbs_catalog
```

Aggiornare il certificato dell'agente della console con il certificato StorageGRID in base al sistema operativo dell'agente

Ubuntu

1. Copia il certificato SGWS in `/usr/local/share/ca-certificates` . Ecco un esempio:

```
cp /config/sgws.crt /usr/local/share/ca-certificates/
```

   Dove `sgws.crt` è il certificato CA radice.

2. Aggiornare i certificati host con il certificato StorageGRID . Correre

```
sudo update-ca-certificates
```

Red Hat Enterprise Linux

1. Copia il certificato SGWS in `/etc/pki/ca-trust/source/anchors/` .

```
cp /config/sgws.crt /etc/pki/ca-trust/source/anchors/
```

   Dove `sgws.crt` è il certificato CA radice.

2. Aggiornare i certificati host con il certificato StorageGRID .

```
update-ca-trust extract
```

3. Aggiorna il `ca-bundle.crt`

```
cd /etc/pki/tls/certs/
openssl x509 -in ca-bundle.crt -text -noout
```

4. Per verificare se i certificati sono presenti, eseguire il seguente comando:

```
openssl crl2pkcs7 -nocrl -certfile /etc/pki/tls/certs/ca-bundle.crt |
openssl pkcs7 -print_certs | grep subject | head
```

Creare un certificato di sicurezza per ONTAP

Se la comunicazione tra i contenitori NetApp Backup and Recovery e ONTAP deve convalidare il certificato ONTAP , completare i seguenti passaggi.

NetApp Backup and Recovery utilizza l'IP di gestione del cluster per connettersi a ONTAP. Immettere l'indirizzo IP del cluster nei nomi alternativi dell'oggetto del certificato. Specificare questo passaggio quando si genera la CSR tramite l'interfaccia utente di System Manager.

Utilizzare la documentazione di System Manager per creare un nuovo certificato CA per ONTAP.

- "Gestisci i certificati con System Manager"
- "Come gestire i certificati SSL ONTAP con System Manager"

Passi

1. Accedi all'agente della console come root. Correre:

```
sudo su
```

2. Ottieni il volume Docker NetApp Backup and Recovery . Correre:

```
docker volume ls | grep cbs
```

Esempio di output:

```
local service-manager-2_cloudmanager_cbs_volume
```

> Il nome del volume varia tra le modalità di distribuzione Standard, Privata e Limitata. Questo esempio mostra una distribuzione cloud standard. Fare riferimento a "Modalità di distribuzione NetApp Console" .

3. Procuratevi il supporto per il volume. Correre:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
Mountpoint
```

Esempio di output:

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

> Il punto di montaggio varia tra le modalità di distribuzione Standard, Privata e Limitata. Questo esempio mostra una distribuzione cloud standard. Fare riferimento a "Modalità di distribuzione NetApp Console" .

4. Passare alla directory del punto di montaggio. Correre:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

5. Completa uno dei seguenti passaggi:
   - Se il certificato ONTAP è firmato dalla CA radice e da una CA intermedia, aggiungere `pem` file di entrambi in un unico file denominato `ontap.crt` nella posizione attuale.
   - Se il certificato ONTAP è firmato da una singola CA, rinominarlo `pem` archiviare come `ontap.crt` e copiarlo nella posizione corrente. Non aggiungere il certificato foglia a questo file.

Passaggi per il contenitore cloudmanager_cbs

Successivamente, abilitare la verifica del certificato del server ONTAP in NetApp Backup and Recovery (Cloud Backup Service).

1. Passare alle directory del volume Docker ottenuto nei passaggi precedenti.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Passare alla directory config. Correre:

```
cd cbs_config
```

3. Creare un file di configurazione come mostrato di seguito con uno dei seguenti nomi in base all'ambiente di distribuzione:
   - `production-customer.json`Utilizzato per le distribuzioni in modalità Standard e in modalità Ristretta.
   - `darksite-customer.json`Utilizzato per le distribuzioni in modalità privata.

     Fare riferimento a "Modalità di distribuzione NetApp Console" .

     File di configurazione

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Uscire dal contenitore. Correre:

```
exit
```

5. Riavviare NetApp Backup and Recovery. Correre:

```
docker restart cloudmanager_cbs
```

Passaggi per il contenitore cloudmanager_cbs_catalog

Abilitare la verifica del certificato del server ONTAP per il servizio di catalogazione.

1. Passare alla directory del volume Docker. Correre:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Correre:

```
cd cbs_catalog_config
```

3. Creare un file di configurazione come mostrato di seguito con uno dei seguenti nomi in base all'ambiente di distribuzione:

   - `production-customer.json`Utilizzato per le distribuzioni in modalità Standard e in modalità Ristretta.
   - `darksite-customer.json`Utilizzato per le distribuzioni in modalità privata.

   Fare riferimento a "Modalità di distribuzione NetApp Console" .

   File di configurazione

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Riavviare NetApp Backup and Recovery. Correre:

```
docker restart cloudmanager_cbs_catalog
```

Creare un certificato sia per ONTAP che per StorageGRID

Se è necessario abilitare il certificato sia per ONTAP che per StorageGRID, il file di configurazione apparirà come segue:

File di configurazione per ONTAP e StorageGRID

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  },
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

Configurare le destinazioni di backup prima di utilizzare NetApp Backup and Recovery

Prima di utilizzare NetApp Backup and Recovery, eseguire alcuni passaggi per configurare le destinazioni di backup.

Prima di iniziare, rivedere"prerequisiti" per garantire che il tuo ambiente sia pronto.

Preparare la destinazione del backup

Preparare una o più delle seguenti destinazioni di backup:

- NetApp StorageGRID.

  Fare riferimento a "Scopri StorageGRID" .

  Fare riferimento a "Documentazione StorageGRID" per i dettagli su StorageGRID.

- Servizi Web Amazon. Fare riferimento a "Documentazione di Amazon S3" .

  Per preparare AWS come destinazione di backup, procedere come segue:

  - Crea un account su AWS.
  - Configurare le autorizzazioni S3 in AWS, elencate nella sezione successiva.

    - Per i dettagli sulla gestione dello storage AWS nella Console, fare riferimento a "Gestisci i tuoi bucket Amazon S3" .
- Microsoft Azure.
    - Fare riferimento a "Documentazione Azure NetApp Files" .
    - Configura un account in Azure.
    - Configurare "Autorizzazioni di Azure" in Azzurro.
    - Per informazioni dettagliate sulla gestione dell'archiviazione di Azure nella console, fare riferimento a "Gestisci i tuoi account di archiviazione di Azure" .

Dopo aver configurato le opzioni nella destinazione di backup stessa, in seguito la configurerai come destinazione di backup in NetApp Backup and Recovery. Per i dettagli su come configurare la destinazione di backup in NetApp Backup and Recovery, fare riferimento a"Scopri le destinazioni di backup" .

Imposta le autorizzazioni S3

Sarà necessario configurare due set di autorizzazioni AWS S3:

- Autorizzazioni per l'agente della console per creare e gestire il bucket S3.
- Autorizzazioni per il cluster ONTAP locale in modo che possa leggere e scrivere dati nel bucket S3.

Passi

1. Assicurarsi che l'agente della console disponga delle autorizzazioni richieste. Per i dettagli, vedere "Autorizzazioni dei criteri NetApp Console" .

    Quando si creano backup nelle regioni AWS Cina, è necessario modificare il nome della risorsa AWS "arn" in tutte le sezioni *Resource* nelle policy IAM da "aws" a "aws-cn"; ad esempio `arn:aws-cn:s3:::netapp-backup-*` .

2. Quando attivi il servizio, la procedura guidata di backup ti chiederà di immettere una chiave di accesso e una chiave segreta. Queste credenziali vengono trasmesse al cluster ONTAP in modo che ONTAP possa eseguire il backup e il ripristino dei dati nel bucket S3. Per farlo, dovrai creare un utente IAM con le seguenti autorizzazioni.

    Fare riferimento al "Documentazione AWS: creazione di un ruolo per delegare le autorizzazioni a un utente IAM" .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

Accedi a NetApp Backup and Recovery

Per accedere a NetApp Backup and Recovery , utilizzare la NetApp Console .

NetApp Backup and Recovery utilizza la gestione dell'identità e dell'accesso per controllare cosa può fare ogni utente.

Per i dettagli sulle azioni che ogni ruolo può eseguire, vedere"Ruoli utente di NetApp Backup and Recovery" .

Per accedere alla NetApp Console, puoi utilizzare le credenziali del sito di supporto NetApp oppure registrarti per accedere alla NetApp Console utilizzando il tuo indirizzo email e una password. "Scopri di più sull'accesso" .

Ruolo NetApp Console obbligatorio Ruolo di super amministratore di Backup and Recovery o di amministratore di ripristino di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Per aggiungere un agente Console, è necessario disporre del ruolo di super amministratore di Backup e ripristino.

Passi

1. Apri un browser web e vai su "NetApp Console" .

   Viene visualizzata la pagina di accesso NetApp Console .

2. Accedi alla Console.
3. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Backup e ripristino**.
   - Se è la prima volta che accedi a Backup and Recovery e non hai ancora aggiunto un sistema alla pagina **Sistemi**, Backup and Recovery visualizza la pagina di destinazione "Benvenuti nel nuovo NetApp Backup and Recovery" con un'opzione per aggiungere un sistema. Per i dettagli sull'aggiunta di un sistema alla pagina **Sistemi**, fare riferimento a "Introduzione alla modalità standard NetApp Console".
   - Se si accede a Backup and Recovery per la prima volta e si ha un sistema nella Console ma non sono state rilevate risorse, viene visualizzata la pagina *Benvenuti nel nuovo NetApp Backup and Recovery* con l'opzione **Rileva risorse**.
4. Se non lo hai ancora fatto, seleziona l'opzione **Scopri e gestisci**.
   - Per i carichi di lavoro di Microsoft SQL Server, fare riferimento a"Scopri i carichi di lavoro di Microsoft SQL Server" .
   - Per i carichi di lavoro VMware, fare riferimento a"Scopri i carichi di lavoro VMware" .
   - Per i carichi di lavoro KVM, fare riferimento a"Scopri i carichi di lavoro KVM" .
   - Per i carichi di lavoro di Oracle Database, fare riferimento a "Scopri i carichi di lavoro Oracle Database".
   - Per i carichi di lavoro Hyper-V, fare riferimento a"Scopri i carichi di lavoro Hyper-V" .
   - Per i carichi di lavoro Kubernetes, fare riferimento a"Scopri i carichi di lavoro di Kubernetes" .

Scopri le destinazioni di backup fuori sede in NetApp Backup and Recovery

Completa alcuni passaggi per scoprire o aggiungere manualmente destinazioni di backup offsite in NetApp Backup and Recovery.

Scopri un target di backup

Configurare le destinazioni di backup (Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage o StorageGRID) prima di utilizzare NetApp Backup and Recovery.

È possibile scoprire questi obiettivi automaticamente oppure aggiungerli manualmente.

Fornire le credenziali per accedere all'account di archiviazione. NetApp Backup and Recovery utilizza queste credenziali per individuare i carichi di lavoro di cui si desidera eseguire il backup.

Prima di iniziare

È necessario individuare almeno un carico di lavoro prima di poter aggiungere una destinazione di backup fuori sede.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare la scheda **Destinazioni di backup fuori sede**.
3. Seleziona **Scopri destinazione di backup**.
4. Selezionare uno dei tipi di destinazione del backup: **Amazon Web Services (AWS) S3**, **Microsoft Azure Blob Storage**, * StorageGRID* o * ONTAP S3*.
5. Nella sezione **Scegli posizione credenziali**, seleziona la posizione in cui risiedono le credenziali, quindi scegli come associarle.
6. Selezionare **Avanti**.
7. Inserisci le informazioni delle credenziali. Le informazioni variano a seconda del tipo di destinazione di backup selezionata e della posizione delle credenziali scelta.
   - Per AWS:
     - **Nome credenziale**: inserisci il nome della credenziale AWS.
     - **Chiave di accesso**: inserisci il segreto AWS.
     - **Chiave segreta**: inserisci la chiave segreta AWS.
   - Per Azure:
     - **Nome credenziale**: immettere il nome della credenziale di Azure Blob Storage.
     - **Segreto client**: immettere il segreto client di Azure Blob Storage.
     - **ID applicazione (client)**: seleziona l'ID applicazione di Azure Blob Storage.
     - **ID tenant directory**: immettere l'ID tenant di Azure Blob Storage.
   - Per StorageGRID:
     - **Nome credenziale**: immettere il nome della credenziale StorageGRID .
     - **FQDN del nodo gateway**: immettere un nome FQDN per StorageGRID.

- **Porta**: immettere il numero di porta per StorageGRID.
- **Chiave di accesso**: immettere la chiave di accesso StorageGRID S3.
- **Chiave segreta**: immettere la chiave segreta StorageGRID S3.

◦ Per ONTAP S3:

- **Nome credenziale**: immettere il nome della credenziale ONTAP S3.
- **FQDN del nodo gateway**: immettere un nome FQDN per ONTAP S3.
- **Porta**: immettere il numero di porta per ONTAP S3.
- **Chiave di accesso**: immettere la chiave di accesso ONTAP S3.
- **Chiave segreta**: Inserisci la chiave segreta ONTAP S3.

8. Seleziona **Scopri**.

Aggiungi un bucket per una destinazione di backup

Invece di lasciare che NetApp Backup and Recovery rilevi automaticamente i bucket, puoi aggiungere manualmente un bucket a una destinazione di backup fuori sede.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare **Destinazioni di backup fuori sede**.
3. Seleziona il target e sulla destra seleziona **Azioni*** **icona e seleziona *Aggiungi bucket**.
4. Inserisci le informazioni sul bucket. Le informazioni variano a seconda del tipo di destinazione di backup selezionata.

◦ Per AWS:

- **Nome bucket**: immettere il nome del bucket S3. Il prefisso "netapp-backup" è obbligatorio e viene aggiunto automaticamente al nome fornito.
- **Account AWS**: inserisci il nome dell'account AWS.
- **Regione del bucket**: immettere la regione AWS per il bucket.
- **Abilita blocco oggetto S3**: seleziona questa opzione per abilitare il blocco oggetto S3 per il bucket. S3 Object Lock impedisce che gli oggetti vengano eliminati o sovrascritti per un periodo di conservazione specificato, fornendo un ulteriore livello di protezione dei dati. Puoi abilitare questa opzione solo quando crei un bucket e non potrai disattivarla in seguito.
  - **Modalità di governance**: selezionare questa opzione per abilitare la modalità di governance per il bucket S3 Object Lock. La modalità di governance consente di proteggere gli oggetti dall'eliminazione o dalla sovrascrittura da parte della maggior parte degli utenti, ma consente ad alcuni utenti di modificare le impostazioni di conservazione.
  - **Modalità di conformità**: selezionare questa opzione per abilitare la modalità di conformità per il bucket S3 Object Lock. La modalità di conformità impedisce a qualsiasi utente, incluso l'utente root, di modificare le impostazioni di conservazione o di eliminare oggetti fino alla scadenza del periodo di conservazione.
- **Versioning**: seleziona questa opzione per abilitare il versioning per il bucket S3. Il controllo delle versioni consente di conservare più versioni degli oggetti nel bucket, il che può essere utile per scopi di backup e ripristino.
- **Tag**: seleziona i tag per il bucket S3. I tag sono coppie chiave-valore che possono essere utilizzate per organizzare e gestire le risorse S3.

        - **Crittografia**: seleziona il tipo di crittografia per il bucket S3. Le opzioni sono chiavi gestite da AWS S3 o chiavi AWS Key Management Service. Se selezioni le chiavi AWS Key Management Service, devi fornire l'ID della chiave.
    - Per Azure:
        - **Sottoscrizione**: seleziona il nome del contenitore Azure Blob Storage.
        - **Gruppo di risorse**: seleziona il nome del gruppo di risorse di Azure.
        - **Dettagli dell'istanza**:
            - **Nome account di archiviazione**: immettere il nome del contenitore Azure Blob Storage.
            - **Regione di Azure**: immettere la regione di Azure per il contenitore.
            - **Tipo di prestazioni**: selezionare il tipo di prestazioni, standard o premium, per il contenitore Azure Blob Storage, indicando il livello di prestazioni richiesto.
            - **Crittografia**: seleziona il tipo di crittografia per il contenitore Azure Blob Storage. Le opzioni sono chiavi gestite da Microsoft o chiavi gestite dal cliente. Se selezioni chiavi gestite dal cliente, devi fornire il nome del key vault e il nome della chiave.
    - Per StorageGRID:
        - **Nome destinazione backup**: seleziona il nome del bucket StorageGRID .
        - **Nome bucket**: immettere il nome del bucket StorageGRID .
        - **Regione**: immettere la regione StorageGRID per il bucket.
        - **Abilita controllo delle versioni**: seleziona questa opzione per abilitare il controllo delle versioni per il bucket StorageGRID . Il controllo delle versioni consente di conservare più versioni degli oggetti nel bucket, il che può essere utile per scopi di backup e ripristino.
        - **Blocco degli oggetti**: selezionare questa opzione per abilitare il blocco degli oggetti per il bucket StorageGRID . Il blocco degli oggetti impedisce che gli oggetti vengano eliminati o sovrascritti per un periodo di conservazione specificato, fornendo un ulteriore livello di protezione dei dati. Puoi abilitare questa opzione solo quando crei un bucket e non potrai disattivarla in seguito.
        - **Capacità**: immettere la capacità del bucket StorageGRID . Questa è la quantità massima di dati che può essere archiviata nel bucket.
    - Per ONTAP S3:
        - **Nome destinazione backup**: seleziona il nome del bucket ONTAP S3.
        - **Nome destinazione bucket**: immettere il nome del bucket ONTAP S3.
        - **Capacità**: immettere la capacità del bucket ONTAP S3. Questa è la quantità massima di dati che può essere archiviata nel bucket.
        - **Abilita controllo delle versioni**: seleziona questa opzione per abilitare il controllo delle versioni per il bucket ONTAP S3. Il controllo delle versioni consente di conservare più versioni degli oggetti nel bucket, il che può essere utile per scopi di backup e ripristino.
        - **Blocco degli oggetti**: selezionare questa opzione per abilitare il blocco degli oggetti per il bucket ONTAP S3. Il blocco degli oggetti impedisce che gli oggetti vengano eliminati o sovrascritti per un periodo di conservazione specificato, fornendo un ulteriore livello di protezione dei dati. Puoi abilitare questa opzione solo quando crei un bucket e non potrai disattivarla in seguito.
5. Selezionare **Aggiungi**.

Modificare le credenziali per una destinazione di backup

Immettere le credenziali necessarie per accedere alla destinazione di backup.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare **Destinazioni di backup fuori sede**.
3. Seleziona il target e sulla destra seleziona **Azioni*** **icona e seleziona *Modifica credenziali**.
4. Immettere le nuove credenziali per la destinazione di backup. Le informazioni variano a seconda del tipo di destinazione di backup selezionata.
5. Selezionare **Fatto**.

Passa a diversi carichi di lavoro NetApp Backup and Recovery

È possibile passare da un carico di lavoro all'altro NetApp Backup and Recovery .

Passa a un carico di lavoro diverso

È possibile passare a un carico di lavoro diverso nell'interfaccia utente NetApp Backup and Recovery .

Passi

1. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Backup e ripristino**.
2. Dall'angolo in alto a destra della pagina, seleziona l'elenco a discesa **Cambia carico di lavoro**.
3. Seleziona il carico di lavoro a cui vuoi passare.

   La pagina si aggiorna e mostra il carico di lavoro selezionato.

Configurare le impostazioni NetApp Backup and Recovery

Dopo aver configurato NetApp Console, configurare le impostazioni di backup e ripristino. Aggiungere credenziali per le risorse host, importare risorse SnapCenter , configurare directory di registro e impostare le impostazioni VMware vCenter. Completare questi passaggi prima di eseguire il backup o il ripristino dei dati.

- Aggiungere credenziali per le risorse host per qualsiasi host Windows, Microsoft SQL Server, Oracle Database o Linux con cui NetApp Backup and Recovery deve autenticarsi. Sono incluse le credenziali del sistema operativo guest Windows utilizzate durante il ripristino di file o cartelle guest.
- Gestire le impostazioni di VMware vCenter.
- Importa e gestisci le risorse host SnapCenter. (Solo carichi di lavoro di Microsoft SQL Server)
- Aggiungere una piattaforma di gestione KVM. (Solo carichi di lavoro KVM)
- Configurare le directory di registro negli snapshot per gli host Windows.
- Creare un modello di hook di esecuzione per eseguire script prima e dopo i processi di backup. (Solo carichi di lavoro Kubernetes)

*Ruolo richiesto NetApp Console * Super amministratore di Backup e ripristino, amministratore di backup di Backup e ripristino, amministratore di ripristino di Backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Aggiungere credenziali per le risorse host

Aggiungere credenziali per le risorse host. NetApp Backup and Recovery utilizza queste credenziali per individuare i carichi di lavoro e applicare policy di backup.

Se non si dispone di credenziali, crearle con le autorizzazioni per accedere e gestire i carichi di lavoro dell'host.

È necessario configurare i seguenti tipi di credenziali:

- Credenziali di Microsoft SQL Server
- Credenziali host Windows SnapCenter
- Credenziali del sistema operativo guest Windows utilizzate durante il ripristino di file o cartelle guest
- Credenziali del database Oracle
- Credenziali host Linux

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Impostazioni**.
2. Selezionare la freccia rivolta verso il basso per **Credenziali**.
3. Seleziona **Aggiungi nuove credenziali**.
4. Inserisci le informazioni per le credenziali. A seconda della modalità di autenticazione selezionata, vengono visualizzati campi diversi. Passa il mouse sull'icona Informazioni **i** per maggiori informazioni sui campi.
    - **Nome credenziali**: immettere un nome per le credenziali.
    - **Modalità di autenticazione**: selezionare **Windows**, **Microsoft SQL**, **Oracle Database** o **Linux**.

Per i carichi di lavoro di Microsoft SQL Server, è necessario immettere le credenziali sia per Windows che per Microsoft SQL Server, quindi sarà necessario aggiungere due set di credenziali.

Finestre

i. Se hai selezionato **Windows**:

- **Agenti**: seleziona un agente della console dall'elenco.
- **Dominio e nome utente**: immettere il NetBIOS o il nome di dominio completo (FQDN) e il nome utente per le credenziali.
- **Password**: Inserisci la password per le credenziali.

Microsoft SQL Server

i. Se hai selezionato **Microsoft SQL Server**:

- **Dominio e nome utente**: immettere il NetBIOS o il nome di dominio completo (FQDN) e il nome utente per le credenziali.
- **Password**: Inserisci la password per le credenziali.
- **Host**: seleziona un indirizzo host di SQL Server scoperto.
- **Istanza di SQL Server**: seleziona un'istanza di SQL Server rilevata.

Database Oracle

i. Se hai selezionato **Oracle Database**:

- **Agenti**: seleziona un agente della console dall'elenco.
- **Nome utente**: immettere il nome utente per le credenziali.
- **Password**: Inserisci la password per le credenziali.

Linux

i. Se hai selezionato **Linux**:

- **Agenti**: seleziona un agente della console dall'elenco.
- **Nome utente**: immettere il nome utente per le credenziali.
- **Password**: Inserisci la password per le credenziali.

5. Selezionare **Aggiungi**.

Modifica le credenziali per le risorse host

In seguito potrai modificare la password per tutte le credenziali che hai creato.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Impostazioni**.
2. Selezionare la freccia rivolta verso il basso per espandere la sezione **Credenziali**.
3. Seleziona l'icona Azioni ••• > **Modifica credenziali**.
   - **Password**: Inserisci la password per le credenziali.
4. Seleziona **Salva**.

Gestire le impostazioni di VMware vCenter

Fornire le credenziali VMware vCenter per individuare i carichi di lavoro per il backup. Se non si dispone di

credenziali, crearle con le autorizzazioni per accedere e gestire i carichi di lavoro di VMware vCenter Server.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Impostazioni**.
2. Selezionare la freccia rivolta verso il basso per espandere la sezione **VMware vCenter**.
3. Selezionare **Aggiungi vCenter**.
4. Immettere le informazioni su VMware vCenter Server.
   - **FQDN o indirizzo IP vCenter**: immettere un nome FQDN o l'indirizzo IP per VMware vCenter Server.
   - **Nome utente** e **Password**: immettere il nome utente e la password per VMware vCenter Server.
   - **Porta**: immettere il numero di porta per VMware vCenter Server.
   - **Protocollo**: Selezionare **HTTP** o **HTTPS**.
5. Selezionare **Aggiungi**.

Importa e gestisci le risorse host SnapCenter

Se in precedenza hai utilizzato SnapCenter per eseguire il backup delle tue risorse, puoi importare e gestire tali risorse in NetApp Backup and Recovery. Questa opzione consente di importare le informazioni del server SnapCenter per registrare più server SnapCenter e individuare i carichi di lavoro del database.

Si tratta di un processo in due fasi:

- Importa l'applicazione SnapCenter Server e le risorse host
- Gestisci le risorse host SnapCenter selezionate

Importa l'applicazione SnapCenter Server e le risorse host

Questo primo passaggio importa le risorse host da SnapCenter e le visualizza nella pagina Inventario NetApp Backup and Recovery . A quel punto, le risorse non sono ancora gestite da NetApp Backup and Recovery.

Dopo aver importato le risorse host SnapCenter , NetApp Backup and Recovery non assume la gestione della protezione. Per farlo, è necessario selezionare esplicitamente la gestione di queste risorse in NetApp Backup and Recovery.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Impostazioni**.
2. Selezionare la freccia rivolta verso il basso per espandere la sezione **Importa da SnapCenter**.
3. Selezionare **Importa da SnapCenter** per importare le risorse SnapCenter .
4. Inserisci * credenziali dell'applicazione SnapCenter *:
   a. * FQDN o indirizzo IP SnapCenter *: immettere il FQDN o l'indirizzo IP dell'applicazione SnapCenter stessa.
   b. **Porta**: immettere il numero di porta per il server SnapCenter .
   c. **Nome utente** e **Password**: immettere il nome utente e la password per il server SnapCenter .
   d. **Agente console**: seleziona l'agente console per SnapCenter.
5. Inserisci * credenziali dell'host del server SnapCenter *:
   a. **Credenziali esistenti**: se selezioni questa opzione, puoi utilizzare le credenziali esistenti che hai già

aggiunto. Inserisci il nome delle credenziali.

b. **Aggiungi nuove credenziali**: se non disponi di credenziali host SnapCenter esistenti, puoi aggiungerne di nuove. Immettere il nome delle credenziali, la modalità di autenticazione, il nome utente e la password.

6. Selezionare **Importa** per convalidare le voci e registrare SnapCenter Server.

> Se SnapCenter Server è già registrato, è possibile aggiornare i dettagli di registrazione esistenti.

Risultato

La pagina Inventario mostra le risorse SnapCenter importate.

Gestire le risorse host SnapCenter

Dopo aver importato le risorse SnapCenter , gestisci tali risorse host in NetApp Backup and Recovery. Dopo aver scelto di gestire le risorse importate, NetApp Backup and Recovery può eseguire il backup e il ripristino delle risorse che stai importando da SnapCenter. Non è più necessario gestire tali risorse in SnapCenter Server.

Passi

1. Dopo aver importato le risorse SnapCenter , nella pagina Inventario visualizzata, seleziona le risorse SnapCenter importate che desideri vengano gestite da NetApp Backup and Recovery da ora in poi.
2. Seleziona l'icona Azioni ••• > **Gestisci** per gestire le risorse.
3. Selezionare **Gestisci nella NetApp Console**.

   Nella pagina Inventario viene visualizzato **Gestito** sotto il nome host per indicare che le risorse host selezionate sono ora gestite da NetApp Backup and Recovery.

Modifica le risorse SnapCenter importate

In seguito potrai reimportare le risorse SnapCenter o modificare le risorse SnapCenter importate per aggiornare i dettagli di registrazione.

È possibile modificare solo i dettagli della porta e della password per SnapCenter Server.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Impostazioni**.
2. Selezionare la freccia rivolta verso il basso per **Importa da SnapCenter**.

   La pagina Importa da SnapCenter mostra tutte le importazioni precedenti.

3. Seleziona l'icona Azioni ••• > **Modifica** per aggiornare le risorse.
4. Aggiornare la password e i dettagli della porta di SnapCenter , se necessario.
5. Selezionare **Importa**.

Aggiungere una piattaforma di gestione KVM

Se si utilizza la piattaforma di gestione Apache CloudStack per gestire le risorse KVM, è necessario integrarla con NetApp Backup and Recovery in modo che Backup and Recovery possa individuare e proteggere gli host

KVM e le VM gestiti.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Impostazioni**.
2. Selezionare la freccia rivolta verso il basso per espandere la sezione **Piattaforma di gestione**.
3. Seleziona **Aggiungi credenziali della piattaforma di gestione**.
4. Inserisci le seguenti informazioni:
   - **Indirizzo IP o FQDN della piattaforma di gestione**: immettere l'indirizzo IP o il nome di dominio completo della piattaforma di gestione.
   - **Chiave API**: inserisci la chiave API da utilizzare per autenticare le richieste API.
   - **Chiave segreta**: inserisci la chiave segreta da utilizzare per autenticare le richieste API.
   - **Porta**: immettere la porta da utilizzare per la comunicazione tra Backup and Recovery e la piattaforma di gestione.
   - **Agenti**: selezionare un agente della console da utilizzare per facilitare la comunicazione tra Backup and Recovery e la piattaforma di gestione.
5. Al termine, seleziona **Aggiungi**.

Configurare le directory di registro negli snapshot per gli host Windows

Prima di creare policy per gli host Windows, è necessario configurare le directory di registro negli snapshot per gli host Windows. Le directory di registro vengono utilizzate per archiviare i registri generati durante il processo di backup.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Dalla pagina Inventario, seleziona un carico di lavoro e quindi seleziona l'icona Azioni ••• > **Visualizza dettagli** per visualizzare i dettagli del carico di lavoro.
3. Nella pagina dei dettagli dell'inventario che mostra Microsoft SQL Server, selezionare la scheda Host.
4. Dalla pagina dei dettagli dell'inventario, seleziona un host e seleziona l'icona Azioni ••• > **Configura directory registro**.
5. Sfogliare o immettere il percorso della directory del registro.
6. Seleziona **Salva**.

Creare un modello di hook di esecuzione

È possibile creare un modello di hook di esecuzione personalizzato da utilizzare per eseguire azioni prima o dopo un'operazione di protezione dei dati su un'applicazione.

I modelli che crei qui sono utilizzabili solo quando proteggi i carichi di lavoro Kubernetes.

Passi

1. Nella Console, vai a **Protezione** > **Backup e ripristino**.
2. Selezionare la scheda **Impostazioni**.
3. Espandi la sezione **Modello di hook di esecuzione**.
4. Selezionare **Crea modello di hook di esecuzione**.

5. Immettere un nome per l'hook di esecuzione.
6. Facoltativamente, scegli un tipo di hook. Ad esempio, un hook post-restore viene eseguito al termine dell'operazione di ripristino.
7. Nella casella di testo **Script**, immettere lo script shell eseguibile che si desidera eseguire come parte del modello di hook di esecuzione. Facoltativamente, puoi selezionare **Carica script** per caricare un file di script.
8. Seleziona **Crea**.

   Dopo aver creato il modello, questo viene visualizzato nell'elenco dei modelli nella sezione **Modello di hook di esecuzione**.

Imposta il controllo degli accessi in base al ruolo in NetApp Backup e ripristino

Per aumentare la sicurezza e controllare l'accesso alle risorse, configura l'accesso in base al ruolo per NetApp Backup and Recovery. La NetApp Console supporta il controllo degli accessi in base al ruolo (RBAC) per alcuni carichi di lavoro di Backup and Recovery. Puoi assegnare ruoli amministrativi o di visualizzazione specifici per questi carichi di lavoro. Altri carichi di lavoro che non supportano ancora il controllo degli accessi in base al ruolo rimangono accessibili a tutti gli utenti con ruoli di Backup and Recovery finché non viene supportata l'associazione a livello di progetto.

Segui questi passaggi per controllare l'accesso alle risorse nella tua organizzazione. Apporta le modifiche nella pagina **Amministrazione > Identità e accesso** nel menu NetApp Console.

Questi passaggi presuppongono che ti sia stato assegnato il ruolo di Organization Admin nella Console.

Passi

1. Crea la struttura del progetto di identità e accesso.

   In qualità di amministratore dell'organizzazione, configura la cartella Identity and access e la struttura del progetto in cui risiederanno i carichi di lavoro.

2. Assegna ruoli utente.
   a. Opzione primaria:

      Aggiungi utenti a ciascun progetto designato per i carichi di lavoro e assegna loro il ruolo appropriato. Ad esempio:

      - **Organization admin** e **Backup and Recovery super admin**: un utente con questi ruoli può visualizzare tutte le risorse in tutte le organizzazioni, individuare i workload di Backup and Recovery e assegnarli ai progetti (ad esempio, US East o US West).
      - **Amministratore di cartelle o progetti** e **Backup and Recovery super admin**: un utente con questi ruoli può visualizzare solo le risorse nella cartella o nel progetto per cui dispone delle autorizzazioni, ma può individuare i workload di Backup and Recovery e assegnarli a tale progetto.

   b. Opzione alternativa:

Invece di concedere a un utente l’accesso completo come amministratore di Backup and Recovery, puoi assegnarti il ruolo di super admin di Backup and Recovery e scoprire direttamente i workload.

3. Scopri i carichi di lavoro in Backup and Recovery.

   Gli amministratori dell’organizzazione o gli amministratori di cartelle o progetti individuano i carichi di lavoro disponibili e selezionano il progetto appropriato (ad esempio, US East o US West). Ogni carico di lavoro viene automaticamente associato al progetto selezionato.

4. Aggiungi utenti ai progetti.

   Gli amministratori dell’organizzazione o gli amministratori di cartelle/progetti aggiungono utenti della Console ai progetti con carichi di lavoro. Assegna agli utenti il ruolo di Organization viewer e un ruolo di Backup and Recovery in base alle loro esigenze di accesso. Gli utenti con il ruolo di Backup and Recovery corretto otterranno automaticamente l’accesso ai nuovi carichi di lavoro in questi progetti.

Informazioni correlate

- "Scopri la gestione dell’identità e dell’accesso della NetApp Console".
- "Ruoli NetApp Backup and Recovery nella NetApp Console".

Utilizzare NetApp Backup and Recovery

Visualizza lo stato di protezione sulla dashboard di NetApp Backup and Recovery

Monitorando lo stato dei carichi di lavoro sarai a conoscenza di eventuali problemi relativi alla protezione dei carichi di lavoro e potrai adottare misure per risolverli. Visualizza lo stato dei tuoi backup e ripristini nella dashboard NetApp Backup and Recovery . È possibile esaminare il riepilogo del sistema, il riepilogo della protezione, il riepilogo del processo, il riepilogo del ripristino e altro ancora.

*Ruolo richiesto NetApp Console * Visualizzatore di storage, super amministratore di Backup and Recovery, amministratore di backup di Backup and Recovery, amministratore di ripristino di Backup and Recovery, amministratore di clonazione di Backup and Recovery o ruolo di visualizzatore di Backup and Recovery. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Console , selezionare **Protezione** > **Backup e ripristino**.
2. Selezionare un riquadro del carico di lavoro (ad esempio, Microsoft SQL Server).
3. Dal menu Backup e ripristino, seleziona **Dashboard**.

   È possibile esaminare i seguenti tipi di informazioni:

   - Numero di host o VM scoperti
   - Numero di cluster Kubernetes scoperti
   - Numero di destinazioni di backup su storage di oggetti
   - Numero di vCenter
   - Numero di cluster di archiviazione in ONTAP

Visualizza il riepilogo della protezione

Esaminare le seguenti informazioni nel Riepilogo della protezione:

- Numero totale di database, VM e datastore protetti e non protetti.

  Un database protetto è un database a cui è assegnata una policy di backup. Un database non protetto è un database a cui non è assegnata alcuna policy di backup.

- Numero di backup riusciti, con avviso o non riusciti.
- La capacità totale rilevata dal servizio di backup e la capacità protetta rispetto a quella non protetta. Passa il mouse sull'icona **"i"** per visualizzare i dettagli.

Visualizza il riepilogo del lavoro

Esamina il totale dei lavori completati, in esecuzione o non riusciti nel Riepilogo lavori.

Passi

1. Per ogni distribuzione dei lavori, modifica un filtro per visualizzare il riepilogo di quelli non riusciti, in esecuzione e completati in base al numero di giorni, ad esempio gli ultimi 30 giorni, gli ultimi 7 giorni, le ultime 24 ore o l'ultimo anno.
2. Visualizza i dettagli dei processi non riusciti, in esecuzione e completati selezionando **Visualizza monitoraggio processi**.

Visualizza il riepilogo del ripristino

Esaminare le seguenti informazioni nel riepilogo del ripristino:

- Numero totale di processi di ripristino eseguiti
- La quantità totale di capacità che è stata ripristinata
- Numero di processi di ripristino eseguiti su storage locale, secondario e di oggetti. Passa il mouse sul grafico per visualizzare i dettagli.

Crea e gestisci policy per gestire i backup in NetApp Backup and Recovery

In NetApp Backup and Recovery, puoi creare policy personalizzate che stabiliscono la frequenza dei backup, l'ora in cui vengono eseguiti e il numero di file di backup conservati.

Alcune di queste opzioni e sezioni di configurazione non sono disponibili per tutti i carichi di lavoro.

Se importi risorse da SnapCenter, potresti riscontrare alcune differenze tra i criteri utilizzati in SnapCenter e quelli utilizzati in NetApp Backup and Recovery. Vedere"Differenze di policy tra SnapCenter e NetApp Backup and Recovery" .

È possibile raggiungere i seguenti obiettivi relativi alle politiche:

- Creare un criterio di snapshot locale
- Creare una policy per la replica su storage secondario
- Creare una policy per le impostazioni di archiviazione degli oggetti
- Configurare le impostazioni avanzate dei criteri
- Modifica policy (non disponibile per i carichi di lavoro di anteprima VMware)
- Elimina le policy

Visualizza le politiche

1. Dal menu NetApp Backup and Recovery , selezionare **Criteri**.
2. Esaminare i dettagli di questa politica.
    - **Carico di lavoro**: esempi includono Microsoft SQL Server, Volumes, VMware, KVM, Hyper-V, Oracle Database o Kubernetes.
    - **Tipo di backup**: alcuni esempi includono il backup completo e il backup del registro.

- **Architettura**: Alcuni esempi includono snapshot locale, fan-out, cascading, disco su disco e disco su archivio oggetti.
- **Risorse protette**: mostra quante risorse sul totale delle risorse di quel carico di lavoro sono protette.
- **Protezione ransomware**: indica se la policy include il blocco degli snapshot sullo snapshot locale, il blocco degli snapshot sull'archiviazione secondaria o il blocco DataLock sull'archiviazione degli oggetti.

Crea una politica

È possibile creare policy che regolano gli snapshot locali, le repliche su storage secondario e i backup su storage di oggetti. Una parte della strategia 3-2-1 prevede la creazione di uno snapshot delle istanze, dei database, delle applicazioni o delle VM sul sistema di archiviazione **primario**.

*Ruolo richiesto NetApp Console * Visualizzatore di storage, super amministratore di backup e ripristino, amministratore di backup di backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Prima di iniziare

Se si prevede di replicare su un archivio secondario e si desidera utilizzare il blocco degli snapshot sugli snapshot locali o sull'archivio secondario ONTAP remoto, è necessario innanzitutto inizializzare il clock di conformità ONTAP a livello di cluster. Questo è un requisito per abilitare il blocco degli snapshot nella policy.

Per istruzioni su come fare, fare riferimento a "Inizializza l'orologio di conformità in ONTAP" .

Per informazioni generali sul blocco degli snapshot, fare riferimento a "Blocco degli snapshot in ONTAP" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Criteri**.
2. Dalla pagina Criteri, seleziona **Crea nuovo criterio**.
3. Nella pagina Criteri, fornire le seguenti informazioni.

    - Sezione **Dettagli**:
        - Tipo di carico di lavoro: seleziona il carico di lavoro che utilizzerà il criterio.
        - Inserisci un nome per la policy.

            Per un elenco dei personaggi da evitare, vedere il suggerimento.

        - Selezionare un agente della console dall'elenco **Agente**.
    - Sezione **Architettura di backup**: selezionare la freccia rivolta verso il basso e scegliere il flusso di dati per il backup, ad esempio fan-out 3-2-1, cascata 3-2-1 o disco su disco.
        - **Fanout 3-2-1**: da storage primario (disco) a storage secondario (disco) a cloud (archivio di oggetti). Crea più copie dei dati su diversi sistemi di storage, come configurazioni ONTAP a ONTAP e ONTAP a archivio di oggetti. Può trattarsi di un archivio di oggetti cloud hyperscaler o di un archivio di oggetti privato. Queste configurazioni aiutano a ottenere una protezione dei dati e un disaster recovery ottimali.

            Questa opzione non è disponibile per Amazon FSx for NetApp ONTAP.

            Per i carichi di lavoro VMware, questa operazione configura lo snapshot locale sui datastore o sulle VM sul primario e lo replica dall'archiviazione su disco primaria all'archiviazione su disco

secondaria, nonché dallo storage primario allo storage di oggetti cloud.

- **Cascata 3-2-1**: (non disponibile per i carichi di lavoro Kubernetes) Da storage primario (disco) a storage secondario (disco) e da storage primario (disco) a storage cloud (archivio oggetti). Può trattarsi di un archivio di oggetti cloud hyperscaler o di un archivio di oggetti privato: StorageGRID. Ciò crea una catena di replicazione dei dati su più sistemi per garantire ridondanza e affidabilità.

  Questa opzione non è disponibile per Amazon FSx for NetApp ONTAP.

Per i carichi di lavoro VMware, questo configura lo snapshot locale sui datastore o sulle VM sullo storage primario e una cascata dallo storage su disco primario allo storage su disco secondario e quindi allo storage di oggetti cloud.

- **Da disco a disco**: (non disponibile per i carichi di lavoro Kubernetes) Da storage primario (disco) a storage secondario (disco). La strategia di protezione dei dati ONTAP - ONTAP replica i dati tra due sistemi ONTAP per garantire elevata disponibilità e ripristino in caso di emergenza. In genere, questo risultato viene ottenuto utilizzando SnapMirror, che supporta sia la replica sincrona che quella asincrona. Questo metodo garantisce che i tuoi dati siano costantemente aggiornati e disponibili in più posizioni, offrendo una solida protezione contro la perdita di dati.

  Per i carichi di lavoro VMware, questa operazione configura lo snapshot locale sui datastore o VMware sul sistema di storage primario e quindi replica i dati dal sistema di storage su disco primario al sistema di storage su disco secondario.

- **Archiviazione da disco a oggetto**: archiviazione primaria (disco) nel cloud (archivio oggetti). Questa replica i dati da un sistema ONTAP a un sistema di archiviazione di oggetti, come AWS S3, Azure Blob Storage o StorageGRID. In genere, questo risultato viene ottenuto utilizzando SnapMirror Cloud, che fornisce backup incrementali permanenti trasferendo solo i blocchi di dati modificati dopo il trasferimento di base iniziale. Può trattarsi di un archivio di oggetti cloud hyperscaler o di un archivio di oggetti privato: StorageGRID. Questo metodo è ideale per la conservazione e l'archiviazione dei dati a lungo termine, offrendo una soluzione conveniente e scalabile per la protezione dei dati.

  Per i carichi di lavoro VMWare, questa opzione configura lo snapshot locale sui datastore o sulle VM sul server primario e la replica dall'archiviazione su disco primario all'archiviazione di oggetti cloud.

- **Fanout da disco a disco**: (non disponibile per i carichi di lavoro Kubernetes) Da storage primario (disco) a storage secondario (disco) e da storage primario (disco) a storage secondario (disco).

  È possibile configurare più impostazioni secondarie per l'opzione fanout da disco a disco.

Per i carichi di lavoro VMware, questa operazione configura l'archiviazione su disco primaria in quella su disco secondaria e replica l'archiviazione su disco primaria in quella su disco secondaria.

- **Snapshot locali**: snapshot locale sul volume selezionato (Microsoft SQL Server). Gli snapshot locali sono una componente fondamentale delle strategie di protezione dei dati, poiché catturano lo stato dei dati in momenti specifici. In questo modo vengono create copie di sola lettura e in un dato momento dei volumi di produzione in cui vengono eseguiti i carichi di lavoro. Lo snapshot consuma uno spazio di archiviazione minimo e comporta un sovraccarico di prestazioni trascurabile perché registra solo le modifiche apportate ai file dall'ultimo snapshot. È possibile utilizzare snapshot locali per ripristinare dati persi o danneggiati, nonché per creare backup per scopi di disaster recovery.

Per i carichi di lavoro VMware, questa operazione configura lo snapshot locale sui datastore o sulle VM sul sistema di storage primario.

Creare un criterio di snapshot locale

Fornire informazioni per lo snapshot locale.

- Selezionare l'opzione **Aggiungi pianificazione** per selezionare la pianificazione o le pianificazioni degli snapshot. È possibile avere un massimo di 5 pianificazioni.
- **Frequenza snapshot**: seleziona la frequenza oraria, giornaliera, settimanale, mensile o annuale. La frequenza annuale non è disponibile per i carichi di lavoro Kubernetes.
- **Conservazione degli snapshot**: immettere il numero di snapshot da conservare.
- **Abilita backup del log**: (si applica solo ai carichi di lavoro di Microsoft SQL Server e Oracle Database.) Abilitare questa opzione per eseguire il backup dei registri e impostare la frequenza e la conservazione dei backup dei registri. Per fare ciò, è necessario aver già configurato un backup del registro. Vedere"Configurare le directory di registro" .
  - **Elimina i log di archivio dopo il backup**: (solo carichi di lavoro di Oracle Database) Se i backup dei log sono abilitati, è possibile abilitare facoltativamente questa funzionalità per limitare il periodo di tempo per cui Backup and Recovery conserva i log di archivio di Oracle. È possibile scegliere il periodo di conservazione e il punto in cui Backup e Recovery devono eliminare i registri di archivio.
- **Provider**: (solo carichi di lavoro Kubernetes) Seleziona il provider di archiviazione che ospita le risorse dell'applicazione Kubernetes.

Creare una policy per le impostazioni secondarie (replica su storage secondario)

Fornire informazioni per la replicazione su storage secondario. Le informazioni sulla pianificazione delle impostazioni degli snapshot locali vengono visualizzate nelle impostazioni secondarie. Queste impostazioni non sono disponibili per i carichi di lavoro Kubernetes.

- **Backup**: seleziona la frequenza oraria, giornaliera, settimanale, mensile o annuale.
- **Destinazione backup**: seleziona il sistema di destinazione sull'archiviazione secondaria per il backup.
- **Conservazione**: immettere il numero di snapshot da conservare.
- **Abilita blocco snapshot**: seleziona se desideri abilitare gli snapshot antimanomissione.
- **Periodo di blocco dello snapshot**: immettere il numero di giorni, mesi o anni per i quali si desidera bloccare lo snapshot.
- **Trasferimento alla secondaria**:
  - L'opzione * Pianificazione trasferimento ONTAP - Inline* è selezionata per impostazione predefinita e indica che gli snapshot vengono trasferiti immediatamente al sistema di archiviazione secondario. Non è necessario pianificare il backup.
  - Altre opzioni: se si sceglie un trasferimento differito, i trasferimenti non sono immediati e si può impostare una pianificazione.
- * Relazione secondaria SMAS tra SnapMirror e SnapVault *: utilizzare le relazioni secondarie SMAS tra SnapMirror e SnapVault per i carichi di lavoro di SQL Server.

Creare una policy per le impostazioni di archiviazione degli oggetti

Fornire informazioni per il backup nell'archiviazione degli oggetti. Queste impostazioni sono chiamate "Impostazioni di backup" per i carichi di lavoro Kubernetes.

I campi visualizzati variano a seconda del provider e dell'architettura selezionati.

Creare una policy per l'archiviazione di oggetti AWS

Inserisci le informazioni in questi campi:

- **Provider**: seleziona **AWS**.
- **Account AWS**: seleziona l'account AWS.
- **Destinazione di backup**: seleziona una destinazione di archiviazione di oggetti S3 registrata. Assicurarsi che la destinazione sia accessibile all'interno dell'ambiente di backup.
- **Spazio IP**: seleziona lo spazio IP da utilizzare per le operazioni di backup. Questa funzione è utile se si hanno più spazi IP e si desidera controllare quale viene utilizzato per i backup.
- **Impostazioni pianificazione**: seleziona la pianificazione impostata per gli snapshot locali. È possibile rimuovere una pianificazione, ma non aggiungerne una, perché le pianificazioni sono impostate in base alle pianificazioni degli snapshot locali.
- **Copie di conservazione**: immettere il numero di snapshot da conservare.
- **Esegui a**: scegli la pianificazione del trasferimento ONTAP per eseguire il backup dei dati nell'archivio oggetti.
- **Suddividi i backup dall'archivio oggetti allo storage di archiviazione**: se scegli di suddividere i backup in livelli per lo storage di archiviazione (ad esempio, AWS Glacier), seleziona l'opzione del livello e il numero di giorni di archiviazione.
- **Abilita scansione integrità**: (non disponibile per i carichi di lavoro Kubernetes) Seleziona se desideri abilitare le scansioni di integrità (blocco snapshot) sull'archiviazione degli oggetti. Ciò garantisce che i backup siano validi e possano essere ripristinati correttamente. Per impostazione predefinita, la frequenza della scansione dell'integrità è impostata su 7 giorni. Per proteggere i backup da modifiche o eliminazioni, seleziona l'opzione **Scansione di integrità**. La scansione avviene solo sull'ultimo snapshot. È possibile abilitare o disabilitare le scansioni di integrità sull'ultimo snapshot.

Creare un criterio per l'archiviazione degli oggetti di Microsoft Azure

Inserisci le informazioni in questi campi:

- **Provider**: seleziona **Azure**.
- **Sottoscrizione Azure**: seleziona la sottoscrizione Azure tra quelle individuate.
- **Gruppo di risorse di Azure**: seleziona il gruppo di risorse di Azure tra quelli individuati.
- **Destinazione di backup**: seleziona una destinazione di archiviazione di oggetti registrata. Assicurarsi che la destinazione sia accessibile all'interno dell'ambiente di backup.
- **Spazio IP**: seleziona lo spazio IP da utilizzare per le operazioni di backup. Questa funzione è utile se si hanno più spazi IP e si desidera controllare quale viene utilizzato per i backup.
- **Impostazioni pianificazione**: seleziona la pianificazione impostata per gli snapshot locali. È possibile rimuovere una pianificazione, ma non aggiungerne una, perché le pianificazioni sono impostate in base alle pianificazioni degli snapshot locali.
- **Copie di conservazione**: immettere il numero di snapshot da conservare.
- **Esegui a**: scegli la pianificazione del trasferimento ONTAP per eseguire il backup dei dati nell'archivio oggetti.
- **Suddividere i backup in livelli dall'archivio oggetti all'archiviazione**: se si sceglie di suddividere i backup in livelli nell'archiviazione, selezionare l'opzione del livello e il numero di giorni di archiviazione.

- **Abilita scansione integrità**: (non disponibile per i carichi di lavoro Kubernetes) Seleziona se desideri abilitare le scansioni di integrità (blocco snapshot) sull'archiviazione degli oggetti. Ciò garantisce che i backup siano validi e possano essere ripristinati correttamente. Per impostazione predefinita, la frequenza della scansione dell'integrità è impostata su 7 giorni. Per proteggere i backup da modifiche o eliminazioni, seleziona l'opzione **Scansione di integrità**. La scansione avviene solo sull'ultimo snapshot. È possibile abilitare o disabilitare le scansioni di integrità sull'ultimo snapshot.

Creare una policy per l'archiviazione degli oggetti StorageGRID

Inserisci le informazioni in questi campi:

- **Provider**: Seleziona * StorageGRID*.
- * Credenziali StorageGRID *: seleziona le credenziali StorageGRID tra quelle rilevate. Queste credenziali vengono utilizzate per accedere al sistema di archiviazione degli oggetti StorageGRID e sono state immesse nell'opzione Impostazioni.
- **Destinazione di backup**: seleziona una destinazione di archiviazione di oggetti S3 registrata. Assicurarsi che la destinazione sia accessibile all'interno dell'ambiente di backup.
- **Spazio IP**: seleziona lo spazio IP da utilizzare per le operazioni di backup. Questa funzione è utile se si hanno più spazi IP e si desidera controllare quale viene utilizzato per i backup.
- **Impostazioni pianificazione**: seleziona la pianificazione impostata per gli snapshot locali. È possibile rimuovere una pianificazione, ma non aggiungerne una, perché le pianificazioni sono impostate in base alle pianificazioni degli snapshot locali.
- **Copie di conservazione**: immettere il numero di snapshot da conservare per ciascuna frequenza.
- **Pianificazione del trasferimento per l'archiviazione di oggetti**: (non disponibile per i carichi di lavoro Kubernetes) Scegli la pianificazione del trasferimento ONTAP per eseguire il backup dei dati nell'archiviazione di oggetti.
- **Abilita scansione integrità**: (non disponibile per i carichi di lavoro Kubernetes) Seleziona se desideri abilitare le scansioni di integrità (blocco snapshot) sull'archiviazione degli oggetti. Ciò garantisce che i backup siano validi e possano essere ripristinati correttamente. Per impostazione predefinita, la frequenza della scansione dell'integrità è impostata su 7 giorni. Per proteggere i backup da modifiche o eliminazioni, seleziona l'opzione **Scansione di integrità**. La scansione avviene solo sull'ultimo snapshot. È possibile abilitare o disabilitare le scansioni di integrità sull'ultimo snapshot.
- **Suddividere i backup in livelli dall'archivio oggetti all'archiviazione**: (non disponibile per i carichi di lavoro Kubernetes) Se si sceglie di suddividere i backup in livelli nell'archiviazione, selezionare l'opzione del livello e il numero di giorni di archiviazione.

Configurare le impostazioni avanzate nella policy

Facoltativamente, è possibile configurare le impostazioni avanzate nel criterio. Queste impostazioni sono disponibili per tutte le architetture di backup, inclusi gli snapshot locali, la replica su storage secondario e i backup su storage di oggetti. Queste impostazioni non sono disponibili per i carichi di lavoro Kubernetes. Le impostazioni avanzate disponibili variano a seconda del carico di lavoro selezionato nella parte superiore della pagina, pertanto le impostazioni avanzate descritte qui potrebbero non essere applicabili a tutti i carichi di lavoro. Le impostazioni avanzate non sono disponibili quando si configura un criterio per i carichi di lavoro Kubernetes.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Criteri**.
2. Dalla pagina Criteri, seleziona **Crea nuovo criterio**.

3. Nella sezione Impostazioni **Criteri > Avanzate**, seleziona il menu **Seleziona azione avanzata** per scegliere da un elenco di impostazioni avanzate.
4. Abilita le impostazioni che desideri visualizzare o modificare, quindi seleziona **Accetta**.
5. Fornire le seguenti informazioni:
   - **Backup di sola copia**: (si applica solo ai carichi di lavoro di Microsoft SQL Server) Scegli il backup di sola copia (un tipo di backup di Microsoft SQL Server) se devi eseguire il backup delle tue risorse utilizzando un'altra applicazione di backup.
   - **Impostazioni del gruppo di disponibilità**: (si applica solo ai carichi di lavoro di Microsoft SQL Server) Seleziona le repliche di backup preferite o specifica una replica specifica. Questa impostazione è utile se si dispone di un gruppo di disponibilità di SQL Server e si desidera controllare quale replica viene utilizzata per i backup.
   - **Velocità di trasferimento massima**: per non impostare un limite all'utilizzo della larghezza di banda, selezionare **Illimitato**. Se si desidera limitare la velocità di trasferimento, selezionare **Limitata** e selezionare la larghezza di banda di rete tra 1 e 1.000 Mbps assegnata per caricare i backup nell'archiviazione degli oggetti. Per impostazione predefinita, ONTAP può utilizzare una quantità illimitata di larghezza di banda per trasferire i dati di backup dai volumi del sistema all'archiviazione degli oggetti. Se noti che il traffico di backup influisce sui normali carichi di lavoro degli utenti, valuta la possibilità di ridurre la quantità di larghezza di banda di rete utilizzata durante il trasferimento.
   - **Nuovi tentativi di backup**: (non applicabile ai carichi di lavoro VMware) Per riprovare il processo in caso di errore o interruzione, selezionare **Abilita nuovi tentativi di processo in caso di errore**. Immettere il numero massimo di tentativi di snapshot e backup e l'intervallo di tempo tra i tentativi. Il riconteggio deve essere inferiore a 10. Questa impostazione è utile se si desidera garantire che il processo di backup venga ripetuto in caso di errore o interruzione.

     Se la frequenza degli snapshot è impostata su 1 ora, il ritardo massimo, insieme al conteggio dei nuovi tentativi, non dovrebbe superare i 45 minuti.

   - **Abilita snapshot coerenti con la VM**: seleziona se desideri abilitare snapshot coerenti con la VM. Ciò garantisce che gli snapshot appena creati siano coerenti con lo stato della macchina virtuale al momento dello snapshot. Ciò è utile per garantire che i backup possano essere ripristinati correttamente e che i dati siano in uno stato coerente. Ciò non si applica agli snapshot esistenti.
   - **Scansione ransomware**: seleziona se desideri abilitare la scansione ransomware su ciascun bucket. Ciò richiede il blocco DataLock sull'archiviazione degli oggetti. Inserire la frequenza della scansione in giorni. Questa opzione si applica all'archiviazione di oggetti AWS e Microsoft Azure. Tieni presente che questa opzione potrebbe comportare costi aggiuntivi, a seconda del provider cloud.
   - **Verifica del backup**: (non applicabile ai carichi di lavoro VMware) Seleziona se desideri abilitare la verifica del backup e se desideri eseguirla immediatamente o in un secondo momento. Questa funzionalità garantisce che i backup siano validi e possano essere ripristinati correttamente. Ti consigliamo di abilitare questa opzione per garantire l'integrità dei tuoi backup. Per impostazione predefinita, la verifica del backup viene eseguita dall'archivio secondario, se questo è configurato. Se l'archiviazione secondaria non è configurata, la verifica del backup viene eseguita dall'archiviazione primaria.

     Inoltre, configurare le seguenti opzioni:

     - Verifica **Giornaliera**, **Settimanale**, **Mensile** o **Annuale**: se hai scelto **Più tardi** come verifica del backup, seleziona la frequenza della verifica del backup. Ciò garantisce che l'integrità dei backup venga regolarmente verificata e che sia possibile ripristinarli correttamente.
     - **Etichette di backup**: immettere un'etichetta per il backup. Questa etichetta viene utilizzata per identificare il backup nel sistema e può essere utile per monitorare e gestire i backup.

        - **Controllo della coerenza del database**: (non applicabile ai carichi di lavoro VMware) Seleziona se desideri abilitare i controlli della coerenza del database. Questa opzione garantisce che i database siano in uno stato coerente prima che venga eseguito il backup, il che è fondamentale per garantire l'integrità dei dati.
        - **Verifica backup del registro**: (non applicabile ai carichi di lavoro VMware) Seleziona se desideri verificare i backup del registro. Seleziona il server di verifica. Se hai scelto disk-to-disk o 3-2-1, seleziona anche la posizione di archiviazione della verifica. Questa opzione garantisce che i backup del registro siano validi e possano essere ripristinati correttamente, il che è importante per mantenere l'integrità dei database.
    - **Rete**: selezionare l'interfaccia di rete da utilizzare per le operazioni di backup. Questa funzionalità è utile se si dispone di più interfacce di rete e si desidera controllare quale viene utilizzata per i backup.
        - **Spazio IP**: seleziona lo spazio IP da utilizzare per le operazioni di backup. Questa funzione è utile se si hanno più spazi IP e si desidera controllare quale viene utilizzato per i backup.
        - **Configurazione endpoint privato**: se si utilizza un endpoint privato per l'archiviazione degli oggetti, selezionare la configurazione dell'endpoint privato da utilizzare per le operazioni di backup. Questa funzionalità è utile se si desidera garantire che i backup vengano trasferiti in modo sicuro tramite una connessione di rete privata.
    - **Notifica**: seleziona se desideri abilitare le notifiche e-mail per le operazioni di backup. Questa funzione è utile se si desidera ricevere una notifica quando un'operazione di backup viene avviata, completata o non riesce.
    - **Dischi indipendenti**: (si applica solo ai carichi di lavoro VMware) Selezionare questa opzione per includere nel backup tutti gli archivi dati con dischi indipendenti che contengono dati temporanei. Un disco indipendente è un disco VM non incluso negli snapshot VMware.
    - * Formato del volume e dello snapshot SnapMirror *: facoltativamente, inserisci il nome del tuo snapshot in un criterio che regola i backup per i carichi di lavoro di Microsoft SQL Server. Inserisci il formato e il testo personalizzato. Se si sceglie di eseguire il backup su un archivio secondario, è anche possibile aggiungere un prefisso e un suffisso del volume SnapMirror .

Modifica una policy

È possibile modificare l'architettura di backup, la frequenza di backup, i criteri di conservazione e altre impostazioni per un criterio.

È possibile aggiungere un altro livello di protezione quando si modifica una policy, ma non è possibile rimuovere un livello di protezione. Ad esempio, se il criterio protegge solo gli snapshot locali, è possibile aggiungere la replica all'archiviazione secondaria o i backup all'archiviazione degli oggetti. Se si dispone di snapshot e repliche locali, è possibile aggiungere l'archiviazione di oggetti. Tuttavia, se si dispone di snapshot locali, replica e archiviazione di oggetti, non è possibile rimuovere uno di questi livelli.

Se si modifica un criterio che esegue il backup nell'archiviazione degli oggetti, è possibile abilitare l'archiviazione.

Se hai importato risorse da SnapCenter, potresti riscontrare alcune differenze tra i criteri utilizzati in SnapCenter e quelli utilizzati in NetApp Backup and Recovery. Vedere"Differenze di policy tra SnapCenter e NetApp Backup and Recovery" .

Ruolo richiesto NetApp Console

Super amministratore di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Nella NetApp Console, vai su **Protezione** > **Backup e ripristino**.
2. Selezionare l'opzione **Criteri**.
3. Seleziona la policy che vuoi modificare.
4. Seleziona **Azioni*** **icona e seleziona *Modifica**.

Elimina una policy

Puoi eliminare una policy se non ti serve più.

Non è possibile eliminare un criterio associato a un carico di lavoro.

Passi

1. Nella Console, vai a **Protezione** > **Backup e ripristino**.
2. Selezionare l'opzione **Criteri**.
3. Seleziona la policy che vuoi eliminare.
4. Seleziona **Azioni*** **icona e seleziona *Elimina**.
5. Conferma l'azione e seleziona **Elimina**.

Proteggere i carichi di lavoro del volume ONTAP

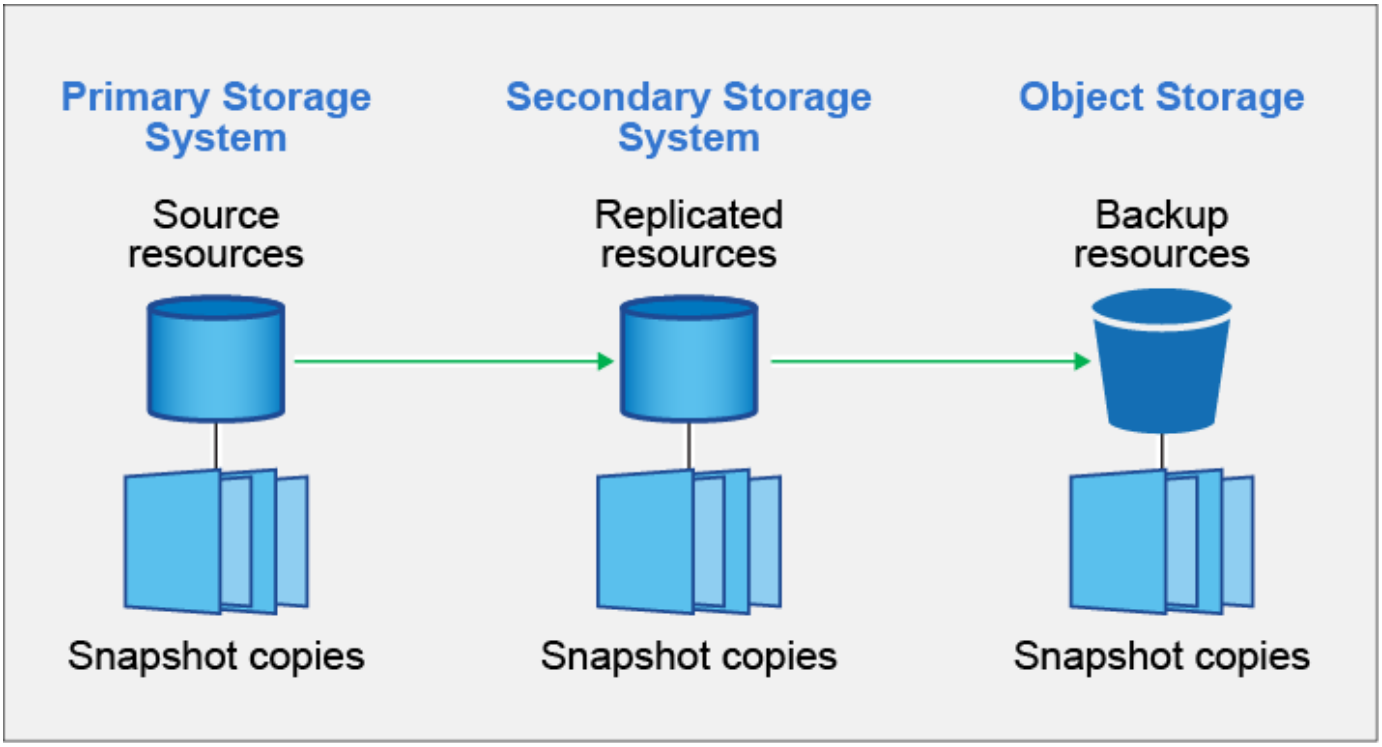
Proteggi i dati del tuo volume ONTAP utilizzando NetApp Backup and Recovery

NetApp Backup and Recovery offre funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del volume ONTAP . È possibile implementare una strategia 3-2-1 in cui si hanno 3 copie dei dati di origine su 2 sistemi di archiviazione diversi, oltre a 1 copia nel cloud.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Dopo l'attivazione, il backup e il ripristino creano backup incrementali a livello di blocco, permanenti, che vengono archiviati su un altro cluster ONTAP e nell'archiviazione di oggetti nel cloud. Oltre al volume sorgente, avrai:

- Istantanea del volume sul sistema sorgente
- Volume replicato su un sistema di archiviazione diverso
- Backup del volume nell'archiviazione degli oggetti



NetApp Backup and Recovery sfrutta la tecnologia di replicazione dei dati SnapMirror di NetApp per garantire che tutti i backup siano completamente sincronizzati creando snapshot e trasferendoli nelle posizioni di backup.

I vantaggi dell'approccio 3-2-1 includono:

- Più copie di dati proteggono dalle minacce informatiche interne ed esterne.
- L'utilizzo di diversi tipi di supporto aiuta a recuperare i dati se un tipo non funziona.
- È possibile ripristinare rapidamente dalla copia in loco e utilizzare le copie fuori sede se la copia in loco è compromessa.

Se necessario, è possibile ripristinare un intero *volume*, una *cartella* o uno o più *file* da una qualsiasi delle copie di backup sullo stesso sistema o su un sistema diverso.

Caratteristiche

Caratteristiche di replicazione:

- Replicare i dati tra i sistemi di archiviazione ONTAP per supportare il backup e il ripristino di emergenza.
- Garantisci l'affidabilità del tuo ambiente DR con elevata disponibilità.
- Crittografia ONTAP nativa in volo impostata tramite chiave pre-condivisa (PSK) tra i due sistemi.
- I dati copiati sono immutabili finché non vengono resi scrivibili e pronti per l'uso.
- La replicazione è auto-riparante in caso di errore di trasferimento.
- Rispetto a "NetApp Replication" , la replica in NetApp Backup and Recovery include le seguenti funzionalità:
  - Replicare più volumi FlexVol contemporaneamente su un sistema secondario.
  - Ripristina un volume replicato sul sistema di origine o su un sistema diverso tramite l'interfaccia utente.

Vedere"Limitazioni di replica per i volumi ONTAP" per un elenco delle funzionalità di replica non disponibili con NetApp Backup and Recovery per volumi ONTAP .

Funzionalità di backup su oggetto:

- Esegui il backup di copie indipendenti dei tuoi volumi di dati su un archivio di oggetti a basso costo.
- Applicare un singolo criterio di backup a tutti i volumi in un cluster oppure assegnare criteri di backup diversi ai volumi che hanno obiettivi di punto di ripristino univoci.
- Creare una policy di backup da applicare a tutti i volumi futuri creati nel cluster.
- Crea file di backup immutabili in modo che siano bloccati e protetti per il periodo di conservazione.
- Esegui la scansione dei file di backup per individuare possibili attacchi ransomware e rimuovi/sostituisci automaticamente i backup infetti.
- Per risparmiare sui costi, archivia i file di backup più vecchi.
- Eliminare la relazione di backup in modo da poter archiviare i volumi di origine non necessari, conservando al contempo i backup dei volumi.
- Esegui il backup da cloud a cloud e da sistemi on-premise a cloud pubblici o privati.
- I dati di backup sono protetti tramite crittografia AES a 256 bit a riposo e connessioni HTTPS TLS 1.2 in transito.
- Utilizza le tue chiavi gestite dal cliente per la crittografia dei dati anziché utilizzare le chiavi di crittografia predefinite del tuo provider cloud.
- Supporto per un massimo di 4.000 backup di un singolo volume.

Ripristina le funzionalità:

- Ripristina i dati da un punto specifico nel tempo da snapshot locali, volumi replicati o volumi sottoposti a backup nell'archiviazione di oggetti.
- Ripristina un volume, una cartella o singoli file nel sistema di origine o in un sistema diverso.
- Ripristinare i dati su un sistema utilizzando un abbonamento/account diverso o che si trova in una regione diversa.
- Esegue un *ripristino rapido* di un volume da un archivio cloud a un sistema Cloud Volumes ONTAP o a un sistema locale; perfetto per situazioni di disaster recovery in cui è necessario fornire l'accesso a un volume il prima possibile.
- Ripristina i dati a livello di blocco, posizionandoli direttamente nella posizione specificata, preservando al contempo gli ACL originali.
- Sfoglia e cerca nei cataloghi dei file per selezionare facilmente singole cartelle e file per il ripristino di singoli file.

Sistemi supportati per operazioni di backup e ripristino

NetApp Backup and Recovery supporta i sistemi ONTAP e i provider di cloud pubblici e privati.

Regioni supportate

NetApp Backup and Recovery è supportato con Cloud Volumes ONTAP in molte regioni di Amazon Web Services, Microsoft Azure e Google Cloud.

"Scopri di più utilizzando la mappa delle regioni globali"

Destinazioni di backup supportate

NetApp Backup and Recovery consente di eseguire il backup di volumi ONTAP dai seguenti sistemi di origine ai seguenti sistemi secondari e storage di oggetti nei provider di cloud pubblici e privati. Gli snapshot risiedono sul sistema di origine.

Sistema sorgente	Sistema secondario (Replicazione)	Archivio oggetti di destinazione (backup)
Cloud Volumes ONTAP in AWS	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Amazon S3
Cloud Volumes ONTAP in Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Blob azzurro
Cloud Volumes ONTAP in Google	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP	Google Cloud Storage
Sistema ONTAP in sede	Cloud Volumes ONTAP Sistema ONTAP locale	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID ONTAP S3

Destinazioni di ripristino supportate

È possibile ripristinare i dati ONTAP da un file di backup che risiede in un sistema secondario (un volume replicato) o in un archivio oggetti (un file di backup) nei seguenti sistemi. Gli snapshot risiedono nel sistema di origine e possono essere ripristinati solo sullo stesso sistema.

Posizione del file di backup		Sistema di destinazione
Archivio oggetti (backup)	**Sistema secondario (replicazione)**	
Amazon S3	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS
Blob azzurro	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure
Google Cloud Storage	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP
NetApp StorageGRID	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP in sede
ONTAP S3	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP in sede

Si noti che i riferimenti ai "sistemi ONTAP locali" includono i sistemi FAS, AFF e ONTAP Select .

Volumi supportati

NetApp Backup and Recovery supporta i seguenti tipi di volumi:

- Volumi di lettura-scrittura FlexVol
- Volumi FlexGroup (richiede ONTAP 9.12.1 o versione successiva)
- Volumi SnapLock Enterprise (richiede ONTAP 9.11.1 o versione successiva)

- SnapLock Compliance per volumi on-premise (richiede ONTAP 9.14 o versione successiva)
- Volumi di destinazione della protezione dati (DP) SnapMirror

NetApp Backup and Recovery non supporta i backup dei volumi FlexCache .

Vedi le sezioni su"Limitazioni di backup e ripristino per i volumi ONTAP" per ulteriori requisiti e limitazioni.

Costo

L'utilizzo di NetApp Backup and Recovery con i sistemi ONTAP comporta due tipi di costi: costi delle risorse e costi dei servizi. Entrambi gli addebiti riguardano la parte di backup dell'oggetto del servizio.

Non vi è alcun costo per la creazione di snapshot o volumi replicati, a parte lo spazio su disco necessario per archiviare gli snapshot e i volumi replicati.

Costi delle risorse

I costi delle risorse vengono pagati al provider cloud per la capacità di archiviazione degli oggetti e per la scrittura e la lettura dei file di backup sul cloud.

- Per il backup su storage di oggetti, paghi al tuo provider cloud i costi di storage di oggetti.

  Poiché NetApp Backup and Recovery preserva l'efficienza di archiviazione del volume di origine, si pagano al provider cloud i costi di archiviazione degli oggetti per i dati *dopo* le efficienze ONTAP (per la quantità minore di dati dopo l'applicazione della deduplicazione e della compressione).

- Per ripristinare i dati tramite Search & Restore, alcune risorse vengono fornite dal tuo provider cloud e vi è un costo per TiB associato alla quantità di dati scansionati dalle tue richieste di ricerca. (Queste risorse non sono necessarie per Sfoglia e ripristina.)
  - In AWS, "Amazzone Atena" E "AWS Glue" le risorse vengono distribuite in un nuovo bucket S3.
  - In Azure, un "Area di lavoro di Azure Synapse" E "Archiviazione di Azure Data Lake" sono predisposti nel tuo account di archiviazione per archiviare e analizzare i tuoi dati.
  - In Google, viene distribuito un nuovo bucket e il "Servizi Google Cloud BigQuery" sono forniti a livello di account/progetto.
- Se si prevede di ripristinare i dati del volume da un file di backup che è stato spostato in un archivio di oggetti, il provider cloud applicherà una tariffa aggiuntiva per il recupero per GiB e una tariffa per richiesta.
- Se intendi analizzare un file di backup alla ricerca di ransomware durante il processo di ripristino dei dati del volume (se hai abilitato DataLock e Ransomware Resilience per i tuoi backup cloud), dovrai sostenere anche costi di uscita aggiuntivi dal tuo provider cloud.

Spese di servizio

I costi del servizio vengono pagati a NetApp e coprono sia il costo per *creare* backup nell'archiviazione di oggetti sia per *ripristinare* volumi o file da tali backup. Si paga solo per i dati protetti nell'archiviazione di oggetti, calcolati in base alla capacità logica utilizzata all'origine (prima delle efficienze ONTAP) dei volumi ONTAP sottoposti a backup nell'archiviazione di oggetti. Questa capacità è anche nota come Front-End Terabyte (FETB).

Esistono tre modi per pagare il servizio Backup. La prima opzione è quella di abbonarsi al tuo provider cloud, che ti consente di pagare mensilmente. La seconda opzione è quella di stipulare un contratto annuale. La terza opzione è quella di acquistare le licenze direttamente da NetApp.

Licenza

NetApp Backup and Recovery è disponibile con i seguenti modelli di consumo:

- **BYOL**: licenza acquistata da NetApp che può essere utilizzata con qualsiasi provider cloud.
- **PAYGO**: un abbonamento orario dal marketplace del tuo provider cloud.
- **Annuale**: un contratto annuale dal marketplace del tuo provider cloud.

Una licenza di backup è richiesta solo per il backup e il ripristino da un archivio di oggetti. La creazione di snapshot e volumi replicati non richiede una licenza.

Porta la tua patente

BYOL è basato sulla durata (1, 2 o 3 anni) e sulla capacità, con incrementi di 1 TiB. Si paga NetApp per utilizzare il servizio per un periodo di tempo, ad esempio 1 anno, e per una capacità massima, ad esempio 10 TiB.

Riceverai un numero di serie che dovrai inserire nella NetApp Console per abilitare il servizio. Una volta raggiunto uno dei due limiti, sarà necessario rinnovare la licenza. La licenza Backup BYOL si applica a tutti i sistemi sorgente associati all'organizzazione o all'account NetApp Console .

"Scopri come gestire le tue licenze BYOL".

Abbonamento a consumo

NetApp Backup and Recovery offre licenze basate sul consumo con un modello di pagamento a consumo. Dopo aver sottoscritto l'abbonamento tramite il marketplace del tuo provider cloud, paghi per GiB per i dati sottoposti a backup, senza alcun pagamento anticipato. La fatturazione avviene tramite la bolletta mensile del tuo provider cloud.

"Scopri come impostare un abbonamento a consumo".

Tieni presente che è disponibile una prova gratuita di 30 giorni quando ti registri inizialmente con un abbonamento PAYGO.

Contratto annuale

Quando utilizzi AWS, sono disponibili due contratti annuali della durata di 1, 2 o 3 anni:

- Un piano "Cloud Backup" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP locali.
- Un piano "CVO Professional" che consente di raggruppare Cloud Volumes ONTAP e NetApp Backup and Recovery. Sono inclusi backup illimitati per i Cloud Volumes ONTAP addebitati su questa licenza (la capacità di backup non viene conteggiata sulla licenza).

Quando si utilizza Azure, sono disponibili due contratti annuali della durata di 1, 2 o 3 anni:

- Un piano "Cloud Backup" che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP locali.
- Un piano "CVO Professional" che consente di raggruppare Cloud Volumes ONTAP e NetApp Backup and Recovery. Sono inclusi backup illimitati per i Cloud Volumes ONTAP addebitati su questa licenza (la capacità di backup non viene conteggiata sulla licenza).

Quando utilizzi GCP, puoi richiedere un'offerta privata da NetApp e quindi selezionare il piano quando ti iscrivi

da Google Cloud Marketplace durante l'attivazione di NetApp Backup and Recovery .

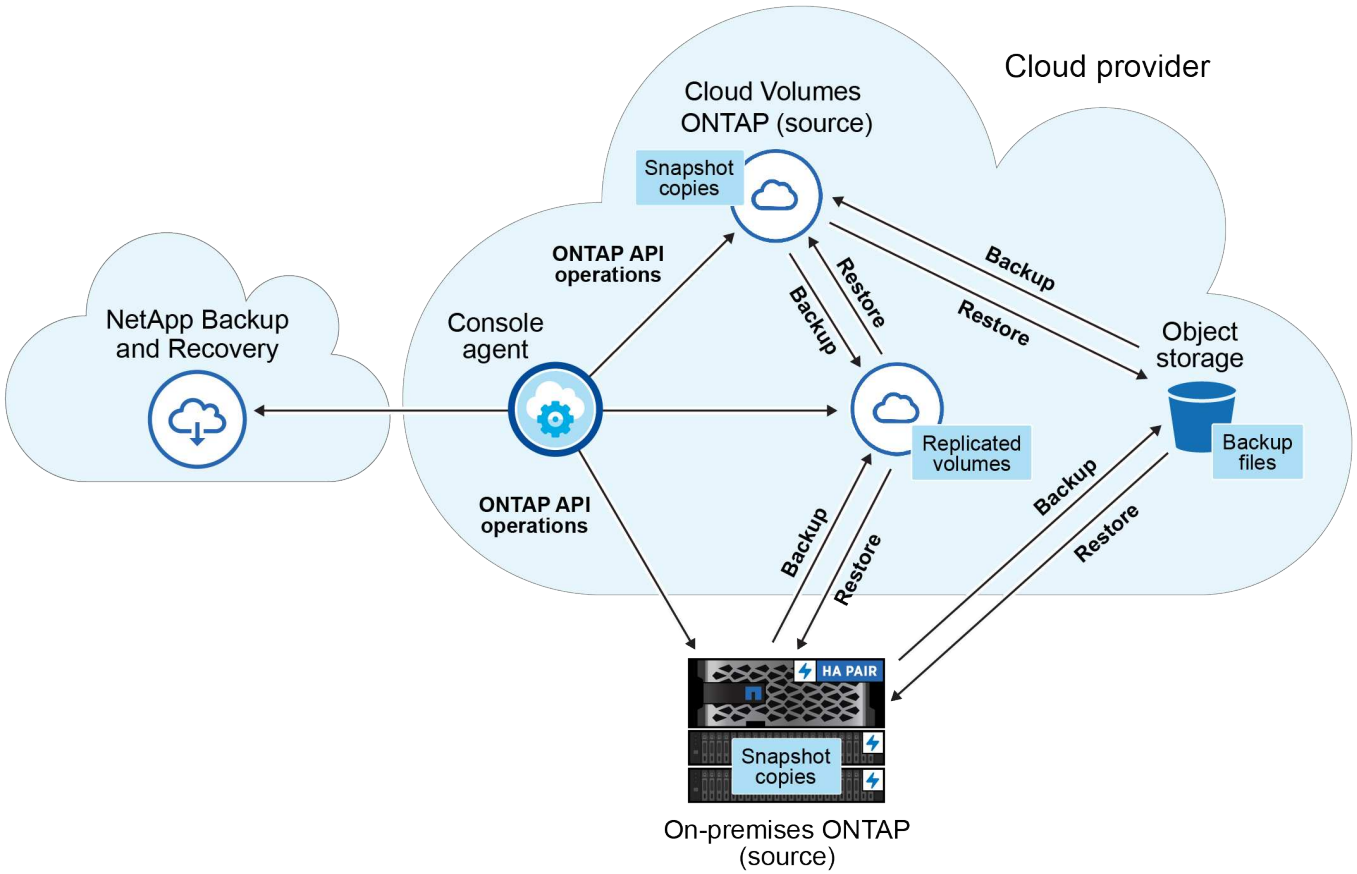
"Scopri come impostare contratti annuali".

Come funziona NetApp Backup and Recovery

Quando si abilita NetApp Backup and Recovery su un sistema Cloud Volumes ONTAP o ONTAP locale, il servizio esegue un backup completo dei dati. Dopo il backup iniziale, tutti i backup aggiuntivi sono incrementali, ovvero vengono sottoposti a backup solo i blocchi modificati e quelli nuovi. In questo modo il traffico di rete viene ridotto al minimo. Il backup su storage di oggetti è costruito sulla base di "Tecnologia NetApp SnapMirror Cloud" .

> Qualsiasi azione intrapresa direttamente dall'ambiente del tuo provider cloud per gestire o modificare i file di backup cloud potrebbe danneggiare i file e dare luogo a una configurazione non supportata.

L'immagine seguente mostra la relazione tra ciascun componente:



Questo diagramma mostra i volumi replicati su un sistema Cloud Volumes ONTAP , ma i volumi potrebbero essere replicati anche su un sistema ONTAP locale.

Dove risiedono i backup

I backup risiedono in posizioni diverse in base al tipo di backup:

- Gli *snapshot* risiedono sul volume di origine nel sistema di origine.
- I *volumi replicati* risiedono sul sistema di archiviazione secondario: un sistema Cloud Volumes ONTAP o

ONTAP locale.

- Le *copie di backup* vengono archiviate in un archivio oggetti creato dalla Console nel tuo account cloud. Esiste un archivio oggetti per cluster/sistema e la Console assegna a tale archivio il seguente nome: "netapp-backup-clusteruuid". Assicurarsi di non eliminare questo archivio oggetti.
  - In AWS, la Console abilita la "Funzionalità di blocco dell'accesso pubblico di Amazon S3" sul bucket S3.
  - In Azure, la console utilizza un gruppo di risorse nuovo o esistente con un account di archiviazione per il contenitore BLOB. La console "blocca l'accesso pubblico ai dati del tuo blob" per impostazione predefinita.
  - In GCP, la Console utilizza un progetto nuovo o esistente con un account di archiviazione per il bucket Google Cloud Storage.
  - In StorageGRID, la console utilizza un account tenant esistente per il bucket S3.
  - In ONTAP S3, la console utilizza un account utente esistente per il bucket S3.

Se in futuro si desidera modificare l'archivio oggetti di destinazione per un cluster, sarà necessario"annullare la registrazione NetApp Backup and Recovery per il sistema" e quindi abilitare NetApp Backup and Recovery utilizzando le informazioni del nuovo provider cloud.

Pianificazione di backup e impostazioni di conservazione personalizzabili

Quando si abilita NetApp Backup and Recovery per un sistema, tutti i volumi inizialmente selezionati vengono sottoposti a backup utilizzando i criteri selezionati. È possibile selezionare policy separate per snapshot, volumi replicati e file di backup. Se si desidera assegnare policy di backup diverse a determinati volumi con obiettivi di punto di ripristino (RPO) diversi, è possibile creare policy aggiuntive per quel cluster e assegnarle agli altri volumi dopo l'attivazione di NetApp Backup and Recovery .

È possibile scegliere una combinazione di backup orari, giornalieri, settimanali, mensili e annuali di tutti i volumi. Per il backup dell'oggetto è anche possibile selezionare una delle policy definite dal sistema che prevedono backup e conservazione per 3 mesi, 1 anno e 7 anni. Anche i criteri di protezione del backup creati sul cluster tramite ONTAP System Manager o ONTAP CLI verranno visualizzati come selezioni. Sono incluse le policy create utilizzando etichette SnapMirror personalizzate.

> Il criterio Snapshot applicato al volume deve avere una delle etichette utilizzate nel criterio di replica e nel criterio di backup su oggetto. Se non vengono trovate etichette corrispondenti, non verrà creato alcun file di backup. Ad esempio, se si desidera creare volumi replicati e file di backup "settimanali", è necessario utilizzare un criterio Snapshot che crei snapshot "settimanali".

Una volta raggiunto il numero massimo di backup per una categoria o un intervallo, i backup più vecchi vengono rimossi in modo da avere sempre i backup più recenti (e quindi i backup obsoleti non continuano a occupare spazio).

> Il periodo di conservazione per i backup dei volumi di protezione dei dati è lo stesso definito nella relazione SnapMirror di origine. Se lo desideri, puoi modificarlo utilizzando l'API.

Impostazioni di protezione dei file di backup

Se il tuo cluster utilizza ONTAP 9.11.1 o versione successiva, puoi proteggere i tuoi backup nell'archiviazione degli oggetti da eliminazioni e attacchi ransomware. Ogni policy di backup prevede una sezione per *DataLock e Ransomware Resilience* che può essere applicata ai file di backup per un periodo di tempo specifico, il *periodo di conservazione*.

- *DataLock* protegge i file di backup da modifiche o eliminazioni.
- La *protezione ransomware* analizza i file di backup per cercare prove di un attacco ransomware quando viene creato un file di backup e quando i dati di un file di backup vengono ripristinati.

Le scansioni di protezione anti-ransomware pianificate sono abilitate per impostazione predefinita. L'impostazione predefinita per la frequenza di scansione è 7 giorni. La scansione avviene solo sull'ultimo snapshot. Per ridurre i costi, è possibile disattivare le scansioni pianificate. È possibile abilitare o disabilitare le scansioni ransomware pianificate sull'ultimo snapshot utilizzando l'opzione nella pagina Impostazioni avanzate. Se si attiva questa opzione, per impostazione predefinita le scansioni vengono eseguite settimanalmente. È possibile modificare la programmazione in giorni o settimane oppure disattivarla, risparmiando sui costi.

Il periodo di conservazione del backup è lo stesso del periodo di conservazione del backup programmato, più un buffer massimo di 31 giorni. Ad esempio, i backup *settimanali* con *5* copie conservate bloccheranno ogni file di backup per 5 settimane. I backup *mensili* con *6* copie conservate bloccheranno ogni file di backup per 6 mesi.

Il supporto è attualmente disponibile quando la destinazione del backup è Amazon S3, Azure Blob o NetApp StorageGRID. Nelle versioni future verranno aggiunte altre destinazioni di provider di archiviazione.

Per maggiori dettagli fare riferimento a questa informativa:

- "Come funzionano la protezione da DataLock e Ransomware".
- "Come aggiornare le opzioni di protezione Ransomware nella pagina Impostazioni avanzate".

DataLock non può essere abilitato se si suddividono i backup in livelli di archiviazione.

Archiviazione per vecchi file di backup

Quando si utilizza un determinato tipo di archiviazione cloud, è possibile spostare i file di backup più vecchi in una classe di archiviazione/livello di accesso meno costoso dopo un certo numero di giorni. Puoi anche scegliere di inviare immediatamente i tuoi file di backup all'archivio, senza che vengano salvati nell'archiviazione cloud standard. Tieni presente che l'archiviazione non può essere utilizzata se hai abilitato DataLock.

- In AWS, i backup iniziano nella classe di archiviazione *Standard* e passano alla classe di archiviazione *Standard-Infrequent Access* dopo 30 giorni.

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile scegliere di suddividere i backup più vecchi in storage *S3 Glacier* o *S3 Glacier Deep Archive* nell'interfaccia utente NetApp Backup and Recovery dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sullo storage di archiviazione AWS" .

- In Azure, i backup sono associati al livello di accesso *Cool*.

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile scegliere di suddividere i backup più vecchi nell'archiviazione *Azure Archive* nell'interfaccia utente NetApp Backup and Recovery dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sull'archiviazione di Azure" .

- In GCP, i backup sono associati alla classe di archiviazione *Standard*.

  Se il cluster utilizza ONTAP 9.12.1 o versione successiva, è possibile scegliere di suddividere i backup più vecchi in livelli di storage *Archive* nell'interfaccia utente NetApp Backup and Recovery dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sull'archiviazione di Google" .

- In StorageGRID, i backup sono associati alla classe di archiviazione *Standard*.

  Se il cluster locale utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza la versione 11.4 o versione successiva, è possibile archiviare i file di backup più vecchi nell'archiviazione cloud pubblica dopo un certo numero di giorni. Il supporto attuale riguarda i livelli di archiviazione AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive. "Scopri di più sull'archiviazione dei file di backup da StorageGRID" .

Per maggiori dettagli sull'archiviazione dei file di backup più vecchi, vedere il collegamento:prev-ontap-policy-object-options.html.

Considerazioni sulla politica di tiering FabricPool

Ci sono alcune cose di cui devi essere a conoscenza quando il volume di cui stai eseguendo il backup risiede su un aggregato FabricPool e ha una politica di suddivisione in livelli assegnata diversa da `none` :

- Il primo backup di un volume FabricPool a livelli richiede la lettura di tutti i dati locali e a livelli (dall'archivio oggetti). Un'operazione di backup non "riscalda" i dati inattivi archiviati in livelli nell'archiviazione degli oggetti.

  Questa operazione potrebbe comportare un aumento una tantum dei costi di lettura dei dati dal tuo provider cloud.

  - I backup successivi sono incrementali e non hanno questo effetto.
  - Se il criterio di suddivisione in livelli viene assegnato al volume al momento della sua creazione iniziale, questo problema non verrà visualizzato.
- Considerare l'impatto dei backup prima di assegnare il `all` politica di suddivisione in livelli in base ai volumi. Poiché i dati vengono suddivisi immediatamente in livelli, NetApp Backup and Recovery leggerà i dati dal livello cloud anziché dal livello locale. Poiché le operazioni di backup simultanee condividono il collegamento di rete con l'archivio oggetti cloud, potrebbe verificarsi un calo delle prestazioni se le risorse di rete diventano sature. In questo caso, potrebbe essere opportuno configurare in modo proattivo più interfacce di rete (LIF) per ridurre questo tipo di saturazione della rete.

Pianifica il tuo percorso di protezione con NetApp Backup and Recovery

NetApp Backup and Recovery consente di creare fino a tre copie dei volumi di origine per proteggere i dati. Sono numerose le opzioni che puoi selezionare quando attivi Backup e Ripristino sui tuoi volumi, quindi dovresti rivedere le tue scelte per essere preparato.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Esamineremo le seguenti opzioni:

- Quali funzionalità di protezione utilizzerai: snapshot, volumi replicati e/o backup sul cloud
- Quale architettura di backup utilizzerai: un backup a cascata o a fan-out dei tuoi volumi
- Utilizzerai i criteri di backup predefiniti o dovrai creare criteri personalizzati?
- Desideri che il servizio crei i bucket cloud per te o desideri creare i contenitori di archiviazione degli oggetti prima di iniziare?
- Quale modalità di distribuzione dell'agente della console stai utilizzando (modalità standard, limitata o

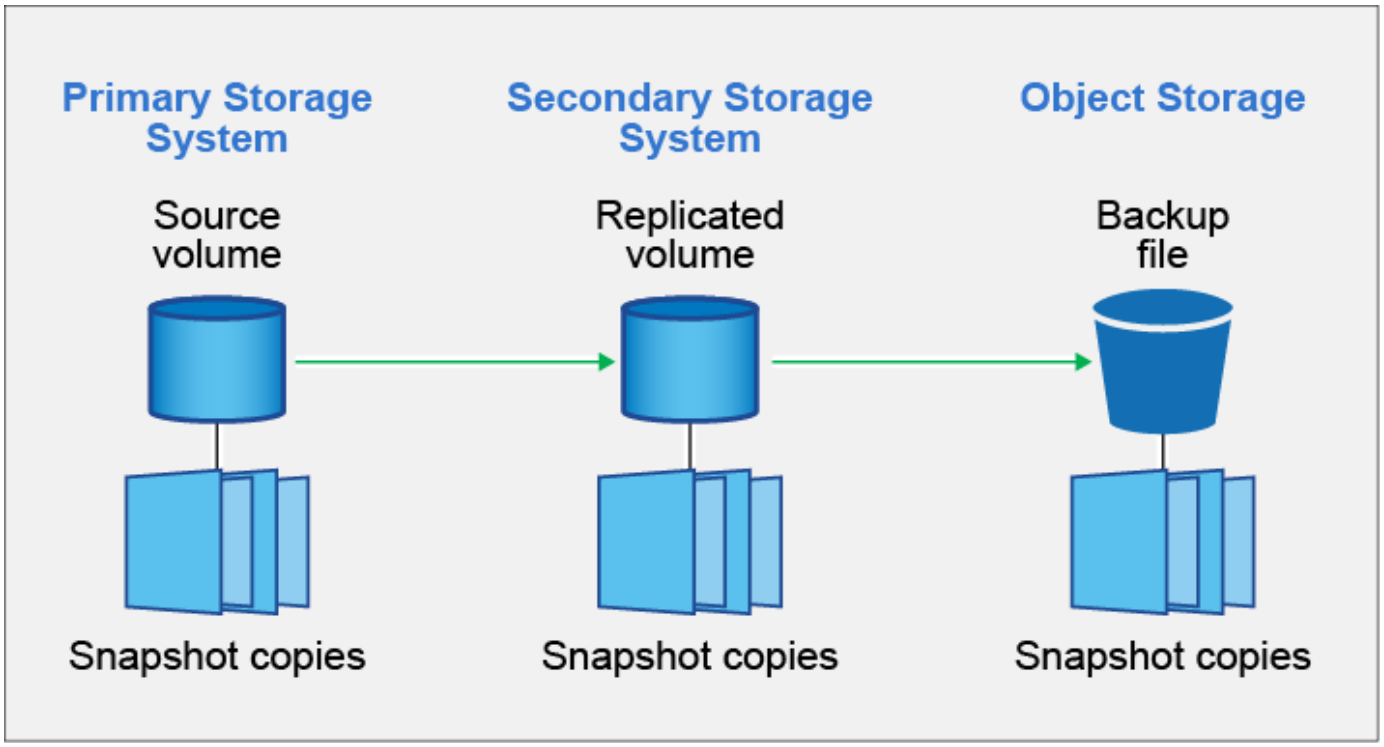
privata)

Quali funzionalità di protezione utilizzerai?

Prima di selezionare le funzionalità da utilizzare, ecco una breve spiegazione delle funzioni di ciascuna funzionalità e del tipo di protezione che offre.

Tipo di backup	Descrizione
Istantanea	Crea un'immagine di sola lettura e in un punto temporale specifico di un volume all'interno del volume di origine come snapshot. È possibile utilizzare lo snapshot per recuperare singoli file oppure per ripristinare l'intero contenuto di un volume.
Replicazione	Crea una copia secondaria dei dati su un altro sistema di archiviazione ONTAP e aggiorna continuamente i dati secondari. I tuoi dati saranno sempre aggiornati e disponibili ogni volta che ne avrai bisogno.
Backup su cloud	Crea backup dei tuoi dati sul cloud per proteggerli e archiviarli a lungo termine. Se necessario, è possibile ripristinare un volume, una cartella o singoli file dal backup sullo stesso sistema o su un sistema diverso.

Gli snapshot sono la base di tutti i metodi di backup e sono necessari per utilizzare il servizio di backup e ripristino. Uno snapshot è un'immagine di un volume, di sola lettura e memorizzata in un punto preciso nel tempo. L'immagine occupa uno spazio di archiviazione minimo e comporta un sovraccarico di prestazioni trascurabile, poiché registra solo le modifiche apportate ai file dall'ultima istantanea. Lo snapshot creato sul volume viene utilizzato per mantenere il volume replicato e il file di backup sincronizzati con le modifiche apportate al volume di origine, come mostrato nella figura.



È possibile scegliere di creare sia volumi replicati su un altro sistema di archiviazione ONTAP sia file di backup nel cloud. Oppure puoi semplicemente scegliere di creare volumi replicati o file di backup: la scelta è tua.

Riassumendo, ecco i flussi di protezione validi che puoi creare per i volumi nel tuo sistema ONTAP :

- Volume di origine → Snapshot → Volume replicato → File di backup
- Volume sorgente → Snapshot → File di backup
- Volume sorgente → Snapshot → Volume replicato

La creazione iniziale di un volume replicato o di un file di backup include una copia completa dei dati di origine: questo processo è denominato *trasferimento di base*. I trasferimenti successivi contengono solo copie differenziali dei dati di origine (lo snapshot).

Confronto tra i diversi metodi di backup

La tabella seguente mostra un confronto generalizzato dei tre metodi di backup. Sebbene lo spazio di archiviazione degli oggetti sia in genere meno costoso dell'archiviazione su disco in locale, se pensi di dover ripristinare frequentemente i dati dal cloud, le tariffe di uscita dei provider cloud possono ridurre parte dei tuoi risparmi. Dovrai stabilire con quale frequenza dovrai ripristinare i dati dai file di backup nel cloud.

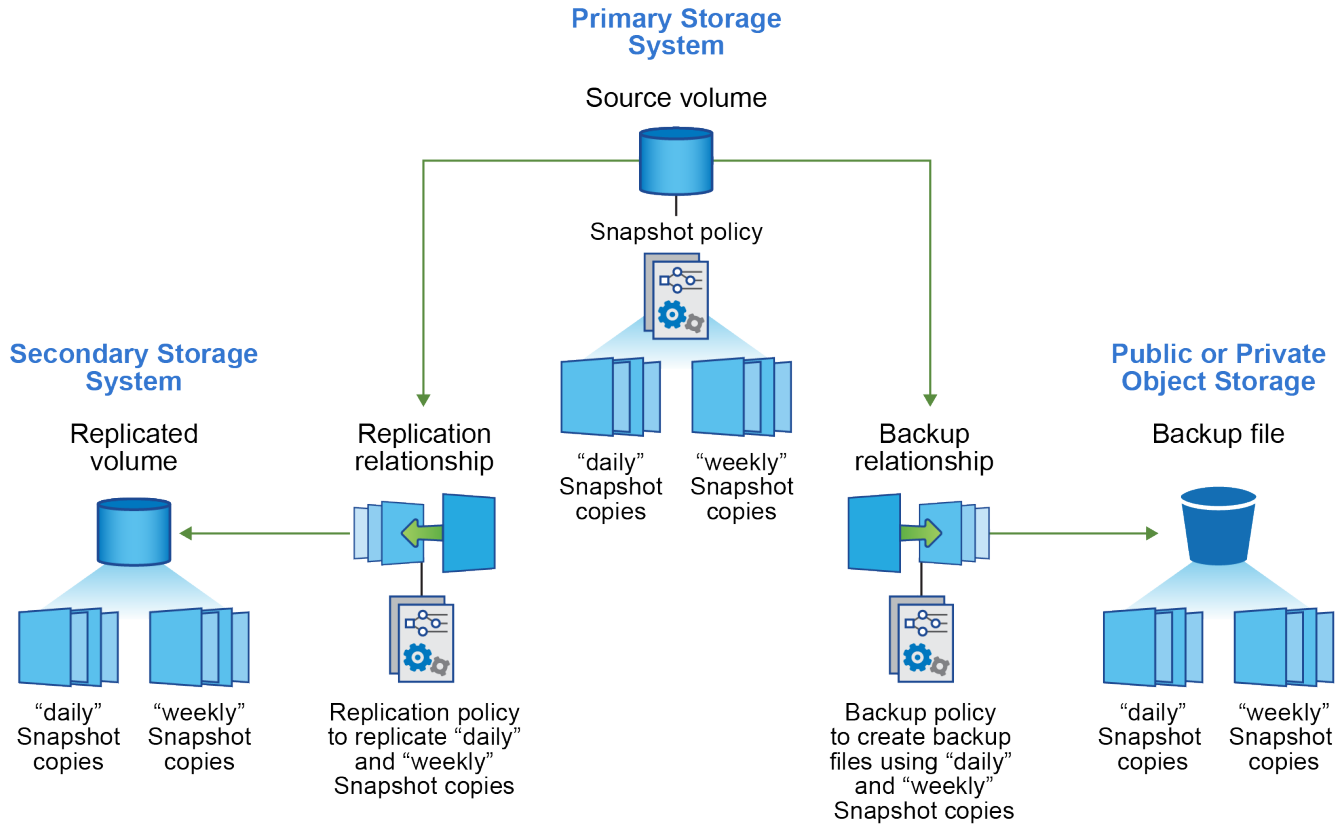
Oltre a questo criterio, l'archiviazione cloud offre opzioni di sicurezza aggiuntive se si utilizza la funzionalità DataLock e Ransomware Resilience, nonché ulteriori risparmi sui costi selezionando classi di archiviazione per i file di backup più vecchi. "Scopri di più sulla protezione DataLock e Ransomware e sulle impostazioni di archiviazione" .

Tipo di backup	Velocità di backup	Costo di backup	Ripristinare la velocità	Costo di ripristino
Istantanea	Alto	Basso (spazio su disco)	Alto	Basso
Replicazione	Medio	Mezzo (spazio su disco)	Medio	Mezzo (rete)
Backup su cloud	Basso	Basso (spazio oggetto)	Basso	Alto (commissioni del fornitore)

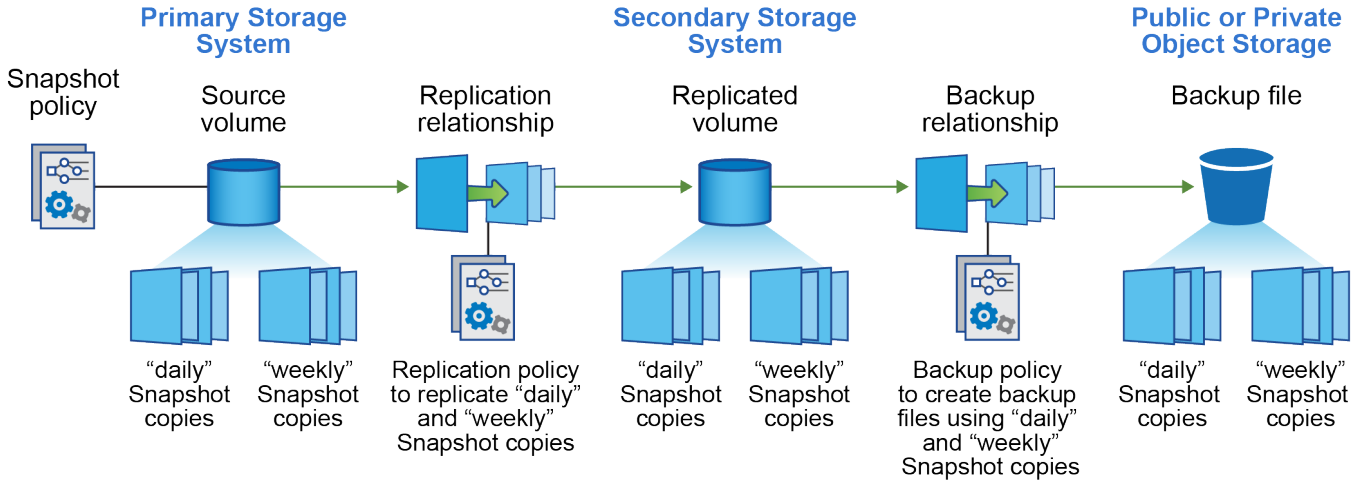
Quale architettura di backup utilizzerai?

Quando si creano sia volumi replicati sia file di backup, è possibile scegliere un'architettura fan-out o a cascata per eseguire il backup dei volumi.

Un'architettura **fan-out** trasferisce lo snapshot in modo indipendente sia al sistema di archiviazione di destinazione sia all'oggetto di backup nel cloud.



Un'architettura **a cascata** trasferisce prima lo snapshot al sistema di archiviazione di destinazione, dopodiché il sistema trasferisce la copia all'oggetto di backup nel cloud.



Confronto tra le diverse scelte architettoniche

Questa tabella fornisce un confronto tra le architetture fan-out e a cascata.

Fan-out	Cascata
Piccolo impatto sulle prestazioni del sistema sorgente perché invia snapshot a 2 sistemi distinti	Minore impatto sulle prestazioni del sistema di archiviazione di origine perché invia lo snapshot una sola volta

Fan-out	Cascata
Più facile da configurare perché tutte le policy, le reti e le configurazioni ONTAP vengono eseguite sul sistema sorgente	Richiede che alcune configurazioni di rete e ONTAP vengano eseguite anche dal sistema secondario.

Utilizzerai i criteri predefiniti per snapshot, repliche e backup?

Per creare i backup è possibile utilizzare i criteri predefiniti forniti da NetApp oppure creare criteri personalizzati. Quando si utilizza la procedura guidata di attivazione per abilitare il servizio di backup e ripristino per i volumi, è possibile selezionare tra i criteri predefiniti e qualsiasi altro criterio già esistente nel sistema (Cloud Volumes ONTAP o sistema ONTAP locale). Se si desidera utilizzare una policy diversa da quelle esistenti, è possibile crearla prima di iniziare o durante l'utilizzo della procedura guidata di attivazione.

- Il criterio di snapshot predefinito crea snapshot orari, giornalieri e settimanali, conservando 6 snapshot orari, 2 giornalieri e 2 settimanali.
- La policy di replica predefinita replica snapshot giornalieri e settimanali, conservando 7 snapshot giornalieri e 52 snapshot settimanali.
- La policy di backup predefinita replica snapshot giornalieri e settimanali, conservando 7 snapshot giornalieri e 52 settimanali.

Se si creano policy personalizzate per la replica o il backup, le etichette delle policy (ad esempio, "giornaliera" o "settimanale") devono corrispondere alle etichette presenti nelle policy snapshot, altrimenti i volumi replicati e i file di backup non verranno creati.

È possibile creare policy di archiviazione di snapshot, repliche e backup su oggetti nell'interfaccia utente NetApp Backup and Recovery . Vedi la sezione per"aggiunta di una nuova politica di backup" per i dettagli.

Oltre a utilizzare NetApp Backup and Recovery per creare policy personalizzate, è possibile utilizzare System Manager o l'interfaccia della riga di comando (CLI) ONTAP :

- "Creare un criterio di snapshot utilizzando System Manager o ONTAP CLI"
- "Creare una policy di replicazione utilizzando System Manager o ONTAP CLI"

Nota: quando si utilizza System Manager, selezionare **Asincrono** come tipo di policy per le policy di replica e selezionare **Asincrono** e **Backup su cloud** per le policy di backup su oggetto.

Ecco alcuni esempi di comandi ONTAP CLI che potrebbero essere utili se si creano policy personalizzate. Si noti che è necessario utilizzare il vserver *admin* (VM di archiviazione) come `<vserver_name>` in questi comandi.

Descrizione della politica	Comando
Criterio di snapshot semplice	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`
Backup semplice sul cloud	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Descrizione della politica	Comando
Backup su cloud con protezione DataLock e Ransomware	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
Backup su cloud con classe di archiviazione	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Semplice replica su un altro sistema di archiviazione	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Per il backup delle relazioni cloud è possibile utilizzare solo criteri di vault.

Dove risiedono le mie polizze?

Le policy di backup risiedono in posizioni diverse a seconda dell'architettura di backup che si intende utilizzare: Fan-out o Cascading. Le policy di replicazione e le policy di backup non sono progettate allo stesso modo perché le repliche accoppiano due sistemi di archiviazione ONTAP e il backup su oggetto utilizza un provider di archiviazione come destinazione.

- I criteri di snapshot risiedono sempre sul sistema di archiviazione primario.
- Le policy di replica risiedono sempre sul sistema di archiviazione secondario.
- I criteri di backup su oggetto vengono creati sul sistema in cui risiede il volume di origine: si tratta del cluster primario per le configurazioni fan-out e del cluster secondario per le configurazioni a cascata.

Queste differenze sono mostrate nella tabella.

Architettura	Politica di snapshot	Politica di replicazione	Politica di backup
Fan-out	Primario	Secondario	Primario
Cascata	Primario	Secondario	Secondario

Pertanto, se si prevede di creare policy personalizzate quando si utilizza l'architettura a cascata, sarà necessario creare le policy di replica e backup sugli oggetti sul sistema secondario in cui verranno creati i volumi replicati. Se si prevede di creare policy personalizzate quando si utilizza l'architettura fan-out, sarà necessario creare le policy di replica sul sistema secondario in cui verranno creati i volumi replicati e il backup sulle policy degli oggetti sul sistema primario.

Se si utilizzano i criteri predefiniti presenti su tutti i sistemi ONTAP , allora è tutto a posto.

Vuoi creare il tuo contenitore di archiviazione di oggetti

Quando si creano file di backup nell'archiviazione oggetti per un sistema, per impostazione predefinita il servizio di backup e ripristino crea il contenitore (bucket o account di archiviazione) per i file di backup nell'account di archiviazione oggetti configurato. Per impostazione predefinita, il bucket AWS o GCP è denominato "netapp-backup-<uuid>". L'account di archiviazione BLOB di Azure è denominato "netappbackup<uuid>".

È possibile creare autonomamente il contenitore nell'account del provider di oggetti se si desidera utilizzare un determinato prefisso o assegnare proprietà speciali. Se si desidera creare un contenitore personalizzato, è necessario crearlo prima di avviare la procedura guidata di attivazione. NetApp Backup and Recovery può utilizzare qualsiasi bucket e condividere i bucket. La procedura guidata di attivazione del backup rileverà automaticamente i contenitori forniti per l'account e le credenziali selezionati, in modo da poter selezionare quello che si desidera utilizzare.

Puoi creare il bucket dalla Console o dal tuo provider cloud.

- "Crea bucket Amazon S3 dalla console"
- "Creare account di archiviazione BLOB di Azure dalla console"
- "Crea bucket di Google Cloud Storage dalla Console"

Se si prevede di utilizzare un prefisso bucket diverso da "netapp-backup-xxxxxx", sarà necessario modificare le autorizzazioni S3 per il ruolo IAM dell'agente della console.

Impostazioni avanzate del bucket

Se intendi spostare i vecchi file di backup in un archivio o se intendi abilitare la protezione DataLock e Ransomware per bloccare i file di backup ed eseguirne la scansione alla ricerca di possibili ransomware, dovrai creare il contenitore con determinate impostazioni di configurazione:

- Al momento, l'archiviazione sui tuoi bucket è supportata nell'archiviazione AWS S3 quando utilizzi il software ONTAP 9.10.1 o versioni successive sui tuoi cluster. Per impostazione predefinita, i backup vengono avviati nella classe di archiviazione S3 *Standard*. Assicurati di creare il bucket con le regole del ciclo di vita appropriate:
  - Spostare gli oggetti nell'intero ambito del bucket in S3 *Standard-IA* dopo 30 giorni.
  - Sposta gli oggetti con il tag "smc_push_to_archive: true" in *Glacier Flexible Retrieval* (in precedenza S3 Glacier)
- La protezione DataLock e Ransomware è supportata nello storage AWS quando si utilizza il software ONTAP 9.11.1 o versione successiva sui cluster e nello storage Azure quando si utilizza il software ONTAP 9.12.1 o versione successiva.
  - Per AWS, è necessario abilitare il blocco degli oggetti sul bucket utilizzando un periodo di conservazione di 30 giorni.
  - Per Azure, è necessario creare la classe di archiviazione con supporto di immutabilità a livello di versione.

Quale modalità di distribuzione dell'agente della console stai utilizzando?

Se stai già utilizzando la Console per gestire il tuo storage, significa che è già stato installato un agente Console. Se intendi utilizzare lo stesso agente Console con NetApp Backup and Recovery, sei a posto. Se è necessario utilizzare un agente Console diverso, sarà necessario installarlo prima di avviare l'implementazione del backup e del ripristino.

NetApp Console offre diverse modalità di distribuzione che consentono di utilizzare la console in base alle proprie esigenze aziendali e di sicurezza. La *modalità standard* sfrutta il livello SaaS della console per fornire funzionalità complete, mentre la *modalità limitata* e la *modalità privata* sono disponibili per le organizzazioni con restrizioni di connettività.

"Scopri di più sulle modalità di distribuzione NetApp Console".

Supporto per siti con connettività Internet completa

Quando NetApp Backup and Recovery viene utilizzato in un sito con connettività Internet completa (nota anche come *modalità standard* o *modalità SaaS*), è possibile creare volumi replicati su qualsiasi sistema ONTAP locale o Cloud Volumes ONTAP gestito dalla Console, nonché creare file di backup su storage di oggetti in uno qualsiasi dei provider cloud supportati. "Visualizza l'elenco completo delle destinazioni di backup supportate" .

Per un elenco delle posizioni valide degli agenti della console, fare riferimento a una delle seguenti procedure di backup per il provider cloud in cui si prevede di creare i file di backup. Esistono alcune restrizioni per cui l'agente Console deve essere installato manualmente su una macchina Linux o distribuito in uno specifico provider cloud.

- "Esegui il backup dei dati Cloud Volumes ONTAP su Amazon S3"
- "Eseguire il backup dei dati Cloud Volumes ONTAP su Azure Blob"
- "Esegui il backup dei dati Cloud Volumes ONTAP su Google Cloud"
- "Eseguire il backup dei dati ONTAP locali su Amazon S3"
- "Eseguire il backup dei dati ONTAP locali su Azure Blob"
- "Esegui il backup dei dati ONTAP locali su Google Cloud"
- "Eseguire il backup dei dati ONTAP locali su StorageGRID"
- "Eseguire il backup ONTAP in sede su ONTAP S3"

Supporto per siti con connettività Internet limitata

NetApp Backup and Recovery può essere utilizzato in un sito con connettività Internet limitata (nota anche come *modalità limitata*) per eseguire il backup dei dati del volume. In questo caso, sarà necessario distribuire l'agente Console nella regione cloud di destinazione.

- È possibile eseguire il backup dei dati dai sistemi ONTAP locali o dai sistemi Cloud Volumes ONTAP installati nelle regioni commerciali AWS su Amazon S3. "Esegui il backup dei dati Cloud Volumes ONTAP su Amazon S3" .
- È possibile eseguire il backup dei dati dai sistemi ONTAP locali o dai sistemi Cloud Volumes ONTAP installati nelle aree commerciali di Azure su Azure Blob. "Eseguire il backup dei dati Cloud Volumes ONTAP su Azure Blob" .

Supporto per siti senza connettività Internet

NetApp Backup and Recovery può essere utilizzato in un sito senza connettività Internet (noto anche come *modalità privata* o *siti oscuri*) per eseguire il backup dei dati del volume. In questo caso, sarà necessario distribuire l'agente Console su un host Linux nello stesso sito.

La modalità privata BlueXP (interfaccia BlueXP legacy) viene in genere utilizzata con ambienti locali privi di connessione Internet e con regioni cloud sicure, tra cui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. NetApp continua a supportare questi ambienti con l'interfaccia legacy BlueXP . Per la documentazione sulla modalità privata nell'interfaccia legacy BlueXP , fare riferimento a "Documentazione PDF per la modalità privata BlueXP" .

- È possibile eseguire il backup dei dati dai sistemi ONTAP locali sui sistemi NetApp StorageGRID locali. "Eseguire il backup dei dati ONTAP locali su StorageGRID" .
- È possibile eseguire il backup dei dati dai sistemi ONTAP locali in sede ai sistemi ONTAP locali in sede o ai sistemi Cloud Volumes ONTAP configurati per l'archiviazione di oggetti S3. "Eseguire il backup dei dati ONTAP locali su ONTAP S3".

Gestisci le policy di backup per i volumi ONTAP con NetApp Backup and Recovery

Con NetApp Backup and Recovery, puoi utilizzare le policy di backup predefinite fornite da NetApp per creare i tuoi backup oppure creare policy personalizzate. Le policy regolano la frequenza del backup, l'ora in cui viene eseguito e il numero di file di backup conservati.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Quando si utilizza la procedura guidata di attivazione per abilitare il servizio di backup e ripristino per i volumi, è possibile selezionare tra i criteri predefiniti e qualsiasi altro criterio già esistente nel sistema (Cloud Volumes ONTAP o sistema ONTAP locale). Se si desidera utilizzare una policy diversa da quelle esistenti, è possibile crearla prima o durante l'utilizzo della procedura guidata di attivazione.

Per informazioni sulle policy di backup predefinite fornite, fare riferimento a"Pianifica il tuo percorso di protezione" .

NetApp Backup and Recovery fornisce tre tipi di backup dei dati ONTAP : snapshot, repliche e backup su storage di oggetti. Le loro policy risiedono in posizioni diverse in base all'architettura utilizzata e al tipo di backup:

Architettura	Posizione di archiviazione dei criteri di snapshot	Posizione di archiviazione della politica di replica	Backup nella posizione di archiviazione dei criteri degli oggetti
Fan-out	Primario	Secondario	Primario
Cascata	Primario	Secondario	Secondario

Crea criteri di backup utilizzando i seguenti strumenti in base al tuo ambiente, alle tue preferenze e al tipo di protezione:

- UI NetApp Console
- Interfaccia utente del gestore di sistema
- ONTAP CLI

Quando si utilizza System Manager, selezionare **Asincrono** come tipo di policy per le policy di replica e selezionare **Asincrono** e **Backup su cloud** per le policy di backup su oggetto.

Visualizza le policy per un sistema

1. Nell'interfaccia utente della console, seleziona **Volumi** > **Impostazioni di backup**.
2. Dalla pagina Impostazioni di backup, seleziona il sistema, seleziona **Azioni*** ••• **icona e seleziona *Gestione criteri**.

   Viene visualizzata la pagina di gestione delle policy. Per impostazione predefinita, vengono visualizzati i criteri snapshot.

3. Per visualizzare altre policy presenti nel sistema, selezionare **Replication Policies** o **Backup Policies**. Se le policy esistenti possono essere utilizzate per i tuoi piani di backup, sei a posto. Se hai bisogno di una polizza con caratteristiche diverse, puoi creare nuove polizze da questa pagina.

Creare politiche

È possibile creare policy che regolano gli snapshot, le repliche e i backup nell'archiviazione degli oggetti:

- Creare un criterio di snapshot prima di avviare lo snapshot
- Creare una politica di replicazione prima di avviare la replica
- Creare una policy di backup su storage di oggetti prima di avviare il backup

Creare un criterio di snapshot prima di avviare lo snapshot

Una parte della strategia 3-2-1 prevede la creazione di uno snapshot del volume sul sistema di archiviazione **primario**.

Una parte del processo di creazione delle policy prevede l'identificazione delle etichette snapshot e SnapMirror che indicano la pianificazione e la conservazione. È possibile utilizzare etichette predefinite o crearne di proprie.

Passi

1. Nell'interfaccia utente della console, seleziona **Volumi** > **Impostazioni di backup**.
2. Dalla pagina Impostazioni di backup, seleziona il sistema, seleziona **Azioni*** ••• **icona e seleziona *Gestione criteri**.

   Viene visualizzata la pagina di gestione delle policy.

3. Nella pagina Criteri, seleziona **Crea criterio** > **Crea criterio Snapshot**.
4. Specificare il nome della policy.
5. Selezionare la pianificazione o le pianificazioni degli snapshot. Puoi avere un massimo di 5 etichette. Oppure crea un programma.
6. Se scegli di creare una pianificazione:
   a. Seleziona la frequenza: oraria, giornaliera, settimanale, mensile o annuale.
   b. Specificare le etichette degli snapshot che indicano la pianificazione e la conservazione.
   c. Inserisci quando e con quale frequenza verrà scattata l'istantanea.
   d. Conservazione: immettere il numero di snapshot da conservare.
7. Seleziona **Crea**.

Esempio di policy snapshot utilizzando l'architettura a cascata

Questo esempio crea un criterio snapshot con due cluster:

1. Gruppo 1:
   a. Selezionare Cluster 1 nella pagina dei criteri.
   b. Ignorare le sezioni relative ai criteri di replica e backup su oggetto.
   c. Creare il criterio di snapshot.
2. Gruppo 2:
   a. Selezionare Cluster 2 nella pagina Policy.
   b. Ignorare la sezione relativa ai criteri di snapshot.
   c. Configurare i criteri di replica e backup sugli oggetti.

Creare una politica di replicazione prima di avviare la replica

La strategia 3-2-1 potrebbe includere la replica di un volume su un sistema di archiviazione diverso. La politica di replica risiede sul sistema di archiviazione **secondario**.

Passi

1. Nella pagina Criteri, seleziona **Crea criterio** > **Crea criterio di replicazione**.
2. Nella sezione Dettagli policy, specificare il nome della policy.
3. Specificare le etichette SnapMirror (massimo 5) che indicano la conservazione per ciascuna etichetta.
4. Specificare il programma di trasferimento.
5. Seleziona **Crea**.

Creare una policy di backup su storage di oggetti prima di avviare il backup

La strategia 3-2-1 potrebbe includere il backup di un volume su un archivio di oggetti.

Questa policy di archiviazione risiede in diverse posizioni del sistema di archiviazione a seconda dell'architettura di backup:

- Fan-out: sistema di archiviazione primario
- A cascata: sistema di stoccaggio secondario

Passi

1. Nella pagina Gestione policy, seleziona **Crea policy** > **Crea policy di backup**.
2. Nella sezione Dettagli policy, specificare il nome della policy.
3. Specificare le etichette SnapMirror (massimo 5) che indicano la conservazione per ciascuna etichetta.
4. Specificare le impostazioni, tra cui la pianificazione del trasferimento e quando archiviare i backup.
5. (Facoltativo) Per spostare i file di backup più vecchi in una classe di archiviazione o in un livello di accesso meno costosi dopo un certo numero di giorni, selezionare l'opzione **Archivia** e indicare il numero di giorni che devono trascorrere prima che i dati vengano archiviati. Inserisci **0** come "Archivia dopo giorni" per inviare il file di backup direttamente all'archivio.

   "Scopri di più sulle impostazioni di archiviazione".

6. (Facoltativo) Per proteggere i backup da modifiche o eliminazioni, seleziona l'opzione **Protezione DataLock e Ransomware**.

Se il cluster utilizza ONTAP 9.11.1 o versione successiva, è possibile scegliere di proteggere i backup dall'eliminazione configurando *DataLock* e *Protezione ransomware*.

"Scopri di più sulle impostazioni DataLock disponibili".

7. Seleziona **Crea**.

Modifica una policy

È possibile modificare uno snapshot personalizzato, una replica o un criterio di backup.

La modifica della policy di backup influisce su tutti i volumi che utilizzano tale policy.

Passi

1. Nella pagina di gestione delle policy, seleziona la policy, seleziona **Azioni*** **icona e seleziona *Modifica criterio**.

   Il processo è lo stesso per le policy di replica e backup.

2. Nella pagina Modifica policy, apporta le modifiche.
3. Seleziona **Salva**.

Elimina una policy

È possibile eliminare i criteri che non sono associati ad alcun volume.

Se una policy è associata a un volume e si desidera eliminarla, è necessario prima rimuoverla dal volume.

Passi

1. Nella pagina di gestione delle policy, seleziona la policy, seleziona **Azioni*** **icona e seleziona *Elimina criterio Snapshot**.
2. Seleziona **Elimina**.

Trova maggiori informazioni

Per istruzioni sulla creazione di policy tramite System Manager o ONTAP CLI, vedere quanto segue:

"Creare un criterio Snapshot utilizzando System Manager" "Creare un criterio Snapshot utilizzando ONTAP CLI" "Creare una policy di replicazione utilizzando System Manager" "Creare una policy di replicazione utilizzando ONTAP CLI" "Creare un backup per la policy di archiviazione degli oggetti utilizzando System Manager" "Creare un backup per la policy di archiviazione degli oggetti utilizzando ONTAP CLI"

Opzioni della policy di backup su oggetto in NetApp Backup and Recovery

NetApp Backup and Recovery consente di creare policy di backup con una varietà di impostazioni per i sistemi ONTAP locali e Cloud Volumes ONTAP .

Queste impostazioni dei criteri sono rilevanti solo per l'archiviazione di backup su oggetti. Nessuna di queste impostazioni influisce sui criteri di snapshot o replica.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Opzioni di pianificazione del backup

NetApp Backup and Recovery consente di creare più policy di backup con pianificazioni univoche per ciascun sistema (cluster). È possibile assegnare criteri di backup diversi ai volumi che hanno obiettivi del punto di ripristino (RPO) diversi.

Ogni criterio di backup fornisce una sezione per *Etichette e conservazione* che è possibile applicare ai file di backup. Si noti che il criterio Snapshot applicato al volume deve essere uno dei criteri riconosciuti da NetApp Backup and Recovery , altrimenti i file di backup non verranno creati.

La pianificazione è composta da due parti: l'etichetta e il valore di conservazione:

- L'**etichetta** definisce la frequenza con cui un file di backup viene creato (o aggiornato) dal volume. È possibile scegliere tra i seguenti tipi di etichette:
  - Puoi scegliere uno o più intervalli di tempo **orari**, **giornalieri**, **settimanali**, **mensili** e **annuali**.
  - È possibile selezionare una delle policy definite dal sistema che forniscono backup e conservazione per 3 mesi, 1 anno o 7 anni.
  - Se sono stati creati criteri di protezione del backup personalizzati sul cluster utilizzando ONTAP System Manager o ONTAP CLI, è possibile selezionare uno di tali criteri.
- Il valore **retention** definisce quanti file di backup per ogni etichetta (intervallo di tempo) vengono conservati. Una volta raggiunto il numero massimo di backup in una categoria o intervallo, i backup più vecchi vengono rimossi, in modo da avere sempre a disposizione i backup più recenti. In questo modo si risparmia anche sui costi di archiviazione, perché i backup obsoleti non continuano a occupare spazio nel cloud.

Ad esempio, supponiamo di creare una policy di backup che crea 7 backup **settimanali** e 12 backup **mensili**:

- ogni settimana e ogni mese viene creato un file di backup per il volume
- all'ottava settimana, il primo backup settimanale viene rimosso e viene aggiunto il nuovo backup settimanale per l'ottava settimana (mantenendo un massimo di 7 backup settimanali)
- al 13° mese, il primo backup mensile viene rimosso e viene aggiunto il nuovo backup mensile per il 13° mese (mantenendo un massimo di 12 backup mensili)

I backup annuali vengono eliminati automaticamente dal sistema di origine dopo essere stati trasferiti nell'archiviazione degli oggetti. Questo comportamento predefinito può essere modificato nella pagina Impostazioni avanzate del sistema.

Opzioni di protezione DataLock e Ransomware

NetApp Backup and Recovery fornisce supporto per la protezione da DataLock e Ransomware per i backup dei volumi. Queste funzionalità consentono di bloccare i file di backup e di analizzarli per rilevare eventuali ransomware presenti sui file di backup. Si tratta di un'impostazione facoltativa che puoi definire nei tuoi criteri di backup quando desideri una protezione extra per i backup dei volumi di un cluster.

Entrambe queste funzionalità proteggono i tuoi file di backup, così avrai sempre a disposizione un file di backup valido da cui recuperare i dati in caso di tentativo di attacco ransomware ai tuoi backup. È utile anche per soddisfare determinati requisiti normativi in base ai quali i backup devono essere bloccati e conservati per un determinato periodo di tempo. Quando l'opzione DataLock and Ransomware Resilience è abilitata, il bucket

cloud fornito come parte dell'attivazione di NetApp Backup and Recovery avrà il blocco degli oggetti e il controllo delle versioni degli oggetti abilitati.

Questa funzionalità non fornisce protezione per i volumi di origine, ma solo per i backup di tali volumi di origine. Utilizzare alcuni dei "protezioni anti-ransomware fornite da ONTAP" per proteggere i volumi sorgente.

- Se si prevede di utilizzare la protezione DataLock e Ransomware, è possibile abilitarla durante la creazione del primo criterio di backup e l'attivazione NetApp Backup and Recovery per quel cluster. Successivamente potrai abilitare o disabilitare la scansione ransomware utilizzando le impostazioni avanzate NetApp Backup and Recovery .
- Quando la Console esegue la scansione di un file di backup alla ricerca di ransomware durante il ripristino dei dati del volume, verranno addebitati costi di uscita aggiuntivi al provider cloud per accedere al contenuto del file di backup.

Che cos'è DataLock

Con questa funzionalità, è possibile bloccare gli snapshot cloud replicati tramite SnapMirror su Cloud e abilitare la funzionalità per rilevare un attacco ransomware e recuperare una copia coerente dello snapshot nell'archivio oggetti. Questa funzionalità è supportata su AWS, Azure, Google Cloud Platform e StorageGRID.

DataLock protegge i file di backup da modifiche o eliminazioni per un certo periodo di tempo, noto anche come *archiviazione immutabile*. Questa funzionalità utilizza la tecnologia del provider di archiviazione oggetti per il "blocco degli oggetti".

I provider cloud utilizzano una data di conservazione fino alla scadenza (RUD), calcolata in base al periodo di conservazione degli snapshot. Il periodo di conservazione degli snapshot viene calcolato in base all'etichetta e al conteggio di conservazione definiti nella policy di backup.

Il periodo minimo di conservazione degli snapshot è di 30 giorni. Diamo un'occhiata ad alcuni esempi di come funziona:

- Se si sceglie l'etichetta **Giornaliera** con conteggio di conservazione 20, il periodo di conservazione dello snapshot è di 20 giorni, che per impostazione predefinita è il minimo di 30 giorni.
- Se si sceglie l'etichetta **Settimanale** con conteggio di conservazione 4, il periodo di conservazione dello snapshot è di 28 giorni, che per impostazione predefinita è il minimo di 30 giorni.
- Se si sceglie l'etichetta **Mensile** con conteggio di conservazione 3, il periodo di conservazione dello snapshot è di 90 giorni.
- Se si sceglie l'etichetta **Annuale** con Conteggio conservazione 1, il periodo di conservazione dello snapshot è di 365 giorni.

Che cosa è la data di conservazione (RUD) e come viene calcolata?

La data di conservazione fino alla data (RUD) viene determinata in base al periodo di conservazione dello snapshot. La data di conservazione fino alla data viene calcolata sommando il periodo di conservazione dello snapshot e un buffer.

- Il buffer è il buffer per il tempo di trasferimento (3 giorni) + il buffer per l'ottimizzazione dei costi (28 giorni), per un totale di 31 giorni.
- La data minima di conservazione fino alla data è 30 giorni + 31 giorni di buffer = 61 giorni.

Ecco alcuni esempi:

- Se si crea una pianificazione di backup mensile con 12 conservazioni, i backup vengono bloccati per 12 mesi (più 31 giorni) prima di essere eliminati (sostituiti dal file di backup successivo).
- Se si crea un criterio di backup che prevede 30 backup giornalieri, 7 settimanali e 12 mensili, sono presenti tre periodi di conservazione bloccati:
  - I backup "30 giornalieri" vengono conservati per 61 giorni (30 giorni più 31 giorni di buffer),
  - I backup "settimanali" vengono conservati per 11 settimane (7 settimane più 31 giorni) e
  - I backup "12 mensili" vengono conservati per 12 mesi (più 31 giorni).
- Se si crea una pianificazione di backup oraria con 24 periodi di conservazione, si potrebbe pensare che i backup siano bloccati per 24 ore. Tuttavia, poiché questo periodo è inferiore al minimo di 30 giorni, ogni backup verrà bloccato e conservato per 61 giorni (30 giorni più 31 giorni di buffer).

I vecchi backup vengono eliminati dopo la scadenza del periodo di conservazione di DataLock, non dopo il periodo di conservazione dei criteri di backup.

L'impostazione di conservazione di DataLock sostituisce l'impostazione di conservazione dei criteri dei criteri di backup. Ciò potrebbe influire sui costi di archiviazione, poiché i file di backup verranno salvati nell'archivio oggetti per un periodo di tempo più lungo.

Abilita la protezione DataLock e Ransomware

È possibile abilitare la protezione DataLock e Ransomware quando si crea un criterio. Non è possibile abilitare, modificare o disabilitare questa opzione dopo aver creato il criterio.

1. Quando si crea un criterio, espandere la sezione **DataLock e Resilienza Ransomware**.
2. Scegli una delle seguenti opzioni:
   - **Nessuno**: la protezione DataLock e la resilienza al ransomware sono disabilitate.
   - **Sbloccato**: la protezione DataLock e la resilienza al ransomware sono abilitate. Gli utenti con autorizzazioni specifiche possono sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione.
   - **Bloccato**: la protezione DataLock e la resilienza al ransomware sono abilitate. Nessun utente può sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione. Ciò soddisfa pienamente la conformità normativa.

Fare riferimento a"Come aggiornare le opzioni di protezione Ransomware nella pagina Impostazioni avanzate" .

Che cos'è la protezione dal ransomware

La protezione ransomware analizza i file di backup per cercare prove di un attacco ransomware. Il rilevamento degli attacchi ransomware viene eseguito tramite un confronto di checksum. Se in un nuovo file di backup viene identificato un potenziale ransomware rispetto al file di backup precedente, il file di backup più recente viene sostituito dal file di backup più recente che non mostra alcun segno di attacco ransomware. (Il file identificato come vittima di un attacco ransomware viene eliminato 1 giorno dopo essere stato sostituito.)

Le scansioni vengono eseguite nelle seguenti situazioni:

- Le scansioni sugli oggetti di backup nel cloud vengono avviate subito dopo il loro trasferimento nell'archivio oggetti nel cloud. La scansione non viene eseguita sul file di backup quando viene scritto per la prima volta nell'archivio cloud, ma quando viene scritto il file di backup successivo.

- Le scansioni ransomware possono essere avviate quando il backup viene selezionato per il processo di ripristino.
- Le scansioni possono essere eseguite su richiesta in qualsiasi momento.

Come funziona il processo di recupero?

Quando viene rilevato un attacco ransomware, il servizio utilizza l'API REST Integrity Checker dell'agente Active Data Console per avviare il processo di ripristino. La versione più vecchia degli oggetti dati è la fonte della verità e viene trasformata nella versione corrente come parte del processo di ripristino.

Vediamo come funziona:

- In caso di attacco ransomware, il servizio tenta di sovrascrivere o eliminare l'oggetto nel bucket.
- Poiché l'archiviazione cloud è abilitata al controllo delle versioni, crea automaticamente una nuova versione dell'oggetto di backup. Se un oggetto viene eliminato con il controllo delle versioni attivato, viene contrassegnato come eliminato ma è ancora recuperabile. Se un oggetto viene sovrascritto, le versioni precedenti vengono memorizzate e contrassegnate.
- Quando viene avviata una scansione ransomware, i checksum vengono convalidati per entrambe le versioni dell'oggetto e confrontati. Se i checksum non sono coerenti, è stato rilevato un potenziale ransomware.
- Il processo di recupero prevede il ripristino dell'ultima copia valida conosciuta.

Sistemi supportati e provider di archiviazione di oggetti

È possibile abilitare la protezione DataLock e Ransomware sui volumi ONTAP dai seguenti sistemi quando si utilizza l'archiviazione di oggetti nei seguenti provider di cloud pubblici e privati.

Sistema sorgente	Destinazione del file di backup
Cloud Volumes ONTAP in AWS	Amazon S3
Cloud Volumes ONTAP in Azure	Blob azzurro
Cloud Volumes ONTAP in Google Cloud	Google Cloud
Sistema ONTAP in sede	Blob di Azure Amazon S3 Google Cloud NetApp StorageGRID

Requisiti

- Per AWS:
  - I tuoi cluster devono eseguire ONTAP 9.11.1 o versione successiva
  - L'agente della console può essere distribuito nel cloud o in sede
  - Le seguenti autorizzazioni S3 devono far parte del ruolo IAM che fornisce le autorizzazioni all'agente della console. Si trovano nella sezione "backupS3Policy" per la risorsa "arn:aws:s3:::netapp-backup-*":

Autorizzazioni AWS S3

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:EliminaOggetto
- s3:EliminaTaggingOggetto
- s3:OttieniRitenzioneOggetto
- s3:EliminaObjectVersionTagging
- s3:PutObject
- s3:OttieniOggetto
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:OttieniTaggingBucket
- s3:EliminaVersioneOggetto
- s3:ListBucketVersions
- s3:ElencoBucket
- s3:PutBucketTagging
- s3:OttieniTaggingOggetto
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:OttieniPosizioneBucket
- s3:GetObjectVersion

"Visualizza il formato JSON completo per la policy in cui puoi copiare e incollare le autorizzazioni richieste".

- Per Azure:
  - I tuoi cluster devono eseguire ONTAP 9.12.1 o versione successiva
  - L'agente della console può essere distribuito nel cloud o in sede
- Per Google Cloud:
  - I cluster devono eseguire ONTAP 9.17.1 o versione successiva
  - L'agente della console può essere distribuito nel cloud o in sede
- Per StorageGRID:

- I tuoi cluster devono eseguire ONTAP 9.11.1 o versione successiva
- I sistemi StorageGRID devono eseguire la versione 11.6.0.3 o successiva
- L'agente Console deve essere distribuito presso la tua sede (può essere installato in un sito con o senza accesso a Internet)
- Le seguenti autorizzazioni S3 devono far parte del ruolo IAM che fornisce le autorizzazioni all'agente della console:

Autorizzazioni StorageGRID S3

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:EliminaOggetto
- s3:EliminaTaggingOggetto
- s3:OttieniRitenzioneOggetto
- s3:EliminaObjectVersionTagging
- s3:PutObject
- s3:OttieniOggetto
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:OttieniTaggingBucket
- s3:EliminaVersioneOggetto
- s3:ListBucketVersions
- s3:ElencoBucket
- s3:PutBucketTagging
- s3:OttieniTaggingOggetto
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:PutObjectRetention
- s3:OttieniPosizioneBucket
- s3:GetObjectVersion

Restrizioni

- La funzionalità di protezione DataLock e Ransomware non è disponibile se è stata configurata l'archiviazione nel criterio di backup.
- L'opzione DataLock selezionata durante l'attivazione NetApp Backup and Recovery deve essere utilizzata

per tutti i criteri di backup per quel cluster.

- Non è possibile utilizzare più modalità DataLock su un singolo cluster.
- Se si abilita DataLock, tutti i backup dei volumi verranno bloccati. Non è possibile combinare backup di volumi bloccati e non bloccati per un singolo cluster.
- La protezione DataLock e Ransomware è applicabile ai backup di nuovi volumi utilizzando un criterio di backup con protezione DataLock e Ransomware abilitata. Successivamente potrai abilitare o disabilitare queste funzionalità utilizzando l'opzione Impostazioni avanzate.
- I volumi FlexGroup possono utilizzare la protezione DataLock e Ransomware solo se si utilizza ONTAP 9.13.1 o versione successiva.

Suggerimenti su come ridurre i costi di DataLock

È possibile abilitare o disabilitare la funzionalità Ransomware Scan mantenendo attiva la funzionalità DataLock. Per evitare costi aggiuntivi, puoi disattivare le scansioni ransomware pianificate. Ciò consente di personalizzare le impostazioni di sicurezza ed evitare di sostenere costi con il provider cloud.

Anche se le scansioni ransomware pianificate sono disattivate, è comunque possibile eseguire scansioni su richiesta quando necessario.

Puoi scegliere diversi livelli di protezione:

- **DataLock *senza* scansioni ransomware**: fornisce protezione per i dati di backup nell'archiviazione di destinazione che può essere in modalità Governance o Compliance.
  - **Modalità di governance**: offre agli amministratori la flessibilità di sovrascrivere o eliminare i dati protetti.
  - **Modalità di conformità**: garantisce la completa indelebilità fino alla scadenza del periodo di conservazione. Ciò contribuisce a soddisfare i più rigorosi requisiti di sicurezza dei dati degli ambienti altamente regolamentati. I dati non possono essere sovrascritti o modificati durante il loro ciclo di vita, garantendo il massimo livello di protezione per le copie di backup.

    Microsoft Azure utilizza invece una modalità di blocco e sblocco.

- **DataLock *con* scansioni ransomware**: fornisce un ulteriore livello di sicurezza per i tuoi dati. Questa funzione aiuta a rilevare eventuali tentativi di modifica delle copie di backup. In caso di tentativo, viene creata una nuova versione dei dati in modo discreto. La frequenza di scansione può essere modificata su 1, 2, 3, 4, 5, 6 o 7 giorni. Impostando le scansioni ogni 7 giorni, i costi diminuiscono notevolmente.

Per ulteriori suggerimenti su come ridurre i costi di DataLock, fare riferimento ahttps://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-NetApp-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475[]

Inoltre, è possibile ottenere preventivi per i costi associati a DataLock visitando il "Calcolatore del costo totale di proprietà (TCO) NetApp Backup and Recovery" .

Opzioni di archiviazione

Quando si utilizza AWS, Azure o Google Cloud Storage, è possibile spostare i file di backup più vecchi in una classe di archiviazione o in un livello di accesso meno costosi dopo un certo numero di giorni. Puoi anche scegliere di inviare immediatamente i tuoi file di backup all'archivio, senza che vengano salvati nell'archiviazione cloud standard. Basta inserire **0** come "Archivio dopo giorni" per inviare il file di backup direttamente all'archivio. Ciò può essere particolarmente utile per gli utenti che hanno raramente bisogno di accedere ai dati dai backup su cloud o per gli utenti che stanno sostituendo una soluzione di backup su nastro.

I dati nei livelli di archiviazione non sono accessibili immediatamente quando necessario e comportano costi di recupero più elevati, pertanto è necessario valutare la frequenza con cui potrebbe essere necessario ripristinare i dati dai file di backup prima di decidere di archiviare i file di backup.

- Anche se selezioni "0" per inviare tutti i blocchi di dati all'archiviazione cloud, i blocchi di metadati vengono sempre scritti nell'archiviazione cloud standard.
- L'archiviazione non può essere utilizzata se è stato abilitato DataLock.
- Non è possibile modificare i criteri di archiviazione dopo aver selezionato **0** giorni (archiviazione immediata).

Ogni criterio di backup fornisce una sezione per i *Criteri di archiviazione* che è possibile applicare ai file di backup.

- In AWS, i backup iniziano nella classe di archiviazione *Standard* e passano alla classe di archiviazione *Standard-Infrequent Access* dopo 30 giorni.

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile suddividere i backup più vecchi in storage *S3 Glacier* o *S3 Glacier Deep Archive*. "Scopri di più sullo storage di archiviazione AWS" .

  - Se non selezioni alcun livello di archivio nella tua prima policy di backup quando attivi NetApp Backup and Recovery, *S3 Glacier* sarà la tua unica opzione di archiviazione per le policy future.
  - Se selezioni *S3 Glacier* nella tua prima policy di backup, puoi passare al livello *S3 Glacier Deep Archive* per le future policy di backup per quel cluster.
  - Se selezioni *S3 Glacier Deep Archive* nella tua prima policy di backup, quel livello sarà l'unico livello di archivio disponibile per le future policy di backup per quel cluster.
- In Azure, i backup sono associati al livello di accesso *Cool*.

  Se il cluster utilizza ONTAP 9.10.1 o versione successiva, è possibile suddividere i backup più vecchi nell'archiviazione *Azure Archive*. "Scopri di più sull'archiviazione di Azure" .

- In GCP, i backup sono associati alla classe di archiviazione *Standard*.

  Se il cluster locale utilizza ONTAP 9.12.1 o versione successiva, è possibile scegliere di suddividere i backup più vecchi nello storage *Archive* nell'interfaccia utente NetApp Backup and Recovery dopo un certo numero di giorni per un'ulteriore ottimizzazione dei costi. "Scopri di più sull'archiviazione di Google" .

- In StorageGRID, i backup sono associati alla classe di archiviazione *Standard*.

  Se il cluster locale utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza la versione 11.4 o versione successiva, è possibile archiviare i file di backup più vecchi nell'archiviazione cloud pubblica.

  - Per AWS, è possibile suddividere i backup in livelli nello storage AWS *S3 Glacier* o *S3 Glacier Deep Archive*. "Scopri di più sullo storage di archiviazione AWS".
  - Per Azure, è possibile suddividere i backup più vecchi nell'archiviazione *Azure Archive*. "Scopri di più sull'archiviazione di Azure".

Gestisci le opzioni di archiviazione del backup su oggetto nelle impostazioni avanzate NetApp Backup and Recovery

È possibile modificare le impostazioni di archiviazione del backup su oggetto a livello di

cluster definite durante l'attivazione di NetApp Backup and Recovery per ciascun sistema ONTAP utilizzando la pagina Impostazioni avanzate. È anche possibile modificare alcune impostazioni applicate come impostazioni di backup "predefinite". Ciò include la modifica della velocità di trasferimento dei backup nell'archiviazione degli oggetti, se gli snapshot storici vengono esportati come file di backup e se si abilitano o disabilitano le scansioni ransomware per un sistema.

Queste impostazioni sono disponibili solo per l'archiviazione di backup su oggetti. Nessuna di queste impostazioni influisce sulle impostazioni di snapshot o replica.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Nella pagina Impostazioni avanzate è possibile modificare le seguenti opzioni:

- Modifica delle chiavi di archiviazione che consentono al sistema ONTAP di accedere all'archiviazione degli oggetti
- Modifica dello spazio IP ONTAP connesso all'archiviazione degli oggetti
- Modifica della larghezza di banda di rete assegnata per caricare i backup nell'archiviazione degli oggetti utilizzando l'opzione Velocità di trasferimento massima
- Modificare se gli snapshot storici vengono esportati come file di backup e inclusi nei file di backup di base iniziali per i volumi futuri
- Modificare se gli snapshot "annuali" vengono rimossi dal sistema sorgente
- Abilitazione o disabilitazione delle scansioni ransomware per un sistema, incluse le scansioni pianificate

Visualizza le impostazioni di backup a livello di cluster

È possibile visualizzare le impostazioni di sistema a livello di cluster e le impostazioni del provider per ciascun sistema.

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
3. Dalla pagina *Impostazioni di backup*, seleziona ••• per il sistema e seleziona **Configura impostazioni avanzate > Impostazioni di sistema** per visualizzare le impostazioni di sistema e **Configura impostazioni avanzate > Impostazioni del provider** per visualizzare le impostazioni del provider.

   La pagina risultante mostra le impostazioni correnti per quel sistema. Quando si visualizzano le impostazioni del provider, le impostazioni del provider mostrate sono rilevanti per il bucket selezionato nella parte superiore della pagina.

Si noti che alcune opzioni non sono disponibili in base alla versione di ONTAP sul cluster di origine e alla destinazione del provider cloud in cui risiedono i backup.

Modifica la larghezza di banda di rete disponibile per caricare i backup nell'archiviazione degli oggetti

Quando si attiva NetApp Backup and Recovery per un sistema, per impostazione predefinita ONTAP può utilizzare una quantità illimitata di larghezza di banda per trasferire i dati di backup dai volumi del sistema

all'archiviazione degli oggetti. Se noti che il traffico di backup influisce sui normali carichi di lavoro degli utenti, puoi limitare la quantità di larghezza di banda di rete utilizzata durante il trasferimento utilizzando l'opzione Velocità di trasferimento massima nella pagina Impostazioni avanzate.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per il sistema e selezionare **Configura impostazioni avanzate > Impostazioni di sistema**.
3. Nella pagina Impostazioni avanzate, espandi la sezione **Velocità di trasferimento massima**.
4. Scegli un valore compreso tra 1 e 1.000 Mbps come velocità di trasferimento massima.
5. Selezionare il pulsante di opzione **Limitato** e immettere la larghezza di banda massima utilizzabile, oppure selezionare **Illimitato** per indicare che non vi è alcun limite.
6. Selezionare **Applica**.

Questa impostazione non influisce sulla larghezza di banda assegnata ad altre relazioni di replicazione che potrebbero essere configurate per i volumi nel sistema.

Modifica se gli snapshot storici vengono esportati come file di backup

Se sono presenti snapshot locali per volumi che corrispondono all'etichetta di pianificazione del backup utilizzata in questo sistema (ad esempio, giornaliera, settimanale, ecc.), è possibile esportare tali snapshot storici nell'archiviazione degli oggetti come file di backup. Ciò consente di inizializzare i backup nel cloud spostando gli snapshot più vecchi nella copia di backup di base.

Si noti che questa opzione si applica solo ai nuovi file di backup per nuovi volumi di lettura/scrittura e non è supportata con volumi di protezione dati (DP).

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per il sistema e selezionare **Configura impostazioni avanzate > Impostazioni di sistema**.
3. Nella pagina Impostazioni avanzate, espandi la sezione **Esporta copie snapshot esistenti**.
4. Seleziona se desideri esportare gli snapshot esistenti.
5. Selezionare **Applica**.

Modifica se gli snapshot "annuali" vengono rimossi dal sistema sorgente

Quando si seleziona l'etichetta di backup "annuale" per un criterio di backup per uno qualsiasi dei volumi, lo snapshot creato è molto grande. Per impostazione predefinita, questi snapshot annuali vengono eliminati automaticamente dal sistema di origine dopo essere stati trasferiti nell'archiviazione degli oggetti. È possibile modificare questo comportamento predefinito dalla sezione Eliminazione snapshot annuale.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per il sistema e selezionare **Configura impostazioni avanzate > Impostazioni di sistema**.
3. Nella pagina Impostazioni avanzate, espandi la sezione **Eliminazione snapshot annuale**.
4. Selezionare **Disabilitato** per conservare gli snapshot annuali sul sistema di origine.

5. Selezionare **Applica**.

Abilita o disabilita le scansioni ransomware

Le scansioni di protezione dal ransomware sono abilitate per impostazione predefinita. L'impostazione predefinita per la frequenza di scansione è 7 giorni. La scansione avviene solo sull'ultimo snapshot.

Per i dettagli sulle opzioni DataLock e Ransomware Resilience, fare riferimento a"Opzioni di resilienza DataLock e Ransomware" .

È possibile modificare la programmazione in giorni o settimane oppure disattivarla, risparmiando sui costi.

L'attivazione delle scansioni ransomware comporterà costi aggiuntivi a seconda del provider cloud.

Se le scansioni ransomware pianificate sono disattivate, è comunque possibile eseguire scansioni su richiesta e la scansione durante un'operazione di ripristino verrà comunque eseguita.

Fare riferimento a"Gestire le politiche" per maggiori dettagli sulla gestione delle policy che implementano il rilevamento del ransomware.

Abilita o disabilita le scansioni ransomware per un sistema

È possibile abilitare o disabilitare le scansioni ransomware per un cluster.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per il sistema e selezionare **Configura impostazioni avanzate > Impostazioni di sistema**.
3. Nella pagina visualizzata, espandi la sezione **Scansione ransomware**.
4. Abilita o disabilita la **Scansione ransomware**.
5. Seleziona **Scansione ransomware pianificata**.
6. Facoltativamente, è possibile modificare la scansione predefinita ogni settimana in giorni o settimane.
7. Imposta la frequenza in giorni o settimane con cui deve essere eseguita la scansione.
8. Selezionare **Applica**.

Abilita o disabilita le scansioni ransomware per un provider

È possibile abilitare o disabilitare le scansioni ransomware a livello di provider tramite la pagina delle impostazioni del provider. Le impostazioni nella pagina sono pertinenti al bucket selezionato nella parte superiore della pagina.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, fare clic su ••• per il sistema e selezionare **Configura impostazioni avanzate > Impostazioni provider**.
3. Nella parte superiore della pagina risultante, seleziona il bucket per il quale desideri modificare le impostazioni.
4. Espandi la sezione **Scansione ransomware**.

5. Abilita o disabilita la **Scansione ransomware**.
6. Seleziona **Scansione ransomware pianificata**.
7. Facoltativamente, è possibile modificare la scansione predefinita ogni settimana in giorni o settimane.
8. Imposta la frequenza in giorni o settimane con cui deve essere eseguita la scansione.
9. Selezionare **Applica**.

Esegui il backup dei dati Cloud Volumes ONTAP su Amazon S3 con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi Cloud Volumes ONTAP su Amazon S3.

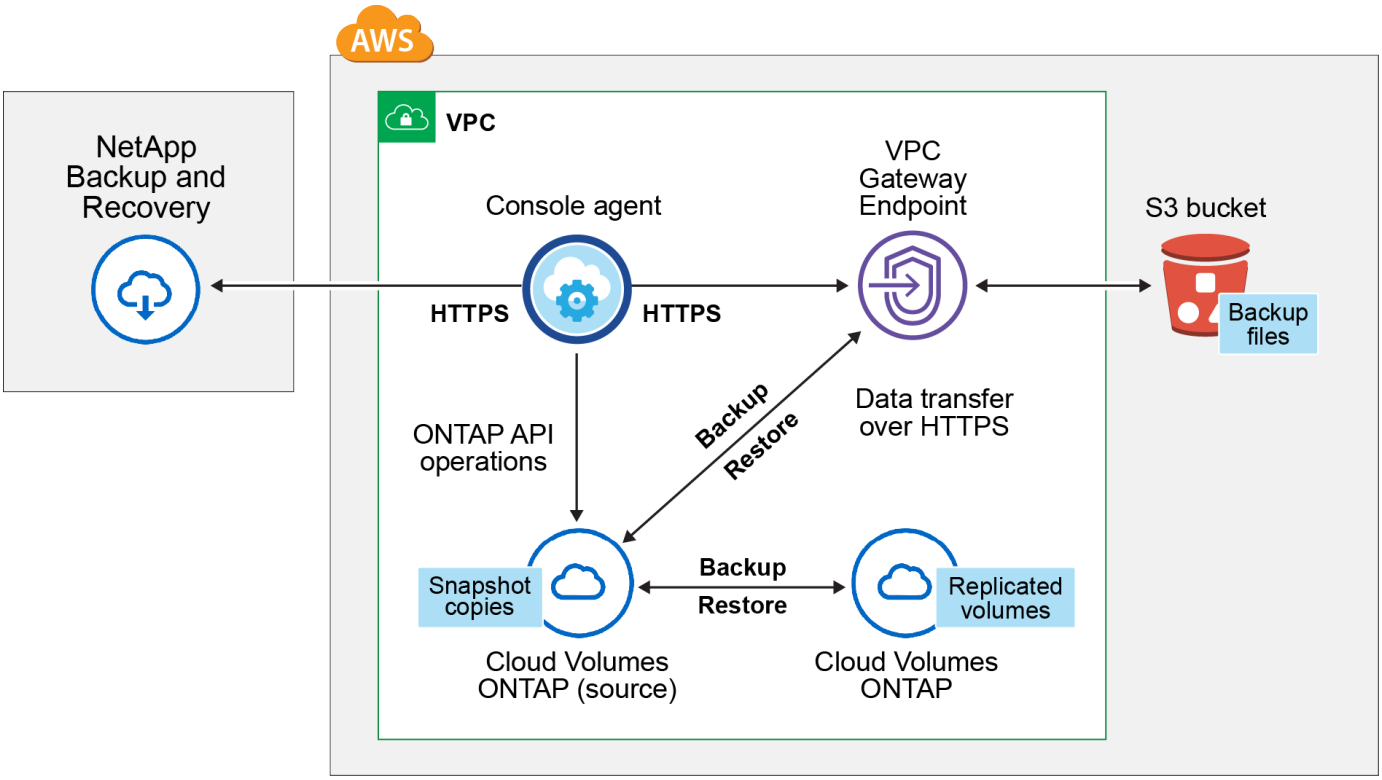
Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Verifica il supporto per la tua configurazione

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di iniziare il backup dei volumi su S3.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario predisporre tra di essi.

Facoltativamente, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.



L'endpoint del gateway VPC deve già esistere nella tua VPC. "Scopri di più sugli endpoint gateway" .

Versioni ONTAP supportate

Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.

Informazioni richieste per l'utilizzo di chiavi gestite dal cliente per la crittografia dei dati

Puoi scegliere le tue chiavi gestite dal cliente per la crittografia dei dati nella procedura guidata di attivazione anziché utilizzare le chiavi di crittografia Amazon S3 predefinite. In questo caso sarà necessario che le chiavi di crittografia gestite siano già impostate. "Scopri come usare le tue chiavi" .

Verificare i requisiti della licenza

Per le licenze NetApp Backup and Recovery PAYGO, è disponibile un abbonamento alla console in AWS Marketplace che consente le distribuzioni di Cloud Volumes ONTAP e NetApp Backup and Recovery. Devi "iscriviti a questo abbonamento NetApp Console" prima di abilitare NetApp Backup and Recovery. La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento.

Per un contratto annuale che consente di eseguire il backup sia dei dati Cloud Volumes ONTAP che dei dati ONTAP locali, è necessario abbonarsi da "Pagina AWS Marketplace" poi "associa l'abbonamento alle tue credenziali AWS" .

Per un contratto annuale che consente di raggruppare Cloud Volumes ONTAP e NetApp Backup and Recovery, è necessario impostare il contratto annuale quando si crea un sistema Cloud Volumes ONTAP . Questa opzione non consente di eseguire il backup dei dati locali.

Per la licenza BYOL NetApp Backup and Recovery , è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL" . È necessario utilizzare una licenza BYOL quando l'agente Console e il sistema Cloud Volumes ONTAP vengono distribuiti in un dark site.

Inoltre, è necessario disporre di un account AWS per lo spazio di archiviazione in cui verranno salvati i backup.

Prepara il tuo agente Console

L'agente Console deve essere installato in una regione AWS con accesso a Internet completo o limitato (modalità "standard" o "limitata"). "Per i dettagli, vedere le modalità di distribuzione NetApp Console" .

- "Scopri di più sugli agenti della console"
- "Distribuisci un agente Console in AWS in modalità standard (accesso completo a Internet)"
- "Installa l'agente Console in modalità limitata (accesso in uscita limitato)"

Verificare o aggiungere autorizzazioni all'agente della console

Il ruolo IAM che fornisce alla Console le autorizzazioni deve includere le autorizzazioni S3 dall'ultima versione "Politica della console" . Se la policy non contiene tutte queste autorizzazioni, vedere "Documentazione AWS: modifica delle policy IAM" .

Ecco le autorizzazioni specifiche previste dalla policy:

```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "s3:GetObjectVersionTagging",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetObjectVersionAcl",
    "s3:PutObjectTagging",
    "s3:DeleteObjectTagging",
    "s3:GetObjectRetention",
    "s3:DeleteObjectVersionTagging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:DeleteObjectVersion",
    "s3:GetObjectTagging",
    "s3:PutBucketVersioning",
    "s3:PutObjectVersionTagging",
    "s3:GetBucketVersioning",
    "s3:BypassGovernanceRetention",
    "s3:PutObjectRetention",
    "s3:GetObjectVersion",
    "athena:StartQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryExecution",
    "glue:GetDatabase",
    "glue:GetTable",
```

```
            "glue:CreateTable",
            "glue:CreateDatabase",
            "glue:GetPartitions",
            "glue:BatchCreatePartition",
            "glue:BatchDeletePartition"
        ],
        "Resource": [
            "arn:aws:s3:::netapp-backup-*"
        ]
    }
```

Quando si creano backup nelle regioni AWS Cina, è necessario modificare il nome della risorsa AWS "arn" in tutte le sezioni *Resource* nelle policy IAM da "aws" a "aws-cn"; ad esempio `arn:aws-cn:s3:::netapp-backup-*` .

Autorizzazioni Cloud Volumes ONTAP richieste

Quando il sistema Cloud Volumes ONTAP esegue il software ONTAP 9.12.1 o versione successiva, il ruolo IAM che fornisce le autorizzazioni a tale sistema deve includere un nuovo set di autorizzazioni S3 specifiche per NetApp Backup and Recovery dalla versione più recente "Criterio Cloud Volumes ONTAP" .

Se hai creato il sistema Cloud Volumes ONTAP utilizzando la versione 3.9.23 o successiva della console, queste autorizzazioni dovrebbero già far parte del ruolo IAM. Altrimenti sarà necessario aggiungere le autorizzazioni mancanti.

Regioni AWS supportate

NetApp Backup and Recovery è supportato in tutte le regioni AWS, comprese le regioni AWS GovCloud.

Configurazione richiesta per la creazione di backup in un account AWS diverso

Per impostazione predefinita, i backup vengono creati utilizzando lo stesso account utilizzato per il sistema Cloud Volumes ONTAP . Se desideri utilizzare un account AWS diverso per i tuoi backup, devi:

- Verificare che le autorizzazioni "s3:PutBucketPolicy" e "s3:PutBucketOwnershipControls" facciano parte del ruolo IAM che fornisce le autorizzazioni all'agente della console.
- Aggiungere le credenziali dell'account AWS di destinazione nella Console. "Scopri come fare" .
- Aggiungere le seguenti autorizzazioni nelle credenziali utente del secondo account:

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea dei bucket per te. Se desideri utilizzare i tuoi bucket, puoi crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione ONTAP" .

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste: in particolare, le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di sicurezza predefinito.
- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in subnet diverse, le subnet devono essere instradate insieme (questa è l'impostazione predefinita).

Abilita NetApp Backup and Recovery su Cloud Volumes ONTAP

Abilitare NetApp Backup and Recovery è semplice. I passaggi variano leggermente a seconda che si disponga di un sistema Cloud Volumes ONTAP esistente o di uno nuovo.

Abilita NetApp Backup and Recovery su un nuovo sistema

NetApp Backup and Recovery è abilitato per impostazione predefinita nella procedura guidata di sistema. Assicuratevi di mantenere l'opzione abilitata.

Vedere "Avvio di Cloud Volumes ONTAP in AWS" per requisiti e dettagli sulla creazione del sistema Cloud Volumes ONTAP .

Passi

1. Dalla pagina **Sistemi** della console, seleziona **Aggiungi sistema**, scegli il provider cloud e seleziona **Aggiungi nuovo**. Selezionare **Crea Cloud Volumes ONTAP**.
2. Seleziona **Amazon Web Services** come provider cloud, quindi scegli un singolo nodo o un sistema HA.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina Servizi, lascia il servizio abilitato e seleziona **Continua**.
5. Completare le pagine della procedura guidata per distribuire il sistema.

Risultato

NetApp Backup and Recovery è abilitato sul sistema. Dopo aver creato volumi su questi sistemi Cloud Volumes ONTAP , avviare NetApp Backup and Recovery e"attiva il backup su ogni volume che vuoi proteggere" .

Abilita NetApp Backup and Recovery su un sistema esistente

Abilita NetApp Backup and Recovery su un sistema esistente in qualsiasi momento direttamente dalla Console.

Passi

1. Dalla pagina **Sistemi** della console, seleziona il cluster e seleziona **Abilita** accanto a Backup e ripristino nel pannello di destra.

   Se la destinazione Amazon S3 per i backup esiste come cluster nella pagina **Sistemi**, è possibile trascinare il cluster sul sistema Amazon S3 per avviare la procedura guidata di configurazione.

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione AWS per i backup esiste come sistema nella pagina **Sistemi** della Console, è

possibile trascinare il cluster ONTAP nell'archivio oggetti AWS.

- Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni** ••• opzione icona e seleziona **Attiva protezione 3-2-1** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:
   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock . Tutti i volumi devono avere SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora, per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti. Quando si selezionano bucket esistenti o si configurano nuovi bucket, è possibile eseguire il backup dei volumi fino a un massimo di sei bucket per cluster.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario e da quello secondario all'archiviazione degli oggetti.
   - **Fan out**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario *e* dal primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .
3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

   a. Inserisci il nome della policy.
   b. Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   c. Seleziona **Crea**.
4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e la VM di archiviazione. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno.

     Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     i. Inserisci il nome della policy.
     ii. Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     iii. Seleziona **Crea**.

5. **Backup**: imposta le seguenti opzioni:
   - **Provider**: seleziona **Amazon Web Services**.
   - **Impostazioni del provider**: immettere i dettagli del provider e la regione in cui verranno archiviati i backup.

     Inserisci l'account AWS utilizzato per archiviare i backup. Può trattarsi di un account diverso da quello in cui risiede il sistema Cloud Volumes ONTAP .

     Se si desidera utilizzare un account AWS diverso per i backup, è necessario aggiungere le credenziali dell'account AWS di destinazione nella Console e aggiungere le autorizzazioni "s3:PutBucketPolicy" e "s3:PutBucketOwnershipControls" al ruolo IAM che fornisce le autorizzazioni alla Console.

     Selezionare la regione in cui verranno archiviati i backup. Può trattarsi di una regione diversa da quella in cui risiede il sistema Cloud Volumes ONTAP .

     Crea un nuovo bucket oppure selezionane uno esistente.

   - **Crittografia**: se hai creato un nuovo bucket, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia AWS predefinite oppure scegliere le chiavi gestite dal cliente dal tuo account AWS per gestire la crittografia dei tuoi dati. ("Scopri come utilizzare le tue chiavi di crittografia").

     Se si sceglie di utilizzare le chiavi gestite dal cliente, immettere il vault delle chiavi e le informazioni sulla chiave.

     > Se hai scelto un bucket esistente, le informazioni di crittografia sono già disponibili, quindi non è necessario inserirle ora.

   - **Rete**: configura le opzioni di rete per questo provider.
   - **Criterio di backup**: seleziona un criterio di archiviazione di backup su oggetto esistente o creane uno.

     > Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     i. Inserisci il nome della policy.
     ii. Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     iii. Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
     iv. Seleziona **Crea**.

   - **Esporta snapshot esistente**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliero, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.
6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Correggere automaticamente le etichette non corrispondenti su snapshot, replica e backup locali**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di snapshot, replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di archiviazione primario contenuti negli snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di archiviazione primario.

Viene creato un bucket S3 nell'account di servizio indicato dalla chiave di accesso S3 e dalla chiave segreta immesse, e i file di backup vengono archiviati lì.

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando"Pagina di monitoraggio dei lavori" .

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati Cloud Volumes ONTAP nell'archiviazione BLOB di Azure con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi Cloud Volumes ONTAP allo storage BLOB di Azure.

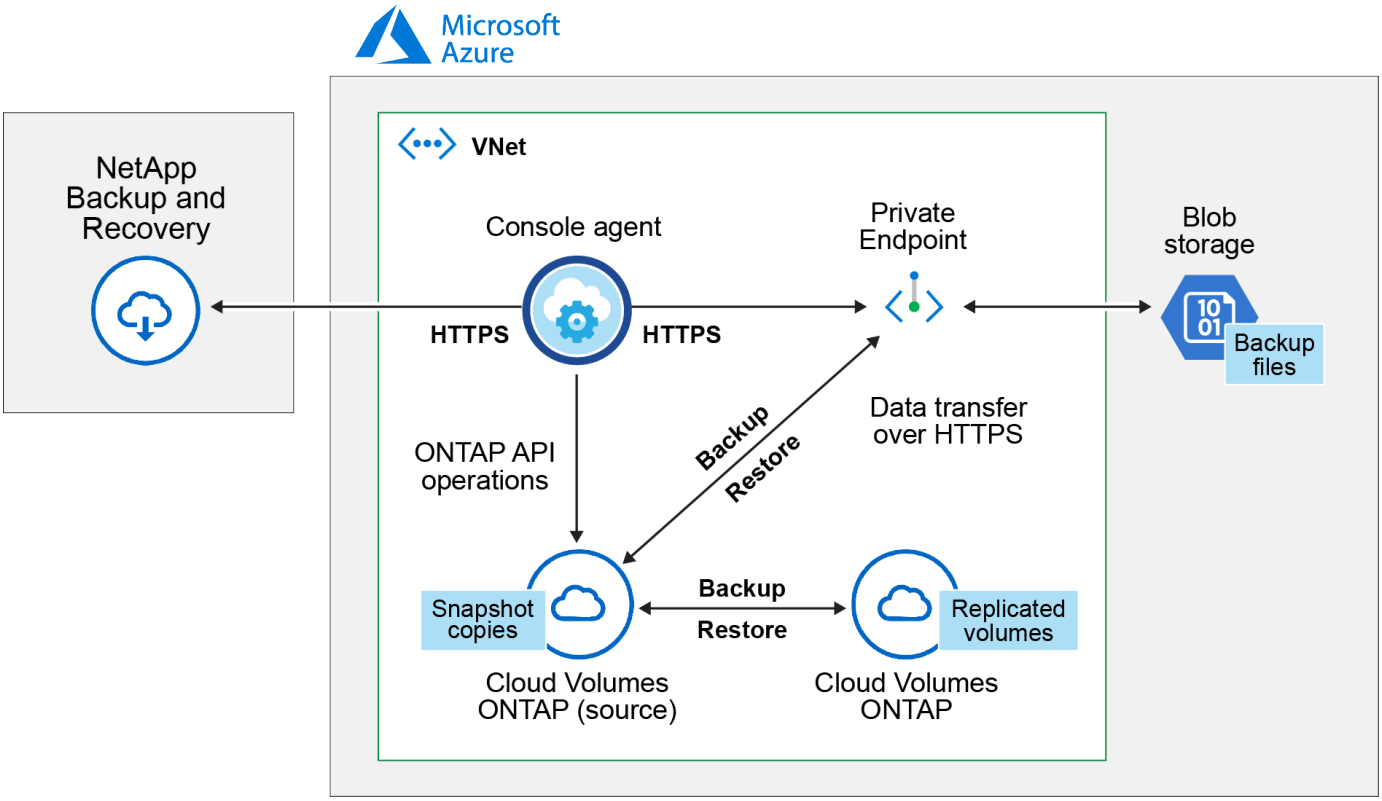
Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Verifica il supporto per la tua configurazione

Leggere i requisiti seguenti per assicurarsi di disporre di una configurazione supportata prima di iniziare il backup dei volumi nell'archiviazione BLOB di Azure.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario predisporre tra di essi.

Facoltativamente, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.



Versioni ONTAP supportate

Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.

Regioni di Azure supportate

NetApp Backup and Recovery è supportato in tutte le regioni di Azure, comprese le regioni di Azure Government.

Per impostazione predefinita, NetApp Backup and Recovery fornisce al contenitore Blob la ridondanza locale (LRS) per ottimizzare i costi. È possibile modificare questa impostazione in Ridondanza di zona (ZRS) dopo aver attivato NetApp Backup and Recovery se si desidera assicurarsi che i dati vengano replicati tra zone diverse. Consultare le istruzioni Microsoft per "modificando il modo in cui viene replicato il tuo account di archiviazione" .

Configurazione richiesta per la creazione di backup in una sottoscrizione Azure diversa

Per impostazione predefinita, i backup vengono creati utilizzando lo stesso abbonamento utilizzato per il sistema Cloud Volumes ONTAP .

Verificare i requisiti della licenza

Per le licenze NetApp Backup and Recovery PAYGO, è necessario un abbonamento tramite Azure Marketplace prima di abilitare NetApp Backup and Recovery. La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento. "Puoi iscriverti dalla pagina Dettagli e credenziali della procedura guidata di sistema" .

Per la licenza BYOL NetApp Backup and Recovery , è necessario il numero di serie di NetApp che consente di

utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL" . È necessario utilizzare una licenza BYOL quando l'agente Console e il sistema Cloud Volumes ONTAP vengono distribuiti in un sito oscuro ("modalità privata").

Inoltre, è necessario disporre di un abbonamento a Microsoft Azure per lo spazio di archiviazione in cui verranno salvati i backup.

Prepara il tuo agente Console

L'agente Console può essere installato in un'area di Azure con accesso a Internet completo o limitato (modalità "standard" o "limitata"). "Per i dettagli, vedere le modalità di distribuzione NetApp Console" .

- "Scopri di più sugli agenti della console"
- "Distribuisci un agente Console in Azure in modalità standard (accesso completo a Internet)"
- "Installa l'agente Console in modalità limitata (accesso in uscita limitato)"

Verificare o aggiungere autorizzazioni all'agente della console

Per utilizzare la funzionalità di ricerca e ripristino NetApp Backup and Recovery , è necessario disporre di autorizzazioni specifiche nel ruolo per l'agente della console, in modo che possa accedere ad Azure Synapse Workspace e all'account Data Lake Storage. Consultare le autorizzazioni riportate di seguito e seguire i passaggi se è necessario modificare la policy.

Prima di iniziare

- È necessario registrare il provider di risorse di Azure Synapse Analytics (denominato "Microsoft.Synapse") con la sottoscrizione. "Scopri come registrare questo fornitore di risorse per il tuo abbonamento" . Per registrare il fornitore di risorse, devi essere il **Proprietario** o il **Collaboratore** dell'abbonamento.
- La porta 1433 deve essere aperta per la comunicazione tra l'agente della console e i servizi Azure Synapse SQL.

Passi

1. Identificare il ruolo assegnato alla macchina virtuale dell'agente Console:
   a. Nel portale di Azure, aprire il servizio Macchine virtuali.
   b. Selezionare la macchina virtuale dell'agente Console.
   c. In Impostazioni, seleziona **Identità**.
   d. Selezionare **Assegnazioni di ruolo di Azure**.
   e. Prendi nota del ruolo personalizzato assegnato alla macchina virtuale dell'agente Console.
2. Aggiorna il ruolo personalizzato:
   a. Nel portale di Azure, apri la tua sottoscrizione di Azure.
   b. Selezionare **Controllo accessi (IAM) > Ruoli**.
   c. Selezionare i puntini di sospensione (**…**) per il ruolo personalizzato, quindi selezionare **Modifica**.
   d. Selezionare **JSON** e aggiungere le seguenti autorizzazioni:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Visualizza il formato JSON completo per la policy"

e. Seleziona **Revisiona + aggiorna** e poi seleziona **Aggiorna**.

Informazioni richieste per l'utilizzo di chiavi gestite dal cliente per la crittografia dei dati

È possibile utilizzare le chiavi gestite dal cliente per la crittografia dei dati nella procedura guidata di attivazione anziché utilizzare le chiavi di crittografia predefinite gestite da Microsoft. In questo caso, sarà necessario disporre della sottoscrizione di Azure, del nome del Key Vault e della chiave. "Scopri come usare le tue chiavi" .

NetApp Backup and Recovery supporta i *criteri di accesso di Azure*, il modello di autorizzazione *Azure role-based access control* (Azure RBAC) e il *Managed Hardware Security Model* (HSM) (fare riferimento a "Che cos'è Azure Key Vault Managed HSM?").

Crea il tuo account di archiviazione BLOB di Azure

Per impostazione predefinita, il servizio crea account di archiviazione per te. Se si desidera utilizzare account di archiviazione personali, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali account di archiviazione nella procedura guidata.

"Scopri di più sulla creazione dei tuoi account di archiviazione".

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione ONTAP" .

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste: in particolare, le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di sicurezza predefinito.
- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in subnet diverse, le subnet devono essere instradate insieme (questa è l'impostazione predefinita).

Abilita NetApp Backup and Recovery su Cloud Volumes ONTAP

Abilitare NetApp Backup and Recovery è semplice. I passaggi variano leggermente a seconda che si disponga di un sistema Cloud Volumes ONTAP esistente o di uno nuovo.

Abilita NetApp Backup and Recovery su un nuovo sistema

NetApp Backup and Recovery è abilitato per impostazione predefinita nella procedura guidata di sistema. Assicuratevi di mantenere l'opzione abilitata.

Vedere "Avvio di Cloud Volumes ONTAP in Azure" per requisiti e dettagli sulla creazione del sistema Cloud Volumes ONTAP .

Se si desidera scegliere il nome del gruppo di risorse, **disabilitare** NetApp Backup and Recovery durante la distribuzione Cloud Volumes ONTAP.

Passi

1. Dalla pagina **Sistemi** della console, seleziona **Aggiungi sistema**, scegli il provider cloud e seleziona **Aggiungi nuovo**. Selezionare **Crea Cloud Volumes ONTAP**.
2. Seleziona **Microsoft Azure** come provider cloud, quindi scegli un singolo nodo o un sistema HA.
3. Nella pagina Definisci credenziali di Azure, immetti il nome delle credenziali, l'ID client, il segreto client e l'ID directory, quindi seleziona **Continua**.
4. Compila la pagina Dettagli e credenziali e assicurati che sia attivo un abbonamento ad Azure Marketplace, quindi seleziona **Continua**.
5. Nella pagina Servizi, lascia il servizio abilitato e seleziona **Continua**.
6. Completare le pagine della procedura guidata per distribuire il sistema.

Risultato

NetApp Backup and Recovery è abilitato sul sistema. Dopo aver creato volumi su questi sistemi Cloud Volumes ONTAP , avviare NetApp Backup and Recovery e"attiva il backup su ogni volume che vuoi proteggere" .

Abilita NetApp Backup and Recovery su un sistema esistente

Abilita NetApp Backup and Recovery in qualsiasi momento direttamente dal sistema.

Passi

1. Dalla pagina **Sistemi** della console, seleziona il sistema e seleziona **Abilita** accanto a Backup e ripristino nel pannello di destra.

   Se la destinazione di Azure Blob per i backup esiste come sistema nella pagina **Sistemi** della console, è possibile trascinare il cluster sul sistema Azure Blob per avviare la procedura guidata di configurazione.

2. Completare le pagine della procedura guidata per distribuire NetApp Backup and Recovery.
3. Quando si desidera avviare i backup, continuare conAttiva i backup sui tuoi volumi ONTAP .

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi ancheMostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione di Azure per i backup esiste come sistema nella pagina **Sistemi**, è possibile trascinare il cluster ONTAP nell'archivio oggetti BLOB di Azure.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:

   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock . Tutti i volumi devono avere SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora, per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol . (I volumi FlexGroup possono essere selezionati solo uno alla volta.) Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

> Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario e da quello secondario all'archiviazione degli oggetti.
   - **Fan out**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario *e* dal primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .
3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno.

   > Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.
4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno.

     > Per creare una policy personalizzata prima di attivare la replica, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

- Inserisci il nome della policy.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: seleziona **Microsoft Azure**.
   - **Impostazioni del provider**: inserisci i dettagli del provider.

     Inserisci la regione in cui verranno archiviati i backup. Può trattarsi di una regione diversa da quella in cui risiede il sistema Cloud Volumes ONTAP .

     Crea un nuovo account di archiviazione oppure selezionane uno esistente.

     Immettere la sottoscrizione di Azure utilizzata per archiviare i backup. Potrebbe trattarsi di un abbonamento diverso da quello in cui risiede il sistema Cloud Volumes ONTAP .

     Crea il tuo gruppo di risorse che gestisce il contenitore BLOB oppure seleziona il tipo di gruppo di risorse e il gruppo.

     > Se vuoi proteggere i tuoi file di backup da modifiche o eliminazioni, assicurati che l'account di archiviazione sia stato creato con l'archiviazione immutabile abilitata utilizzando un periodo di conservazione di 30 giorni.

   - **Chiave di crittografia**: se hai creato un nuovo account di archiviazione di Azure, immetti le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Azure oppure scegliere le chiavi gestite dal cliente dal tuo account Azure per gestire la crittografia dei tuoi dati.

     Se si sceglie di utilizzare le chiavi gestite dal cliente, immettere il vault delle chiavi e le informazioni sulla chiave. "Impara a usare le tue chiavi" .

     > Se hai scelto un account di archiviazione Microsoft esistente, le informazioni sulla crittografia sono già disponibili, quindi non è necessario immetterle ora.

   - **Networking**: scegli lo spazio IP e se utilizzerai un endpoint privato. Per impostazione predefinita, l'endpoint privato è disabilitato.
     i. Lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
     ii. Facoltativamente, scegli se utilizzerai un endpoint privato di Azure precedentemente configurato. "Scopri di più sull'utilizzo di un endpoint privato di Azure" .
   - **Criterio di backup**: seleziona un criterio di archiviazione di backup su oggetto esistente.

     > Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     - Inserisci il nome della policy.
     - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di

backup su oggetto" .

- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Seleziona **Crea**.

◦ **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati di archiviazione primaria contenuti negli snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume primario.

Viene creato un contenitore di archiviazione BLOB nel gruppo di risorse immesso e i file di backup vengono archiviati lì.

Per impostazione predefinita, NetApp Backup and Recovery fornisce al contenitore Blob la ridondanza locale (LRS) per ottimizzare i costi. È possibile modificare questa impostazione in Ridondanza di zona (ZRS) se si desidera assicurarsi che i dati vengano replicati tra zone diverse. Consultare le istruzioni Microsoft per "modificando il modo in cui viene replicato il tuo account di archiviazione" .

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando"Pagina di monitoraggio dei lavori" .

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Cosa succederà ora?

- Puoi"gestire i file di backup e le policy di backup" . Ciò include l'avvio e l'interruzione dei backup, l'eliminazione dei backup, l'aggiunta e la modifica della pianificazione dei backup e altro ancora.
- Puoi"gestire le impostazioni di backup a livello di cluster" . Ciò include la modifica delle chiavi di archiviazione utilizzate ONTAP per accedere all'archiviazione cloud, la modifica della larghezza di banda di rete disponibile per caricare i backup nell'archiviazione degli oggetti, la modifica dell'impostazione di backup automatico per i volumi futuri e altro ancora.
- Puoi anche"ripristinare volumi, cartelle o singoli file da un file di backup" a un sistema Cloud Volumes ONTAP in AWS o a un sistema ONTAP locale.

Esegui il backup dei dati Cloud Volumes ONTAP su Google Cloud Storage con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi Cloud Volumes ONTAP su Google Cloud Storage.

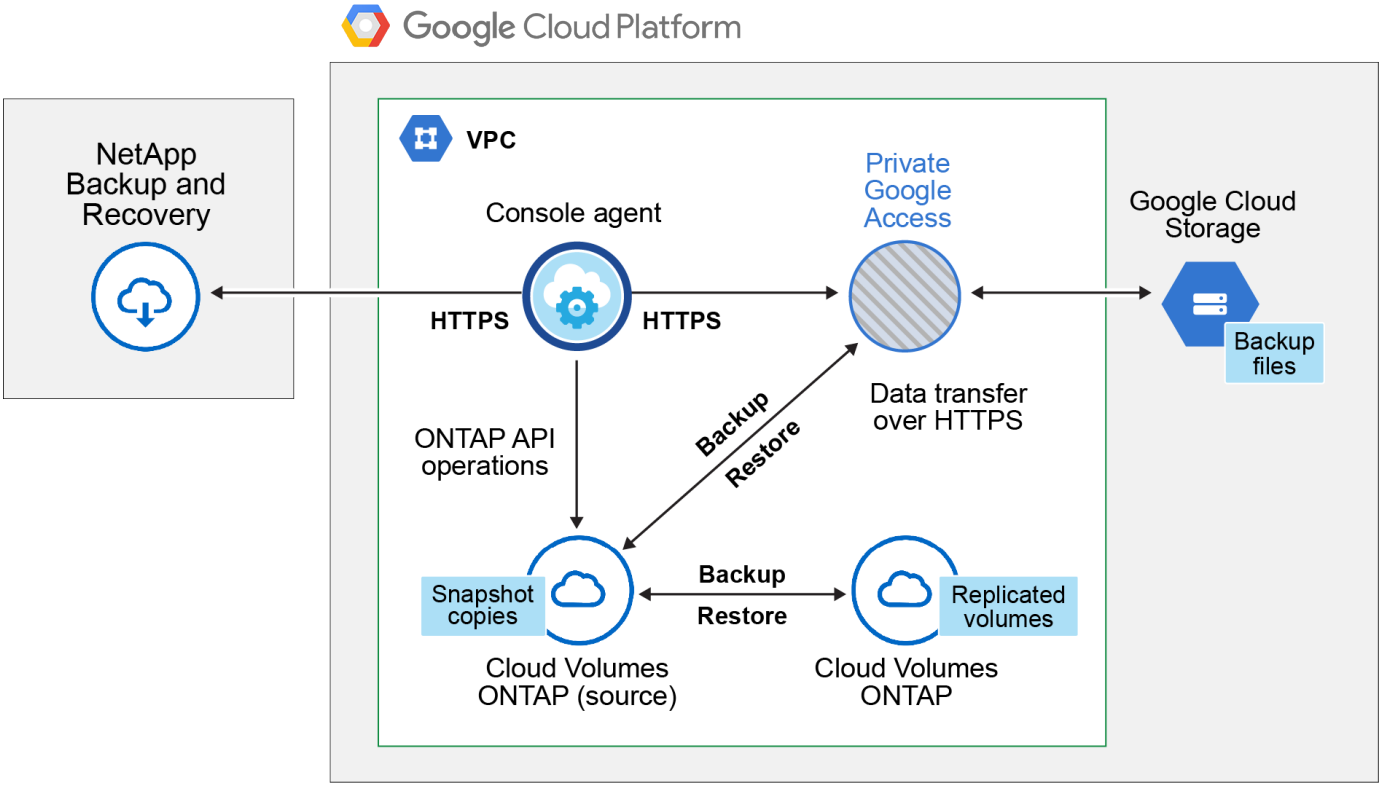
Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Verifica il supporto per la tua configurazione

Leggi i seguenti requisiti per assicurarti di disporre di una configurazione supportata prima di iniziare il backup dei volumi su Google Cloud Storage.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario predisporre tra di essi.

Facoltativamente, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.



Versioni ONTAP supportate

Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.

Regioni GCP supportate

NetApp Backup and Recovery è supportato in tutte le regioni GCP.

Account di servizio GCP

Devi disporre di un account di servizio nel tuo progetto Google Cloud che abbia il ruolo personalizzato. "Scopri come creare un account di servizio" .

Il ruolo di amministratore di archiviazione non è più necessario per l'account di servizio che consente a NetApp Backup and Recovery di accedere ai bucket di Google Cloud Storage.

Verificare i requisiti della licenza

Per le licenze NetApp Backup and Recovery PAYGO, è disponibile un abbonamento alla console in Google Marketplace che consente le distribuzioni di Cloud Volumes ONTAP e NetApp Backup and Recovery. Devi "iscriviti a questo abbonamento alla Console" prima di abilitare NetApp Backup and Recovery. La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento. "Puoi iscriverti dalla pagina Dettagli e credenziali della procedura guidata di sistema" .

Per la licenza BYOL NetApp Backup and Recovery , è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL" .

Inoltre, è necessario disporre di un abbonamento Google per lo spazio di archiviazione in cui verranno salvati i backup.

Prepara il tuo agente Console

L'agente Console deve essere installato in una regione Google con accesso a Internet.

- "Scopri di più sugli agenti della console"
- "Distribuisci un agente Console in Google Cloud"

Verificare o aggiungere autorizzazioni all'agente della console

Per utilizzare la funzionalità "Cerca e ripristina" NetApp Backup and Recovery , è necessario disporre di autorizzazioni specifiche nel ruolo per l'agente della console, in modo che possa accedere al servizio Google Cloud BigQuery. Consultare le autorizzazioni riportate di seguito e seguire i passaggi se è necessario modificare la policy.

Passi

1. Nel "Google Cloud Console" , vai alla pagina **Ruoli**.
2. Utilizzando l'elenco a discesa nella parte superiore della pagina, seleziona il progetto o l'organizzazione che contiene il ruolo che desideri modificare.
3. Seleziona un ruolo personalizzato.
4. Selezionare **Modifica ruolo** per aggiornare le autorizzazioni del ruolo.
5. Selezionare **Aggiungi autorizzazioni** per aggiungere le seguenti nuove autorizzazioni al ruolo.

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. Selezionare **Aggiorna** per salvare il ruolo modificato.

Informazioni richieste per l'utilizzo delle chiavi di crittografia gestite dal cliente (CMEK)

Puoi utilizzare le tue chiavi gestite dal cliente per la crittografia dei dati anziché le chiavi di crittografia predefinite gestite da Google. Sono supportate sia le chiavi interregionali che quelle interprogetto, quindi è possibile scegliere un progetto per un bucket diverso dal progetto della chiave CMEK. Se intendi utilizzare le tue chiavi gestite dal cliente:

- Per poter aggiungere queste informazioni nella procedura guidata di attivazione, è necessario disporre del Key Ring e del Key Name. "Scopri di più sulle chiavi di crittografia gestite dal cliente" .
- Sarà necessario verificare che le seguenti autorizzazioni richieste siano incluse nel ruolo dell'agente della console:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Dovrai verificare che l'API "Cloud Key Management Service (KMS)" di Google sia abilitata nel tuo progetto. Vedi il "Documentazione di Google Cloud: abilitazione delle API" per i dettagli.

Considerazioni CMEK:

- Sono supportate sia le chiavi HSM (supportate da hardware) sia quelle generate da software.
- Sono supportate sia le chiavi Cloud KMS appena create che quelle importate.
- Sono supportate solo le chiavi regionali; le chiavi globali non sono supportate.
- Attualmente è supportata solo la funzione "Crittografia/decifratura simmetrica".
- All'agente di servizio associato all'account di archiviazione viene assegnato il ruolo IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" da NetApp Backup and Recovery.

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea dei bucket per te. Se desideri utilizzare i tuoi bucket, puoi crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione ONTAP" .

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste: in particolare, le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di sicurezza predefinito.

- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in subnet diverse, le subnet devono essere instradate insieme (questa è l'impostazione predefinita).

Abilita NetApp Backup and Recovery su Cloud Volumes ONTAP

I passaggi per abilitare NetApp Backup and Recovery variano leggermente a seconda che si disponga di un sistema Cloud Volumes ONTAP esistente o di uno nuovo.

Abilita NetApp Backup and Recovery su un nuovo sistema

NetApp Backup and Recovery può essere abilitato una volta completata la procedura guidata di sistema per creare un nuovo sistema Cloud Volumes ONTAP .

È necessario che sia già configurato un account di servizio. Se non selezioni un account di servizio quando crei il sistema Cloud Volumes ONTAP , dovrai disattivare il sistema e aggiungere l'account di servizio a Cloud Volumes ONTAP dalla console GCP.

Vedere "Avvio di Cloud Volumes ONTAP in GCP" per requisiti e dettagli sulla creazione del sistema Cloud Volumes ONTAP .

Passi

1. Dalla pagina **Sistemi** della console, seleziona **Aggiungi sistema**, scegli il provider cloud e seleziona **Aggiungi nuovo**. Selezionare **Crea Cloud Volumes ONTAP**.
2. **Scegli una posizione**: seleziona **Google Cloud Platform**.
3. **Scegli tipo**: seleziona * Cloud Volumes ONTAP* (nodo singolo o alta disponibilità).
4. **Dettagli e credenziali**: Inserisci le seguenti informazioni:
   a. Fare clic su **Modifica progetto** e selezionare un nuovo progetto se quello che si desidera utilizzare è diverso dal progetto predefinito (in cui risiede l'agente della console).
   b. Specificare il nome del cluster.
   c. Abilitare l'opzione **Account di servizio** e selezionare l'Account di servizio che ha il ruolo di Amministratore di archiviazione predefinito. Ciò è necessario per abilitare i backup e la suddivisione in livelli.
   d. Specificare le credenziali.

      Assicurati di avere un abbonamento a GCP Marketplace.
5. **Servizi**: Lasciare abilitato NetApp Backup and Recovery e fare clic su **Continua**.
6. Completare le pagine della procedura guidata per distribuire il sistema come descritto in "Avvio di Cloud Volumes ONTAP in GCP" .

Risultato

NetApp Backup and Recovery è abilitato sul sistema. Dopo aver creato volumi su questi sistemi Cloud Volumes ONTAP , avviare NetApp Backup and Recovery e"attiva il backup su ogni volume che vuoi proteggere" .

Abilita NetApp Backup and Recovery su un sistema esistente

È possibile abilitare NetApp Backup and Recovery in qualsiasi momento direttamente dal sistema.

Passi

1. Dalla pagina **Sistemi** della console, seleziona il sistema e seleziona **Abilita** accanto a Backup e ripristino nel pannello di destra.

   Se la destinazione di Google Cloud Storage per i backup esiste come sistema nella pagina **Sistemi** della console, puoi trascinare il cluster sul sistema Google Cloud Storage per avviare la procedura guidata di configurazione.

Prepara Google Cloud Storage come destinazione di backup

Per preparare Google Cloud Storage come destinazione di backup, sono necessari i seguenti passaggi:

- Imposta le autorizzazioni.
- (Facoltativo) Crea i tuoi bucket. (Se lo desideri, il servizio creerà dei bucket per te.)
- (Facoltativo) Impostare le chiavi gestite dal cliente per la crittografia dei dati

Imposta i permessi

È necessario fornire le chiavi di accesso all'archiviazione per un account di servizio che dispone di autorizzazioni specifiche utilizzando un ruolo personalizzato. Un account di servizio consente a NetApp Backup and Recovery di autenticare e accedere ai bucket di Cloud Storage utilizzati per archiviare i backup. Le chiavi sono necessarie affinché Google Cloud Storage sappia chi sta effettuando la richiesta.

Passi

1. Nel "Google Cloud Console" , vai alla pagina **Ruoli**.
2. "Crea un nuovo ruolo"con le seguenti autorizzazioni:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Nella console di Google Cloud, "vai alla pagina Account di servizio" .
4. Seleziona il tuo progetto Cloud.
5. Seleziona **Crea account di servizio** e fornisci le informazioni richieste:
   a. **Dettagli dell'account di servizio**: inserisci un nome e una descrizione.
   b. **Concedi a questo account di servizio l'accesso al progetto**: seleziona il ruolo personalizzato appena creato.
   c. Selezionare **Fatto**.

6. Vai a "Impostazioni di archiviazione GCP" e creare chiavi di accesso per l'account di servizio:
   a. Seleziona un progetto e seleziona **Interoperabilità**. Se non lo hai già fatto, seleziona **Abilita accesso interoperabilità**.
   b. In **Chiavi di accesso per gli account di servizio**, seleziona **Crea una chiave per un account di servizio**, seleziona l'account di servizio appena creato e fai clic su **Crea chiave**.

      Sarà necessario immettere le chiavi in NetApp Backup and Recovery in un secondo momento, quando si configura il servizio di backup.

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea dei bucket per te. In alternativa, se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Impostare le chiavi di crittografia gestite dal cliente (CMEK) per la crittografia dei dati

Puoi utilizzare le tue chiavi gestite dal cliente per la crittografia dei dati anziché le chiavi di crittografia predefinite gestite da Google. Sono supportate sia le chiavi interregionali che quelle interprogetto, quindi è possibile scegliere un progetto per un bucket diverso dal progetto della chiave CMEK.

Se intendi utilizzare le tue chiavi gestite dal cliente:

- Per poter aggiungere queste informazioni nella procedura guidata di attivazione, è necessario disporre del Key Ring e del Key Name. "Scopri di più sulle chiavi di crittografia gestite dal cliente" .
- Sarà necessario verificare che le seguenti autorizzazioni richieste siano incluse nel ruolo dell'agente della console:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Dovrai verificare che l'API "Cloud Key Management Service (KMS)" di Google sia abilitata nel tuo progetto. Vedi il "Documentazione di Google Cloud: abilitazione delle API" per i dettagli.

Considerazioni CMEK:

- Sono supportate sia le chiavi HSM (supportate da hardware) sia quelle generate da software.
- Sono supportate sia le chiavi Cloud KMS appena create che quelle importate.
- Sono supportate solo le chiavi regionali, le chiavi globali non sono supportate.
- Attualmente è supportata solo la funzione "Crittografia/decifratura simmetrica".

- All’agente di servizio associato all’account di archiviazione viene assegnato il ruolo IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" da NetApp Backup and Recovery.

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l’attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione GCP per i backup esiste come sistema nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nell’archivio oggetti GCP.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** ••• **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:

   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l’opzione **Aggiungi un agente Console**. Fare riferimento a Prepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come "attiva il backup per volumi aggiuntivi nel sistema" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock . Tutti i volumi devono avere SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

Tieni presente che se ai volumi scelti sono già applicati criteri di snapshot o di replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora, per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

  Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario e da quello secondario all'archiviazione degli oggetti.
   - **Fan out**: le informazioni fluiscono dal sistema di archiviazione primario a quello secondario *e* dal primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno.

   Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Per i criteri di backup su oggetto, configurare Datalock e Ransomware Resilience. Per i dettagli su Datalock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
   - Seleziona **Crea**.

4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno.

     Per creare una policy personalizzata prima di attivare la replica, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: seleziona **Google Cloud**.
   - **Impostazioni del provider**: immettere i dettagli del provider e la regione in cui verranno archiviati i backup.

     Crea un nuovo bucket oppure selezionane uno esistente.

   - **Chiave di crittografia**: se hai creato un nuovo bucket Google, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Google Cloud oppure scegliere le chiavi gestite dal cliente dal tuo account Google per gestire la crittografia dei tuoi dati.

     Se si sceglie di utilizzare le chiavi gestite dal cliente, immettere il vault delle chiavi e le informazioni sulla chiave.

     Se hai scelto un bucket Google Cloud esistente, le informazioni sulla crittografia sono già disponibili, quindi non è necessario inserirle ora.

   - **Criterio di backup**: seleziona un criterio di archiviazione di backup su oggetto esistente o creane uno.

     Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

- Inserisci il nome della policy.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Seleziona **Crea**.

◦ **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di archiviazione primario contenuti negli snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume del sistema di archiviazione primario.

Viene creato un bucket di Google Cloud Storage nell'account di servizio indicato dalla chiave di accesso e dalla chiave segreta di Google immesse, dove vengono archiviati i file di backup.

Per impostazione predefinita, i backup sono associati alla classe di archiviazione *Standard*. È possibile utilizzare le classi di archiviazione più economiche *Nearline*, *Coldline* o *Archive*. Tuttavia, la classe di archiviazione viene configurata tramite Google e non tramite l'interfaccia utente NetApp Backup and Recovery . Vedi l'argomento di Google "Modifica della classe di archiviazione predefinita di un bucket" per i dettagli.

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando"Pagina di monitoraggio dei lavori" .

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Cosa succederà ora?

- Puoi"gestire i file di backup e le policy di backup" . Ciò include l'avvio e l'interruzione dei backup, l'eliminazione dei backup, l'aggiunta e la modifica della pianificazione dei backup e altro ancora.
- Puoi"gestire le impostazioni di backup a livello di cluster" . Ciò include la modifica delle chiavi di archiviazione utilizzate ONTAP per accedere all'archiviazione cloud, la modifica della larghezza di banda di rete disponibile per caricare i backup nell'archiviazione degli oggetti, la modifica dell'impostazione di backup automatico per i volumi futuri e altro ancora.
- Puoi anche"ripristinare volumi, cartelle o singoli file da un file di backup" a un sistema Cloud Volumes ONTAP in AWS o a un sistema ONTAP locale.

Esegui il backup dei dati ONTAP locali su Amazon S3 con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP locali a un sistema di storage secondario e allo storage cloud Amazon S3.

I "sistemi ONTAP on-premises" includono i sistemi FAS, AFF e ONTAP Select .

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

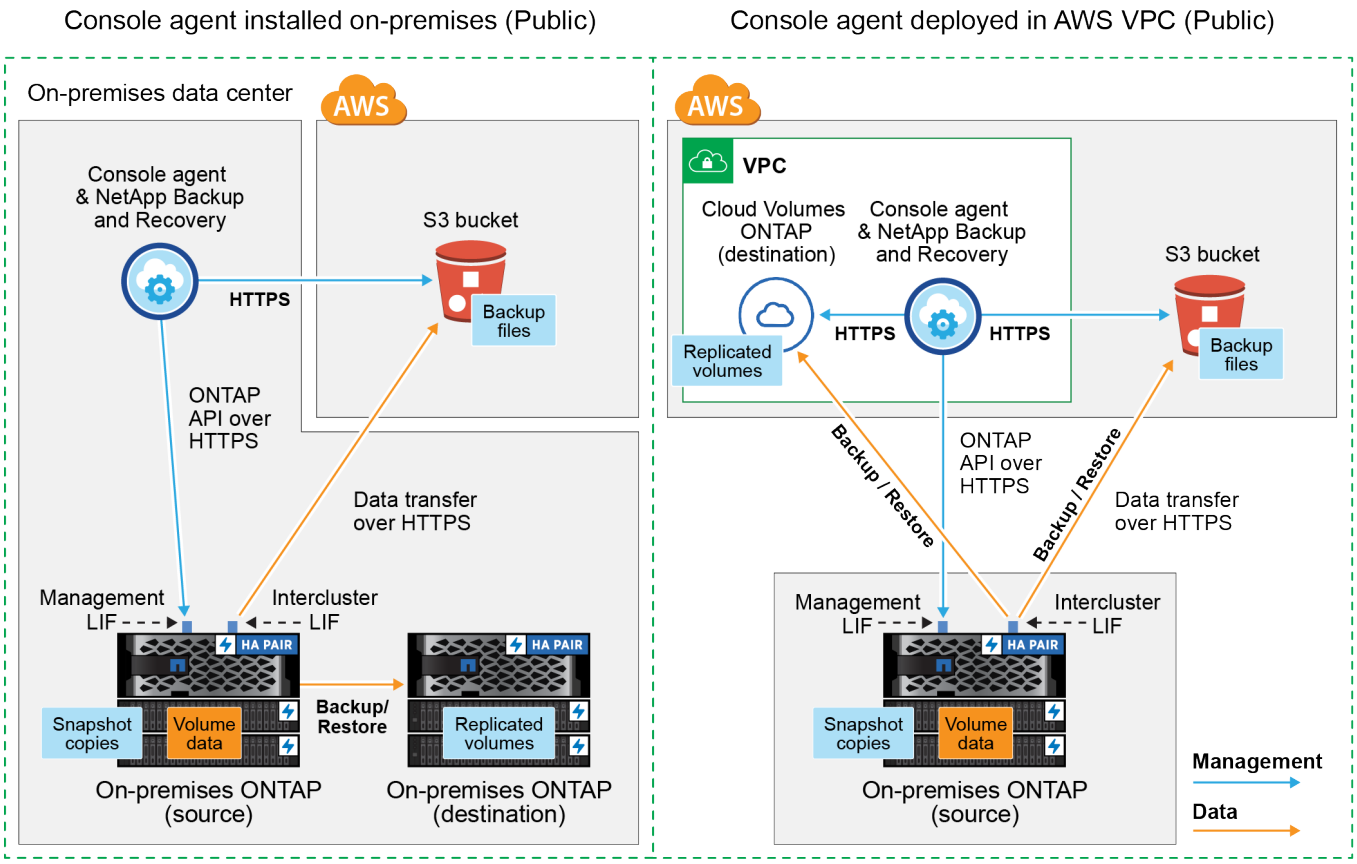
Identificare il metodo di connessione

Scegli quale dei due metodi di connessione utilizzerai durante la configurazione dei backup dai sistemi ONTAP locali ad AWS S3.

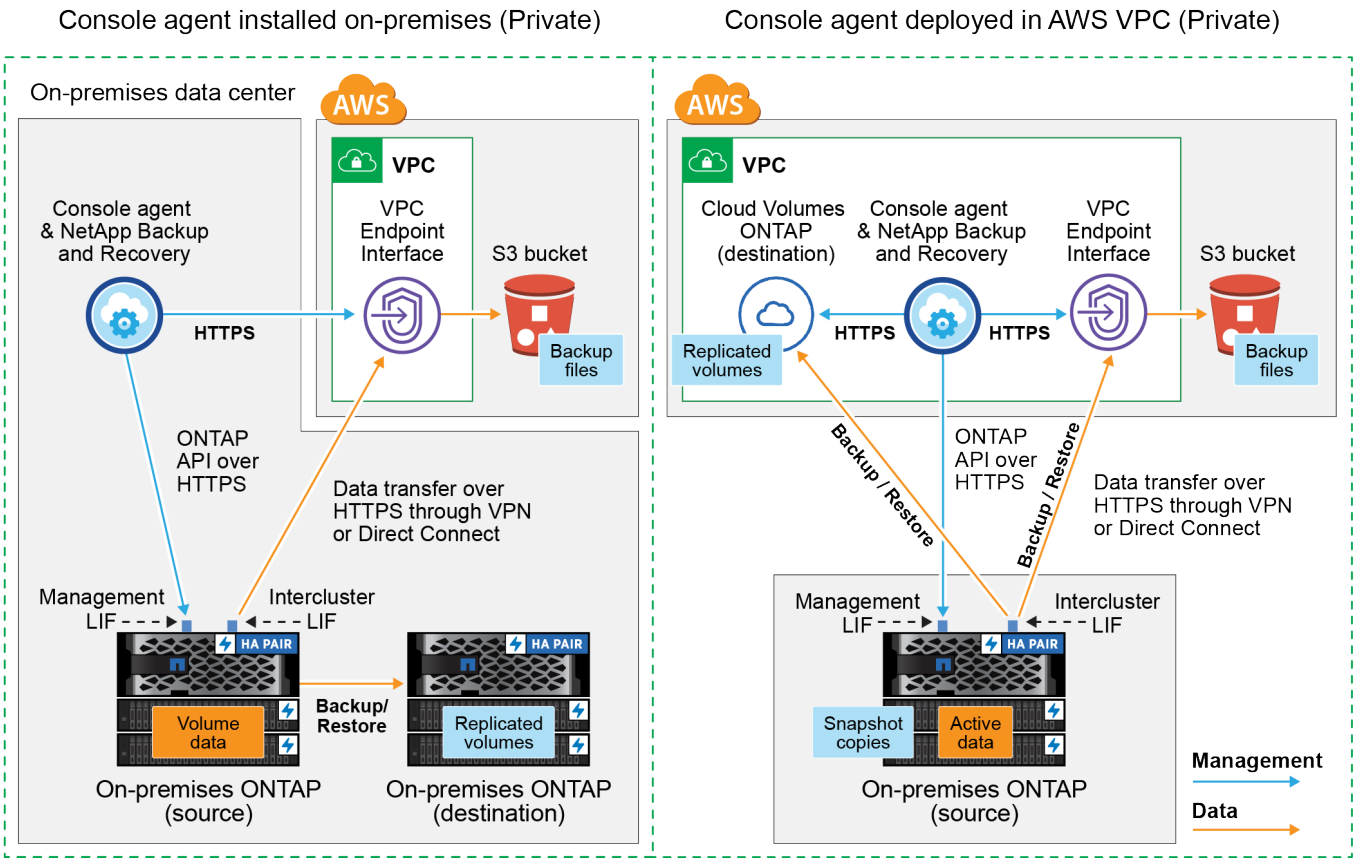
- **Connessione pubblica** - Connetti direttamente il sistema ONTAP ad AWS S3 utilizzando un endpoint S3 pubblico.
- **Connessione privata**: utilizza una VPN o AWS Direct Connect e instrada il traffico tramite un'interfaccia endpoint VPC che utilizza un indirizzo IP privato.

Facoltativamente, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.

Il diagramma seguente mostra il metodo di **connessione pubblica** e le connessioni che è necessario preparare tra i componenti. Puoi utilizzare un agente Console installato in sede oppure un agente Console distribuito nella VPC AWS.



Il diagramma seguente mostra il metodo di **connessione privata** e le connessioni che è necessario preparare tra i componenti. Puoi utilizzare un agente Console installato in sede oppure un agente Console distribuito nella VPC AWS.



Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità NetApp Console . Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Se hai già un agente Console distribuito nella tua AWS VPC o in sede, sei a posto.

In caso contrario, sarà necessario creare un agente Console in una di queste posizioni per eseguire il backup dei dati ONTAP nello storage AWS S3. Non è possibile utilizzare un agente Console distribuito in un altro provider cloud.

- "Scopri di più sugli agenti della console"
- "Installa un agente Console in AWS"
- "Installa un agente Console nei tuoi locali"
- "Installa un agente Console in una regione AWS GovCloud"

  NetApp Backup and Recovery è supportato nelle regioni GovCloud quando l'agente Console è distribuito nel cloud, non quando è installato nella tua sede. Inoltre, è necessario distribuire l'agente della console da AWS Marketplace. Non è possibile distribuire l'agente Console in una regione governativa dal sito Web NetApp Console SaaS.

Preparare i requisiti di rete dell'agente della console

Assicurarsi che siano soddisfatti i seguenti requisiti di rete:

- Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:
  - Una connessione HTTPS sulla porta 443 a NetApp Backup and Recovery e al tuo archivio di oggetti S3("vedere l'elenco degli endpoint")
  - Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP
  - Per le distribuzioni AWS e AWS GovCloud sono necessarie regole aggiuntive per i gruppi di sicurezza in entrata e in uscita. Vedere "Regole per l'agente della console in AWS" per i dettagli.
- Se disponi di una connessione Direct Connect o VPN dal tuo cluster ONTAP alla VPC e desideri che la comunicazione tra l'agente della console e S3 rimanga nella tua rete interna AWS (una connessione **privata**), dovrai abilitare un'interfaccia VPC Endpoint per S3. Configura il tuo sistema per una connessione privata utilizzando un'interfaccia endpoint VPC .

Verificare i requisiti della licenza

Sarà necessario verificare i requisiti di licenza sia per AWS che per la NetApp Console:

- Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai abbonarti a un'offerta NetApp Console Marketplace con pagamento in base al consumo (PAYGO) di AWS oppure acquistare e attivare una licenza NetApp Backup and Recovery BYOL da NetApp. Queste licenze sono riservate al tuo account e possono essere utilizzate su più sistemi.
  - Per la licenza NetApp Backup and Recovery PAYGO, è necessario un abbonamento a "Offerta NetApp Console da AWS Marketplace" . La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento.
  - Per la licenza BYOL NetApp Backup and Recovery , avrai bisogno del numero di serie di NetApp che ti consentirà di utilizzare il servizio per la durata e la capacità della licenza.
- È necessario disporre di un abbonamento AWS per lo spazio di archiviazione degli oggetti in cui verranno archiviati i backup.

Regioni supportate

È possibile creare backup dai sistemi locali ad Amazon S3 in tutte le regioni, comprese le regioni AWS GovCloud. Quando si configura il servizio, è possibile specificare la regione in cui verranno archiviati i backup.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .
- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .
- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette all'archiviazione di oggetti.

- Per un'architettura di backup fan-out, configurare le seguenti impostazioni sul sistema *primario*.
- Per un'architettura di backup a cascata, configurare le seguenti impostazioni sul sistema *secondario*.

Sono necessari i seguenti requisiti di rete del cluster ONTAP :

- Il cluster richiede una connessione HTTPS in ingresso dall'agente della console al LIF di gestione del cluster.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Questi LIF intercluster devono essere in grado di accedere all'archivio oggetti.

  Il cluster avvia una connessione HTTPS in uscita tramite la porta 443 dai LIF intercluster allo storage Amazon S3 per le operazioni di backup e ripristino. ONTAP legge e scrive dati da e verso l'archiviazione di oggetti: l'archiviazione di oggetti non si avvia mai, si limita a rispondere.
- I LIF intercluster devono essere associati allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui sono associati questi LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.

  Se si utilizza uno spazio IP diverso da "Default", potrebbe essere necessario creare un percorso statico per accedere all'archiviazione degli oggetti.

  Tutti i LIF intercluster all'interno dell'IPspace devono avere accesso all'archivio oggetti. Se non è possibile

configurarlo per l'IPspace corrente, sarà necessario creare un IPspace dedicato in cui tutti i LIF intercluster abbiano accesso all'archivio oggetti.

- I server DNS devono essere stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .
- Se necessario, aggiornare le regole del firewall per consentire le connessioni NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta 443 e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).
- Se si utilizza un endpoint di interfaccia VPC privata in AWS per la connessione S3, affinché venga utilizzato HTTPS/443 sarà necessario caricare il certificato dell'endpoint S3 nel cluster ONTAP . Configura il tuo sistema per una connessione privata utilizzando un'interfaccia endpoint VPC.
- Assicurati che il tuo cluster ONTAP disponga delle autorizzazioni per accedere al bucket S3.

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione ONTAP" .

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste: in particolare, le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di sicurezza predefinito.

Prepara Amazon S3 come destinazione di backup

Per preparare Amazon S3 come destinazione di backup, sono necessari i seguenti passaggi:

- Impostare le autorizzazioni S3.
- (Facoltativo) Crea i tuoi bucket S3. (Se lo desideri, il servizio creerà dei bucket per te.)
- (Facoltativo) Configurare le chiavi AWS gestite dal cliente per la crittografia dei dati.
- (Facoltativo) Configurare il sistema per una connessione privata utilizzando un'interfaccia endpoint VPC.

Imposta le autorizzazioni S3

Sarà necessario configurare due set di autorizzazioni:

- Autorizzazioni per l'agente della console per creare e gestire il bucket S3.
- Autorizzazioni per il cluster ONTAP locale in modo che possa leggere e scrivere dati nel bucket S3.

Passi

1. Assicurarsi che l'agente della console disponga delle autorizzazioni richieste. Per i dettagli, vedere "Autorizzazioni dei criteri NetApp Console" .

   Quando si creano backup nelle regioni AWS Cina, è necessario modificare il nome della risorsa AWS "arn" in tutte le sezioni *Resource* nelle policy IAM da "aws" a "aws-cn"; ad esempio `arn:aws-cn:s3:::netapp-backup-*` .

2. Quando attivi il servizio, la procedura guidata di backup ti chiederà di immettere una chiave di accesso e una chiave segreta. Queste credenziali vengono trasmesse al cluster ONTAP in modo che ONTAP possa eseguire il backup e il ripristino dei dati nel bucket S3. Per farlo, dovrai creare un utente IAM con le seguenti autorizzazioni.

   Fare riferimento al "Documentazione AWS: creazione di un ruolo per delegare le autorizzazioni a un utente IAM" .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea dei bucket per te. In alternativa, se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Se si creano bucket personalizzati, è consigliabile utilizzare il nome "netapp-backup". Se è necessario utilizzare un nome personalizzato, modificare il `ontapcloud-instance-policy-netapp-backup` IAMRole per i CVO esistenti e aggiungere il seguente blocco JSON alle autorizzazioni S3 `Statement` vettore. Devi includere `"Resource": "arn:aws:s3:::*"` e assegnare tutte le autorizzazioni necessarie che devono essere associate al bucket.

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListAllMyBuckets",
      "s3:PutObjectTagging",
      "s3:GetObjectTagging",
      "s3:RestoreObject",
      "s3:GetBucketObjectLockConfiguration",
      "s3:GetObjectRetention",
      "s3:PutBucketObjectLockConfiguration",
      "s3:PutObjectRetention"
    ],
    "Resource": "arn:aws:s3:::*"
  }
]
```

Imposta le chiavi AWS gestite dal cliente per la crittografia dei dati

Se desideri utilizzare le chiavi di crittografia Amazon S3 predefinite per crittografare i dati trasmessi tra il cluster locale e il bucket S3, sei a posto perché l'installazione predefinita utilizza quel tipo di crittografia.

Se invece si desidera utilizzare le chiavi gestite dal cliente per la crittografia dei dati anziché le chiavi predefinite, sarà necessario che le chiavi di crittografia gestite siano già configurate prima di avviare la procedura guidata NetApp Backup and Recovery .

"Scopri come utilizzare le tue chiavi di crittografia Amazon con Cloud Volumes ONTAP".

"Scopri come utilizzare le tue chiavi di crittografia Amazon con NetApp Backup and Recovery".

Configura il tuo sistema per una connessione privata utilizzando un'interfaccia endpoint VPC

Se si desidera utilizzare una connessione Internet pubblica standard, tutte le autorizzazioni vengono impostate dall'agente Console e non è necessario fare altro.

Se desideri una connessione Internet più sicura dal tuo data center locale alla VPC, puoi selezionare una connessione AWS PrivateLink nella procedura guidata di attivazione del backup. È obbligatorio se si prevede di utilizzare una VPN o AWS Direct Connect per connettere il sistema locale tramite un'interfaccia VPC Endpoint che utilizza un indirizzo IP privato.

Passi

1. Crea una configurazione dell'endpoint dell'interfaccia utilizzando la console Amazon VPC o la riga di comando. "Fare riferimento ai dettagli sull'utilizzo di AWS PrivateLink per Amazon S3" .
2. Modificare la configurazione del gruppo di sicurezza associato all'agente Console. Devi modificare la policy in "Personalizzata" (da "Accesso completo") e deviaggiungere le autorizzazioni S3 dalla policy di backup come mostrato in precedenza.

   Se si utilizza la porta 80 (HTTP) per la comunicazione con l'endpoint privato, il problema è risolto. Ora puoi abilitare NetApp Backup and Recovery sul cluster.

   Se si utilizza la porta 443 (HTTPS) per la comunicazione con l'endpoint privato, è necessario copiare il certificato dall'endpoint VPC S3 e aggiungerlo al cluster ONTAP , come mostrato nei 4 passaggi successivi.

3. Ottieni il nome DNS dell'endpoint dalla console AWS.
4. Ottieni il certificato dall'endpoint VPC S3. Lo fai tramite "accesso alla VM che ospita l'agente della console" ed eseguendo il seguente comando. Quando si immette il nome DNS dell'endpoint, aggiungere "bucket" all'inizio, sostituendo "*":

   ```
   openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
   ```

5. Dall'output di questo comando, copiare i dati per il certificato S3 (tutti i dati compresi tra i tag BEGIN / END CERTIFICATE inclusi):

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
…
…
GqvbOz/oO2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. Accedi alla CLI del cluster ONTAP e applica il certificato copiato utilizzando il seguente comando (sostituisci il nome della tua VM di archiviazione):

```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione Amazon S3 per i backup esiste come sistema nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nello storage di oggetti Amazon S3.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** ••• **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina

Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:
   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock . Tutti i volumi devono avere SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora, per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

  Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dall'archivio primario a quello secondario, all'archivio degli oggetti, e da quello secondario all'archivio degli oggetti.
   - **Distribuzione a ventaglio**: le informazioni fluiscono dal primario al secondario *e* dal primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .
3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a"Crea una politica" .
4. Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
   - Seleziona **Crea**.
5. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno nuovo.

     Per creare una policy personalizzata prima di attivare la replica, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.
6. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: seleziona **Amazon Web Services**.
   - **Impostazioni del provider**: immettere i dettagli del provider e la regione AWS in cui verranno archiviati i backup.

La chiave di accesso e la chiave segreta sono destinate all'utente IAM creato per consentire al cluster ONTAP di accedere al bucket S3.

- **Bucket**: scegli un bucket S3 esistente o creane uno nuovo. Fare riferimento a "Aggiungi bucket S3" .
- **Chiave di crittografia**: se hai creato un nuovo bucket S3, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Amazon S3 oppure scegliere le chiavi gestite dal cliente dal tuo account AWS per gestire la crittografia dei tuoi dati.

  Se hai scelto un bucket esistente, le informazioni di crittografia sono già disponibili, quindi non è necessario inserirle ora.

- **Networking**: scegli lo spazio IP e se utilizzerai un endpoint privato. Per impostazione predefinita, l'endpoint privato è disabilitato.
  i. Lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
  ii. Facoltativamente, scegli se utilizzare un AWS PrivateLink precedentemente configurato. "Visualizza i dettagli sull'utilizzo di AWS PrivateLink per Amazon S3" .
- **Criterio di backup**: seleziona un criterio di backup esistente o creane uno nuovo.

  Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

  Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

  - Inserisci il nome della policy.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Seleziona **Crea**.
- **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

7. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati primari contenuti negli snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di archiviazione primario.

Il bucket S3 viene creato nell'account di servizio indicato dalla chiave di accesso S3 e dalla chiave segreta immesse e i file di backup vengono archiviati lì. Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando"Pagina di monitoraggio dei lavori" .

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali nell'archiviazione BLOB di Azure con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP locali a un sistema di archiviazione secondario e all'archiviazione BLOB di Azure.

I "sistemi ONTAP on-premises" includono i sistemi FAS, AFF e ONTAP Select .

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

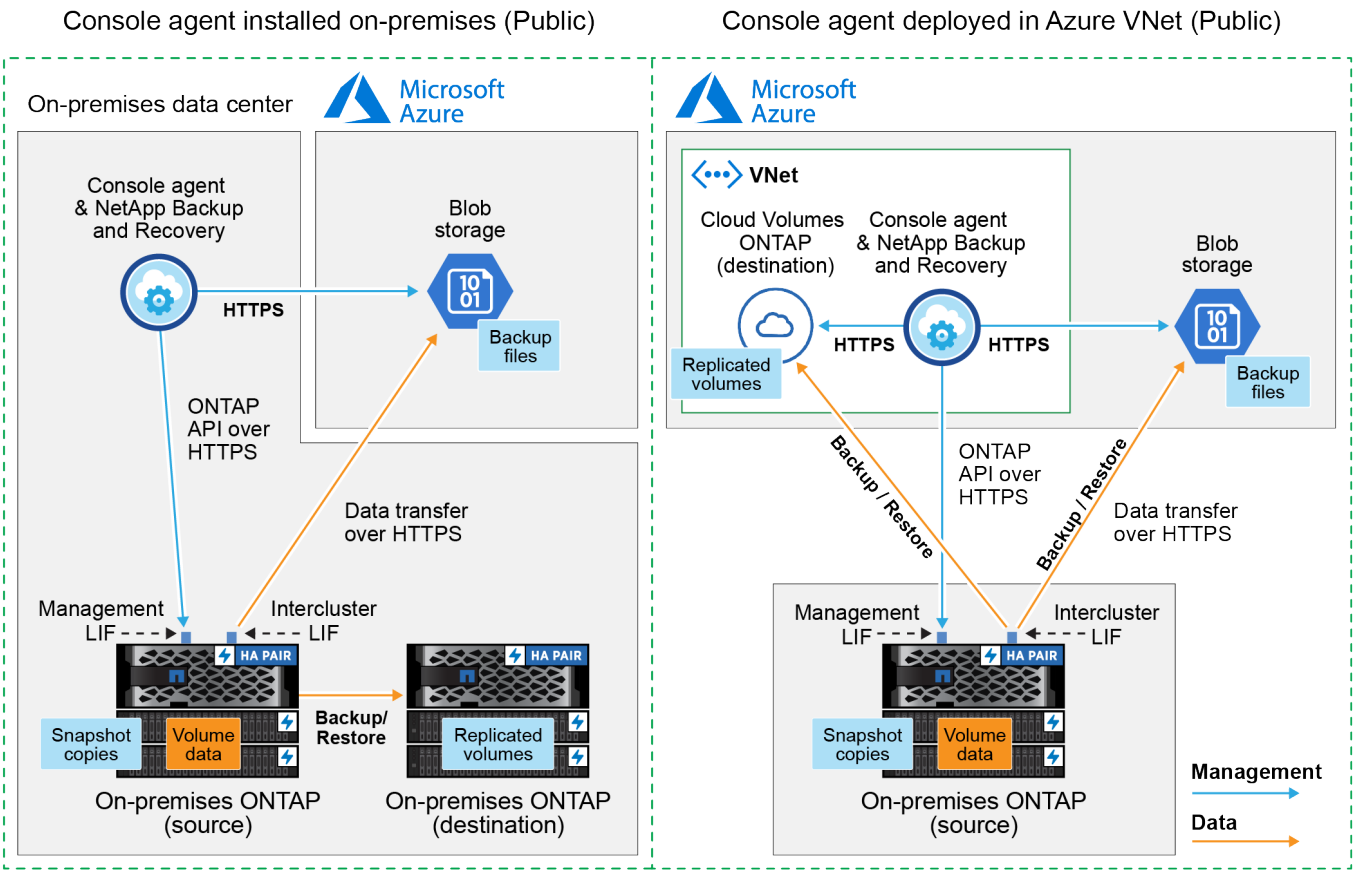
Identificare il metodo di connessione

Scegli quale dei due metodi di connessione utilizzerai durante la configurazione dei backup dai sistemi ONTAP locali ad Azure Blob.

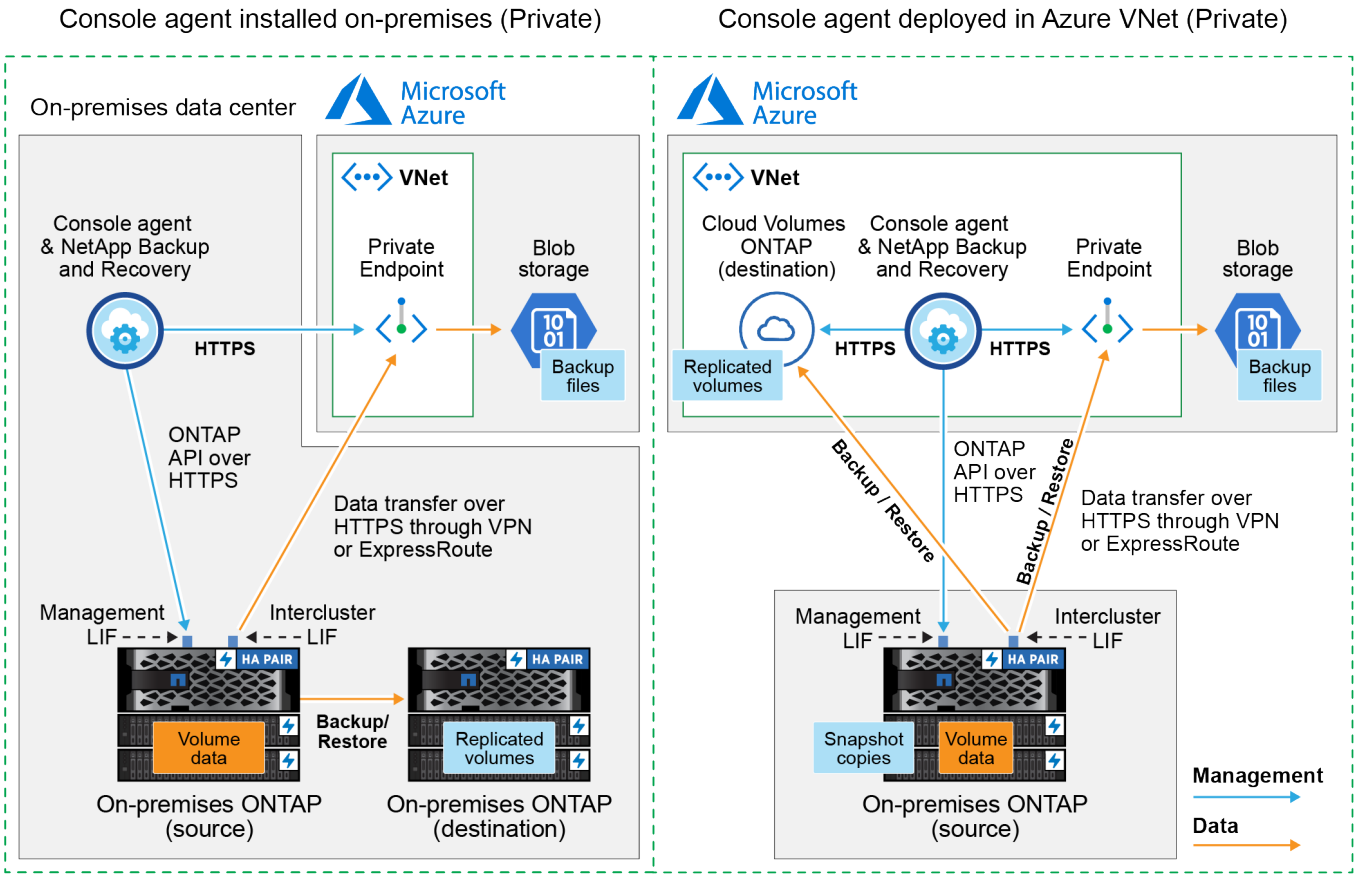
- **Connessione pubblica**: connette direttamente il sistema ONTAP all'archiviazione BLOB di Azure tramite un endpoint pubblico di Azure.
- **Connessione privata**: utilizza una VPN o ExpressRoute e instrada il traffico attraverso un endpoint privato VNet che utilizza un indirizzo IP privato.

Facoltativamente, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.

Il diagramma seguente mostra il metodo di **connessione pubblica** e le connessioni che è necessario preparare tra i componenti. È possibile utilizzare un agente Console installato in locale oppure un agente Console distribuito nella rete virtuale di Azure.



Il diagramma seguente mostra il metodo di **connessione privata** e le connessioni che è necessario preparare tra i componenti. È possibile utilizzare un agente Console installato in locale oppure un agente Console distribuito nella rete virtuale di Azure.



Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità NetApp Console . Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Se hai già un agente Console distribuito nella tua rete virtuale di Azure o in locale, sei a posto.

In caso contrario, sarà necessario creare un agente Console in una di queste posizioni per eseguire il backup dei dati ONTAP nell'archiviazione BLOB di Azure. Non è possibile utilizzare un agente Console distribuito in un altro provider cloud.

- "Scopri di più sugli agenti della console"
- "Installa un agente console in Azure"
- "Installa un agente Console nei tuoi locali"
- "Installare un agente Console in un'area di Azure Government"

  NetApp Backup and Recovery è supportato nelle regioni Azure Government quando l'agente Console è distribuito nel cloud, non quando è installato in sede. Inoltre, è necessario distribuire l'agente Console da Azure Marketplace. Non è possibile distribuire l'agente Console in una regione governativa dal sito Web Console SaaS.

Preparare la rete per l'agente della console

Assicurarsi che l'agente della console disponga delle connessioni di rete richieste.

Passi

1. Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:
   - Una connessione HTTPS sulla porta 443 a NetApp Backup and Recovery e al tuo archivio di oggetti BLOB("vedere l'elenco degli endpoint")
   - Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP
   - Per il corretto funzionamento della funzionalità NetApp Backup and Recovery Search & Restore, la porta 1433 deve essere aperta per la comunicazione tra l'agente della console e i servizi Azure Synapse SQL.
   - Per le distribuzioni di Azure e Azure Government sono necessarie regole aggiuntive per i gruppi di sicurezza in ingresso. Vedere "Regole per l'agente Console in Azure" per i dettagli.
2. Abilitare un endpoint privato VNet per l'archiviazione di Azure. Questa operazione è necessaria se si dispone di una connessione ExpressRoute o VPN dal cluster ONTAP alla VNet e si desidera che la comunicazione tra l'agente della console e l'archiviazione BLOB rimanga nella rete privata virtuale (una connessione **privata**).

Verificare o aggiungere autorizzazioni all'agente della console

Per utilizzare la funzionalità di ricerca e ripristino NetApp Backup and Recovery , è necessario disporre di autorizzazioni specifiche nel ruolo per l'agente della console, in modo che possa accedere ad Azure Synapse Workspace e all'account Data Lake Storage. Consultare le autorizzazioni riportate di seguito e seguire i passaggi se è necessario modificare la policy.

Prima di iniziare

È necessario registrare il provider di risorse di Azure Synapse Analytics (denominato "Microsoft.Synapse") con la sottoscrizione. "Scopri come registrare questo fornitore di risorse per il tuo abbonamento" . Per registrare il fornitore di risorse, devi essere il **Proprietario** o il **Collaboratore** dell'abbonamento.

Passi

1. Identificare il ruolo assegnato alla macchina virtuale dell'agente Console:
   a. Nel portale di Azure, aprire il servizio Macchine virtuali.
   b. Selezionare la macchina virtuale dell'agente Console.
   c. In **Impostazioni**, seleziona **Identità**.
   d. Selezionare **Assegnazioni di ruolo di Azure**.
   e. Prendi nota del ruolo personalizzato assegnato alla macchina virtuale dell'agente Console.
2. Aggiorna il ruolo personalizzato:
   a. Nel portale di Azure, apri la tua sottoscrizione di Azure.
   b. Selezionare **Controllo accessi (IAM) > Ruoli**.
   c. Selezionare i puntini di sospensione (**…**) per il ruolo personalizzato, quindi selezionare **Modifica**.
   d. Selezionare **JSON** e aggiungere le seguenti autorizzazioni:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Visualizza il formato JSON completo per la policy"

e. Seleziona **Revisiona + aggiorna** e poi seleziona **Aggiorna**.

Verificare i requisiti della licenza

Sarà necessario verificare i requisiti di licenza sia per Azure che per la console:

- Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai abbonarti a un'offerta di Console Marketplace con pagamento in base al consumo (PAYGO) di Azure oppure acquistare e attivare una licenza BYOL di NetApp Backup and Recovery da NetApp. Queste licenze sono riservate al tuo account e possono essere utilizzate su più sistemi.
  - Per la licenza NetApp Backup and Recovery PAYGO, è necessario un abbonamento a "Offerta NetApp Console da Azure Marketplace" . La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento.
  - Per la licenza BYOL NetApp Backup and Recovery , avrai bisogno del numero di serie di NetApp che ti consentirà di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL" .
- È necessario disporre di un abbonamento Azure per lo spazio di archiviazione degli oggetti in cui verranno salvati i backup.

Regioni supportate

È possibile creare backup dai sistemi locali ad Azure Blob in tutte le aree geografiche, comprese le aree di Azure Government. Quando si configura il servizio, si specifica la regione in cui verranno archiviati i backup.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .

- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .
- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette all'archiviazione di oggetti.

- Per un'architettura di backup fan-out, configurare le seguenti impostazioni sul sistema *primario*.
- Per un'architettura di backup a cascata, configurare le seguenti impostazioni sul sistema *secondario*.

Sono necessari i seguenti requisiti di rete del cluster ONTAP :

- Il cluster ONTAP avvia una connessione HTTPS sulla porta 443 dal LIF intercluster all'archiviazione BLOB di Azure per le operazioni di backup e ripristino.

  ONTAP legge e scrive dati da e verso l'archiviazione di oggetti. L'archiviazione degli oggetti non si avvia mai, risponde e basta.

- ONTAP richiede una connessione in ingresso dall'agente della console al LIF di gestione del cluster. L'agente della console può risiedere in una rete virtuale di Azure.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Il LIF deve essere associato allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui è associato ciascun LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.

- I LIF dei nodi e degli intercluster sono in grado di accedere all'archivio oggetti.
- I server DNS sono stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .
- Se si utilizza uno spazio IP diverso da quello predefinito, potrebbe essere necessario creare un percorso statico per accedere all'archiviazione degli oggetti.
- Se necessario, aggiornare le regole del firewall per consentire le connessioni del servizio NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta 443 e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione ONTAP" .

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste: in particolare, le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di sicurezza predefinito.

Preparare Azure Blob come destinazione di backup

1. È possibile utilizzare le proprie chiavi personalizzate per la crittografia dei dati nella procedura guidata di attivazione anziché utilizzare le chiavi di crittografia predefinite gestite da Microsoft. In questo caso sarà necessario disporre della sottoscrizione di Azure, del nome del Key Vault e della chiave. "Impara a usare le tue chiavi" .

   Si noti che Backup e ripristino supportano *criteri di accesso di Azure* come modello di autorizzazione. Il modello di autorizzazione *Azure role-based access control* (Azure RBAC) non è attualmente supportato.

2. Se desideri una connessione più sicura tramite Internet pubblica dal tuo data center locale alla rete virtuale, è disponibile un'opzione per configurare un endpoint privato di Azure nella procedura guidata di attivazione. In questo caso sarà necessario conoscere la VNet e la Subnet per questa connessione. "Fare riferimento ai dettagli sull'utilizzo di un endpoint privato" .

Crea il tuo account di archiviazione BLOB di Azure

Per impostazione predefinita, il servizio crea account di archiviazione per te. Se si desidera utilizzare account di archiviazione personali, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali account di archiviazione nella procedura guidata.

"Scopri di più sulla creazione dei tuoi account di archiviazione".

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto al servizio Backup e ripristino nel pannello di destra.

Se la destinazione di Azure per i backup è presente nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nell'archivio oggetti BLOB di Azure.

- Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** ••• **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:
   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock . Tutti i volumi devono avere SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

Tieni presente che se ai volumi scelti sono già applicati criteri di snapshot o di replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora, per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio Snapshot locale
- Destinazione e politica di replicazione

Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal primario al secondario e dal secondario all'archiviazione degli oggetti.
   - **Distribuzione a ventaglio**: le informazioni fluiscono dal primario al secondario *e* dal primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .
3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Per creare una policy personalizzata prima di attivare lo snapshot, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.
4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno nuovo.

     Per creare una policy personalizzata prima di attivare la replica, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.
5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:

- **Provider**: seleziona **Microsoft Azure**.
- **Impostazioni del provider**: immettere i dettagli del provider e la regione in cui verranno archiviati i backup.

  Crea un nuovo account di archiviazione oppure selezionane uno esistente.

  Crea il tuo gruppo di risorse che gestisce il contenitore BLOB oppure seleziona il tipo di gruppo di risorse e il gruppo.

  > Se vuoi proteggere i tuoi file di backup da modifiche o eliminazioni, assicurati che l'account di archiviazione sia stato creato con l'archiviazione immutabile abilitata utilizzando un periodo di conservazione di 30 giorni.

  > Se si desidera suddividere i file di backup più vecchi in Azure Archive Storage per un'ulteriore ottimizzazione dei costi, assicurarsi che l'account di archiviazione disponga della regola del ciclo di vita appropriata.

- **Chiave di crittografia**: se hai creato un nuovo account di archiviazione di Azure, immetti le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Azure oppure scegliere le chiavi gestite dal cliente dal tuo account Azure per gestire la crittografia dei tuoi dati.

  Se si sceglie di utilizzare le chiavi gestite dal cliente, immettere il vault delle chiavi e le informazioni sulla chiave.

  > Se hai scelto un account di archiviazione Microsoft esistente, le informazioni sulla crittografia sono già disponibili, quindi non è necessario immetterle ora.

- **Networking**: scegli lo spazio IP e se utilizzerai un endpoint privato. Per impostazione predefinita, l'endpoint privato è disabilitato.
  i. Lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
  ii. Facoltativamente, scegli se utilizzerai un endpoint privato di Azure precedentemente configurato. "Scopri di più sull'utilizzo di un endpoint privato di Azure" .
- **Criterio di backup**: seleziona un criterio di backup esistente per l'archiviazione degli oggetti oppure creane uno nuovo.

  > Per creare una policy personalizzata prima di attivare il backup, fare riferimento a"Crea una politica" .

  Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

  - Inserisci il nome della policy.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
  - Seleziona **Crea**.
- **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot

locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di archiviazione primario contenuti negli snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume primario.

Viene creato un account di archiviazione BLOB nel gruppo di risorse immesso e i file di backup vengono archiviati lì. Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando"Pagina di monitoraggio dei lavori" .

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali su Google Cloud Storage con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP primari locali a un sistema di storage secondario e a Google Cloud Storage.

I "sistemi ONTAP on-premises" includono i sistemi FAS, AFF e ONTAP Select .

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

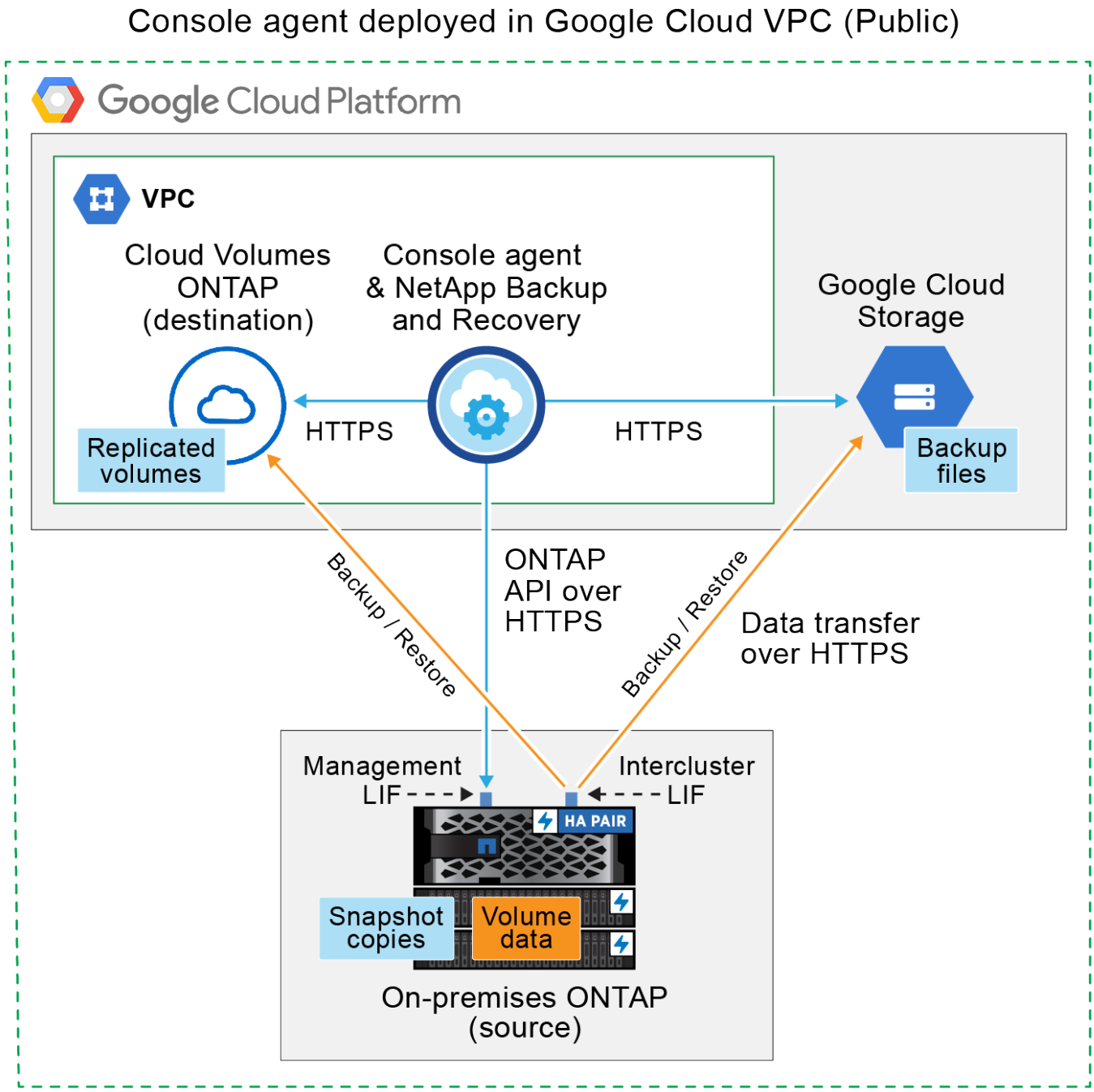
Identificare il metodo di connessione

Scegli quale dei due metodi di connessione utilizzerai quando configuri i backup dai sistemi ONTAP locali a Google Cloud Storage.

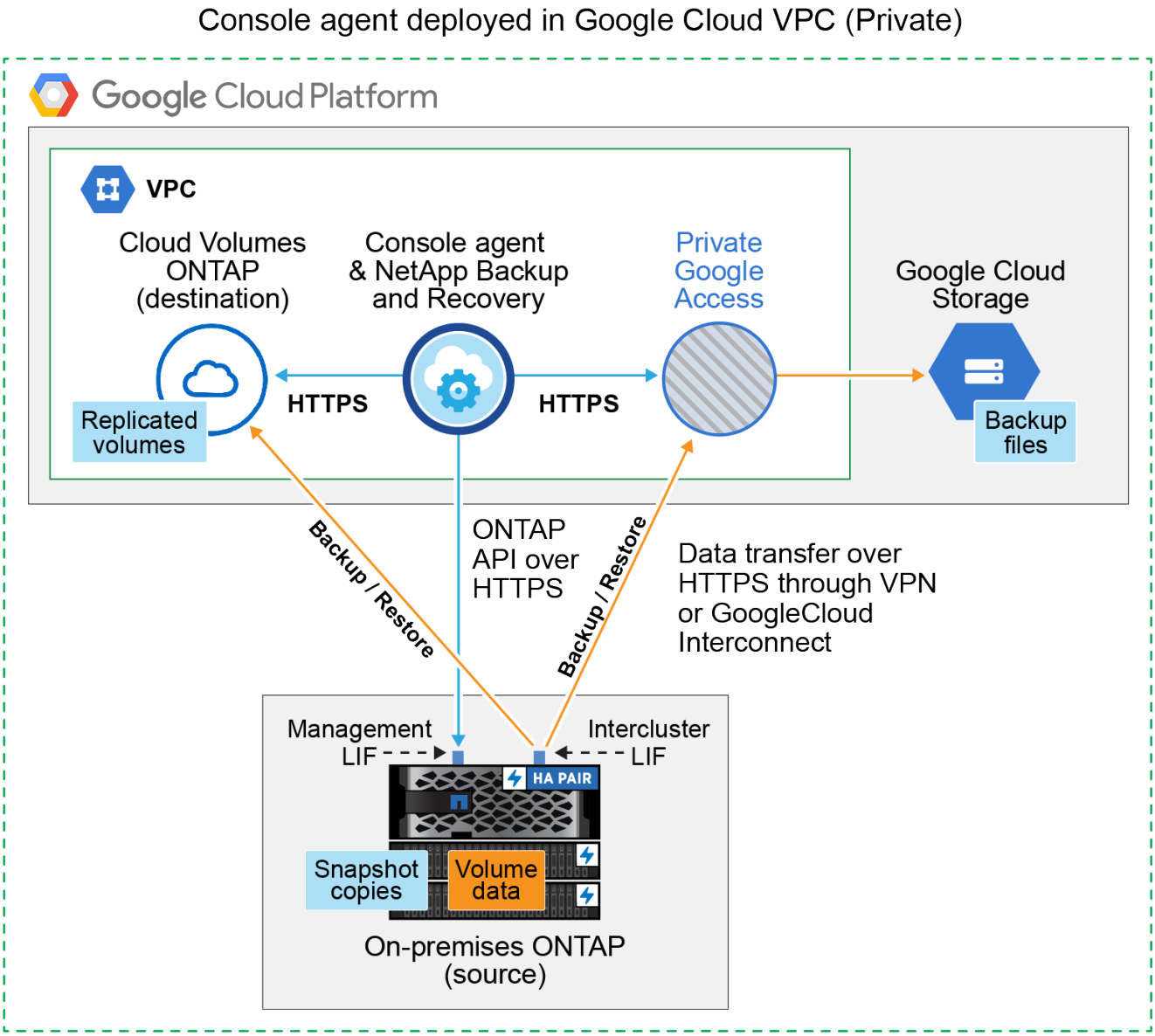
- **Connessione pubblica** - Collega direttamente il sistema ONTAP a Google Cloud Storage tramite un endpoint pubblico di Google.
- **Connessione privata**: utilizza una VPN o Google Cloud Interconnect e instrada il traffico tramite un'interfaccia Google Access privata che utilizza un indirizzo IP privato.

Facoltativamente, è possibile connettersi a un sistema ONTAP secondario per i volumi replicati utilizzando anche la connessione pubblica o privata.

Il diagramma seguente mostra il metodo di **connessione pubblica** e le connessioni che è necessario preparare tra i componenti. L'agente della console deve essere distribuito nella VPC di Google Cloud Platform.



Il diagramma seguente mostra il metodo di **connessione privata** e le connessioni che è necessario preparare tra i componenti. L'agente della console deve essere distribuito nella VPC di Google Cloud Platform.



Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità Console. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Se hai già un agente Console distribuito nella tua VPC di Google Cloud Platform, sei a posto.

In caso contrario, sarà necessario creare un agente Console in quella posizione per eseguire il backup dei dati ONTAP su Google Cloud Storage. Non è possibile utilizzare un agente Console distribuito in un altro provider cloud o in locale.

- "Scopri di più sugli agenti della console"
- "Installa un agente Console in GCP"

Preparare la rete per l'agente della console

Assicurarsi che l'agente della console disponga delle connessioni di rete richieste.

Passi

1. Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:
   - Una connessione HTTPS sulla porta 443 a NetApp Backup and Recovery e al tuo spazio di archiviazione Google Cloud("vedere l'elenco degli endpoint")
   - Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP
2. Abilitare Private Google Access (o Private Service Connect) sulla subnet in cui si prevede di distribuire l'agente Console. "Accesso privato a Google" O "Connessione al servizio privato" sono necessari se si dispone di una connessione diretta dal cluster ONTAP alla VPC e si desidera che la comunicazione tra l'agente della console e Google Cloud Storage rimanga nella rete privata virtuale (una connessione **privata**).

   Segui le istruzioni di Google per impostare queste opzioni di accesso privato. Assicurati che i tuoi server DNS siano stati configurati per puntare `www.googleapis.com` E `storage.googleapis.com` agli indirizzi IP interni (privati) corretti.

Verificare o aggiungere autorizzazioni all'agente della console

Per utilizzare la funzionalità "Cerca e ripristina" NetApp Backup and Recovery , è necessario disporre di autorizzazioni specifiche nel ruolo per l'agente della console, in modo che possa accedere al servizio Google Cloud BigQuery. Esaminare le autorizzazioni riportate di seguito e seguire i passaggi se è necessario modificare la policy.

Passi

1. Nel "Google Cloud Console" , vai alla pagina **Ruoli**.
2. Utilizzando l'elenco a discesa nella parte superiore della pagina, seleziona il progetto o l'organizzazione che contiene il ruolo che desideri modificare.
3. Seleziona un ruolo personalizzato.
4. Selezionare **Modifica ruolo** per aggiornare le autorizzazioni del ruolo.
5. Selezionare **Aggiungi autorizzazioni** per aggiungere le seguenti nuove autorizzazioni al ruolo.

   ```
   bigquery.jobs.get
   bigquery.jobs.list
   bigquery.jobs.listAll
   bigquery.datasets.create
   bigquery.datasets.get
   bigquery.jobs.create
   bigquery.tables.get
   bigquery.tables.getData
   bigquery.tables.list
   bigquery.tables.create
   ```

6. Selezionare **Aggiorna** per salvare il ruolo modificato.

Verificare i requisiti della licenza

- Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai abbonarti a un'offerta Console Marketplace pay-as-you-go (PAYGO) di Google oppure acquistare e attivare una licenza BYOL NetApp Backup and Recovery da NetApp. Queste licenze sono riservate al tuo account e possono essere utilizzate su più sistemi.
  - Per la licenza NetApp Backup and Recovery PAYGO, è necessario un abbonamento a "Offerta NetApp Console da Google Marketplace" . La fatturazione per NetApp Backup and Recovery avviene tramite questo abbonamento.
  - Per la licenza BYOL NetApp Backup and Recovery , avrai bisogno del numero di serie di NetApp che ti consentirà di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL" .
- È necessario disporre di un abbonamento Google per lo spazio di archiviazione degli oggetti in cui verranno salvati i backup.

Regioni supportate

È possibile creare backup dai sistemi locali su Google Cloud Storage in tutte le regioni. Quando si configura il servizio, è possibile specificare la regione in cui verranno archiviati i backup.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .
- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .

- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette all'archiviazione di oggetti.

- Per un'architettura di backup fan-out, configurare le seguenti impostazioni sul sistema *primario*.
- Per un'architettura di backup a cascata, configurare le seguenti impostazioni sul sistema *secondario*.

Sono necessari i seguenti requisiti di rete del cluster ONTAP :

- Il cluster ONTAP avvia una connessione HTTPS sulla porta 443 dal LIF intercluster a Google Cloud Storage per le operazioni di backup e ripristino.

  ONTAP legge e scrive dati da e verso l'archiviazione di oggetti. L'archiviazione degli oggetti non si avvia mai, risponde e basta.

- ONTAP richiede una connessione in ingresso dall'agente della console al LIF di gestione del cluster. L'agente della console può risiedere in una VPC di Google Cloud Platform.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Il LIF deve essere associato allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui è associato ciascun LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.

- I LIF intercluster dei nodi sono in grado di accedere all'archivio oggetti.
- I server DNS sono stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .

  Se utilizzi Private Google Access o Private Service Connect, assicurati che i tuoi server DNS siano stati configurati per puntare `storage.googleapis.com` all'indirizzo IP interno (privato) corretto.

- Tieni presente che se utilizzi uno spazio IP diverso da quello predefinito, potrebbe essere necessario creare una route statica per accedere all'archiviazione degli oggetti.
- Se necessario, aggiornare le regole del firewall per consentire le connessioni NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta 443 e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.

- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione ONTAP" .

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste: in particolare, le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di sicurezza predefinito.

Prepara Google Cloud Storage come destinazione di backup

Per preparare Google Cloud Storage come destinazione di backup, sono necessari i seguenti passaggi:

- Imposta le autorizzazioni.
- (Facoltativo) Crea i tuoi bucket. (Se lo desideri, il servizio creerà dei bucket per te.)
- (Facoltativo) Impostare le chiavi gestite dal cliente per la crittografia dei dati

Imposta i permessi

È necessario fornire le chiavi di accesso all'archiviazione per un account di servizio che dispone di autorizzazioni specifiche utilizzando un ruolo personalizzato. Un account di servizio consente a NetApp Backup and Recovery di autenticare e accedere ai bucket di Cloud Storage utilizzati per archiviare i backup. Le chiavi sono necessarie affinché Google Cloud Storage sappia chi sta effettuando la richiesta.

Passi

1. Nel "Google Cloud Console" , vai alla pagina **Ruoli**.
2. "Crea un nuovo ruolo"con le seguenti autorizzazioni:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Nella console di Google Cloud, "vai alla pagina Account di servizio" .
4. Seleziona il tuo progetto Cloud.
5. Seleziona **Crea account di servizio** e fornisci le informazioni richieste:
   a. **Dettagli dell'account di servizio**: inserisci un nome e una descrizione.

b. **Concedi a questo account di servizio l'accesso al progetto**: seleziona il ruolo personalizzato appena creato.

c. Selezionare **Fatto**.

6. Vai a "Impostazioni di archiviazione GCP" e creare chiavi di accesso per l'account di servizio:

   a. Seleziona un progetto e seleziona **Interoperabilità**. Se non lo hai già fatto, seleziona **Abilita accesso interoperabilità**.

   b. In **Chiavi di accesso per gli account di servizio**, seleziona **Crea una chiave per un account di servizio**, seleziona l'account di servizio appena creato e fai clic su **Crea chiave**.

      Sarà necessario immettere le chiavi in NetApp Backup and Recovery in un secondo momento, quando si configura il servizio di backup.

Crea i tuoi bucket

Per impostazione predefinita, il servizio crea dei bucket per te. In alternativa, se si desidera utilizzare i propri bucket, è possibile crearli prima di avviare la procedura guidata di attivazione del backup e quindi selezionare tali bucket nella procedura guidata.

"Scopri di più sulla creazione dei tuoi bucket".

Impostare le chiavi di crittografia gestite dal cliente (CMEK) per la crittografia dei dati

Puoi utilizzare le tue chiavi gestite dal cliente per la crittografia dei dati anziché le chiavi di crittografia predefinite gestite da Google. Sono supportate sia le chiavi interregionali che quelle interprogetto, quindi è possibile scegliere un progetto per un bucket diverso dal progetto della chiave CMEK.

Se intendi utilizzare le tue chiavi gestite dal cliente:

- Per poter aggiungere queste informazioni nella procedura guidata di attivazione, è necessario disporre del Key Ring e del Key Name. "Scopri di più sulle chiavi di crittografia gestite dal cliente" .
- Sarà necessario verificare che le seguenti autorizzazioni richieste siano incluse nel ruolo dell'agente della console:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Dovrai verificare che l'API "Cloud Key Management Service (KMS)" di Google sia abilitata nel tuo progetto. Vedi il "Documentazione di Google Cloud: abilitazione delle API" per i dettagli.

Considerazioni CMEK:

- Sono supportate sia le chiavi HSM (supportate da hardware) sia quelle generate da software.

- Sono supportate sia le chiavi Cloud KMS appena create che quelle importate.
- Sono supportate solo le chiavi regionali, le chiavi globali non sono supportate.
- Attualmente è supportata solo la funzione "Crittografia/decifratura simmetrica".
- All'agente di servizio associato all'account di archiviazione viene assegnato il ruolo IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" da NetApp Backup and Recovery.

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione di Google Cloud Storage per i backup è presente nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nell'archivio oggetti di Google Cloud.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona **Azioni*** ••• **icona e seleziona *Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup su storage di oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:

   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento a Prepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come "attiva il backup per volumi aggiuntivi nel sistema" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock . Tutti i volumi devono avere SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora, per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

  Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: Se hai scelto la replica e il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal primario al secondario e dal secondario all'archiviazione degli oggetti.
   - **Distribuzione a ventaglio**: le informazioni fluiscono dal primario al secondario *e* dal primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.

4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno nuovo.

     Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: seleziona **Google Cloud**.
   - **Impostazioni del provider**: immettere i dettagli del provider e la regione in cui verranno archiviati i backup.

     Crea un nuovo bucket oppure selezionane uno già creato.

     Se desideri suddividere i file di backup più vecchi nell'archiviazione di Google Cloud Archive per un'ulteriore ottimizzazione dei costi, assicurati che il bucket disponga della regola del ciclo di vita appropriata.

     Inserisci la chiave di accesso e la chiave segreta di Google Cloud.

   - **Chiave di crittografia**: se hai creato un nuovo account di archiviazione Google Cloud, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Scegli se utilizzare le chiavi di crittografia predefinite di Google Cloud oppure scegliere le chiavi gestite dal cliente dal tuo account Google Cloud per gestire la crittografia dei tuoi dati.

     Se hai scelto un account di archiviazione Google Cloud esistente, le informazioni sulla crittografia sono già disponibili, quindi non è necessario inserirle ora.

     Se scegli di utilizzare le tue chiavi gestite dal cliente, inserisci il portachiavi e il nome della chiave. "Scopri di più sulle chiavi di crittografia gestite dal cliente" .

   - **Networking**: Seleziona lo spazio IP.

Lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.

- **Criterio di backup**: seleziona un criterio di backup esistente per l'archiviazione degli oggetti oppure creane uno nuovo.

  Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

  Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

  - Inserisci il nome della policy.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Seleziona **Crea**.
- **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati del sistema di archiviazione primario. I trasferimenti successivi contengono copie differenziali dei dati del sistema di archiviazione primario contenuti negli snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di origine.

Un bucket di Google Cloud Storage viene creato automaticamente nell'account di servizio indicato dalla chiave di accesso e dalla chiave segreta di Google immesse, dove vengono archiviati i file di backup. Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando"Pagina di monitoraggio dei lavori" .

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali su ONTAP S3 con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP locali principali. È possibile inviare i backup a un sistema di archiviazione ONTAP secondario (un volume replicato) o a un bucket su un sistema ONTAP configurato come server S3 (un file di backup) o a entrambi.

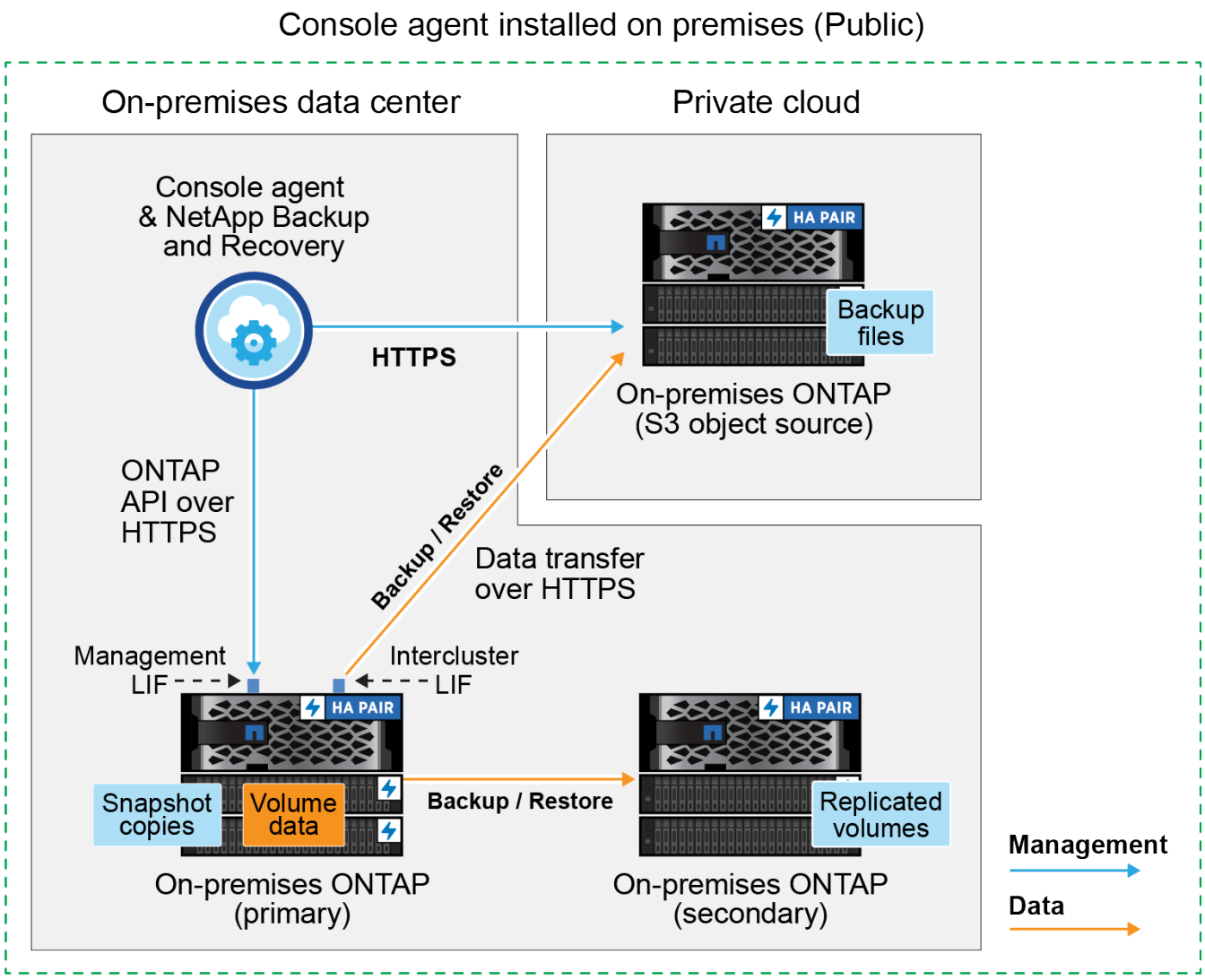
Il sistema ONTAP principale in sede può essere un sistema FAS, AFF o ONTAP Select . Il sistema ONTAP secondario può essere un ONTAP locale o un sistema Cloud Volumes ONTAP . L'archiviazione degli oggetti può essere su un sistema ONTAP locale o su un sistema Cloud Volumes ONTAP su cui è stato abilitato un server di archiviazione degli oggetti Simple Storage Service (S3).

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Identificare il metodo di connessione

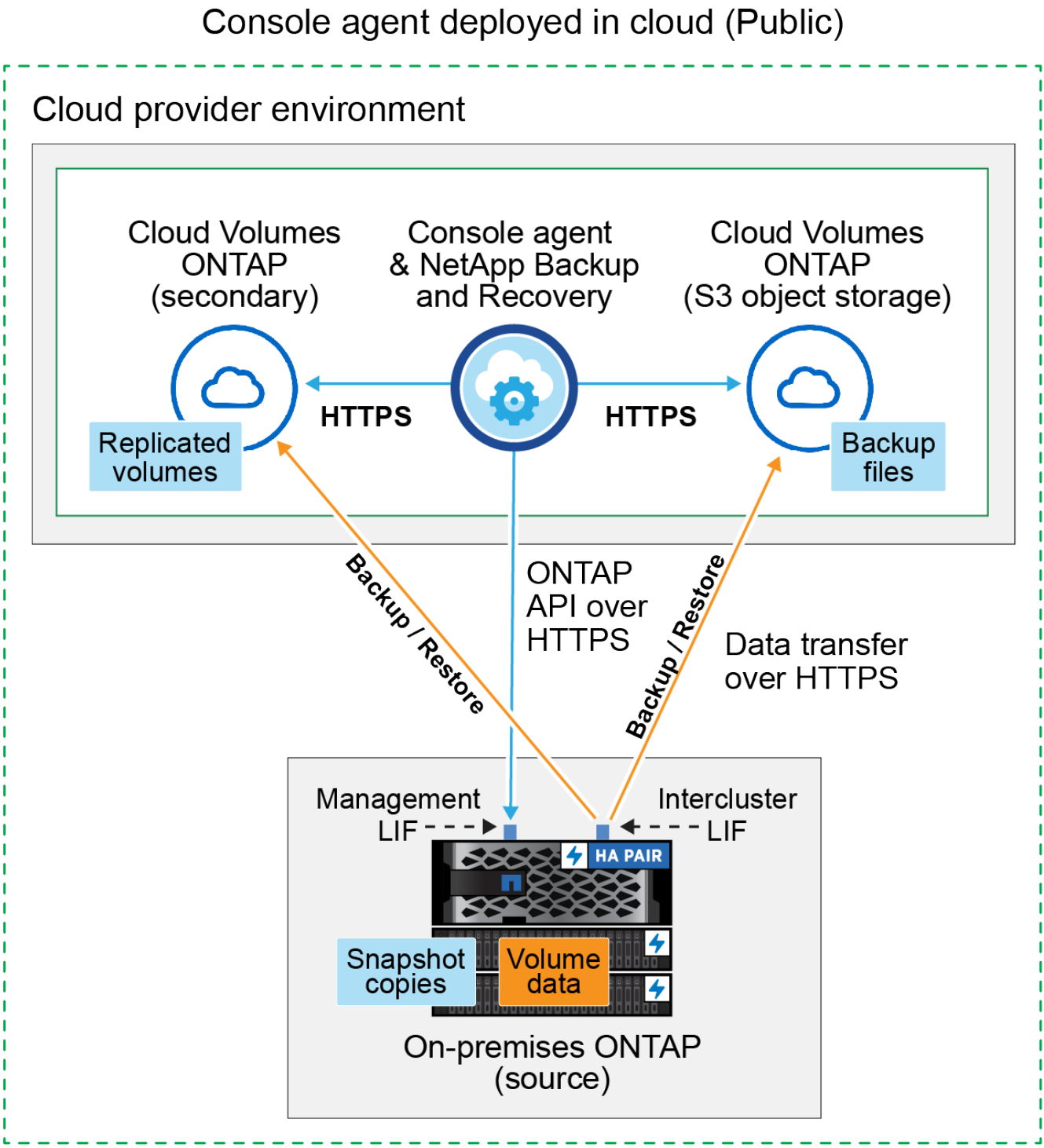
Esistono numerose configurazioni in cui è possibile creare backup su un bucket S3 su un sistema ONTAP . Di seguito sono illustrati due scenari.

L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP primario in locale su un sistema ONTAP in locale configurato per S3 e le connessioni che è necessario preparare tra di essi. Mostra anche una connessione a un sistema ONTAP secondario nella stessa posizione locale per replicare i volumi.



Quando l'agente Console e il sistema ONTAP primario in sede vengono installati in una posizione in sede senza accesso a Internet (una distribuzione in modalità "privata"), il sistema ONTAP S3 deve trovarsi nello stesso data center in sede.

L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP primario on-premise su un sistema Cloud Volumes ONTAP configurato per S3 e le connessioni che è necessario preparare tra di essi. Mostra anche una connessione a un sistema Cloud Volumes ONTAP secondario nello stesso ambiente del provider cloud per replicare i volumi.



In questo scenario, l'agente Console dovrebbe essere distribuito nello stesso ambiente del provider cloud in cui sono distribuiti i sistemi Cloud Volumes ONTAP .

Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità Console. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Quando si esegue il backup dei dati su ONTAP S3, è necessario che un agente Console sia disponibile in sede o nel cloud. Sarà necessario installare un nuovo agente Console oppure assicurarsi che l'agente Console attualmente selezionato risieda in una di queste posizioni. L'agente Console locale può essere installato in un sito con o senza accesso a Internet.

- "Scopri di più sugli agenti della console"
- "Installa l'agente Console nel tuo ambiente cloud"
- "Installazione dell'agente Console su un host Linux con accesso a Internet"
- "Installazione dell'agente Console su un host Linux senza accesso a Internet"
- "Passaggio tra gli agenti della console"

Preparare i requisiti di rete dell'agente della console

Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:

- Una connessione HTTPS sulla porta 443 al server ONTAP S3
- Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP di origine
- Una connessione Internet in uscita sulla porta 443 verso NetApp Backup and Recovery (non necessaria quando l'agente Console è installato in un sito "oscuro")

Considerazioni sulla modalità privata (sito oscuro)

La funzionalità NetApp Backup and Recovery è integrata nell'agente Console. Se installato in modalità privata, sarà necessario aggiornare periodicamente il software dell'agente della console per accedere alle nuove funzionalità. Controlla il"NetApp Backup and Recovery: novità" per vedere le nuove funzionalità di ogni versione NetApp Backup and Recovery . Quando vuoi utilizzare le nuove funzionalità, segui i passaggi per "aggiornare il software dell'agente della console" .

Quando si utilizza NetApp Backup and Recovery in un ambiente SaaS standard, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel cloud. Quando si utilizza NetApp Backup and Recovery in un sito senza accesso a Internet, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel bucket ONTAP S3 in cui vengono archiviati i backup.

Verificare i requisiti della licenza

Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai acquistare e attivare una licenza NetApp Backup and Recovery BYOL da NetApp. La licenza è per il backup e il ripristino su storage di oggetti: non è necessaria alcuna licenza per creare snapshot o volumi replicati. Questa licenza è per l'account e può essere utilizzata su più sistemi.

Avrai bisogno del numero di serie di NetApp che ti consentirà di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL" .

La licenza PAYGO non è supportata durante il backup dei file su ONTAP S3.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .
- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .
- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario assicurarsi che i seguenti requisiti siano soddisfatti sul sistema che si connette all'archiviazione di oggetti.

- Quando si utilizza un'architettura di backup fan-out, le impostazioni devono essere configurate sul sistema di archiviazione *primario*.
- Quando si utilizza un'architettura di backup a cascata, le impostazioni devono essere configurate sul sistema di archiviazione *secondario*.

  "Scopri di più sui tipi di architettura di backup".

Sono necessari i seguenti requisiti di rete del cluster ONTAP :

- Il cluster ONTAP avvia una connessione HTTPS tramite una porta specificata dall'utente dal LIF intercluster al server ONTAP S3 per le operazioni di backup e ripristino. La porta è configurabile durante la configurazione del backup.

  ONTAP legge e scrive dati da e verso l'archiviazione di oggetti. L'archiviazione degli oggetti non si avvia

mai, risponde e basta.

- ONTAP richiede una connessione in ingresso dall'agente della console al LIF di gestione del cluster.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Il LIF deve essere associato allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui è associato ciascun LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.

- I LIF intercluster dei nodi sono in grado di accedere all'archivio oggetti (non necessario quando l'agente Console è installato in un sito "dark").
- I server DNS sono stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .
- Se si utilizza uno spazio IP diverso da quello predefinito, potrebbe essere necessario creare un percorso statico per accedere all'archiviazione degli oggetti.
- Se necessario, aggiornare le regole del firewall per consentire le connessioni del servizio NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta specificata (in genere la porta 443) e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione ONTAP" .

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste: in particolare, le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di sicurezza predefinito.

Prepara ONTAP S3 come destinazione di backup

È necessario abilitare un server di archiviazione oggetti Simple Storage Service (S3) nel cluster ONTAP che si prevede di utilizzare per i backup di archiviazione oggetti. Vedi il "Documentazione ONTAP S3" per i dettagli.

Nota: è possibile aggiungere questo cluster alla pagina **Sistemi** della console, ma non viene identificato come server di archiviazione oggetti S3 e non è possibile trascinare un sistema sorgente su questo sistema S3 per avviare l'attivazione del backup.

Questo sistema ONTAP deve soddisfare i seguenti requisiti.

Versioni ONTAP supportate

Per i sistemi ONTAP locali è richiesto ONTAP 9.8 e versioni successive. Per i sistemi Cloud Volumes ONTAP è richiesto ONTAP 9.9.1 e versioni successive.

Credenziali S3

È necessario aver creato un utente S3 per controllare l'accesso al proprio storage ONTAP S3. "Per i dettagli, consultare la documentazione ONTAP S3" .

Quando si configura il backup su ONTAP S3, la procedura guidata di backup richiede una chiave di accesso S3 e una chiave segreta per un account utente. L'account utente consente a NetApp Backup and Recovery di autenticarsi e accedere ai bucket ONTAP S3 utilizzati per archiviare i backup. Le chiavi sono necessarie affinché ONTAP S3 sappia chi sta effettuando la richiesta.

Queste chiavi di accesso devono essere associate a un utente che dispone delle seguenti autorizzazioni:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket",
"s3:GetBucketLocation"
```

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia e le policy di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:
   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.
   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona l'opzione **Azioni (…)** e seleziona **Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup nell'archiviazione oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, repliche e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina

Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:
   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criteri di snapshot, criteri di replica, criteri di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock . Tutti i volumi devono avere SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

Tieni presente che se ai volumi scelti sono già applicati criteri di snapshot o di replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora, per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

La definizione della strategia di backup comporta la configurazione delle seguenti opzioni:

- Opzioni di protezione: se si desidera implementare una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura: se si desidera utilizzare un'architettura di backup a fan-out o a cascata
- Criterio di snapshot locale
- Destinazione e politica di replicazione
- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:

- **Snapshot locali**: crea snapshot locali.
- **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
- **Backup**: esegue il backup dei volumi in un bucket su un sistema ONTAP configurato per S3.

2. **Architettura**: se hai scelto sia la replica che il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: i dati di backup fluiscono dal sistema primario a quello secondario e poi da quest'ultimo all'archivio oggetti.
   - **Fan out**: i dati di backup fluiscono dal sistema primario a quello secondario *e* dal sistema primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .

3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   Se si desidera creare una policy personalizzata prima di attivare lo Snapshot, è possibile utilizzare System Manager o ONTAP CLI `snapmirror policy create` comando. Fare riferimento a .

   Per creare una policy personalizzata utilizzando Backup e Ripristino, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.

4. **Replica**: se hai selezionato **Replica**, imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato di destinazione (o gli aggregati per i volumi FlexGroup) e un prefisso o un suffisso che verrà aggiunto al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno nuovo.

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: Seleziona * ONTAP S3*.
   - **Impostazioni del provider**: immettere i dettagli del nome di dominio completo (FQDN) del server S3, la porta, la chiave di accesso e la chiave segreta degli utenti.

     La chiave di accesso e la chiave segreta servono all'utente creato per concedere al cluster ONTAP l'accesso al bucket S3.

   - **Networking**: seleziona lo spazio IP nel cluster ONTAP di origine in cui risiedono i volumi di cui vuoi eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita (non richiesto quando l'agente Console è installato in un sito "dark").

Selezionando lo spazio IP corretto si garantisce che NetApp Backup and Recovery possa impostare una connessione da ONTAP al tuo storage di oggetti ONTAP S3.

- **Criterio di backup**: seleziona un criterio di backup esistente o creane uno nuovo.

  È possibile creare una policy con System Manager o ONTAP CLI. Per creare una policy personalizzata utilizzando ONTAP CLI `snapmirror policy create` comando, fare riferimento a .

  Per creare una policy personalizzata utilizzando Backup e Ripristino, fare riferimento a"Crea una politica" .

  Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

  - Inserisci il nome della policy.
  - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
  - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .
  - Seleziona **Crea**.

- **Esporta snapshot esistenti nell'archivio oggetti come file di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup. Se i criteri non corrispondono, i backup non verranno creati.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati di archiviazione primaria contenuti negli snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di archiviazione primario.

Viene creato un bucket S3 nell'account di servizio indicato dalla chiave di accesso S3 e dalla chiave segreta immesse, e i file di backup vengono archiviati lì.

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando"Pagina di monitoraggio dei lavori" .

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Esegui il backup dei dati ONTAP locali su StorageGRID con NetApp Backup and Recovery

Completa alcuni passaggi in NetApp Backup and Recovery per iniziare a eseguire il backup dei dati del volume dai tuoi sistemi ONTAP primari locali a un sistema di storage secondario e allo storage di oggetti nei tuoi sistemi NetApp StorageGRID .

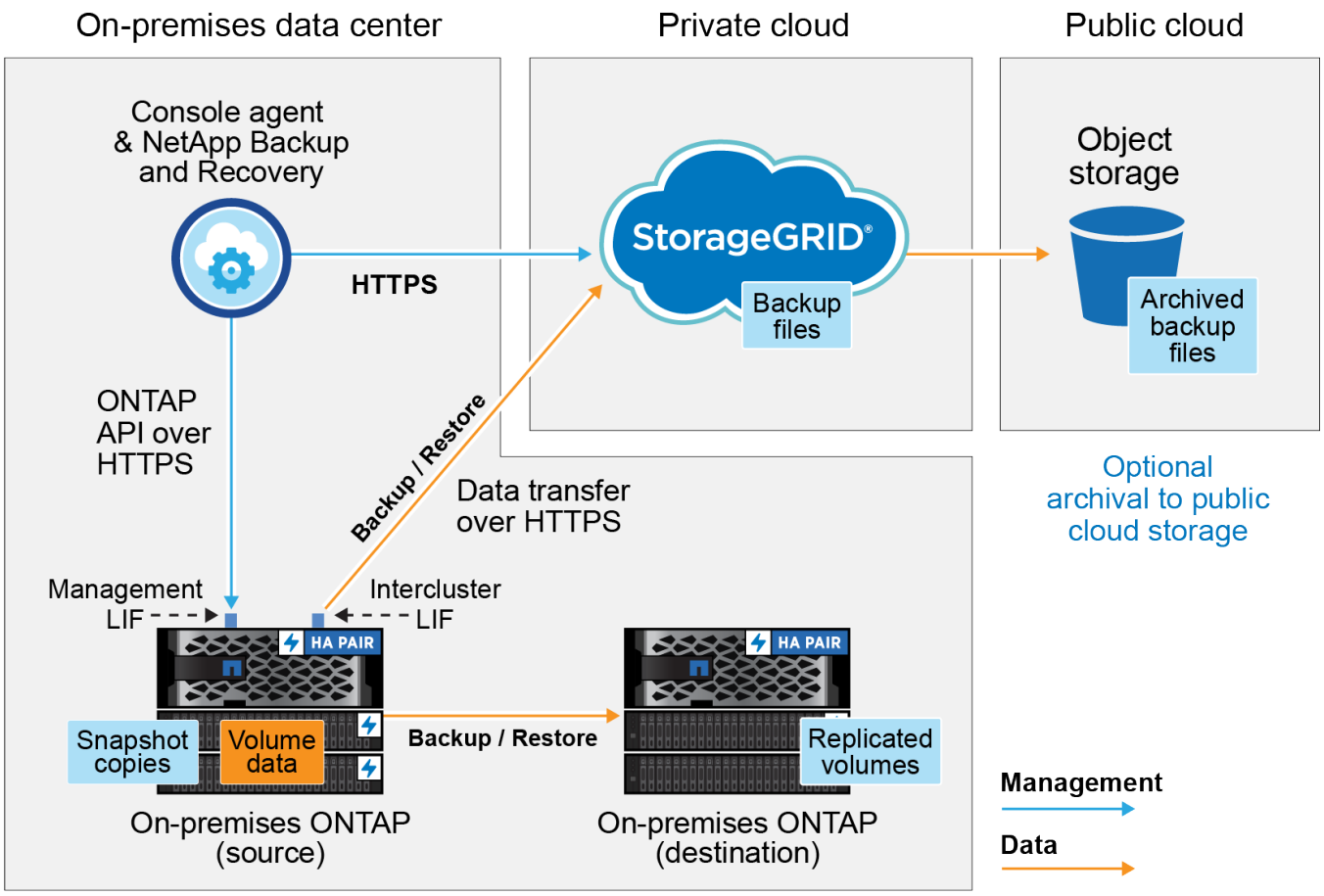
I "sistemi ONTAP on-premises" includono i sistemi FAS, AFF e ONTAP Select .

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Identificare il metodo di connessione

L'immagine seguente mostra ciascun componente durante il backup di un sistema ONTAP locale su StorageGRID e le connessioni che è necessario preparare tra di essi.

Facoltativamente, è possibile connettersi a un sistema ONTAP secondario nella stessa posizione locale per replicare i volumi.



Quando l'agente Console e il sistema ONTAP locale vengono installati in una posizione locale senza accesso a Internet (un "dark site"), il sistema StorageGRID deve trovarsi nello stesso data center locale. L'archiviazione dei vecchi file di backup sul cloud pubblico non è supportata nelle configurazioni dark site.

Prepara il tuo agente Console

L'agente Console è il software principale per la funzionalità Console. Per eseguire il backup e il ripristino dei dati ONTAP è necessario un agente Console.

Crea o cambia agenti della console

Quando si esegue il backup dei dati su StorageGRID, è necessario che un agente Console sia disponibile presso la propria sede. Sarà necessario installare un nuovo agente Console oppure assicurarsi che l'agente Console attualmente selezionato risieda in locale. L'agente Console può essere installato in un sito con o senza accesso a Internet.

- "Scopri di più sugli agenti della console"
- "Installazione dell'agente Console su un host Linux con accesso a Internet"
- "Installazione dell'agente Console su un host Linux senza accesso a Internet"
- "Passaggio tra gli agenti della console"

Preparare i requisiti di rete dell'agente della console

Assicurarsi che la rete in cui è installato l'agente Console consenta le seguenti connessioni:

- Una connessione HTTPS sulla porta 443 al nodo gateway StorageGRID
- Una connessione HTTPS sulla porta 443 al LIF di gestione del cluster ONTAP
- Una connessione Internet in uscita sulla porta 443 verso NetApp Backup and Recovery (non necessaria quando l'agente Console è installato in un sito "oscuro")

Considerazioni sulla modalità privata (sito oscuro)

- La funzionalità NetApp Backup and Recovery è integrata nell'agente Console. Se installato in modalità privata, sarà necessario aggiornare periodicamente il software dell'agente della console per accedere alle nuove funzionalità. Controlla il"NetApp Backup and Recovery: novità" per vedere le nuove funzionalità di ogni versione NetApp Backup and Recovery . Quando vuoi utilizzare le nuove funzionalità, segui i passaggi per "aggiornare il software dell'agente della console" .

  La nuova versione di NetApp Backup and Recovery , che include la possibilità di pianificare e creare snapshot e volumi replicati, oltre a creare backup nell'archiviazione di oggetti, richiede l'utilizzo della versione 3.9.31 o successiva dell'agente Console. Ti consigliamo quindi di scaricare questa versione più recente per gestire tutti i tuoi backup.

- Quando si utilizza NetApp Backup and Recovery in un ambiente SaaS, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel cloud. Quando si utilizza NetApp Backup and Recovery in un sito senza accesso a Internet, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel bucket StorageGRID in cui vengono archiviati i backup.

Verificare i requisiti della licenza

Prima di poter attivare NetApp Backup and Recovery per il tuo cluster, dovrai acquistare e attivare una licenza NetApp Backup and Recovery BYOL da NetApp. Questa licenza è per l'account e può essere utilizzata su più sistemi.

Avrai bisogno del numero di serie di NetApp che ti consentirà di utilizzare il servizio per la durata e la capacità della licenza. "Scopri come gestire le tue licenze BYOL" .

La licenza PAYGO non è supportata durante il backup dei file su StorageGRID.

Prepara i tuoi cluster ONTAP

Preparare il sistema ONTAP locale di origine e tutti i sistemi ONTAP locali secondari o Cloud Volumes ONTAP .

La preparazione dei cluster ONTAP prevede i seguenti passaggi:

- Scopri i tuoi sistemi ONTAP nella NetApp Console
- Verificare i requisiti di sistema ONTAP
- Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti
- Verificare i requisiti di rete ONTAP per la replica dei volumi

Scopri i tuoi sistemi ONTAP nella NetApp Console

Sia il sistema ONTAP locale di origine che eventuali sistemi ONTAP locali secondari o Cloud Volumes ONTAP devono essere disponibili nella pagina **Sistemi** della NetApp Console .

Per aggiungere il cluster, è necessario conoscere l'indirizzo IP di gestione del cluster e la password

dell'account utente amministratore. "Scopri come scoprire un cluster" .

Verificare i requisiti di sistema ONTAP

Assicurati che il tuo sistema ONTAP soddisfi i seguenti requisiti:

- Minimo ONTAP 9.8; si consiglia ONTAP 9.8P13 e versioni successive.
- Una licenza SnapMirror (inclusa come parte del Premium Bundle o del Data Protection Bundle).

  Nota: il "Hybrid Cloud Bundle" non è richiesto quando si utilizza NetApp Backup and Recovery.

  Impara come "gestisci le licenze del tuo cluster" .

- L'ora e il fuso orario sono impostati correttamente. Impara come "configura l'ora del tuo cluster" .
- Se si replicano i dati, verificare che i sistemi di origine e di destinazione eseguano versioni ONTAP compatibili.

  "Visualizza le versioni ONTAP compatibili per le relazioni SnapMirror".

Verificare i requisiti di rete ONTAP per il backup dei dati su storage di oggetti

È necessario configurare i seguenti requisiti sul sistema che si connette all'archiviazione di oggetti.

- Quando si utilizza un'architettura di backup fan-out, è necessario configurare le seguenti impostazioni sul sistema di archiviazione *primario*.
- Quando si utilizza un'architettura di backup a cascata, è necessario configurare le seguenti impostazioni sul sistema di archiviazione *secondario*.

Sono necessari i seguenti requisiti di rete del cluster ONTAP :

- Il cluster ONTAP avvia una connessione HTTPS tramite una porta specificata dall'utente dal LIF intercluster al nodo gateway StorageGRID per le operazioni di backup e ripristino. La porta è configurabile durante la configurazione del backup.

  ONTAP legge e scrive dati da e verso l'archiviazione di oggetti. L'archiviazione degli oggetti non si avvia mai, risponde e basta.

- ONTAP richiede una connessione in ingresso dall'agente della console al LIF di gestione del cluster. L'agente della Console deve risiedere presso la tua sede.
- È necessario un LIF intercluster su ciascun nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup. Il LIF deve essere associato allo *IPspace* che ONTAP deve utilizzare per connettersi all'archiviazione degli oggetti. "Scopri di più su IPspaces" .

  Quando si configura NetApp Backup and Recovery, viene richiesto di specificare lo spazio IP da utilizzare. Dovresti scegliere lo spazio IP a cui è associato ciascun LIF. Potrebbe trattarsi dello spazio IP "predefinito" o di uno spazio IP personalizzato creato da te.

- I LIF intercluster dei nodi sono in grado di accedere all'archivio oggetti (non necessario quando l'agente Console è installato in un sito "dark").
- I server DNS sono stati configurati per la VM di archiviazione in cui si trovano i volumi. Scopri come "configurare i servizi DNS per l'SVM" .
- Se si utilizza uno spazio IP diverso da quello predefinito, potrebbe essere necessario creare un percorso

statico per accedere all'archiviazione degli oggetti.

- Se necessario, aggiornare le regole del firewall per consentire le connessioni del servizio NetApp Backup and Recovery da ONTAP all'archiviazione degli oggetti tramite la porta specificata (in genere la porta 443) e il traffico di risoluzione dei nomi dalla VM di archiviazione al server DNS tramite la porta 53 (TCP/UDP).

Verificare i requisiti di rete ONTAP per la replica dei volumi

Se si prevede di creare volumi replicati su un sistema ONTAP secondario utilizzando NetApp Backup and Recovery, assicurarsi che i sistemi di origine e di destinazione soddisfino i seguenti requisiti di rete.

Requisiti di rete ONTAP in sede

- Se il cluster è in locale, dovresti avere una connessione dalla tua rete aziendale alla tua rete virtuale nel provider cloud. In genere si tratta di una connessione VPN.
- I cluster ONTAP devono soddisfare requisiti aggiuntivi relativi a subnet, porte, firewall e cluster.

  Poiché è possibile replicare su Cloud Volumes ONTAP o su sistemi locali, esaminare i requisiti di peering per i sistemi ONTAP locali. "Visualizza i prerequisiti per il peering dei cluster nella documentazione ONTAP" .

Requisiti di rete Cloud Volumes ONTAP

- Il gruppo di sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste: in particolare, le regole per ICMP e le porte 11104 e 11105. Queste regole sono incluse nel gruppo di sicurezza predefinito.

Prepara StorageGRID come destinazione di backup

StorageGRID deve soddisfare i seguenti requisiti. Vedi il "Documentazione StorageGRID" per maggiori informazioni.

Per i dettagli sui requisiti di DataLock e Ransomware Resilience per StorageGRID, fare riferimento a"Opzioni di policy di backup su oggetto" .

Versioni StorageGRID supportate

StorageGRID 10.3 e versioni successive sono supportati.

Per utilizzare DataLock & Ransomware Resilience per i backup, i sistemi StorageGRID devono eseguire la versione 11.6.0.3 o successiva.

Per suddividere i backup più vecchi in archivi cloud, i sistemi StorageGRID devono eseguire la versione 11.3 o successiva. Inoltre, i sistemi StorageGRID devono essere rilevati nella pagina **Sistemi** della console.

Per l'archiviazione degli utenti è necessario l'accesso IP del nodo amministratore.

L'accesso IP al gateway è sempre necessario.

Credenziali S3

Per controllare l'accesso al tuo storage StorageGRID , devi aver creato un account tenant S3. "Per i dettagli, consultare la documentazione di StorageGRID" .

Quando si configura il backup su StorageGRID, la procedura guidata di backup richiede una chiave di accesso S3 e una chiave segreta per un account tenant. L'account tenant consente a NetApp Backup and Recovery di autenticare e accedere ai bucket StorageGRID utilizzati per archiviare i backup. Le chiavi sono

necessarie affinché StorageGRID sappia chi sta effettuando la richiesta.

Queste chiavi di accesso devono essere associate a un utente che dispone delle seguenti autorizzazioni:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Versionamento degli oggetti

Non è necessario abilitare manualmente il controllo delle versioni degli oggetti StorageGRID sul bucket di archiviazione degli oggetti.

Preparati ad archiviare i vecchi file di backup su un archivio cloud pubblico

L'archiviazione dei file di backup più vecchi consente di risparmiare denaro, utilizzando una classe di archiviazione meno costosa per i backup di cui potresti non aver bisogno. StorageGRID è una soluzione on-premise (cloud privato) che non fornisce archiviazione, ma consente di spostare i file di backup più vecchi nell'archiviazione su cloud pubblico. Quando utilizzati in questo modo, i dati archiviati su cloud storage o ripristinati da cloud storage vengono trasferiti tra StorageGRID e cloud storage: la Console non è coinvolta in questo trasferimento di dati.

Il supporto attuale consente di archiviare i backup nello storage AWS *S3 Glacier*/*S3 Glacier Deep Archive* o *Azure Archive*.

- Requisiti ONTAP *
- Il cluster deve utilizzare ONTAP 9.12.1 o versione successiva.
- Requisiti StorageGRID *
- StorageGRID deve utilizzare la versione 11.4 o successiva.
- Il tuo StorageGRID deve essere "scoperto e disponibile nella Console" .

Requisiti Amazon S3

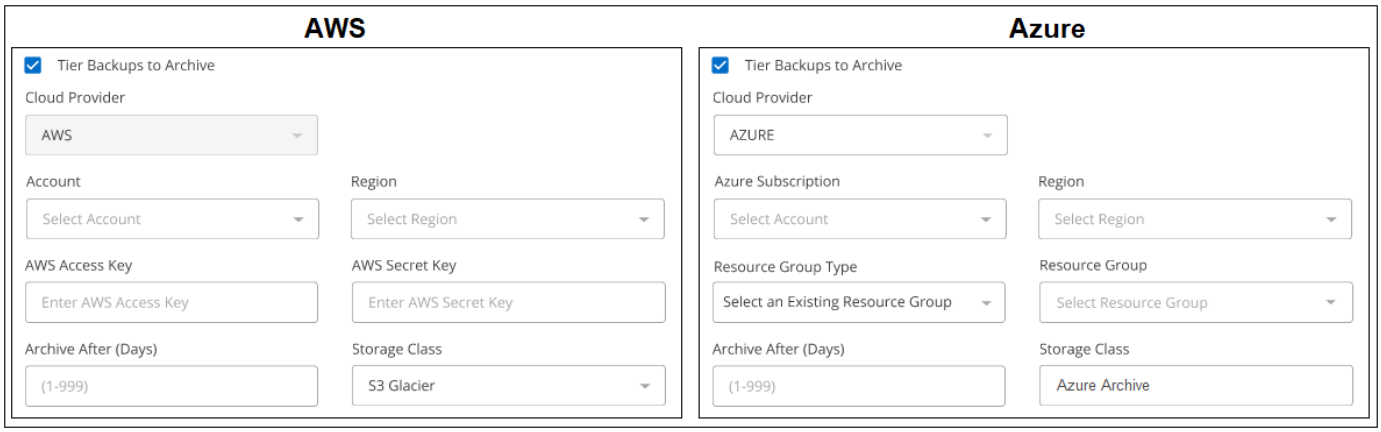
- Sarà necessario registrarsi per un account Amazon S3 per lo spazio di archiviazione in cui verranno archiviati i backup.
- È possibile scegliere di suddividere i backup in livelli su AWS S3 Glacier o S3 Glacier Deep Archive. "Scopri di più sui livelli di archiviazione AWS" .
- StorageGRID dovrebbe avere accesso completo al bucket(`s3:*`); tuttavia, se ciò non è possibile, la policy del bucket deve concedere le seguenti autorizzazioni S3 a StorageGRID:
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`

- s3:ListMultipartUploadParts
- s3:PutObject
- s3:RestoreObject

Requisiti di Azure Blob

- Sarà necessario sottoscrivere un abbonamento Azure per lo spazio di archiviazione in cui verranno archiviati i backup.
- La procedura guidata di attivazione consente di utilizzare un gruppo di risorse esistente per gestire il contenitore BLOB in cui verranno archiviati i backup oppure è possibile creare un nuovo gruppo di risorse.

Quando definisci le impostazioni di archiviazione per la policy di backup del tuo cluster, dovrai immettere le credenziali del tuo provider cloud e selezionare la classe di archiviazione che desideri utilizzare. NetApp Backup and Recovery crea il bucket cloud quando si attiva il backup per il cluster. Di seguito sono riportate le informazioni necessarie per l'archiviazione AWS e Azure.



Le impostazioni dei criteri di archiviazione selezionate genereranno un criterio di gestione del ciclo di vita delle informazioni (ILM) in StorageGRID e aggiungeranno le impostazioni come "regole".

- Se è già presente una policy ILM attiva, verranno aggiunte nuove regole alla policy ILM per spostare i dati al livello di archivio.
- Se esiste una policy ILM nello stato "proposto", non sarà possibile creare e attivare una nuova policy ILM. "Scopri di più sulle policy e le regole StorageGRID ILM" .

Attiva i backup sui tuoi volumi ONTAP

Attiva i backup in qualsiasi momento direttamente dal tuo sistema locale.

Una procedura guidata ti guiderà attraverso i seguenti passaggi principali:

- Seleziona i volumi di cui vuoi eseguire il backup
- Definire la strategia di backup
- Rivedi le tue selezioni

Puoi anche Mostra i comandi API nella fase di revisione, in modo da poter copiare il codice per automatizzare l'attivazione del backup per i sistemi futuri.

Avvia la procedura guidata

Passi

1. Accedere alla procedura guidata di attivazione del backup e del ripristino utilizzando uno dei seguenti metodi:

   - Dalla pagina **Sistemi** della console, selezionare il sistema e selezionare **Abilita > Volumi di backup** accanto a Backup e ripristino nel pannello di destra.

     Se la destinazione dei backup è presente come sistema nella pagina **Sistemi** della console, è possibile trascinare il cluster ONTAP nell'archivio oggetti.

   - Selezionare **Volumi** nella barra Backup e ripristino. Dalla scheda Volumi, seleziona l'opzione **Azioni (…)** e seleziona **Attiva backup** per un singolo volume (che non abbia già abilitato la replica o il backup nell'archiviazione oggetti).

   La pagina Introduzione della procedura guidata mostra le opzioni di protezione, tra cui snapshot locali, replica e backup. Se in questo passaggio è stata scelta la seconda opzione, verrà visualizzata la pagina Definisci strategia di backup con un volume selezionato.

2. Proseguire con le seguenti opzioni:

   - Se hai già un agente Console, sei a posto. Basta selezionare **Avanti**.
   - Se non si dispone già di un agente Console, viene visualizzata l'opzione **Aggiungi un agente Console**. Fare riferimento aPrepara il tuo agente Console .

Seleziona i volumi di cui vuoi eseguire il backup

Seleziona i volumi che vuoi proteggere. Un volume protetto è un volume che presenta una o più delle seguenti caratteristiche: criterio di snapshot, criterio di replica, criterio di backup su oggetto.

È possibile scegliere di proteggere i volumi FlexVol o FlexGroup ; tuttavia, non è possibile selezionare una combinazione di questi volumi quando si attiva il backup per un sistema. Scopri come"attiva il backup per volumi aggiuntivi nel sistema" (FlexVol o FlexGroup) dopo aver configurato il backup per i volumi iniziali.

- È possibile attivare un backup solo su un singolo volume FlexGroup alla volta.
- I volumi selezionati devono avere la stessa impostazione SnapLock . Tutti i volumi devono avere SnapLock Enterprise abilitato o SnapLock disabilitato.

Passi

Se ai volumi scelti sono già applicati criteri di snapshot o replica, i criteri selezionati in seguito sovrascriveranno quelli esistenti.

1. Nella pagina Seleziona volumi, seleziona il volume o i volumi che desideri proteggere.
   - Facoltativamente, filtra le righe per visualizzare solo i volumi con determinati tipi di volume, stili e altro ancora, per semplificare la selezione.
   - Dopo aver selezionato il primo volume, è possibile selezionare tutti i volumi FlexVol (i volumi FlexGroup possono essere selezionati solo uno alla volta). Per eseguire il backup di tutti i volumi FlexVol esistenti, selezionare prima un volume e poi la casella nella riga del titolo.
   - Per eseguire il backup di singoli volumi, selezionare la casella per ciascun volume.
2. Selezionare **Avanti**.

Definire la strategia di backup

Per definire la strategia di backup è necessario impostare le seguenti opzioni:

- Se desideri una o tutte le opzioni di backup: snapshot locali, replica e backup su storage di oggetti
- Architettura
- Criterio di snapshot locale
- Destinazione e politica di replicazione

> Se i volumi scelti hanno policy di snapshot e replica diverse da quelle selezionate in questo passaggio, le policy esistenti verranno sovrascritte.

- Backup delle informazioni di archiviazione degli oggetti (provider, crittografia, rete, criteri di backup e opzioni di esportazione).

Passi

1. Nella pagina Definisci strategia di backup, seleziona una o tutte le seguenti opzioni. Per impostazione predefinita, sono selezionate tutte e tre:
   - **Snapshot locali**: se si esegue la replica o il backup su un archivio di oggetti, è necessario creare snapshot locali.
   - **Replica**: crea volumi replicati su un altro sistema di archiviazione ONTAP .
   - **Backup**: esegue il backup dei volumi nell'archiviazione degli oggetti.
2. **Architettura**: se hai scelto sia la replica che il backup, seleziona uno dei seguenti flussi di informazioni:
   - **A cascata**: le informazioni fluiscono dal primario al secondario e poi dal secondario all'archiviazione degli oggetti.
   - **Distribuzione a ventaglio**: le informazioni fluiscono dal primario al secondario *e* dal primario all'archiviazione degli oggetti.

     Per i dettagli su queste architetture, fare riferimento a"Pianifica il tuo percorso di protezione" .
3. **Snapshot locale**: scegli un criterio di snapshot esistente o creane uno nuovo.

   > Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

   Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:
   - Inserisci il nome della policy.
   - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
   - Seleziona **Crea**.
4. **Replica**: Imposta le seguenti opzioni:
   - **Destinazione di replica**: selezionare il sistema di destinazione e l'SVM. Facoltativamente, selezionare l'aggregato o gli aggregati di destinazione e il prefisso o il suffisso che verranno aggiunti al nome del volume replicato.
   - **Criterio di replicazione**: scegli un criterio di replicazione esistente o creane uno.

     > Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

- Inserisci il nome della policy.
- Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
- Seleziona **Crea**.

5. **Backup su oggetto**: se hai selezionato **Backup**, imposta le seguenti opzioni:
   - **Provider**: Seleziona * StorageGRID*.
   - **Impostazioni del provider**: immettere i dettagli FQDN del nodo gateway del provider, la porta, la chiave di accesso e la chiave segreta.

     La chiave di accesso e la chiave segreta sono destinate all'utente IAM creato per consentire al cluster ONTAP di accedere al bucket.

   - **Networking**: selezionare lo spazio IP nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita (non richiesto quando l'agente Console è installato in un sito "dark").

     Selezionando lo spazio IP corretto si garantisce che NetApp Backup and Recovery possa impostare una connessione da ONTAP al tuo storage di oggetti StorageGRID .

   - **Criterio di backup**: seleziona un criterio di backup su archiviazione oggetti esistente o creane uno.

     Per creare una policy personalizzata, fare riferimento a"Crea una politica" .

     Per creare una policy, seleziona **Crea nuova policy** e procedi come segue:

     - Inserisci il nome della policy.
     - Selezionare fino a cinque pianificazioni, in genere con frequenze diverse.
     - Per i criteri di backup su oggetto, impostare le impostazioni DataLock e Ransomware Resilience. Per i dettagli su DataLock e Ransomware Resilience, fare riferimento a"Impostazioni dei criteri di backup su oggetto" .

       Se il tuo cluster utilizza ONTAP 9.11.1 o versione successiva, puoi scegliere di proteggere i tuoi backup da eliminazioni e attacchi ransomware configurando *DataLock e Ransomware Resilience*. *DataLock* protegge i file di backup da modifiche o eliminazioni, mentre *Ransomware Resilience* esegue la scansione dei file di backup per cercare prove di un attacco ransomware nei file di backup.

     - Seleziona **Crea**.

     Se il cluster utilizza ONTAP 9.12.1 o versione successiva e il sistema StorageGRID utilizza la versione 11.4 o versione successiva, è possibile scegliere di suddividere i backup più vecchi in livelli di archivio cloud pubblico dopo un certo numero di giorni. Il supporto attuale riguarda i livelli di archiviazione AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive. Scopri come configurare i tuoi sistemi per questa funzionalità .

   - **Backup a livelli su cloud pubblico**: seleziona il provider cloud su cui desideri eseguire il backup a livelli e inserisci i dettagli del provider.

     Seleziona o crea un nuovo cluster StorageGRID . Per i dettagli sulla creazione di un cluster StorageGRID in modo che la Console possa rilevarlo, fare riferimento a "Documentazione

StorageGRID" .

- **Esporta snapshot esistenti nell'archivio oggetti come copie di backup**: se sono presenti snapshot locali per i volumi in questo sistema che corrispondono all'etichetta di pianificazione del backup appena selezionata per questo sistema (ad esempio, giornaliera, settimanale, ecc.), viene visualizzato questo prompt aggiuntivo. Seleziona questa casella per copiare tutti gli snapshot storici nell'archivio oggetti come file di backup, per garantire la protezione più completa per i tuoi volumi.

6. Selezionare **Avanti**.

Rivedi le tue selezioni

Questa è l'occasione per rivedere le tue selezioni e apportare modifiche, se necessario.

Passi

1. Nella pagina Revisione, rivedi le tue selezioni.
2. Facoltativamente, seleziona la casella per **Sincronizzare automaticamente le etichette dei criteri Snapshot con le etichette dei criteri di replica e backup**. In questo modo vengono creati snapshot con un'etichetta che corrisponde alle etichette nei criteri di replica e backup.
3. Seleziona **Attiva backup**.

Risultato

NetApp Backup and Recovery inizia a eseguire i backup iniziali dei volumi. Il trasferimento di base del volume replicato e del file di backup include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati di archiviazione primaria contenuti negli snapshot.

Nel cluster di destinazione viene creato un volume replicato che verrà sincronizzato con il volume di archiviazione primario.

Viene creato un bucket S3 nell'account di servizio indicato dalla chiave di accesso S3 e dalla chiave segreta immesse, e i file di backup vengono archiviati lì.

Viene visualizzata la dashboard di backup del volume, in modo da poter monitorare lo stato dei backup.

È inoltre possibile monitorare lo stato dei processi di backup e ripristino utilizzando"Pagina di monitoraggio dei lavori" .

Mostra i comandi API

Potrebbe essere necessario visualizzare e, facoltativamente, copiare i comandi API utilizzati nella procedura guidata Attiva backup e ripristino. Potresti voler fare questo per automatizzare l'attivazione del backup nei sistemi futuri.

Passi

1. Dalla procedura guidata Attiva backup e ripristino, seleziona **Visualizza richiesta API**.
2. Per copiare i comandi negli appunti, selezionare l'icona **Copia**.

Migrare i volumi utilizzando SnapMirror su Cloud Resync in NetApp Backup and Recovery

La funzionalità SnapMirror to Cloud Resync di NetApp Backup and Recovery semplifica la protezione e la continuità dei dati durante le migrazioni dei volumi negli ambienti NetApp . Quando un volume viene migrato tramite SnapMirror Logical Replication

(LRSE) da una distribuzione NetApp locale a un'altra o a una soluzione basata su cloud come Cloud Volumes ONTAP, SnapMirror to Cloud Resync garantisce che i backup cloud esistenti rimangano intatti e operativi.

Questa funzionalità elimina la necessità di un processo di riconfigurazione della baseline e consente di continuare i backup dopo la migrazione. Questa funzionalità è utile negli scenari di migrazione del carico di lavoro, supportando sia FlexVols che FlexGroups ed è disponibile a partire dalla versione 9.16.1 ONTAP .

Questa funzionalità è disponibile a partire dalla versione 4.0.3 NetApp Backup and Recovery, rilasciata a maggio 2025.

SnapMirror to Cloud Resync mantiene la continuità del backup tra gli ambienti, semplificando la gestione dei dati in configurazioni ibride e multi-cloud.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Prima di iniziare

Assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Il cluster ONTAP di destinazione deve eseguire ONTAP versione 9.16.1 o successiva.
- Il vecchio cluster ONTAP di origine deve essere protetto tramite NetApp Backup and Recovery.
- La funzionalità SnapMirror to Cloud Resync è disponibile a partire dalla versione 4.0.3 NetApp Backup and Recovery, rilasciata a maggio 2025.
- Assicurarsi che l'ultimo backup nell'archivio oggetti sia lo snapshot comune tra la vecchia origine, la nuova origine e l'archivio oggetti. Non utilizzare uno snapshot comune più vecchio dell'ultimo snapshot sottoposto a backup nell'archivio oggetti.
- Sia i criteri snapshot che SnapMirror utilizzati sul vecchio cluster ONTAP devono essere creati sul nuovo cluster ONTAP prima di avviare l'operazione di risincronizzazione. Se si utilizza un criterio nel processo di risincronizzazione, è necessario anche creare tale criterio. L'operazione di risincronizzazione non crea policy.
- Assicurarsi che il criterio SnapMirror applicato alla relazione SnapMirror del volume di migrazione includa la stessa etichetta utilizzata dalla relazione cloud. Per evitare problemi, utilizzare la policy che gestisce un mirror esatto del volume e di tutti gli snapshot.

Al momento, SnapMirror su Cloud Resync dopo le migrazioni tramite i metodi SVM-Migrate, SVM-DR o Head Swap non è supportato.

Come funziona NetApp Backup and Recovery SnapMirror to Cloud Resync

Se si completa un aggiornamento tecnico o si migrano volumi da un cluster ONTAP a un altro, è importante che i backup continuino a funzionare senza interruzioni. NetApp Backup and Recovery SnapMirror to Cloud Resync aiuta in questo, garantendo che i backup cloud rimangano coerenti anche dopo una migrazione del volume.

Ecco un esempio:

Immagina di avere un volume locale denominato Vol1a. Questo volume contiene tre istantanee: S1, S2 e S3. Questi snapshot sono punti di ripristino. Il backup di Vol1 sul cloud avviene tramite SnapMirror to Cloud (SM-C), ma solo S1 e S2 sono presenti nell'archivio oggetti.

Ora vuoi migrare Vol1 su un altro cluster ONTAP . Per fare ciò, si crea una relazione SnapMirror Logical Replication (LRSE) su un nuovo volume cloud denominato Vol1b. In questo modo vengono trasferiti tutti e tre gli snapshot (S1, S2 e S3) da Vol1a a Vol1b.

Una volta completata la migrazione, la configurazione sarà la seguente:

- La relazione SM-C originale (Vol1a → Archivio oggetti) viene eliminata.
- Viene eliminata anche la relazione LRSE (Vol1a → Vol1b).
- Vol1b è ora il tuo volume attivo.

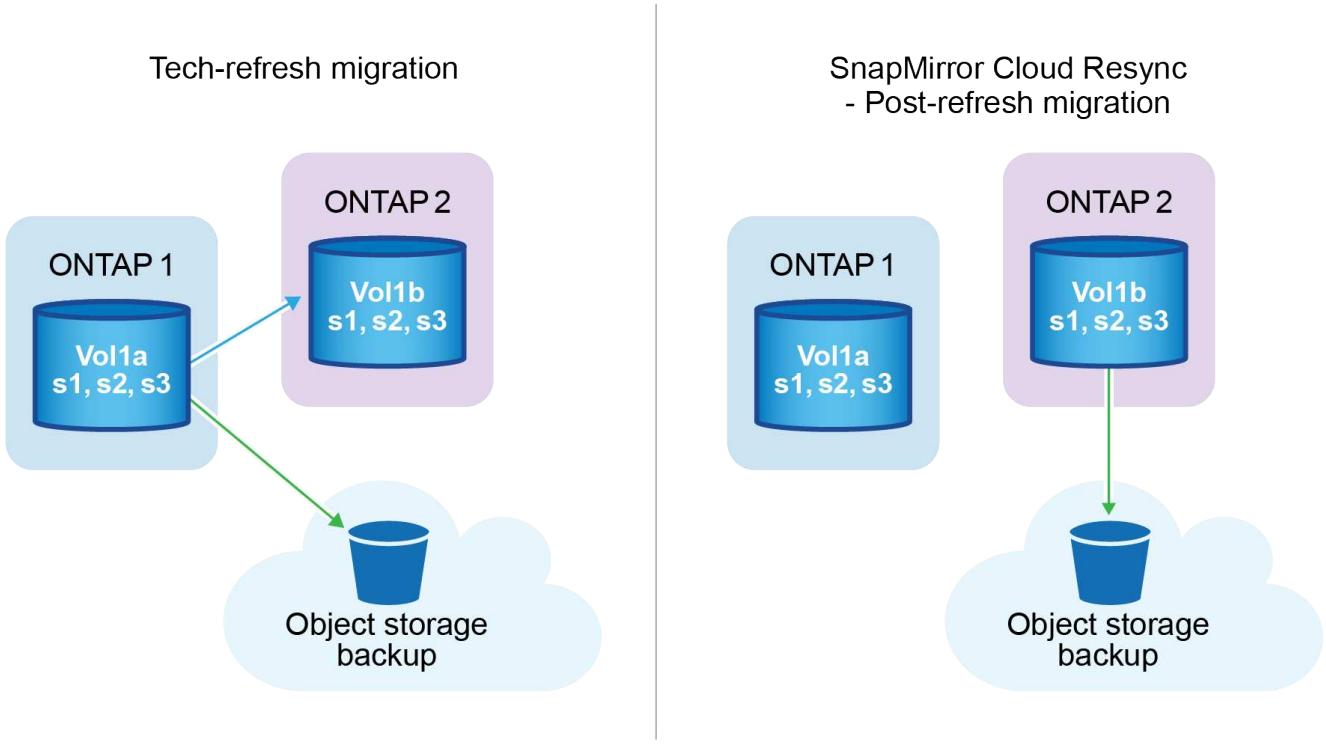
A questo punto, si desidera continuare a eseguire il backup di Vol1b sullo stesso endpoint cloud. Ma invece di avviare un backup completo da zero (che richiederebbe tempo e risorse), puoi usare SnapMirror per Cloud Resync.

Ecco come funziona la risincronizzazione:

- Il sistema verifica la presenza di uno snapshot comune tra Vol1a e Object Store. In questo caso, entrambi hanno S2.
- Grazie a questa istantanea condivisa, il sistema deve trasferire solo le modifiche incrementali tra S2 e S3.

Ciò significa che solo i nuovi dati aggiunti dopo S2 vengono inviati all'archivio oggetti, non l'intero volume.

Questo processo impedisce backup duplicati, consente di risparmiare larghezza di banda e mantiene i backup in esecuzione dopo la migrazione.



Note sulla procedura

- Le migrazioni e gli aggiornamenti tecnologici non vengono eseguiti tramite NetApp Backup and Recovery. Dovrebbero essere eseguiti da un team di servizi professionali o da un amministratore di storage

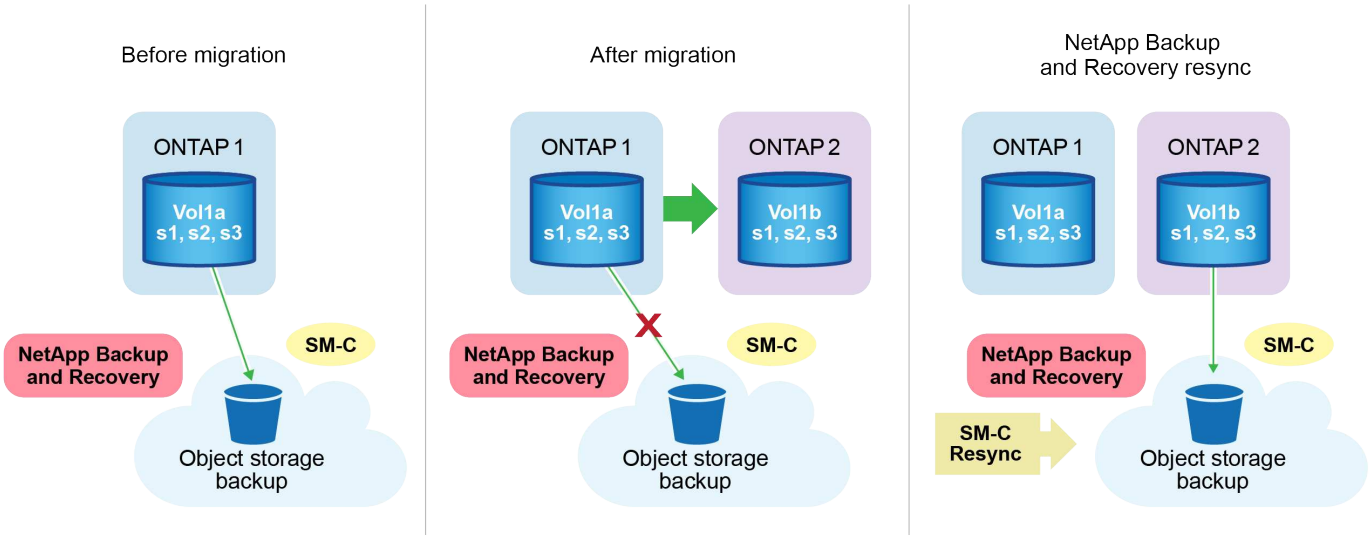
qualificato.

- Un team di migrazione NetApp crea la relazione SnapMirror tra i cluster ONTAP di origine e di destinazione per agevolare lo spostamento dei volumi.
- Assicurarsi che la migrazione durante un aggiornamento tecnologico sia basata sulla migrazione basata su SnapMirror.

Come migrare i volumi utilizzando SnapMirror su Cloud Resync

La migrazione dei volumi tramite SnapMirror su Cloud Resync prevede i seguenti passaggi principali, ciascuno descritto più dettagliatamente di seguito:

- **Seguire una checklist pre-migrazione**: prima di iniziare la migrazione, un team NetApp Tech Refresh verifica che siano soddisfatti i seguenti prerequisiti per evitare la perdita di dati e garantire un processo di migrazione senza intoppi.
- **Seguire una checklist post-migrazione**: dopo la migrazione, un team NetApp Tech Refresh verifica che vengano completati i seguenti passaggi per stabilire la protezione e preparare la risincronizzazione.
- **Eseguire un'operazione di risincronizzazione SnapMirror a Cloud**: dopo la migrazione, un team NetApp Tech Refresh esegue un'operazione di risincronizzazione SnapMirror a Cloud per riprendere i backup su cloud dai volumi appena migrati.



Seguire una checklist pre-migrazione

Prima della migrazione, il team NetApp Tech Refresh verifica questi prerequisiti per evitare la perdita di dati e garantire un processo senza intoppi.

1. Assicurarsi che tutti i volumi da migrare siano protetti tramite NetApp Backup and Recovery.
2. Registra gli UUID delle istanze del volume. Annotare gli UUID delle istanze di tutti i volumi prima di avviare la migrazione. Questi identificatori sono fondamentali per le successive operazioni di mappatura e risincronizzazione.
3. Eseguire uno snapshot finale di ciascun volume per preservare lo stato più recente, prima di eliminare qualsiasi relazione SnapMirror .
4. Criteri SnapMirror del documento. Registrare la policy SnapMirror attualmente associata alla relazione di ciascun volume. Questo sarà necessario in seguito durante il processo di risincronizzazione da SnapMirror a Cloud.

5. Eliminare le relazioni di SnapMirror Cloud con l'archivio oggetti.
6. Creare una relazione SnapMirror standard con il nuovo cluster ONTAP per migrare il volume al nuovo cluster ONTAP di destinazione.

Seguire una checklist post-migrazione

Dopo la migrazione, un team NetApp Tech Refresh verifica che vengano completati i seguenti passaggi per stabilire la protezione e preparare la risincronizzazione.

1. Registra i nuovi UUID delle istanze di volume di tutti i volumi migrati nel cluster ONTAP di destinazione.
2. Verificare che tutti i criteri SnapMirror richiesti disponibili nel vecchio cluster ONTAP siano configurati correttamente nel nuovo cluster ONTAP .
3. Aggiungere il nuovo cluster ONTAP come sistema nella pagina **Sistemi** della Console.

> Deve essere utilizzato l'UUID dell'istanza del volume, non l'ID del volume. L'UUID dell'istanza del volume è un identificatore univoco che rimane coerente durante le migrazioni, mentre l'ID del volume può cambiare dopo la migrazione.

Eseguire una risincronizzazione SnapMirror su Cloud

Dopo la migrazione, un team NetApp Tech Refresh esegue un'operazione SnapMirror to Cloud Resync per riprendere i backup cloud dai volumi appena migrati.

1. Aggiungere il nuovo cluster ONTAP come sistema nella pagina **Sistemi** della Console.
2. Consultare la pagina NetApp Backup and Recovery Volumes per assicurarsi che i dettagli del vecchio sistema di origine siano disponibili.
3. Dalla pagina NetApp Backup and Recovery Volumes, seleziona **Impostazioni di backup**.
   - Nella pagina Impostazioni di backup, seleziona **Visualizza tutto**.
   - Dal menu Azioni … a destra della *nuova* origine, seleziona **Risincronizza backup**.
4. Nella pagina del sistema di risincronizzazione, procedere come segue:
   a. **Nuovo sistema sorgente**: immettere il nuovo cluster ONTAP in cui sono stati migrati i volumi.
   b. **Archivio oggetti di destinazione esistente**: selezionare l'archivio oggetti di destinazione che contiene i backup del vecchio sistema di origine.
5. Selezionare **Scarica modello CSV** per scaricare il foglio Excel dei dettagli di risincronizzazione. Utilizzare questo foglio per immettere i dettagli dei volumi da migrare. Nel file CSV, inserisci i seguenti dettagli:
   - Il vecchio UUID dell'istanza del volume dal cluster di origine
   - Il nuovo UUID dell'istanza del volume dal cluster di destinazione
   - Criterio SnapMirror da applicare alla nuova relazione.
6. Selezionare **Carica** in **Carica dettagli mapping volume** per caricare il foglio CSV completato nell'interfaccia utente NetApp Backup and Recovery .

> Deve essere utilizzato l'UUID dell'istanza del volume, non l'ID del volume. L'UUID dell'istanza del volume è un identificatore univoco che rimane coerente durante le migrazioni, mentre l'ID del volume può cambiare dopo la migrazione.

7. Immettere le informazioni di configurazione del provider e della rete necessarie per l'operazione di

risincronizzazione.

8. Selezionare **Invia** per avviare il processo di convalida.

   NetApp Backup and Recovery verifica che ogni volume selezionato per la risincronizzazione sia lo snapshot più recente e disponga di almeno uno snapshot comune. Ciò garantisce che i volumi siano pronti per l'operazione SnapMirror to Cloud Resync.

9. Esaminare i risultati della convalida, inclusi i nuovi nomi dei volumi di origine e lo stato di risincronizzazione per ciascun volume.
10. Verificare l'idoneità del volume. Il sistema verifica se i volumi sono idonei per la risincronizzazione. Se un volume non è idoneo, significa che non si tratta dell'ultimo snapshot oppure non è stato trovato alcun snapshot comune.

    Per garantire che i volumi rimangano idonei per l'operazione SnapMirror su Cloud Resync, eseguire uno snapshot finale di ciascun volume prima di eliminare qualsiasi relazione SnapMirror durante la fase di pre-migrazione. In questo modo si preserva lo stato più recente dei dati.

11. Selezionare **Risincronizzazione** per avviare l'operazione di risincronizzazione. Il sistema utilizza lo snapshot più recente e comune per trasferire solo le modifiche incrementali, garantendo la continuità del backup.
12. Monitorare il processo di risincronizzazione nella pagina Job Monitor.

Ripristinare i dati di configurazione di NetApp Backup and Recovery in un sito oscuro

Quando si utilizza NetApp Backup and Recovery in un sito senza accesso a Internet, noto come *modalità privata*, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel bucket StorageGRID o ONTAP S3 in cui vengono archiviati i backup. In caso di problemi con il sistema host dell'agente Console, è possibile distribuire un nuovo agente Console e ripristinare i dati critici NetApp Backup and Recovery .

Questa procedura si applica solo ai dati di volume ONTAP .

Quando si utilizza NetApp Backup and Recovery in un ambiente SaaS con l'agente Console distribuito presso il provider cloud o sul proprio host connesso a Internet, il sistema esegue il backup e protegge tutti i dati di configurazione importanti nel cloud. Se riscontri un problema con l'agente Console, crea un nuovo agente Console e aggiungi i tuoi sistemi. I dettagli del backup vengono ripristinati automaticamente.

Esistono due tipi di dati sottoposti a backup:

- Database NetApp Backup and Recovery : contiene un elenco di tutti i volumi, file di backup, policy di backup e informazioni di configurazione.
- File di catalogo indicizzati: contengono indici dettagliati utilizzati per la funzionalità di ricerca e ripristino, che rendono le ricerche molto rapide ed efficienti quando si cercano dati di volume che si desidera ripristinare.

Questi dati vengono sottoposti a backup una volta al giorno a mezzanotte e vengono conservate al massimo 7 copie di ciascun file. Se l'agente Console gestisce più sistemi ONTAP locali, i file NetApp Backup and

Recovery vengono archiviati nel bucket del sistema attivato per primo.

Nessun dato di volume viene mai incluso nel database NetApp Backup and Recovery o nei file del catalogo indicizzato.

Ripristina i dati NetApp Backup and Recovery su un nuovo agente Console

Se l'agente della console locale smette di funzionare, sarà necessario installare un nuovo agente della console e quindi ripristinare i dati di NetApp Backup and Recovery sul nuovo agente della console.

Per ripristinare il funzionamento del sistema NetApp Backup and Recovery, è necessario eseguire le seguenti operazioni:

- Installa un nuovo agente Console
- Ripristinare il database NetApp Backup and Recovery
- Ripristina i file del catalogo indicizzato
- Riscopri tutti i tuoi sistemi ONTAP on-premise e i sistemi StorageGRID nell'interfaccia utente NetApp Console

Dopo aver verificato il funzionamento del sistema, crea nuovi file di backup.

Cosa ti servirà

Sarà necessario accedere ai backup più recenti del database e dell'indice dal bucket StorageGRID o ONTAP S3 in cui sono archiviati i file di backup:

- File del database MySQL NetApp Backup and Recovery

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/mysql_backup/` , e si chiama `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- File zip di backup del catalogo indicizzato

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/catalog_backup/` , e si chiama `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installa un nuovo agente Console su un nuovo host Linux locale

Quando si installa un nuovo agente Console, scaricare la stessa versione software dell'agente originale. Le modifiche apportate al database NetApp Backup and Recovery potrebbero impedire il funzionamento delle versioni software più recenti con i vecchi backup del database. Puoi "aggiornare il software dell'agente della console alla versione più recente dopo aver ripristinato il database di backup" .

1. "Installa l'agente Console su un nuovo host Linux locale"
2. Accedi alla Console utilizzando le credenziali utente amministratore appena create.

Ripristinare il database NetApp Backup and Recovery

1. Copiare il backup MySQL dalla posizione di backup al nuovo host dell'agente della console. Di seguito utilizzeremo il nome file di esempio "CBS_DB_Backup_23_05_2023.sql".
2. Copiare il backup nel contenitore Docker MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Accedere alla shell del contenitore MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Nella shell del contenitore, distribuire "env".
5. Ti servirà la password del database MySQL, quindi copia il valore della chiave "MYSQL_ROOT_PASSWORD".
6. Ripristinare il database MySQL NetApp Backup and Recovery utilizzando il seguente comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verificare che il database MySQL NetApp Backup and Recovery sia stato ripristinato correttamente utilizzando i seguenti comandi SQL:

```
mysql -u root -p cloud_backup
```

8. Inserisci la password.

```
mysql> show tables;
mysql> select * from volume;
```

9. Assicurarsi che i volumi visualizzati siano gli stessi presenti nell'ambiente originale.

Ripristina i file del catalogo indicizzato

1. Copiare il file zip di backup del catalogo indicizzato (utilizzeremo il nome file di esempio "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip") dalla posizione di backup al nuovo host dell'agente della console nella cartella "/opt/application/netapp/cbs".
2. Decomprimere il file "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" utilizzando il seguente comando:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Eseguire il comando **ls** per assicurarsi che sia stata creata la cartella "catalogdb1" con le sottocartelle "changes" e "snapshots".

Scopri i tuoi cluster ONTAP e i sistemi StorageGRID

1. "Scopri tutti i sistemi ONTAP on-prem"che erano disponibili nel tuo ambiente precedente. Ciò include il sistema ONTAP utilizzato come server S3.
2. "Scopri i tuoi sistemi StorageGRID".

Impostare i dettagli dell'ambiente StorageGRID

Aggiungere i dettagli del sistema StorageGRID associato ai sistemi ONTAP così come sono stati configurati nella configurazione originale dell'agente della console utilizzando "API NetApp Console" .

Le seguenti informazioni si applicano alle installazioni in modalità privata a partire da NetApp Console 3.9.xx. Per le versioni precedenti, utilizzare la seguente procedura: "DarkSite Cloud Backup: backup e ripristino di MySQL e catalogo indicizzato" .

Sarà necessario eseguire questi passaggi per ogni sistema che esegue il backup dei dati su StorageGRID.

1. Estrarre il token di autorizzazione utilizzando la seguente API oauth/token.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

Mentre l'indirizzo IP, il nome utente e le password sono valori personalizzati, il nome dell'account non lo è. Il nome dell'account è sempre "account-DARKSITE1". Inoltre, il nome utente deve essere formattato come indirizzo email.

Questa API restituirà una risposta simile alla seguente. È possibile recuperare il token di autorizzazione come mostrato di seguito.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Estrarre l'ID di sistema e l'X-Agent-Id utilizzando l'API tenancy/external/resource.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Questa API restituirà una risposta simile alla seguente. Il valore sotto "resourceIdentifier" indica *WorkingEnvironment Id* e il valore sotto "agentId" indica *x-agent-id*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. Aggiornare il database NetApp Backup and Recovery con i dettagli del sistema StorageGRID associato ai sistemi. Assicurarsi di immettere il nome di dominio completo di StorageGRID, nonché la chiave di accesso e la chiave di archiviazione come mostrato di seguito:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Verificare le impostazioni NetApp Backup and Recovery

1. Selezionare ciascun sistema ONTAP e fare clic su **Visualizza backup** accanto al servizio Backup e ripristino nel pannello di destra.

   Dovresti vedere tutti i backup creati per i tuoi volumi.

2. Nella Dashboard di ripristino, nella sezione Cerca e ripristina, fai clic su **Impostazioni di indicizzazione**.

   Assicurarsi che i sistemi in cui era abilitata in precedenza la catalogazione indicizzata rimangano abilitati.

3. Dalla pagina Cerca e ripristina, esegui alcune ricerche nel catalogo per confermare che il ripristino del catalogo indicizzato sia stato completato correttamente.

Gestisci i backup per i tuoi sistemi ONTAP con NetApp Backup and Recovery

Con NetApp Backup and Recovery puoi gestire i backup per i tuoi sistemi Cloud Volumes ONTAP e ONTAP on-premise modificando la pianificazione dei backup, abilitando/disabilitando i backup dei volumi, sospendendo i backup, eliminando i backup, forzando l'eliminazione dei backup e molto altro. Ciò include tutti i tipi di backup, tra cui snapshot, volumi replicati e file di backup nell'archiviazione di oggetti. È anche possibile annullare la registrazione NetApp Backup and Recovery.

Non gestire o modificare i file di backup direttamente sui tuoi sistemi di archiviazione o dall'ambiente del tuo provider cloud. Ciò potrebbe danneggiare i file e dar luogo a una configurazione non supportata.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

Visualizza lo stato di backup dei volumi nei tuoi sistemi

È possibile visualizzare un elenco di tutti i volumi attualmente sottoposti a backup nella dashboard di backup dei volumi. Ciò include tutti i tipi di backup, tra cui snapshot, volumi replicati e file di backup nell'archiviazione di oggetti. È anche possibile visualizzare i volumi nei sistemi di cui non è attualmente in corso il backup.

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Selezionare il menu **Volumi** per visualizzare l'elenco dei volumi sottoposti a backup per i sistemi Cloud Volumes ONTAP e ONTAP locali.
3. Se stai cercando volumi specifici in determinati sistemi, puoi restringere l'elenco in base al sistema e al volume. È anche possibile utilizzare il filtro di ricerca oppure ordinare le colonne in base allo stile del volume (FlexVol o FlexGroup), al tipo di volume e altro ancora.

   Per visualizzare colonne aggiuntive (aggregati, stile di sicurezza (Windows o UNIX), criterio di snapshot, criterio di replica e criterio di backup), selezionare il segno più.

4. Controllare lo stato delle opzioni di protezione nella colonna "Protezione esistente". Le 3 icone stanno per "Snapshot locali", "Volumi replicati" e "Backup nell'archiviazione di oggetti".

   Ogni icona è illuminata quando il tipo di backup è attivato, mentre è grigia quando il tipo di backup è inattivo. È possibile passare il cursore su ciascuna icona per visualizzare la policy di backup utilizzata e altre informazioni pertinenti per ciascun tipo di backup.

Attiva il backup su volumi aggiuntivi in un sistema

Se hai attivato il backup solo su alcuni volumi di un sistema quando hai abilitato per la prima volta NetApp Backup and Recovery, puoi attivare i backup su volumi aggiuntivi in un secondo momento.

Passi

1. Dalla scheda **Volumi**, identifica il volume su cui desideri attivare i backup, seleziona il menu Azioni ••• alla fine della riga e seleziona **Attiva protezione 3-2-1**.
2. Nella pagina *Definisci strategia di backup*, seleziona l'architettura di backup, quindi definisci i criteri e altri dettagli per snapshot locali, volumi replicati e file di backup. Consulta i dettagli per le opzioni di backup dai volumi iniziali attivati in questo sistema. Quindi seleziona **Avanti**.
3. Rivedere le impostazioni di backup per questo volume, quindi selezionare **Attiva backup**.

Modificare le impostazioni di backup assegnate ai volumi esistenti

È possibile modificare i criteri di backup assegnarti ai volumi esistenti a cui sono stati assegnati criteri. È possibile modificare i criteri per gli snapshot locali, i volumi replicati e i file di backup. Ogni nuovo snapshot, replica o criterio di backup che si desidera applicare ai volumi deve già esistere.

Modifica le impostazioni di backup su un singolo volume

Passi

1. Dal menu **Volumi**, individuare il volume per il quale si desidera modificare le impostazioni dei criteri, selezionare il menu Azioni ••• alla fine della riga e seleziona **Modifica strategia di backup**.
2. Nella pagina *Modifica strategia di backup*, apportare modifiche ai criteri di backup esistenti per snapshot locali, volumi replicati e file di backup e selezionare **Avanti**.

   Se hai abilitato *DataLock e Ransomware Resilience* per i backup cloud nella policy di backup iniziale durante l'attivazione NetApp Backup and Recovery per questo cluster, vedrai solo le altre policy configurate con DataLock. Se non hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery, vedrai solo altri criteri di backup cloud che non hanno DataLock configurato.

3. Rivedere le impostazioni di backup per questo volume, quindi selezionare **Attiva backup**.

Modifica le impostazioni di backup su più volumi

Se si desidera utilizzare le stesse impostazioni di backup su più volumi, è possibile attivare o modificare le impostazioni di backup su più volumi contemporaneamente. È possibile selezionare volumi privi di impostazioni di backup, con solo impostazioni di snapshot, con solo impostazioni di backup su cloud e così via, e apportare modifiche in blocco su tutti questi volumi con diverse impostazioni di backup.

Quando si lavora con più volumi, tutti i volumi devono avere le seguenti caratteristiche comuni:

- stesso sistema
- stesso stile (volume FlexVol o FlexGroup)
- stesso tipo (volume di lettura-scrittura o di protezione dati)

Se sono abilitati più di cinque volumi per il backup, NetApp Backup and Recovery inizializza solo cinque volumi alla volta. Una volta completati, si continua in gruppi di 5 finché tutti i volumi non vengono inizializzati.

Passi

1. Dalla scheda **Volumi**, filtrare in base al sistema su cui risiedono i volumi.
2. Selezionare tutti i volumi su cui si desidera gestire le impostazioni di backup.
3. A seconda del tipo di azione di backup che si desidera configurare, fare clic sul pulsante nel menu Azioni in blocco:

Azione di backup…	Seleziona questo pulsante…
Gestisci le impostazioni di backup degli snapshot	**Gestisci snapshot locali**
Gestisci le impostazioni di backup della replica	**Gestisci replicazione**
Gestisci le impostazioni di backup sul cloud	**Gestisci backup**
Gestisci più tipi di impostazioni di backup. Questa opzione consente anche di modificare l'architettura di backup.	**Gestisci backup e ripristino**

4. Nella pagina di backup visualizzata, apportare modifiche ai criteri di backup esistenti per snapshot locali, volumi replicati o file di backup e selezionare **Salva**.

   Se hai abilitato *DataLock e Ransomware Resilience* per i backup cloud nella policy di backup iniziale durante l'attivazione NetApp Backup and Recovery per questo cluster, vedrai solo le altre policy

configurate con DataLock. Se non hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery, vedrai solo altri criteri di backup cloud che non hanno DataLock configurato.

Crea un backup manuale del volume in qualsiasi momento

È possibile creare un backup su richiesta in qualsiasi momento per acquisire lo stato corrente del volume. Questa opzione può essere utile se sono state apportate modifiche molto importanti a un volume e non si desidera attendere il successivo backup pianificato per proteggere i dati. È possibile utilizzare questa funzionalità anche per creare un backup di un volume di cui non è attualmente in corso il backup e di cui si desidera acquisire lo stato attuale.

È possibile creare uno snapshot ad hoc o un backup nell'archivio oggetti di un volume. Non è possibile creare un volume replicato ad hoc.

Il nome del backup include la marca temporale, in modo da poter distinguere il backup su richiesta da altri backup pianificati.

Se hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery per questo cluster, anche il backup on-demand verrà configurato con DataLock e il periodo di conservazione sarà di 30 giorni. Le scansioni ransomware non sono supportate per i backup ad hoc. "Scopri di più sulla protezione da DataLock e Ransomware" .

Quando si crea un backup ad hoc, viene creato uno snapshot sul volume di origine. Poiché questo snapshot non fa parte di una normale pianificazione degli snapshot, non verrà disattivato. Una volta completato il backup, potrebbe essere necessario eliminare manualmente questo snapshot dal volume di origine. Ciò consentirà di liberare i blocchi correlati a questo snapshot. Il nome dello Snapshot inizierà con `cbs-snapshot-adhoc-` . "Scopri come eliminare uno Snapshot utilizzando ONTAP CLI" .

Il backup del volume su richiesta non è supportato sui volumi di protezione dati.

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume e seleziona **Backup** > **Crea backup ad hoc**.

Nella colonna Stato backup per quel volume viene visualizzato "In corso" finché il backup non viene creato.

Visualizza l'elenco dei backup per ciascun volume

È possibile visualizzare l'elenco di tutti i file di backup esistenti per ciascun volume. Questa pagina mostra i dettagli sul volume di origine, sulla posizione di destinazione e sui dettagli del backup, come l'ultimo backup eseguito, la politica di backup corrente, le dimensioni del file di backup e altro ancora.

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume sorgente e seleziona **Visualizza dettagli volume**.

   Vengono visualizzati i dettagli del volume e l'elenco degli snapshot.

2. Selezionare **Snapshot**, **Replica** o **Backup** per visualizzare l'elenco di tutti i file di backup per ciascun tipo di backup.

Eseguire una scansione ransomware su un backup del volume nell'archiviazione degli oggetti

NetApp Backup and Recovery analizza i file di backup per cercare prove di un attacco ransomware quando

viene creato un backup su file oggetto e quando vengono ripristinati i dati da un file di backup. È inoltre possibile eseguire una scansione su richiesta in qualsiasi momento per verificare l'usabilità di uno specifico file di backup nell'archiviazione degli oggetti. Ciò può essere utile se si è verificato un problema di ransomware su un volume specifico e si desidera verificare che i backup per quel volume non siano interessati.

Questa funzionalità è disponibile solo se il backup del volume è stato creato da un sistema con ONTAP 9.11.1 o versione successiva e se è stato abilitato *DataLock e Ransomware Resilience* nel criterio di backup su oggetto.

Passi

1. Dalla scheda **Volumi**, seleziona ••• per il volume sorgente e seleziona **Visualizza dettagli volume**.

   Vengono visualizzati i dettagli del volume.

2. Selezionare **Backup** per visualizzare l'elenco dei file di backup nell'archivio oggetti.
3. Selezionare ••• per il file di backup del volume che vuoi analizzare per individuare ransomware e clicca su **Analizza ransomware**.

   La colonna Resilienza ransomware indica che la scansione è In corso.

Gestire la relazione di replica con il volume di origine

Dopo aver impostato la replica dei dati tra due sistemi, è possibile gestire la relazione di replica dei dati.

Passi

1. Dalla scheda **Volumi**, seleziona ••• per il volume sorgente e selezionare l'opzione **Replica**. Puoi vedere tutte le opzioni disponibili.
2. Selezionare l'azione di replicazione che si desidera eseguire.

   La tabella seguente descrive le azioni disponibili:

Azione	Descrizione
Visualizza replica	Mostra i dettagli sulla relazione del volume: informazioni sul trasferimento, informazioni sull'ultimo trasferimento, dettagli sul volume e informazioni sulla policy di protezione assegnata alla relazione.
Aggiorna replica	Avvia un trasferimento incrementale per aggiornare il volume di destinazione da sincronizzare con il volume di origine.
Sospendi replicazione	Sospendi il trasferimento incrementale degli snapshot per aggiornare il volume di destinazione. È possibile riprendere in seguito se si desidera riavviare gli aggiornamenti incrementali.
Interrompere la replicazione	Interrompe la relazione tra i volumi di origine e di destinazione e attiva il volume di destinazione per l'accesso ai dati, rendendolo di lettura-scrittura. Questa opzione viene in genere utilizzata quando il volume di origine non può gestire i dati a causa di eventi quali danneggiamento dei dati, eliminazione accidentale o stato offline.https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html["Scopri come configurare un volume di destinazione per l'accesso ai dati e riattivare un volume di origine nella documentazione ONTAP"^]
Interrompere la replicazione	Disabilita i backup di questo volume sul sistema di destinazione e disabilita anche la possibilità di ripristinare un volume. Tutti i backup esistenti non verranno eliminati. Ciò non elimina la relazione di protezione dei dati tra i volumi di origine e di destinazione.

Azione	Descrizione
Risincronizzazione inversa	Inverte i ruoli dei volumi di origine e di destinazione. Il contenuto del volume di origine viene sovrascritto dal contenuto del volume di destinazione. Questa funzione è utile quando si desidera riattivare un volume sorgente che è andato offline. Tutti i dati scritti sul volume di origine originale tra l'ultima replica dei dati e il momento in cui il volume di origine è stato disabilitato non vengono conservati.
Elimina relazione	Elimina la relazione di protezione dei dati tra i volumi di origine e di destinazione, il che significa che la replica dei dati non avviene più tra i volumi. Questa azione non attiva il volume di destinazione per l'accesso ai dati, ovvero non lo rende di lettura/scrittura. Questa azione elimina anche la relazione peer del cluster e la relazione peer della VM di archiviazione (SVM), se non sono presenti altre relazioni di protezione dei dati tra i sistemi.

Risultato

Dopo aver selezionato un'azione, la Console aggiorna la relazione.

Modifica una policy di backup su cloud esistente

È possibile modificare gli attributi di un criterio di backup attualmente applicato ai volumi di un sistema. La modifica della policy di backup influisce su tutti i volumi esistenti che utilizzano la policy.

- Se hai abilitato *DataLock e Ransomware Resilience* nella policy iniziale durante l'attivazione NetApp Backup and Recovery per questo cluster, tutte le policy modificate devono essere configurate con la stessa impostazione DataLock (Governance o Compliance). Se non hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery, non puoi abilitare DataLock ora.
- Quando si creano backup su AWS, se si sceglie *S3 Glacier* o *S3 Glacier Deep Archive* nella prima policy di backup quando si attiva NetApp Backup and Recovery, quel livello sarà l'unico livello di archiviazione disponibile quando si modificano le policy di backup. Se non hai selezionato alcun livello di archivio nella tua prima policy di backup, *S3 Glacier* sarà la tua unica opzione di archiviazione quando modifichi una policy.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, seleziona ••• per il sistema in cui si desidera modificare le impostazioni dei criteri e selezionare **Gestisci criteri**.
3. Dalla pagina *Gestisci criteri*, seleziona **Modifica** per il criterio di backup che desideri modificare in quel sistema.
4. Dalla pagina *Modifica policy*, seleziona la freccia rivolta verso il basso per espandere la sezione *Etichette e conservazione* per modificare la pianificazione e/o la conservazione del backup, quindi seleziona **Salva**.

   Se il cluster esegue ONTAP 9.10.1 o versione successiva, è anche possibile abilitare o disabilitare la suddivisione in livelli dei backup nell'archiviazione dopo un certo numero di giorni.

   "Scopri di più sull'utilizzo dell'archiviazione AWS". "Scopri di più sull'utilizzo dell'archiviazione di Azure". "Scopri di più sull'utilizzo dell'archiviazione di Google". (Richiede ONTAP 9.12.1.)

   Si noti che tutti i file di backup che sono stati suddivisi in livelli di archiviazione vengono lasciati in quel livello se si interrompe la suddivisione dei backup in livelli di archivio; non vengono automaticamente spostati di nuovo nel livello standard. Solo i nuovi backup dei volumi risiederanno nel livello standard.

Aggiungi una nuova policy di backup su cloud

Quando si abilita NetApp Backup and Recovery per un sistema, tutti i volumi inizialmente selezionati vengono sottoposti a backup utilizzando la policy di backup predefinita definita. Se si desidera assegnare criteri di backup diversi a determinati volumi con obiettivi del punto di ripristino (RPO) diversi, è possibile creare criteri aggiuntivi per quel cluster e assegnarli ad altri volumi.

Se si desidera applicare una nuova policy di backup a determinati volumi di un sistema, è necessario prima aggiungere la policy di backup al sistema. Allora puoiapplicare la policy ai volumi in quel sistema .

- Se hai abilitato *DataLock e Ransomware Resilience* nella policy iniziale durante l'attivazione NetApp Backup and Recovery per questo cluster, tutte le policy aggiuntive che crei devono essere configurate con la stessa impostazione DataLock (Governance o Compliance). Se non hai abilitato *DataLock e Ransomware Resilience* durante l'attivazione NetApp Backup and Recovery, non puoi creare nuove policy che utilizzano DataLock.
- Quando si creano backup su AWS, se si sceglie *S3 Glacier* o *S3 Glacier Deep Archive* nella prima policy di backup quando si attiva NetApp Backup and Recovery, quel livello sarà l'unico livello di archiviazione disponibile per le future policy di backup per quel cluster. Se non hai selezionato alcun livello di archivio nella tua prima policy di backup, *S3 Glacier* sarà la tua unica opzione di archiviazione per le policy future.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, seleziona••• per il sistema in cui si desidera aggiungere la nuova policy e selezionare **Gestisci policy**.
3. Dalla pagina *Gestisci criteri*, seleziona **Aggiungi nuovo criterio**.
4. Dalla pagina *Aggiungi nuova policy*, seleziona la freccia rivolta verso il basso per espandere la sezione *Etichette e conservazione* per definire la pianificazione e la conservazione del backup, quindi seleziona **Salva**.

   Se il cluster esegue ONTAP 9.10.1 o versione successiva, è anche possibile abilitare o disabilitare la suddivisione in livelli dei backup nell'archiviazione dopo un certo numero di giorni.

   "Scopri di più sull'utilizzo dell'archiviazione AWS". "Scopri di più sull'utilizzo dell'archiviazione di Azure". "Scopri di più sull'utilizzo dell'archiviazione di Google". (Richiede ONTAP 9.12.1.)

Elimina i backup

NetApp Backup and Recovery consente di eliminare un singolo file di backup, eliminare tutti i backup per un volume o eliminare tutti i backup di tutti i volumi in un sistema. Potresti voler eliminare tutti i backup se non ne hai più bisogno o se hai eliminato il volume di origine e vuoi rimuovere tutti i backup.

Non è possibile eliminare i file di backup bloccati tramite DataLock e la protezione Ransomware. L'opzione "Elimina" non sarà disponibile nell'interfaccia utente se hai selezionato uno o più file di backup bloccati.

Se si prevede di eliminare un sistema o un cluster che dispone di backup, è necessario eliminare i backup **prima** di eliminare il sistema. NetApp Backup and Recovery non elimina automaticamente i backup quando si elimina un sistema e attualmente non è presente alcun supporto nell'interfaccia utente per eliminare i backup dopo l'eliminazione del sistema. Continuerai a pagare i costi di archiviazione degli oggetti per tutti i backup rimanenti.

Elimina tutti i file di backup per un sistema

L'eliminazione di tutti i backup nell'archivio oggetti di un sistema non disabilita i backup futuri dei volumi in questo sistema. Se si desidera interrompere la creazione di backup di tutti i volumi in un sistema, è possibile disattivare i backupcome descritto qui .

Si noti che questa azione non influisce sugli snapshot o sui volumi replicati: questi tipi di file di backup non vengono eliminati.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Selezionare••• per il sistema in cui si desidera eliminare tutti i backup e selezionare **Elimina tutti i backup**.
3. Nella finestra di dialogo di conferma, immettere il nome del sistema.
4. Selezionare **Impostazioni avanzate**.
5. **Forza eliminazione backup**: indica se desideri o meno forzare l'eliminazione di tutti i backup.

   In alcuni casi estremi, potresti voler impedire a NetApp Backup and Recovery di accedere più ai backup. Ciò potrebbe accadere, ad esempio, se il servizio non ha più accesso al bucket di backup o se i backup sono protetti da DataLock ma non si desidera più utilizzarli. In precedenza non era possibile eliminarli autonomamente, ma era necessario contattare l'assistenza NetApp . Con questa versione è possibile utilizzare l'opzione per forzare l'eliminazione dei backup (a livello di volume e di sistema).

   Utilizzare questa opzione con cautela e solo in caso di estrema necessità di pulizia. NetApp Backup and Recovery non avrà più accesso a questi backup, anche se non vengono eliminati dall'archiviazione degli oggetti. Sarà necessario rivolgersi al proprio provider cloud ed eliminare manualmente i backup.

6. Seleziona **Elimina**.

Elimina tutti i file di backup per un volume

L'eliminazione di tutti i backup di un volume disabilita anche i backup futuri per quel volume.

Passi

1. Dalla scheda **Volumi**, fare clic su••• per il volume di origine e selezionare **Dettagli e elenco di backup**.

   Viene visualizzato l'elenco di tutti i file di backup.

2. Selezionare **Azioni** > **Elimina tutti i backup**.
3. Immettere il nome del volume.
4. Selezionare **Impostazioni avanzate**.
5. **Forza eliminazione backup**: indica se desideri o meno forzare l'eliminazione di tutti i backup.

   In alcuni casi estremi, potresti voler impedire a NetApp Backup and Recovery di accedere più ai backup. Ciò potrebbe accadere, ad esempio, se il servizio non ha più accesso al bucket di backup o se i backup sono protetti da DataLock ma non si desidera più utilizzarli. In precedenza non era possibile eliminarli autonomamente, ma era necessario contattare l'assistenza NetApp . Con questa versione è possibile utilizzare l'opzione per forzare l'eliminazione dei backup (a livello di volume e di sistema).

Utilizzare questa opzione con cautela e solo in caso di estrema necessità di pulizia. NetApp Backup and Recovery non avrà più accesso a questi backup, anche se non vengono eliminati dall'archiviazione degli oggetti. Sarà necessario rivolgersi al proprio provider cloud ed eliminare manualmente i backup.

6. Seleziona **Elimina**.

Elimina un singolo file di backup per un volume

È possibile eliminare un singolo file di backup se non ne hai più bisogno. Ciò include l'eliminazione di un singolo backup di uno snapshot del volume o di un backup nell'archiviazione degli oggetti.

Non è possibile eliminare i volumi replicati (volumi di protezione dei dati).

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume sorgente e seleziona **Visualizza dettagli volume**.

   Vengono visualizzati i dettagli del volume ed è possibile selezionare **Snapshot**, **Replica** o **Backup** per visualizzare l'elenco di tutti i file di backup per il volume. Per impostazione predefinita, vengono visualizzati gli snapshot disponibili.

2. Selezionare **Snapshot** o **Backup** per visualizzare il tipo di file di backup che si desidera eliminare.
3. Selezionare••• per il file di backup del volume che vuoi eliminare e seleziona **Elimina**.
4. Nella finestra di dialogo di conferma, seleziona **Elimina**.

Elimina le relazioni di backup del volume

L'eliminazione della relazione di backup per un volume fornisce un meccanismo di archiviazione se si desidera interrompere la creazione di nuovi file di backup ed eliminare il volume di origine, ma conservare tutti i file di backup esistenti. Ciò ti dà la possibilità di ripristinare il volume dal file di backup in futuro, se necessario, liberando spazio dal tuo sistema di archiviazione di origine.

Non è necessario eliminare necessariamente il volume sorgente. È possibile eliminare la relazione di backup per un volume e conservare il volume di origine. In questo caso è possibile "Attivare" il backup sul volume in un secondo momento. In questo caso si continua a utilizzare la copia di backup di base originale: non viene creata né esportata nel cloud una nuova copia di backup di base. Si noti che se si riattiva una relazione di backup, al volume viene assegnato il criterio di backup predefinito.

Questa funzionalità è disponibile solo se il sistema esegue ONTAP 9.12.1 o versione successiva.

Non è possibile eliminare il volume di origine dall'interfaccia utente NetApp Backup and Recovery . Tuttavia, è possibile aprire la pagina Dettagli volume nella pagina **Sistemi** della console e "elimina il volume da lì" .

Non è possibile eliminare singoli file di backup del volume una volta eliminata la relazione. Tuttavia, è possibile eliminare tutti i backup del volume.

Passi

1. Dalla scheda **Volumi**, seleziona••• per il volume di origine e selezionare **Backup** > **Elimina relazione**.

Disattivare NetApp Backup and Recovery per un sistema

La disattivazione di NetApp Backup and Recovery per un sistema disabilita i backup di ciascun volume sul

sistema e disabilita anche la possibilità di ripristinare un volume. Tutti i backup esistenti non verranno eliminati. Ciò non annulla la registrazione del servizio di backup da questo sistema: in pratica consente di sospendere tutte le attività di backup e ripristino per un periodo di tempo.

Tieni presente che il tuo provider cloud continuerà a addebitarti i costi di archiviazione degli oggetti per la capacità utilizzata dai tuoi backup, a meno che tu noneliminare i backup .

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, seleziona••• per il sistema in cui si desidera disattivare i backup e selezionare **Disattiva backup**.
3. Nella finestra di dialogo di conferma, seleziona **Disattiva**.

> Quando il backup è disabilitato, per quel sistema viene visualizzato il pulsante **Attiva backup**. È possibile selezionare questo pulsante quando si desidera riattivare la funzionalità di backup per quel sistema.

Annullare la registrazione NetApp Backup and Recovery per un sistema

È possibile annullare la registrazione di NetApp Backup and Recovery per un sistema se non si desidera più utilizzare la funzionalità di backup e non si desidera più ricevere addebiti per i backup in quel sistema. In genere questa funzionalità viene utilizzata quando si pianifica di eliminare un sistema e si desidera annullare il servizio di backup.

È possibile utilizzare questa funzionalità anche se si desidera modificare l'archivio oggetti di destinazione in cui vengono archiviati i backup del cluster. Dopo aver annullato la registrazione NetApp Backup and Recovery per il sistema, è possibile abilitare NetApp Backup and Recovery per quel cluster utilizzando le informazioni del nuovo provider cloud.

Prima di poter annullare la registrazione NetApp Backup and Recovery, è necessario eseguire i seguenti passaggi, nell'ordine indicato:

- Disattivare NetApp Backup and Recovery per il sistema
- Elimina tutti i backup per quel sistema

L'opzione di annullamento della registrazione non è disponibile finché queste due azioni non sono state completate.

Passi

1. Dalla scheda **Volumi**, seleziona **Impostazioni di backup**.
2. Dalla pagina *Impostazioni di backup*, seleziona••• per il sistema in cui si desidera annullare la registrazione del servizio di backup e selezionare **Annulla registrazione**.
3. Nella finestra di dialogo di conferma, seleziona **Annulla registrazione**.

Ripristina dai backup ONTAP

Ripristina i dati ONTAP dai file di backup con NetApp Backup and Recovery

I backup dei dati del volume ONTAP vengono archiviati come snapshot, su volumi replicati o nell'archiviazione di oggetti. È possibile ripristinare i dati da una qualsiasi di queste posizioni in un momento specifico. Con NetApp Backup and Recovery puoi

ripristinare un intero volume, una cartella o singoli file, a seconda delle tue esigenze.

Per passare da e verso i carichi di lavoro NetApp Backup and Recovery , fare riferimento a"Passa a diversi carichi di lavoro NetApp Backup and Recovery" .

- È possibile ripristinare un **volume** (come nuovo volume) sul sistema originale, su un sistema diverso che utilizza lo stesso account cloud o su un sistema ONTAP locale.
- È possibile ripristinare una **cartella** su un volume nel sistema originale, su un volume in un sistema diverso che utilizza lo stesso account cloud o su un volume in un sistema ONTAP locale.
- È possibile ripristinare **file** su un volume nel sistema originale, su un volume in un sistema diverso che utilizza lo stesso account cloud o su un volume in un sistema ONTAP locale.

Per ripristinare i dati su un sistema di produzione è necessaria una licenza NetApp Backup and Recovery valida.

Riassumendo, ecco i flussi validi che è possibile utilizzare per ripristinare i dati del volume in un sistema ONTAP :

- File di backup → volume ripristinato
- Volume replicato → volume ripristinato
- Snapshot → volume ripristinato

Se l'operazione di ripristino non viene completata, attendere che Job Monitor visualizzi "Fallito" prima di riprovare l'operazione di ripristino.

Per le limitazioni relative al ripristino dei dati ONTAP , vedere"Limitazioni di backup e ripristino per i volumi ONTAP" .

La dashboard di ripristino

Utilizzare la dashboard di ripristino per eseguire operazioni di ripristino di volumi, cartelle e file. Per accedere alla Dashboard di ripristino, selezionare **Backup e ripristino** dal menu Console, quindi selezionare la scheda **Ripristina**. Puoi anche selezionare > **Visualizza la dashboard di ripristino** dal servizio Backup e ripristino dal pannello Servizi.

NetApp Backup and Recovery deve essere già attivato per almeno un sistema e devono esistere i file di backup iniziali.

La dashboard di ripristino offre due modi diversi per ripristinare i dati dai file di backup: **Sfoglia e ripristina** e **Cerca e ripristina**.

Confronto tra Sfoglia e Ripristina e Cerca e Ripristina

In termini generali, *Sfoglia e ripristina* è in genere più indicato quando è necessario ripristinare un volume, una cartella o un file specifico dell'ultima settimana o dell'ultimo mese, e si conoscono il nome e la posizione del file, nonché la data dell'ultima volta in cui era in buone condizioni. *Cerca e ripristina* è in genere la soluzione migliore quando è necessario ripristinare un volume, una cartella o un file, ma non si ricorda il nome esatto, il volume in cui si trova o la data dell'ultima volta in cui è stato in buone condizioni.

Questa tabella fornisce un confronto delle caratteristiche dei due metodi.

Sfoglia e ripristina	Cerca e ripristina
Sfoglia una struttura in stile cartella per trovare il volume, la cartella o il file all'interno di un singolo file di backup.	Cerca un volume, una cartella o un file in **tutti i file di backup** per nome parziale o completo del volume, nome parziale o completo della cartella/file, intervallo di dimensioni e filtri di ricerca aggiuntivi.
Non gestisce il recupero del file se il file è stato eliminato o rinominato e l'utente non conosce il nome originale del file	Gestisce le directory appena create/eliminate/rinominate e i file appena creati/eliminati/rinominati
È supportato il ripristino rapido.	Il ripristino rapido non è supportato.

Questa tabella fornisce un elenco di operazioni di ripristino valide in base alla posizione in cui risiedono i file di backup.

Tipo di backup	Sfoglia e ripristina			Cerca e ripristina		
	Ripristina volume	**Ripristina file**	**Ripristina cartella**	**Ripristina volume**	**Ripristina file**	**Ripristina cartella**
Istantanea	SÌ	NO	NO	SÌ	SÌ	SÌ
Volume replicato	SÌ	NO	NO	SÌ	SÌ	SÌ
File di backup	SÌ	SÌ	SÌ	SÌ	SÌ	SÌ

Prima di utilizzare uno dei due metodi di ripristino, configurare l'ambiente in modo che soddisfi i requisiti delle risorse. Per i dettagli, vedere le sezioni seguenti.

Consultare i requisiti e i passaggi di ripristino per il tipo di operazione di ripristino che si desidera utilizzare:

- "Ripristina i volumi utilizzando Sfoglia e Ripristina"
- "Ripristina cartelle e file utilizzando Sfoglia e Ripristina"
- "Ripristina volumi, cartelle e file utilizzando Cerca e ripristina"

Ripristina dai backup ONTAP utilizzando Cerca e ripristina

È possibile utilizzare Cerca e ripristina per recuperare volumi, cartelle o file dai file di backup ONTAP . Search & Restore consente di effettuare ricerche in tutti i backup (inclusi snapshot locali, volumi replicati e storage di oggetti) senza dover specificare i nomi esatti di sistema, volume o file.

Il ripristino da snapshot locali o volumi replicati è in genere più rapido e meno costoso rispetto al ripristino da storage di oggetti.

Quando si ripristina un volume completo, NetApp Backup and Recovery crea un nuovo volume utilizzando i dati di backup. È possibile ripristinare il sistema originale, un altro sistema all'interno dello stesso account cloud o un sistema ONTAP locale. Le cartelle e i file possono essere ripristinati nella loro posizione originale, in un volume diverso nello stesso sistema, in un altro sistema nello stesso account cloud o in un sistema locale.

Le capacità di ripristino dipendono dalla versione ONTAP :

- **Cartelle:** utilizzando ONTAP 9.13.0 o versioni successive, è possibile ripristinare cartelle con tutti i file e le sottocartelle; con le versioni precedenti, era possibile ripristinare solo i file nella cartella.
- **Archiviazione:** il ripristino dall'archiviazione (disponibile con ONTAP 9.10.1 o versioni successive) è più lento e potrebbe comportare costi aggiuntivi.
- **Requisiti del cluster di destinazione:**
  - Ripristino del volume: ONTAP 9.10.1 o versione successiva
  - Ripristino file: ONTAP 9.11.1 o versione successiva
  - Google Archive and StorageGRID: ONTAP 9.12.1 o versione successiva
  - Ripristino cartella: ONTAP 9.13.1 o versione successiva

"Scopri di più sul ripristino dall'archiviazione AWS". "Scopri di più sul ripristino dall'archiviazione di Azure". "Scopri di più sul ripristino dall'archivio di Google".

- Se il file di backup nell'archiviazione oggetti è stato configurato con protezione DataLock e Ransomware, il ripristino a livello di cartella è supportato solo se la versione ONTAP è 9.13.1 o successiva. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare l'intero volume dal file di backup e quindi accedere alla cartella e ai file necessari.
- Se il file di backup nell'archiviazione degli oggetti risiede nell'archiviazione di archivio, il ripristino a livello di cartella è supportato solo se la versione ONTAP è 9.13.1 o successiva. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare la cartella da un file di backup più recente che non è stato archiviato oppure è possibile ripristinare l'intero volume dal backup archiviato e quindi accedere alla cartella e ai file necessari.
- La priorità di ripristino "Alta" non è supportata quando si ripristinano dati dall'archiviazione di Azure nei sistemi StorageGRID .
- Il ripristino delle cartelle non è attualmente supportato dai volumi nell'archiviazione di oggetti ONTAP S3.

Prima di iniziare, dovresti avere un'idea del nome o della posizione del volume o del file che vuoi ripristinare.

Sistemi supportati da Search & Restore e provider di archiviazione di oggetti

È possibile ripristinare i dati ONTAP da un file di backup che risiede in un sistema secondario (un volume replicato) o in un archivio oggetti (un file di backup) nei seguenti sistemi. Gli snapshot risiedono sul sistema di origine e possono essere ripristinati solo su quello stesso sistema.

Nota: è possibile ripristinare volumi e file da qualsiasi tipo di file di backup, ma al momento è possibile ripristinare una cartella solo dai file di backup nell'archivio oggetti.

Posizione del file di backup		Sistema di destinazione
Archivio oggetti (backup)	**Sistema secondario (replicazione)**	
Amazon S3	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS
Blob azzurro	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure
Google Cloud Storage	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP

Posizione del file di backup		Sistema di destinazione
NetApp StorageGRID	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP in sede
ONTAP S3	Sistema ONTAP on-premise Cloud Volumes ONTAP	Sistema ONTAP in sede

Per Search & Restore, l'agente Console può essere installato nei seguenti percorsi:

- Per Amazon S3, l'agente della console può essere distribuito in AWS o nei tuoi locali
- Per Azure Blob, l'agente Console può essere distribuito in Azure o nei tuoi locali
- Per Google Cloud Storage, l'agente della console deve essere distribuito nella VPC di Google Cloud Platform
- Per StorageGRID, l'agente della console deve essere distribuito nei tuoi locali, con o senza accesso a Internet
- Per ONTAP S3, l'agente della console può essere distribuito presso la tua sede (con o senza accesso a Internet) o in un ambiente di provider cloud

Si noti che i riferimenti ai "sistemi ONTAP locali" includono i sistemi FAS, AFF e ONTAP Select .

Prerequisiti per la ricerca e il ripristino

Prima di abilitare Ricerca e ripristino, assicurati che il tuo ambiente soddisfi questi requisiti:

- Requisiti del cluster:
  - La versione ONTAP deve essere 9.8 o successiva.
  - La VM di archiviazione (SVM) su cui risiede il volume deve avere un LIF dati configurato.
  - NFS deve essere abilitato sul volume (sono supportati sia i volumi NFS che SMB/CIFS).
  - Il server SnapDiff RPC deve essere attivato sull'SVM. La Console esegue questa operazione automaticamente quando si abilita l'indicizzazione sul sistema. (SnapDiff è la tecnologia che identifica rapidamente le differenze di file e directory tra gli snapshot.)
- NetApp consiglia di montare un volume separato sull'agente Console per aumentare la resilienza di Search & Restore. Per le istruzioni, fare riferimento amontare il volume per reindicizzare il catalogo .

Prerequisiti per Legacy Search & Restore (utilizzando Indexed Catalog v1)

Di seguito sono riportati i requisiti per Search & Restore quando si utilizza l'indicizzazione legacy:

- Requisiti AWS:
  - È necessario aggiungere autorizzazioni specifiche per Amazon Athena, AWS Glue e AWS S3 al ruolo utente che fornisce le autorizzazioni alla Console. "Assicurati che tutte le autorizzazioni siano configurate correttamente" .

    Tieni presente che se stavi già utilizzando NetApp Backup and Recovery con un agente Console configurato in passato, ora dovrai aggiungere le autorizzazioni Athena e Glue al ruolo utente Console. Sono necessari per la ricerca e il ripristino.

- Requisiti di Azure:
  - È necessario registrare il provider di risorse di Azure Synapse Analytics (denominato "Microsoft.Synapse") con la sottoscrizione. "Scopri come registrare questo fornitore di risorse per il tuo abbonamento" . Per registrare il fornitore di risorse, devi essere il **Proprietario** o il **Collaboratore** dell'abbonamento.
  - È necessario aggiungere autorizzazioni specifiche per Azure Synapse Workspace e per l'account Data Lake Storage al ruolo utente che fornisce le autorizzazioni alla console. "Assicurati che tutte le autorizzazioni siano configurate correttamente" .

    Tieni presente che se utilizzavi già NetApp Backup and Recovery con un agente Console configurato in passato, ora dovrai aggiungere le autorizzazioni Azure Synapse Workspace e Data Lake Storage Account al ruolo utente Console. Sono necessari per la ricerca e il ripristino.

  - L'agente Console deve essere configurato **senza** un server proxy per la comunicazione HTTP con Internet. Se hai configurato un server proxy HTTP per il tuo agente Console, non puoi utilizzare la funzionalità Cerca e ripristina.
- Requisiti di Google Cloud:
  - È necessario aggiungere autorizzazioni specifiche di Google BigQuery al ruolo utente che fornisce le autorizzazioni alla NetApp Console . "Assicurati che tutte le autorizzazioni siano configurate correttamente" .

    Se utilizzavi già NetApp Backup and Recovery con un agente Console configurato in passato, ora dovrai aggiungere le autorizzazioni BigQuery al ruolo utente Console. Sono necessari per la ricerca e il ripristino.

- Requisiti StorageGRID e ONTAP S3:

  A seconda della configurazione, la funzione Ricerca e ripristino può essere implementata in due modi:

  - Se nel tuo account non sono presenti credenziali del provider cloud, le informazioni del catalogo indicizzato vengono archiviate nell'agente della console.

    Per informazioni sul Catalogo indicizzato v2, vedere la sezione seguente su come abilitare il Catalogo indicizzato.

  - Se si utilizza un agente Console in un sito privato (oscuro), le informazioni del catalogo indicizzato vengono archiviate nell'agente Console (richiede l'agente Console versione 3.9.25 o successiva).
  - Se hai "Credenziali AWS" O "Credenziali di Azure" nell'account, il catalogo indicizzato viene archiviato presso il provider cloud, proprio come con un agente Console distribuito nel cloud. (Se si possiedono entrambe le credenziali, AWS è selezionato per impostazione predefinita.)

    Anche se si utilizza un agente Console locale, è necessario soddisfare i requisiti del provider

cloud sia per le autorizzazioni dell'agente Console sia per le risorse del provider cloud. Per utilizzare questa implementazione, consultare i requisiti AWS e Azure sopra indicati.

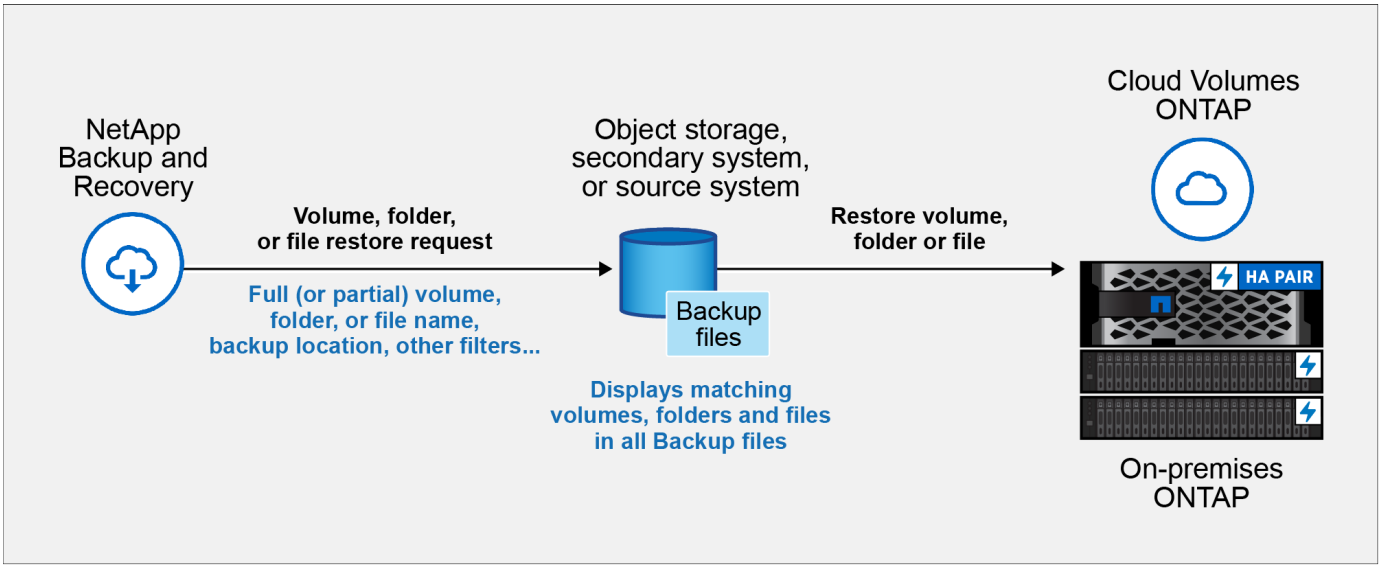
Processo di ricerca e ripristino

Il processo è il seguente:

1. Prima di poter utilizzare Ricerca e ripristino, è necessario abilitare "Indicizzazione" su ciascun sistema sorgente da cui si desidera ripristinare i dati del volume. Ciò consente al catalogo indicizzato di tenere traccia dei file di backup per ogni volume.
2. Quando si desidera ripristinare un volume o dei file da un backup del volume, in *Cerca e ripristina*, selezionare **Cerca e ripristina**.
3. Immettere i criteri di ricerca per un volume, una cartella o un file in base al nome parziale o completo del volume, al nome parziale o completo del file, alla posizione del backup, all'intervallo di dimensioni, all'intervallo di date di creazione, ad altri filtri di ricerca e selezionare **Cerca**.

   La pagina Risultati della ricerca mostra tutte le posizioni in cui è presente un file o un volume che corrisponde ai criteri di ricerca.

4. Selezionare **Visualizza tutti i backup** per la posizione che si desidera utilizzare per ripristinare il volume o il file, quindi selezionare **Ripristina** sul file di backup effettivo che si desidera utilizzare.
5. Selezionare la posizione in cui si desidera ripristinare il volume, la cartella o i file e selezionare **Ripristina**.
6. Il volume, la cartella o il/i file vengono ripristinati.



Basta conoscere un nome parziale e NetApp Backup and Recovery cercherà in tutti i file di backup che corrispondono alla tua ricerca.

Abilita il catalogo indicizzato per ogni sistema

Prima di poter utilizzare Ricerca e ripristino, è necessario abilitare "Indicizzazione" su ciascun sistema di origine da cui si prevede di ripristinare volumi o file. Ciò consente al catalogo indicizzato di tenere traccia di ogni volume e di ogni file di backup, rendendo le ricerche molto rapide ed efficienti.

Il catalogo indicizzato è un database che memorizza i metadati relativi a tutti i volumi e ai file di backup

presenti nel sistema. Viene utilizzato dalla funzionalità Cerca e ripristina per trovare rapidamente i file di backup che contengono i dati che si desidera ripristinare.

Caratteristiche del catalogo indicizzato

NetApp Backup and Recovery non fornisce un bucket separato quando si utilizza il catalogo indicizzato. Invece, per i backup archiviati in AWS, Azure, Google Cloud Platform, StorageGRID o ONTAP S3, il servizio predispone lo spazio sull'agente della console o sull'ambiente del provider cloud.

Il catalogo indicizzato supporta quanto segue:

- Efficienza di ricerca globale in meno di 3 minuti
- Fino a 5 miliardi di file
- Fino a 5000 volumi per cluster
- Fino a 100.000 snapshot per volume
- Il tempo massimo per l'indicizzazione di base è inferiore a 7 giorni. Il tempo effettivo varierà a seconda dell'ambiente.

Passaggi per abilitare l'indicizzazione per un sistema:

Se l'indicizzazione è già stata abilitata per il sistema, passare alla sezione successiva per ripristinare i dati.

Per prima cosa dovrai montare un volume separato per contenere i file di catalogo. In questo modo si evita la perdita di dati se le dimensioni dei file che contengono gli snapshot diventano troppo grandi. Questa operazione non è richiesta su tutti i cluster: è possibile montare un volume qualsiasi da uno qualsiasi dei cluster presenti nel proprio ambiente. In caso contrario, l'indicizzazione potrebbe non funzionare correttamente.

Per il volume montato, utilizzare le seguenti indicazioni di dimensionamento:

- Utilizzare un volume NetApp NFS
- Archiviazione AFF consigliata con throughput del disco di 300 MB/s. Una minore produttività avrà un impatto sulla ricerca e su altre operazioni.
- Abilita gli snapshot NetApp per proteggere i metadati del catalogo oltre ai file zip di backup del catalogo
- 50 GB per 1 miliardo di file
- 20 GB per i dati del catalogo con spazio aggiuntivo per la creazione di file zip e file temporanei

Passaggio per montare il volume per reindicizzare il catalogo

1. Montare il volume su `/opt/application/netapp/cbs` immettendo il seguente comando, dove:
    - `volume name` è il volume sul cluster in cui verranno archiviati i file di catalogo
    - `/opt/application/netapp/cbs` è il percorso in cui viene montato

    ```
    mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
    ```

    Esempio:

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

Passaggi per abilitare l'indice

1. Eseguire una delle seguenti operazioni:
   - Se non è stato indicizzato alcun sistema, nella Dashboard di ripristino in *Cerca e ripristina*, seleziona **Abilita indicizzazione per i sistemi**.
   - Se almeno un sistema è già stato indicizzato, nella Dashboard di ripristino in *Cerca e ripristina*, seleziona **Impostazioni di indicizzazione**.
2. Selezionare **Abilita indicizzazione** per il sistema.

Risultato

Dopo che tutti i servizi sono stati forniti e il catalogo indicizzato è stato attivato, il sistema viene visualizzato come "Attivo".

A seconda delle dimensioni dei volumi nel sistema e del numero di file di backup in tutte e 3 le posizioni di backup, il processo di indicizzazione iniziale potrebbe richiedere fino a un'ora. Successivamente viene aggiornato in modo trasparente ogni ora con modifiche incrementali per rimanere sempre aggiornato.

Ripristina volumi, cartelle e file utilizzando Cerca e ripristina

Dopo averindicizzazione abilitata per il tuo sistema , puoi ripristinare volumi, cartelle e file utilizzando Cerca e ripristina. Ciò consente di utilizzare un'ampia gamma di filtri per trovare il file o il volume esatto che si desidera ripristinare da tutti i file di backup.

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Selezionare la scheda **Ripristina** e verrà visualizzata la Dashboard di ripristino.
3. Dalla sezione *Cerca e ripristina*, seleziona **Cerca e ripristina**.
4. Dalla sezione *Cerca e ripristina*, seleziona **Cerca e ripristina**.
5. Dalla pagina Cerca e ripristina:
   a. Nella *barra di ricerca*, immettere un nome completo o parziale del volume, un nome della cartella o un nome del file.
   b. Selezionare il tipo di risorsa: **Volumi**, **File**, **Cartelle** o **Tutti**.
   c. Nell'area *Filtra per*, seleziona i criteri di filtro. Ad esempio, è possibile selezionare il sistema in cui risiedono i dati e il tipo di file, ad esempio un file .JPEG. In alternativa, è possibile selezionare il tipo di posizione di backup se si desidera cercare risultati solo all'interno degli snapshot disponibili o dei file di backup nell'archiviazione degli oggetti.
6. Seleziona **Cerca** e nell'area Risultati della ricerca verranno visualizzate tutte le risorse che contengono un file, una cartella o un volume corrispondente alla tua ricerca.
7. Individua la risorsa che contiene i dati che desideri ripristinare e seleziona **Visualizza tutti i backup** per visualizzare tutti i file di backup che contengono il volume, la cartella o il file corrispondente.
8. Individua il file di backup che desideri utilizzare per ripristinare i dati e seleziona **Ripristina**.

   Si noti che i risultati identificano gli snapshot dei volumi locali e i volumi replicati remoti che contengono il file nella ricerca. È possibile scegliere di ripristinare dal file di backup cloud, dallo snapshot o dal volume replicato.

9. Selezionare la posizione di destinazione in cui si desidera ripristinare il volume, la cartella o i file e selezionare **Ripristina**.

- Per i volumi, è possibile selezionare il sistema di destinazione originale oppure un sistema alternativo. Quando si ripristina un volume FlexGroup , è necessario scegliere più aggregati.
- Per le cartelle, è possibile ripristinare la posizione originale oppure selezionare una posizione alternativa, tra cui sistema, volume e cartella.
- Per i file, è possibile ripristinarli nella posizione originale oppure selezionare una posizione alternativa, tra cui il sistema, il volume e la cartella. Quando si seleziona la posizione originale, è possibile scegliere di sovrascrivere i file di origine o di crearne di nuovi.

  Se selezioni un sistema ONTAP locale e non hai ancora configurato la connessione del cluster all'archiviazione degli oggetti, ti verrà richiesto di immettere informazioni aggiuntive:

  - Durante il ripristino da Amazon S3, seleziona lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione, immetti la chiave di accesso e la chiave segreta per l'utente creato per concedere al cluster ONTAP l'accesso al bucket S3 e, facoltativamente, scegli un endpoint VPC privato per il trasferimento sicuro dei dati. "Vedi i dettagli su questi requisiti" .
  - Durante il ripristino da Azure Blob, selezionare lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione e, facoltativamente, scegliere un endpoint privato per il trasferimento sicuro dei dati selezionando la rete virtuale e la subnet. "Vedi i dettagli su questi requisiti" .
  - Quando si esegue il ripristino da Google Cloud Storage, selezionare lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione, nonché la chiave di accesso e la chiave segreta per accedere all'archiviazione degli oggetti. "Vedi i dettagli su questi requisiti" .
  - Durante il ripristino da StorageGRID, immettere l'FQDN del server StorageGRID e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con StorageGRID, immettere la chiave di accesso e la chiave segreta necessarie per accedere all'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiede il volume di destinazione. "Vedi i dettagli su questi requisiti" .
  - Durante il ripristino da ONTAP S3, immettere l'FQDN del server ONTAP S3 e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con ONTAP S3, selezionare la chiave di accesso e la chiave segreta necessarie per accedere all'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione. "Vedi i dettagli su questi requisiti" .

Risultati

Il volume, la cartella o i file vengono ripristinati e si torna alla Dashboard di ripristino, dove è possibile esaminare l'avanzamento dell'operazione di ripristino. È anche possibile selezionare la scheda **Monitoraggio processi** per visualizzare l'avanzamento del ripristino. Vedere"Pagina di monitoraggio dei lavori" .

Ripristina i dati ONTAP utilizzando Sfoglia e ripristina

Con NetApp Backup and Recovery, ripristina i dati ONTAP utilizzando Browse & Restore. Prima di effettuare il ripristino, annotare il nome del volume di origine, il sistema di origine e l'SVM, nonché la data del file di backup. È possibile ripristinare i dati ONTAP da uno snapshot, da un volume replicato o da backup archiviati nell'archiviazione di oggetti.

Le capacità di ripristino dipendono dalla versione ONTAP :

- **Cartelle:** utilizzando ONTAP 9.13.0 o versioni successive, è possibile ripristinare cartelle con tutti i file e le sottocartelle; con le versioni precedenti, era possibile ripristinare solo i file nella cartella.
- **Archiviazione:** il ripristino dall'archiviazione (disponibile con ONTAP 9.10.1 o versioni successive) è più lento e potrebbe comportare costi aggiuntivi.
- **Requisiti del cluster di destinazione:**

- Ripristino del volume: ONTAP 9.10.1 o versione successiva
- Ripristino file: ONTAP 9.11.1 o versione successiva
- Google Archive and StorageGRID: ONTAP 9.12.1 o versione successiva
- Ripristino cartella: ONTAP 9.13.1 o versione successiva

"Scopri di più sul ripristino dall'archiviazione AWS". "Scopri di più sul ripristino dall'archiviazione di Azure". "Scopri di più sul ripristino dall'archivio di Google".

La priorità Alta non è supportata durante il ripristino dei dati dall'archiviazione di Azure ai sistemi StorageGRID .

Esplora e ripristina i sistemi supportati e i provider di archiviazione di oggetti

È possibile ripristinare i dati ONTAP da un file di backup che risiede in un sistema secondario (un volume replicato) o in un archivio oggetti (un file di backup) nei seguenti sistemi. Gli snapshot risiedono sul sistema di origine e possono essere ripristinati solo su quello stesso sistema.

Nota: è possibile ripristinare un volume da qualsiasi tipo di file di backup, ma al momento è possibile ripristinare una cartella o singoli file solo da un file di backup nell'archivio oggetti.

Da Object Store (Backup)	Da Primario (Snapshot)	Dal sistema secondario (replicazione)	Al sistema di destinazione
Amazon S3	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Blob azzurro
Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Google Cloud Storage	Cloud Volumes ONTAP nel sistema Google On-premises ONTAP
Cloud Volumes ONTAP nel sistema Google On-premises ONTAP	NetApp StorageGRID	Sistema ONTAP in sede	Sistema ONTAP on-premise Cloud Volumes ONTAP
Al sistema ONTAP locale	ONTAP S3	Sistema ONTAP in sede	Sistema ONTAP on-premise Cloud Volumes ONTAP

Per Sfoglia e Ripristina, l'agente Console può essere installato nei seguenti percorsi:

- Per Amazon S3, l'agente della console può essere distribuito in AWS o nei tuoi locali
- Per Azure Blob, l'agente Console può essere distribuito in Azure o nei tuoi locali
- Per Google Cloud Storage, l'agente della console deve essere distribuito nella VPC di Google Cloud Platform
- Per StorageGRID, l'agente della console deve essere distribuito nei tuoi locali, con o senza accesso a Internet
- Per ONTAP S3, l'agente della console può essere distribuito presso la tua sede (con o senza accesso a Internet) o in un ambiente di provider cloud

Si noti che i riferimenti ai "sistemi ONTAP locali" includono i sistemi FAS, AFF e ONTAP Select .

Se la versione ONTAP sul sistema è precedente alla 9.13.1, non sarà possibile ripristinare cartelle o file se il file di backup è stato configurato con DataLock e Ransomware. In questo caso, puoi ripristinare l'intero volume dal file di backup e quindi accedere ai file di cui hai bisogno.

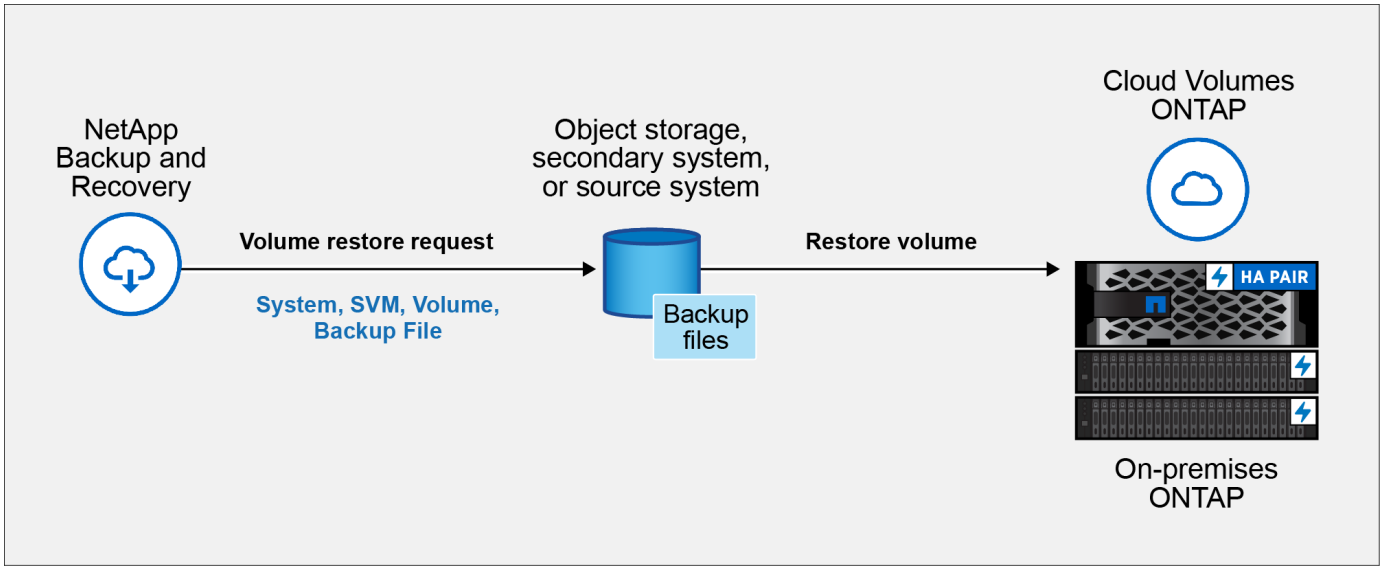
Ripristina i volumi utilizzando Sfoglia e ripristina

Quando si ripristina un volume da un file di backup, NetApp Backup and Recovery crea un *nuovo* volume utilizzando i dati del backup. Quando si utilizza un backup da un archivio di oggetti, è possibile ripristinare i dati su un volume nel sistema originale, su un sistema diverso situato nello stesso account cloud del sistema di origine o su un sistema ONTAP locale.

Quando si ripristina un backup cloud su un sistema Cloud Volumes ONTAP che utilizza ONTAP 9.13.0 o versione successiva oppure su un sistema ONTAP locale che esegue ONTAP 9.14.1, sarà possibile eseguire un'operazione di *ripristino rapido*. Il ripristino rapido è ideale per le situazioni di disaster recovery in cui è necessario fornire l'accesso a un volume il prima possibile. Un ripristino rapido ripristina i metadati dal file di backup a un volume anziché ripristinare l'intero file di backup. Il ripristino rapido non è consigliato per applicazioni sensibili alle prestazioni o alla latenza e non è supportato con i backup in storage archiviati.

Il ripristino rapido è supportato per i volumi FlexGroup solo se il sistema di origine da cui è stato creato il backup cloud eseguiva ONTAP 9.12.1 o versione successiva. Ed è supportato per i volumi SnapLock solo se il sistema di origine eseguiva ONTAP 9.11.0 o versione successiva.

Quando si esegue il ripristino da un volume replicato, è possibile ripristinare il volume sul sistema originale oppure su un sistema Cloud Volumes ONTAP o ONTAP locale.



Per ripristinare un volume sono necessari il nome del sistema di origine, la macchina virtuale di archiviazione, il nome del volume e la data del file di backup.

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Selezionare la scheda **Ripristina** e verrà visualizzata la Dashboard di ripristino.
3. Dalla sezione *Sfoglia e ripristina*, seleziona **Ripristina volume**.
4. Nella pagina *Seleziona origine*, vai al file di backup per il volume che desideri ripristinare. Selezionare il

sistema, il **volume** e il file **backup** con la data/ora da cui si desidera effettuare il ripristino.

La colonna **Posizione** mostra se il file di backup (Snapshot) è **Locale** (uno snapshot sul sistema di origine), **Secondario** (un volume replicato su un sistema ONTAP secondario) o **Archiviazione oggetti** (un file di backup nell'archiviazione oggetti). Seleziona il file che vuoi ripristinare.

5. Selezionare **Avanti**.

   Tieni presente che se selezioni un file di backup nell'archiviazione oggetti e Ransomware Resilience è attivo per quel backup (se hai abilitato DataLock e Ransomware Resilience nel criterio di backup), ti verrà chiesto di eseguire un'ulteriore scansione ransomware sul file di backup prima di ripristinare i dati. Ti consigliamo di eseguire la scansione del file di backup per individuare eventuali ransomware. (Per accedere al contenuto del file di backup, verranno addebitati costi di uscita aggiuntivi dal tuo provider cloud.)

6. Nella pagina *Seleziona destinazione*, seleziona il **sistema** in cui desideri ripristinare il volume.
7. Quando si ripristina un file di backup da un archivio oggetti, se si seleziona un sistema ONTAP locale e non è ancora stata configurata la connessione del cluster all'archivio oggetti, vengono richieste informazioni aggiuntive:
   - Durante il ripristino da Amazon S3, seleziona lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione, immetti la chiave di accesso e la chiave segreta per l'utente creato per concedere al cluster ONTAP l'accesso al bucket S3 e, facoltativamente, scegli un endpoint VPC privato per il trasferimento sicuro dei dati.
   - Durante il ripristino da Azure Blob, selezionare lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione, selezionare la sottoscrizione di Azure per accedere all'archiviazione degli oggetti e, facoltativamente, scegliere un endpoint privato per il trasferimento sicuro dei dati selezionando la rete virtuale e la subnet.
   - Durante il ripristino da Google Cloud Storage, seleziona il progetto Google Cloud, la chiave di accesso e la chiave segreta per accedere all'archiviazione degli oggetti, alla regione in cui sono archiviati i backup e allo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione.
   - Durante il ripristino da StorageGRID, immettere l'FQDN del server StorageGRID e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con StorageGRID, selezionare la chiave di accesso e la chiave segreta necessarie per accedere all'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione.
   - Durante il ripristino da ONTAP S3, immettere l'FQDN del server ONTAP S3 e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con ONTAP S3, selezionare la chiave di accesso e la chiave segreta necessarie per accedere all'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiederà il volume di destinazione.
8. Immettere il nome che si desidera utilizzare per il volume ripristinato e selezionare la VM di archiviazione e l'aggregato in cui risiederà il volume. Quando si ripristina un volume FlexGroup , è necessario selezionare più aggregati. Per impostazione predefinita, come nome del volume viene utilizzato **<source_volume_name>_restore**.

   Quando si ripristina un backup da un archivio di oggetti a un sistema Cloud Volumes ONTAP che utilizza ONTAP 9.13.0 o versione successiva oppure a un sistema ONTAP locale che esegue ONTAP 9.14.1, sarà possibile eseguire un'operazione di *ripristino rapido*.

   Se si ripristina il volume da un file di backup che risiede in un livello di archiviazione (disponibile a partire da ONTAP 9.10.1), è possibile selezionare la priorità di ripristino.

   "Scopri di più sul ripristino dall'archiviazione AWS". "Scopri di più sul ripristino dall'archiviazione di Azure" . "Scopri di più sul ripristino dall'archivio di Google" . I file di backup nel livello di archiviazione di Google

Archive vengono ripristinati quasi immediatamente e non richiedono alcuna priorità di ripristino.

9. Selezionare **Avanti** per scegliere se si desidera eseguire un ripristino normale o un ripristino rapido:
   - **Ripristino normale**: utilizzare il ripristino normale sui volumi che richiedono prestazioni elevate. I volumi non saranno disponibili finché il processo di ripristino non sarà completato.
   - **Ripristino rapido**: i volumi e i dati ripristinati saranno disponibili immediatamente. Non utilizzare questa opzione su volumi che richiedono prestazioni elevate perché durante il processo di ripristino rapido l'accesso ai dati potrebbe essere più lento del solito.
10. Selezionando **Ripristina** si torna alla Dashboard di ripristino, dove è possibile esaminare l'avanzamento dell'operazione di ripristino.

Risultato

NetApp Backup and Recovery crea un nuovo volume in base al backup selezionato.

Si noti che il ripristino di un volume da un file di backup residente in un archivio può richiedere molti minuti o ore, a seconda del livello di archivio e della priorità di ripristino. È possibile selezionare la scheda **Monitoraggio processi** per visualizzare l'avanzamento del ripristino.

Ripristina cartelle e file utilizzando Sfoglia e ripristina

Se è necessario ripristinare solo alcuni file da un backup del volume ONTAP , è possibile scegliere di ripristinare una cartella o singoli file anziché ripristinare l'intero volume. È possibile ripristinare cartelle e file su un volume esistente nel sistema originale oppure su un sistema diverso che utilizza lo stesso account cloud. È anche possibile ripristinare cartelle e file su un volume su un sistema ONTAP locale.

Al momento è possibile ripristinare una cartella o singoli file solo da un file di backup nell'archivio oggetti. Il ripristino di file e cartelle non è attualmente supportato da uno snapshot locale o da un file di backup che risiede in un sistema secondario (un volume replicato).

Se si selezionano più file, questi vengono ripristinati nello stesso volume di destinazione. Per ripristinare i file su volumi diversi, eseguire il processo più volte.

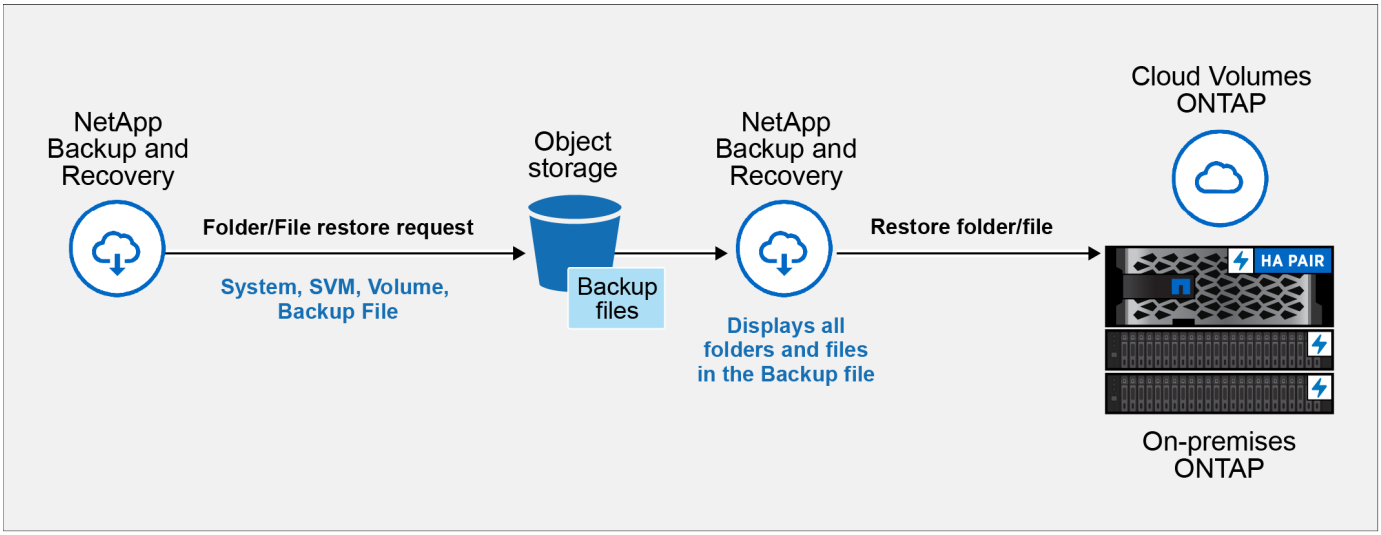
Se si utilizza ONTAP 9.13.0 o versione successiva, è possibile ripristinare una cartella insieme a tutti i file e le sottocartelle in essa contenuti. Quando si utilizza una versione di ONTAP precedente alla 9.13.0, vengono ripristinati solo i file di quella cartella, ma non le sottocartelle o i file nelle sottocartelle.

- Se il file di backup è stato configurato con la protezione DataLock e Ransomware, il ripristino a livello di cartella è supportato solo se la versione ONTAP è 9.13.1 o successiva. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare l'intero volume dal file di backup e quindi accedere alla cartella e ai file necessari.
- Se il file di backup risiede in un archivio, il ripristino a livello di cartella è supportato solo se la versione ONTAP è 9.13.1 o successiva. Se si utilizza una versione precedente di ONTAP, è possibile ripristinare la cartella da un file di backup più recente che non è stato archiviato oppure è possibile ripristinare l'intero volume dal backup archiviato e quindi accedere alla cartella e ai file necessari.
- Con ONTAP 9.15.1 è possibile ripristinare le cartelle FlexGroup utilizzando l'opzione "Sfoglia e ripristina". Questa funzionalità è in modalità Anteprima tecnologica.

  È possibile testarlo utilizzando un flag speciale descritto in "Blog sulla versione NetApp Backup and Recovery di luglio 2024" .

Ripristina cartelle e file

Per ripristinare cartelle o file su un volume da un backup del volume ONTAP , seguire questi passaggi. Dovresti conoscere il nome del volume e la data del file di backup che vuoi utilizzare per ripristinare la cartella o il/i file. Questa funzionalità utilizza la navigazione in tempo reale per consentirti di visualizzare l'elenco delle directory e dei file all'interno di ciascun file di backup.



Prima di iniziare

- Per eseguire operazioni di ripristino dei file, la versione ONTAP deve essere 9.6 o successiva.
- Per eseguire operazioni di ripristino delle *cartelle*, la versione ONTAP deve essere 9.11.1 o successiva. La versione 9.13.1 ONTAP è richiesta se i dati si trovano in un archivio o se il file di backup utilizza la protezione DataLock e Ransomware.
- Per ripristinare le directory FlexGroup utilizzando l'opzione Sfoglia e ripristina, la versione ONTAP deve essere 9.15.1 p2 o successiva.

Passi

1. Dal menu Console, selezionare **Protezione > Backup e ripristino**.
2. Selezionare la scheda **Ripristina** e verrà visualizzata la Dashboard di ripristino.
3. Dalla sezione *Sfoglia e ripristina*, seleziona **Ripristina file o cartella**.
4. Nella pagina *Seleziona origine*, vai al file di backup per il volume che contiene la cartella o i file che desideri ripristinare. Selezionare il **sistema**, il **volume** e il **backup** che presenta la data/ora da cui si desidera ripristinare i file.
5. Selezionare **Avanti** e verrà visualizzato l'elenco delle cartelle e dei file del backup del volume.

   Se si ripristinano cartelle o file da un file di backup che risiede in un livello di archiviazione, è possibile selezionare la Priorità di ripristino.

   "Scopri di più sul ripristino dall'archiviazione AWS". "Scopri di più sul ripristino dall'archiviazione di Azure" . "Scopri di più sul ripristino dall'archivio di Google" . I file di backup nel livello di archiviazione di Google Archive vengono ripristinati quasi immediatamente e non richiedono alcuna priorità di ripristino.

   Se Ransomware Resilience è attivo per il file di backup (se hai abilitato DataLock e Ransomware Resilience nel criterio di backup), ti verrà chiesto di eseguire un'ulteriore scansione ransomware sul file di backup prima di ripristinare i dati. Ti consigliamo di eseguire la scansione del file di backup per individuare eventuali ransomware. (Per accedere al contenuto del file di backup, verranno addebitati costi di uscita

aggiuntivi dal tuo provider cloud.)

6. Nella pagina *Seleziona elementi*, seleziona la cartella o i file che desideri ripristinare e seleziona **Continua**. Per aiutarti a trovare l'articolo:
   - Se vedi il nome della cartella o del file, puoi selezionarlo.
   - È possibile selezionare l'icona di ricerca e immettere il nome della cartella o del file per passare direttamente all'elemento.
   - È possibile spostarsi nei livelli inferiori delle cartelle utilizzando la freccia giù alla fine della riga per trovare file specifici.

     Man mano che selezioni i file, questi vengono aggiunti al lato sinistro della pagina, così puoi vedere i file che hai già scelto. Se necessario, è possibile rimuovere un file da questo elenco selezionando la **x** accanto al nome del file.

7. Nella pagina *Seleziona destinazione*, seleziona il **sistema** in cui desideri ripristinare gli elementi.

   Se selezioni un cluster locale e non hai ancora configurato la connessione del cluster all'archiviazione di oggetti, ti verranno richieste informazioni aggiuntive:

   - Quando si esegue il ripristino da Amazon S3, immettere lo spazio IP nel cluster ONTAP in cui risiede il volume di destinazione, nonché la chiave di accesso AWS e la chiave segreta necessarie per accedere allo storage degli oggetti. È anche possibile selezionare una configurazione di collegamento privato per la connessione al cluster.
   - Quando si esegue il ripristino da Azure Blob, immettere lo spazio IP nel cluster ONTAP in cui risiede il volume di destinazione. È anche possibile selezionare una configurazione endpoint privata per la connessione al cluster.
   - Quando si esegue il ripristino da Google Cloud Storage, immettere lo spazio IP nel cluster ONTAP in cui risiedono i volumi di destinazione, nonché la chiave di accesso e la chiave segreta necessarie per accedere all'archiviazione degli oggetti.
   - Durante il ripristino da StorageGRID, immettere l'FQDN del server StorageGRID e la porta che ONTAP deve utilizzare per la comunicazione HTTPS con StorageGRID, immettere la chiave di accesso e la chiave segreta necessarie per accedere all'archiviazione degli oggetti e lo spazio IP nel cluster ONTAP in cui risiede il volume di destinazione.

8. Quindi seleziona il **Volume** e la **Cartella** in cui desideri ripristinare la cartella o il/i file.

   Sono disponibili alcune opzioni per la posizione durante il ripristino di cartelle e file.

   - Dopo aver scelto **Seleziona cartella di destinazione**, come mostrato sopra:
     - Puoi selezionare qualsiasi cartella.
     - È possibile passare il mouse su una cartella e fare clic alla fine della riga per visualizzare in dettaglio le sottocartelle, quindi selezionare una cartella.
   - Se hai selezionato lo stesso sistema di destinazione e lo stesso volume in cui si trovava la cartella/il file di origine, puoi selezionare **Mantieni percorso cartella di origine** per ripristinare la cartella o i file nella stessa cartella in cui si trovavano nella struttura di origine. Tutte le cartelle e sottocartelle devono già esistere; non vengono create cartelle. Quando si ripristinano i file nella loro posizione originale, è possibile scegliere di sovrascrivere i file di origine o di crearne di nuovi.

9. Selezionare **Ripristina** per tornare alla Dashboard di ripristino e rivedere l'avanzamento dell'operazione di ripristino.

Proteggere i carichi di lavoro di Microsoft SQL Server

Proteggi i carichi di lavoro Microsoft SQL utilizzando la panoramica NetApp Backup and Recovery

Esegui il backup dei dati delle applicazioni Microsoft SQL Server dai sistemi ONTAP locali ad AWS, Azure o StorageGRID utilizzando NetApp Backup and Recovery. Il sistema crea e archivia automaticamente i backup nel tuo account cloud, in base alle tue policy. Utilizza una strategia 3-2-1: conserva tre copie dei tuoi dati su due sistemi di archiviazione e una copia nel cloud.

I vantaggi dell'approccio 3-2-1 includono:

- Più copie di dati proteggono dalle minacce informatiche interne ed esterne.
- L'utilizzo di diversi tipi di supporto aiuta a recuperare i dati se un tipo non funziona.
- È possibile ripristinare rapidamente dalla copia in loco e utilizzare le copie fuori sede se la copia in loco è compromessa.

NetApp Backup and Recovery utilizza NetApp SnapMirror per sincronizzare i backup creando snapshot e trasferendoli nelle posizioni di backup.

Per proteggere i tuoi dati puoi fare quanto segue:

- "Configurare elementi aggiuntivi se si importa da SnapCenter"
- "Scopri i carichi di lavoro di Microsoft SQL Server e, facoltativamente, importa le risorse SnapCenter"
- "Eseguire il backup dei carichi di lavoro con snapshot locali sullo storage primario ONTAP locale"
- "Replicare i carichi di lavoro sullo storage secondario ONTAP"
- "Eseguire il backup dei carichi di lavoro in una posizione di archiviazione oggetti"
- "Esegui subito il backup dei carichi di lavoro"
- "Ripristinare i carichi di lavoro"
- "Clonazione dei carichi di lavoro"
- "Gestire l'inventario dei carichi di lavoro"
- "Gestisci gli snapshot"

Per eseguire il backup dei carichi di lavoro, è necessario creare policy che gestiscano le operazioni di backup e ripristino. Vedere"Creare politiche" per maggiori informazioni.

Destinazioni di backup supportate

NetApp Backup and Recovery consente di eseguire il backup di istanze e database di Microsoft SQL Server dai seguenti sistemi di origine ai seguenti sistemi secondari e storage di oggetti nei provider di cloud pubblici e privati. Gli snapshot risiedono sul sistema di origine.

Sistema sorgente	Sistema secondario (Replicazione)	Archivio oggetti di destinazione (backup)
Cloud Volumes ONTAP in AWS	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Amazon S3 ONTAP S3

Sistema sorgente	Sistema secondario (Replicazione)	Archivio oggetti di destinazione (backup)
Cloud Volumes ONTAP in Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Azure Blob ONTAP S3
Sistema ONTAP in sede	Cloud Volumes ONTAP Sistema ONTAP locale	Blob di Azure Amazon S3 NetApp StorageGRID ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	N / A

Destinazioni di ripristino supportate

È possibile ripristinare istanze e database di Microsoft SQL Server da un backup che risiede nell'archivio primario o in un sistema secondario (un volume replicato) o nell'archivio oggetti (un file di backup) nei seguenti sistemi. Gli snapshot risiedono sul sistema di origine e possono essere ripristinati solo su quello stesso sistema.

Dalla posizione del file di backup		Al sistema di destinazione
Archivio oggetti (backup)	**Sistema secondario (replicazione)**	
Amazon S3	Cloud Volumes ONTAP nel sistema ONTAP locale di AWS	Cloud Volumes nel sistema ONTAP locale AWS ONTAP S3
Blob azzurro	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure	Cloud Volumes ONTAP nel sistema ONTAP locale di Azure ONTAP S3
StorageGRID	Cloud Volumes ONTAP Sistema ONTAP locale	Sistema ONTAP on-premise ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	N / A

I riferimenti ai "sistemi ONTAP locali" includono i sistemi FAS e AFF .

Prerequisiti per l'importazione dal servizio Plug-in in NetApp Backup and Recovery

Se si desidera importare risorse dal servizio plug-in SnapCenter per Microsoft SQL Server in NetApp Backup and Recovery, sarà necessario configurare alcuni altri elementi.

Crea prima i sistemi nella NetApp Console

Se si desidera importare risorse da SnapCenter, è necessario aggiungere prima tutto lo storage del cluster SnapCenter locale alla pagina **Sistemi** della console prima di importare da SnapCenter. Ciò garantisce che le risorse host possano essere scoperte e importate correttamente.

Verificare i requisiti dell'host per installare il plug-in SnapCenter

Per importare risorse dal plug-in SnapCenter per Microsoft SQL Server, assicurarsi che siano soddisfatti i requisiti host per l'installazione del plug-in SnapCenter per Microsoft SQL Server.

Verificare specificamente i requisiti SnapCenter in"Prerequisiti NetApp Backup and Recovery" .

Disabilitare le restrizioni remote del Controllo account utente

Prima di importare risorse da SnapCenter, disabilitare le restrizioni remote del Controllo account utente (UAC) sull'host Windows SnapCenter . Disattivare UAC se si utilizza un account amministrativo locale per connettersi in remoto all'host del server SnapCenter o all'host SQL.

Considerazioni sulla sicurezza

Prima di disattivare le restrizioni remote UAC, tenere presente quanto segue:

- Rischi per la sicurezza: la disattivazione del filtraggio dei token può esporre il sistema a vulnerabilità di sicurezza, soprattutto se gli account amministrativi locali vengono compromessi da malintenzionati.
- Usare con cautela:
  - Modificare questa impostazione solo se è essenziale per le proprie attività amministrative.
  - Assicurarsi che siano in atto password complesse e altre misure di sicurezza per proteggere gli account amministrativi.

Soluzioni alternative

- Se è necessario l'accesso amministrativo remoto, valutare l'utilizzo di account di dominio con privilegi appropriati.
- Utilizzare strumenti di gestione remota sicuri che rispettino le migliori pratiche di sicurezza per ridurre al minimo i rischi.

Passaggi per disattivare le restrizioni remote del Controllo account utente

1. Modificare il `LocalAccountTokenFilterPolicy` chiave di registro sull'host Windows SnapCenter .

   Per farlo, utilizza uno dei seguenti metodi, di seguito le istruzioni:

   - Metodo 1: Editor del Registro di sistema
   - Metodo 2: script PowerShell

Metodo 1: disabilitare il controllo dell'account utente utilizzando l'editor del Registro di sistema

Questo è uno dei metodi che puoi utilizzare per disattivare il Controllo dell'account utente.

Passi

1. Aprire l'Editor del Registro di sistema sull'host Windows di SnapCenter procedendo come segue:
   a. Premere `Windows+R` per aprire la finestra di dialogo Esegui.
   b. Tipo `regedit` e premere `Enter` .
2. Passare alla chiave della policy:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
   ```

3. Crea o modifica il `DWORD` valore:
   a. Individuare: `LocalAccountTokenFilterPolicy`
   b. Se non esiste, creane uno nuovo `DWORD` (32 bit) Valore denominato `LocalAccountTokenFilterPolicy` .

4. Sono supportati i seguenti valori. Per questo scenario, impostare il valore su `1` :
   - `0`(Predefinito): le restrizioni remote UAC sono abilitate. Gli account locali hanno token filtrati quando accedono da remoto.
   - `1`: Le restrizioni remote UAC sono disabilitate. Gli account locali ignorano il filtraggio dei token e dispongono di privilegi amministrativi completi quando accedono da remoto.
5. Fare clic su **OK**.
6. Chiudere l'Editor del Registro di sistema.
7. Riavviare l'host Windows di SnapCenter .

Esempio di modifica del registro

In questo esempio LocalAccountTokenFilterPolicy viene impostato su "1", disabilitando le restrizioni remote UAC.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000001
```

Metodo 2: disabilitare il controllo dell'account utente utilizzando uno script di PowerShell

Questo è un altro metodo che puoi utilizzare per disattivare il Controllo dell'account utente.

L'esecuzione di comandi PowerShell con privilegi elevati può influire sulle impostazioni di sistema. Prima di eseguirli, assicurati di aver compreso i comandi e le loro implicazioni.

Passi

1. Aprire una finestra di PowerShell con privilegi amministrativi sull'host Windows di SnapCenter :
   a. Fare clic sul menu **Start**.
   b. Cerca **PowerShell 7** o **Windows Powershell**.
   c. Fare clic con il tasto destro del mouse su tale opzione e selezionare **Esegui come amministratore**.
2. Assicurati che PowerShell sia installato sul tuo sistema. Dopo l'installazione, dovrebbe apparire nel menu **Start**.

   PowerShell è incluso di default in Windows 7 e nelle versioni successive.

3. Per disabilitare le restrizioni remote UAC, impostare LocalAccountTokenFilterPolicy su "1" eseguendo il seguente comando:

   ```
   Set-ItemProperty -Path
   "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
   "LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
   ```

4. Verificare che il valore corrente sia impostato su "1" in `LocalAccountTokenFilterPolicy` eseguendo:

```
Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"
```

- Se il valore è 1, le restrizioni remote UAC sono disabilitate.
- Se il valore è 0, le restrizioni remote UAC sono abilitate.

5. Per applicare le modifiche, riavviare il computer.

Esempi di comandi di PowerShell 7 per disabilitare le restrizioni remote UAC:

Questo esempio con il valore impostato su "1" indica che le restrizioni remote UAC sono disabilitate.

```
# Disable UAC remote restrictions

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord

# Verify the change

Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"

# Output

LocalAccountTokenFilterPolicy : 1
```

Scopri i carichi di lavoro di Microsoft SQL Server e, facoltativamente, importali da SnapCenter in NetApp Backup and Recovery

Per poter utilizzare il servizio, NetApp Backup and Recovery deve prima rilevare i carichi di lavoro di Microsoft SQL Server. Se lo hai già SnapCenter , puoi facoltativamente importare dati di backup e policy da SnapCenter .

*Ruolo richiesto NetApp Console * Super amministratore di backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Scopri i carichi di lavoro di Microsoft SQL Server e, facoltativamente, importa le risorse SnapCenter

Durante la fase di individuazione, NetApp Backup and Recovery analizza le istanze e i database di Microsoft SQL Server nei sistemi all'interno dell'organizzazione.

NetApp Backup and Recovery valuta le applicazioni Microsoft SQL Server. Il servizio valuta il livello di protezione esistente, comprese le attuali policy di protezione del backup, gli snapshot e le opzioni di backup e ripristino.

La scoperta avviene nei seguenti modi:

- Se hai già SnapCenter, importa le risorse SnapCenter in NetApp Backup and Recovery utilizzando l'interfaccia utente NetApp Backup and Recovery .

> Se hai già SnapCenter, verifica innanzitutto di aver soddisfatto i prerequisiti prima di importare da SnapCenter. Ad esempio, dovresti aggiungere prima i sistemi di storage cluster SnapCenter locali alla NetApp Console prima di importare da SnapCenter. Vedere"Prerequisiti per l'importazione di risorse da SnapCenter" .

- Se non disponi ancora SnapCenter, puoi comunque individuare i carichi di lavoro aggiungendo manualmente un vCenter ed eseguendo l'individuazione.

Se SnapCenter è già installato, importare le risorse SnapCenter in NetApp Backup and Recovery

Se SnapCenter è già installato, importare le risorse SnapCenter in NetApp Backup and Recovery seguendo questi passaggi. NetApp Console rileva risorse, host, credenziali e pianificazioni da SnapCenter; non è necessario ricreare tutte queste informazioni.

Puoi farlo nei seguenti modi:

- Durante la scoperta, seleziona un'opzione per importare risorse da SnapCenter.
- Dopo l'individuazione, dalla pagina Inventario, seleziona un'opzione per importare le risorse SnapCenter .
- Dopo l'individuazione, dal menu Impostazioni, seleziona un'opzione per importare le risorse SnapCenter . Per i dettagli, vedere"Configurare NetApp Backup and Recovery" .

Si tratta di un processo in due fasi:

- Importa l'applicazione SnapCenter Server e le risorse host
- Gestisci le risorse host SnapCenter selezionate

Importa l'applicazione SnapCenter Server e le risorse host

Questo primo passaggio importa le risorse host da SnapCenter e visualizza tali risorse nella pagina Inventario NetApp Backup and Recovery . A quel punto, le risorse non sono ancora gestite da NetApp Backup and Recovery.

> Dopo aver importato le risorse host SnapCenter , NetApp Backup and Recovery non assume automaticamente la gestione della protezione. Per farlo, è necessario selezionare esplicitamente la gestione delle risorse importate in NetApp Backup and Recovery. In questo modo sarai pronto a sottoporre tali risorse a backup tramite NetApp Backup and Recovery.

Passi

1. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Backup e ripristino**.
2. Selezionare **Inventario**.
3. Seleziona **Scopri risorse**.
4. Dalla pagina delle risorse del carico di lavoro NetApp Backup and Recovery Discover, seleziona **Importa da SnapCenter**.
5. Inserisci * credenziali dell'applicazione SnapCenter *:
    a. * FQDN o indirizzo IP SnapCenter *: immettere il FQDN o l'indirizzo IP dell'applicazione SnapCenter

stessa.

b. **Porta**: immettere il numero di porta per il server SnapCenter .

c. **Nome utente** e **Password**: immettere il nome utente e la password per il server SnapCenter .

d. **Agente console**: seleziona l'agente console per SnapCenter.

6. Inserisci * credenziali dell'host del server SnapCenter *:

a. **Credenziali esistenti**: se selezioni questa opzione, puoi utilizzare le credenziali esistenti che hai già aggiunto. Scegli il nome delle credenziali.

b. **Aggiungi nuove credenziali**: se non disponi di credenziali host SnapCenter esistenti, puoi aggiungerne di nuove. Immettere il nome delle credenziali, la modalità di autenticazione, il nome utente e la password.

7. Selezionare **Importa** per convalidare le voci e registrare SnapCenter Server.

Se SnapCenter Server è già registrato, è possibile aggiornare i dettagli di registrazione esistenti.

Risultato

La pagina Inventario mostra le risorse SnapCenter importate, che includono host, istanze e database MS SQL.

Per visualizzare i dettagli delle risorse SnapCenter importate, selezionare l'opzione **Visualizza dettagli** dal menu Azioni.

Gestire le risorse host SnapCenter

Dopo aver importato le risorse SnapCenter , gestisci tali risorse host in NetApp Backup and Recovery. Dopo aver scelto di gestire tali risorse, NetApp Backup and Recovery è in grado di eseguire il backup e il ripristino delle risorse importate da SnapCenter. Non gestisci più tali risorse in SnapCenter Server.

Passi

1. Dopo aver importato le risorse SnapCenter , dal menu Backup e ripristino, selezionare **Inventario**.
2. Dalla pagina Inventario, seleziona l'host SnapCenter importato che da ora in poi desideri che NetApp Backup and Recovery gestisca.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli** per visualizzare i dettagli del carico di lavoro.
4. Dalla pagina Inventario > carico di lavoro, seleziona l'icona Azioni ••• > **Gestisci** per visualizzare la pagina Gestisci host.
5. Selezionare **Gestisci**.
6. Nella pagina Gestisci host, seleziona se utilizzare un vCenter esistente o aggiungerne uno nuovo.
7. Selezionare **Gestisci**.

   La pagina Inventario mostra le risorse SnapCenter appena gestite.

Facoltativamente, è possibile creare un report delle risorse gestite selezionando l'opzione **Genera report** dal menu Azioni.

Importare le risorse SnapCenter dopo la scoperta dalla pagina Inventario

Se hai già scoperto delle risorse, puoi importare le risorse SnapCenter dalla pagina Inventario.

Passi

1. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Backup e ripristino**.
2. Selezionare **Inventario**.
3. Dalla pagina Inventario, seleziona *Importa risorse SnapCenter *.
4. Per importare le risorse SnapCenter , seguire i passaggi descritti nella sezione *Importa risorse SnapCenter * sopra.

Se SnapCenter non è installato, aggiungi un vCenter e scopri le risorse

Se SnapCenter non è ancora installato, è possibile aggiungere informazioni su vCenter e fare in modo che il backup e il ripristino NetApp rilevino i carichi di lavoro. All'interno di ciascun agente della console, seleziona i sistemi in cui desideri rilevare i carichi di lavoro.

Questa operazione è facoltativa se si dispone di un ambiente VMware.

Passi

1. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Backup e ripristino**.

   Se si accede a Backup and Recovery per la prima volta e si ha un sistema nella Console ma non sono state rilevate risorse, viene visualizzata la pagina *Benvenuti nel nuovo NetApp Backup and Recovery* con l'opzione **Rileva risorse**.

2. Seleziona **Scopri risorse**.
3. Inserisci le seguenti informazioni:
   a. **Tipo di carico di lavoro**: per questa versione è disponibile solo Microsoft SQL Server.
   b. **Impostazioni vCenter**: seleziona un vCenter esistente o aggiungine uno nuovo. Per aggiungere un nuovo vCenter, immettere l'FQDN o l'indirizzo IP del vCenter, il nome utente, la password, la porta e il protocollo.

      Se si inseriscono informazioni su vCenter, immettere le informazioni sia per le impostazioni di vCenter sia per la registrazione dell'host. Se hai aggiunto o inserito informazioni su vCenter qui, devi aggiungere anche le informazioni sul plugin nelle Impostazioni avanzate.

   c. **Registrazione host**: seleziona **Aggiungi credenziali** e inserisci le informazioni sugli host che contengono i carichi di lavoro che desideri scoprire.

      Se si aggiunge un server autonomo e non un server vCenter, immettere solo le informazioni sull'host.

4. Seleziona **Scopri**.

   Questo processo potrebbe richiedere alcuni minuti.

5. Continua con Impostazioni avanzate.

Imposta le opzioni delle impostazioni avanzate durante la scoperta e installa il plugin

Con le Impostazioni avanzate puoi installare manualmente l'agente plugin su tutti i server registrati. Ciò consente di importare tutti i carichi di lavoro SnapCenter in NetApp Backup and Recovery, in modo da poter

gestire backup e ripristini da lì. NetApp Backup and Recovery mostra i passaggi necessari per installare il plugin.

Passi

1. Dalla pagina Scopri risorse, vai alle Impostazioni avanzate cliccando sulla freccia rivolta verso il basso a destra.
2. Nella pagina Scopri le risorse del carico di lavoro, immetti le seguenti informazioni.
   - **Inserisci il numero di porta del plug-in**: inserisci il numero di porta utilizzato dal plug-in.
   - **Percorso di installazione**: inserisci il percorso in cui verrà installato il plugin.
3. Se si desidera installare manualmente l'agente SnapCenter , selezionare le caselle relative alle seguenti opzioni:
   - **Usa installazione manuale**: seleziona questa casella per installare manualmente il plugin.
   - **Aggiungi tutti gli host nel cluster**: seleziona questa casella per aggiungere tutti gli host nel cluster a NetApp Backup and Recovery durante l'individuazione.
   - **Salta i controlli pre-installazione facoltativi**: seleziona questa casella per saltare i controlli pre-installazione facoltativi. Potresti volerlo fare, ad esempio, se sai che le considerazioni sulla memoria o sullo spazio cambieranno nel prossimo futuro e vuoi installare il plugin ora.
4. Seleziona **Scopri**.

Continua alla dashboard NetApp Backup and Recovery

1. Dal menu NetApp Console , selezionare **Protezione** > **Backup e ripristino**.
2. Selezionare un riquadro del carico di lavoro (ad esempio, Microsoft SQL Server).
3. Dal menu Backup e ripristino, seleziona **Dashboard**.
4. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai carichi di lavoro appena scoperti, protetti e sottoposti a backup.

   "Scopri cosa ti mostra la Dashboard".

Esegui il backup dei carichi di lavoro di Microsoft SQL Server con NetApp Backup and Recovery

Eseguire il backup dei dati delle applicazioni Microsoft SQL Server dai sistemi ONTAP locali ad Amazon Web Services, Microsoft Azure o StorageGRID. Il sistema crea automaticamente dei backup e li memorizza in un archivio oggetti nel tuo account cloud per la protezione dei dati.

- Per eseguire il backup dei carichi di lavoro in base a una pianificazione, creare policy che gestiscano le operazioni di backup e ripristino. Vedere"Creare politiche" per istruzioni.
- Configurare la directory di registro per gli host rilevati prima di avviare un backup.
- Esegui subito il backup dei carichi di lavoro (crea subito un backup su richiesta).

Visualizza lo stato di protezione del carico di lavoro

Prima di avviare un backup, visualizza lo stato di protezione dei tuoi carichi di lavoro.

*Ruolo richiesto NetApp Console * Visualizzatore di storage, super amministratore di Backup and Recovery,

amministratore di backup di Backup and Recovery, amministratore di ripristino di Backup and Recovery, amministratore di clonazione di Backup and Recovery o ruolo di visualizzatore di Backup and Recovery. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Esaminare i dettagli nelle schede Host, Gruppi di protezione, Gruppi di disponibilità, Istanze e Database.

Configurare la directory dei registri per gli host rilevati

Imposta il percorso del registro attività per gli host rilevati per monitorare lo stato delle operazioni prima di eseguire il backup dei carichi di lavoro.

*Ruolo richiesto NetApp Console * Ruolo di visualizzatore di storage, super amministratore di Backup e Recovery, amministratore di backup di Backup e Recovery o amministratore di ripristino di Backup e Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Seleziona un host.
5. Seleziona l'icona Azioni ••• > **Configura directory registro**.
6. Inserisci il percorso host o sfoglia un elenco di host o nodi per trovare dove desideri archiviare il registro host.
7. Selezionare quelli su cui si desidera memorizzare i registri.

   I campi visualizzati variano a seconda del modello di distribuzione selezionato, ad esempio istanza del cluster di failover o autonomo.

8. Seleziona **Salva**.

Crea un gruppo di protezione

Crea un gruppo di protezione per gestire le operazioni di backup e ripristino per più carichi di lavoro. Un gruppo di protezione è un raggruppamento logico di carichi di lavoro.

Ruolo di NetApp Console obbligatorio Ruolo di visualizzatore di storage, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.

4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare **Crea gruppo di protezione**.
6. Fornire un nome per il gruppo di protezione.
7. Selezionare le istanze o i database che si desidera includere nel gruppo di protezione.
8. Selezionare **Avanti**.
9. Selezionare il **criterio di backup** che si desidera applicare al gruppo di protezione.

   Se si desidera creare una policy, selezionare **Crea nuova policy** e seguire le istruzioni per creare una policy. Vedere"Creare politiche" per maggiori informazioni.

10. Selezionare **Avanti**.
11. Rivedere la configurazione.
12. Selezionare **Crea** per creare il gruppo di protezione.

Esegui subito il backup dei carichi di lavoro con un backup on-demand

Esegui un backup su richiesta prima di apportare modifiche al sistema per garantire la protezione dei dati.

Ruolo di NetApp Console obbligatorio Ruolo di visualizzatore di storage, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu, seleziona **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppo di protezione**, **Istanze** o **Database**.
5. Seleziona l'istanza o il database di cui vuoi eseguire il backup.
6. Seleziona l'icona Azioni ••• > **Esegui il backup ora**.
7. Selezionare il criterio che si desidera applicare al backup.
8. Selezionare il livello di pianificazione.
9. Seleziona **Esegui backup ora**.

Sospendi la pianificazione del backup

Sospendi la pianificazione per interrompere temporaneamente i backup durante la manutenzione o la risoluzione dei problemi.

Ruolo di NetApp Console obbligatorio Ruolo di visualizzatore di storage, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.

4. Selezionare la scheda **Gruppo di protezione**, **Istanze** o **Database**.
5. Selezionare il gruppo di protezione, l'istanza o il database che si desidera sospendere.
6. Seleziona l'icona Azioni ••• > **Sospendi**.

Elimina un gruppo di protezione

L'eliminazione di un gruppo di protezione comporta la rimozione del gruppo stesso e di tutte le pianificazioni di backup associate. Potrebbe essere necessario eliminare un gruppo di protezione se non è più necessario.

Ruolo di NetApp Console obbligatorio Ruolo di visualizzatore di storage, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Seleziona l'icona Azioni ••• > **Elimina gruppo di protezione**.

Rimuovere la protezione da un carico di lavoro

È possibile rimuovere la protezione da un carico di lavoro se non si desidera più eseguirne il backup o se si desidera interromperne la gestione in NetApp Backup and Recovery.

Ruolo di NetApp Console obbligatorio Ruolo di visualizzatore di storage, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppo di protezione**, **Istanze** o **Database**.
5. Selezionare il gruppo di protezione, l'istanza o il database.
6. Seleziona l'icona Azioni ••• > **Rimuovi protezione**.
7. Nella finestra di dialogo Rimuovi protezione, seleziona se desideri conservare i backup e i metadati oppure eliminarli.
8. Selezionare **Rimuovi** per confermare l'azione.

Ripristina i carichi di lavoro di Microsoft SQL Server con NetApp Backup and Recovery

Ripristina i carichi di lavoro di Microsoft SQL Server utilizzando NetApp Backup and Recovery. Utilizzare snapshot, backup replicati su storage secondario o backup in storage di oggetti. Ripristinare i carichi di lavoro sul sistema originale, su un sistema diverso con lo stesso account cloud o su un sistema ONTAP locale.

Ripristina da queste posizioni

È possibile ripristinare i carichi di lavoro da diverse posizioni di partenza:

- Ripristina da una posizione primaria
- Ripristina da una risorsa replicata
- Ripristina da un backup dell'archivio oggetti

Ripristinare questi punti

È possibile ripristinare i dati all'ultimo snapshot o a questi punti:

- Ripristina da snapshot
- Ripristina un punto specifico nel tempo se conosci il nome del file, la posizione e l'ultima data valida
- Ripristina l'ultimo backup

Considerazioni sul ripristino da storage di oggetti

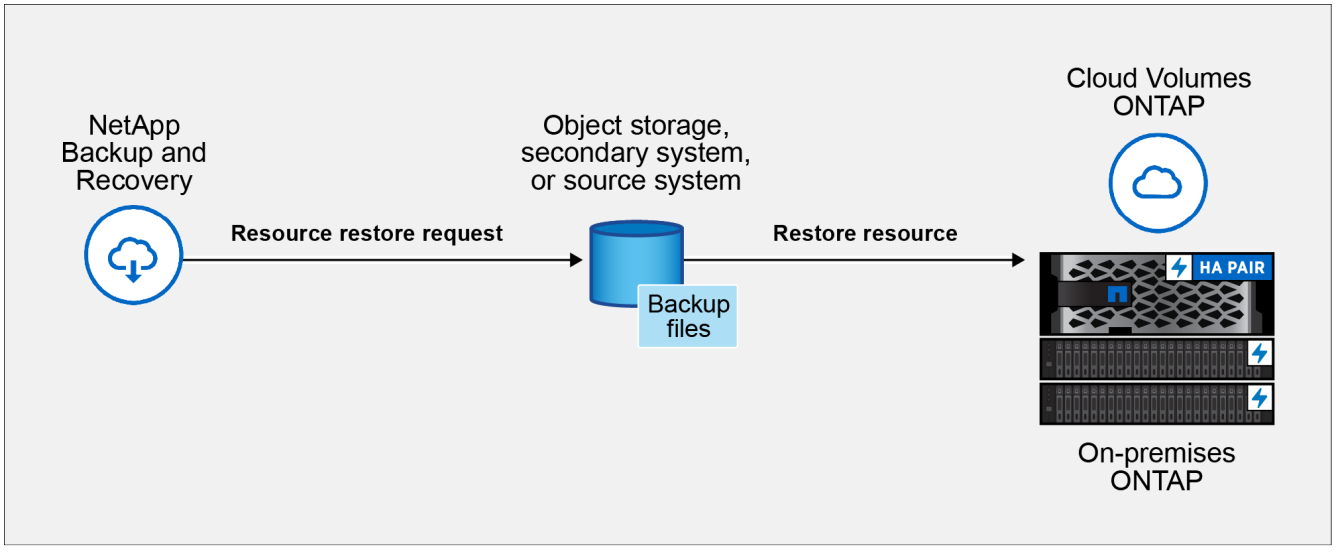
Se selezioni un file di backup nell'archiviazione oggetti e Ransomware Resilience è attivo per quel backup (se hai abilitato DataLock e Ransomware Resilience nel criterio di backup), ti verrà richiesto di eseguire un ulteriore controllo di integrità sul file di backup prima di ripristinare i dati. Ti consigliamo di eseguire la scansione.

Per accedere al file di backup dovrai pagare delle commissioni aggiuntive al tuo provider cloud.

Come funziona il ripristino dei carichi di lavoro

Quando si ripristinano i carichi di lavoro, si verifica quanto segue:

- Quando si ripristina un carico di lavoro da un file di backup, NetApp Backup and Recovery crea una *nuova* risorsa utilizzando i dati del backup.
- Quando si esegue il ripristino da un carico di lavoro replicato, è possibile ripristinare il carico di lavoro sul sistema originale o su un sistema ONTAP locale.



- Quando si ripristina un backup da un archivio di oggetti, è possibile ripristinare i dati nel sistema originale o in un sistema ONTAP locale.

Metodi di ripristino

Ripristinare i carichi di lavoro utilizzando uno di questi metodi:

- **Dalla pagina Ripristina**: usa questa opzione per ripristinare una risorsa quando non ne conosci il nome, la posizione o l'ultima data valida. Cerca l'istantanea utilizzando i filtri.
- **Dalla pagina Inventario**: usa questa opzione per ripristinare una risorsa specifica quando ne conosci il nome, la posizione e l'ultima data di validità. Sfoglia l'elenco per trovare la risorsa.

Ruolo di NetApp Console obbligatorio Ruolo di visualizzatore di storage, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Ripristina i dati del carico di lavoro dall'opzione Ripristina

Ripristinare i carichi di lavoro del database utilizzando l'opzione Ripristina.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Ripristina**.
2. Selezionare il database che si desidera ripristinare. Utilizza i filtri per effettuare la ricerca.
3. Seleziona l'opzione di ripristino:
   - Ripristina da snapshot
   - Ripristina un punto specifico nel tempo se conosci il nome del file, la posizione e l'ultima data valida
   - Ripristina l'ultimo backup

Ripristinare i carichi di lavoro dagli snapshot

1. Proseguendo dalla pagina Opzioni di ripristino, seleziona **Ripristina da snapshot**.

   Viene visualizzato un elenco di istantanee.

2. Seleziona lo snapshot che vuoi ripristinare.
3. Selezionare **Avanti**.

   Successivamente vedrai le opzioni di destinazione.

4. Nella pagina Dettagli destinazione, inserisci le seguenti informazioni:
   - **Impostazioni di destinazione**: scegli se desideri ripristinare i dati nella posizione originale o in una posizione alternativa. Per una posizione alternativa, seleziona il nome host e l'istanza, immetti il nome del database e il percorso di destinazione in cui desideri ripristinare lo snapshot.
   - **Opzioni pre-ripristino**:
     - **Sovrascrivi il database con lo stesso nome durante il ripristino**: durante il ripristino, il nome originale del database viene mantenuto.
     - **Mantieni impostazioni di replica del database SQL**: conserva le impostazioni di replica per il database SQL dopo l'operazione di ripristino.
     - **Crea backup del registro delle transazioni prima del ripristino**: crea un backup del registro delle transazioni prima dell'operazione di ripristino.*** Interrompi il ripristino se il backup del registro delle transazioni prima del ripristino non riesce**: interrompe l'operazione di ripristino se il backup del registro delle transazioni non riesce.

        - **Prescript**: immettere il percorso completo di uno script che deve essere eseguito prima dell'operazione di ripristino, eventuali argomenti richiesti dallo script e il tempo di attesa per il completamento dello script.
    - **Opzioni post-ripristino**:
        - **Operativo**, ma non disponibile per il ripristino di ulteriori registri delle transazioni. In questo modo il database torna online dopo l'applicazione dei backup del registro delle transazioni.
        - **Non operativo**, ma disponibile per il ripristino di ulteriori registri delle transazioni. Mantiene il database in uno stato non operativo dopo l'operazione di ripristino durante il ripristino dei backup del registro delle transazioni. Questa opzione è utile per ripristinare ulteriori registri delle transazioni.
        - **Modalità di sola lettura** e disponibile per il ripristino di registri di transazioni aggiuntivi. Ripristina il database in modalità di sola lettura e applica i backup del registro delle transazioni.
        - **Postscript**: immettere il percorso completo di uno script che deve essere eseguito dopo l'operazione di ripristino e tutti gli argomenti accettati dallo script.
5. Selezionare **Ripristina**.

Ripristinare un punto specifico nel tempo

NetApp Backup and Recovery utilizza i log e gli snapshot più recenti per creare un ripristino puntuale dei dati.

1. Proseguendo dalla pagina Opzioni di ripristino, seleziona **Ripristina in un momento specifico**.
2. Selezionare **Avanti**.
3. Nella pagina Ripristina a un punto specifico nel tempo, immettere le seguenti informazioni:
    - **Data e ora del ripristino dei dati**: immettere la data e l'ora esatte dei dati che si desidera ripristinare. Questa data e ora provengono dall'host del database Microsoft SQL Server.
4. Seleziona **Cerca**.
5. Seleziona lo snapshot che vuoi ripristinare.
6. Selezionare **Avanti**.
7. Nella pagina Dettagli destinazione, inserisci le seguenti informazioni:
    - **Impostazioni di destinazione**: scegli se desideri ripristinare i dati nella posizione originale o in una posizione alternativa. Per una posizione alternativa, seleziona il nome host e l'istanza, inserisci il nome del database e inserisci il percorso di destinazione.
    - **Opzioni pre-ripristino**:
        - **Mantieni il nome originale del database**: durante il ripristino, il nome originale del database viene mantenuto.
        - **Mantieni impostazioni di replica del database SQL**: conserva le impostazioni di replica per il database SQL dopo l'operazione di ripristino.
        - **Prescript**: immettere il percorso completo di uno script che deve essere eseguito prima dell'operazione di ripristino, eventuali argomenti richiesti dallo script e il tempo di attesa per il completamento dello script.
    - **Opzioni post-ripristino**:
        - **Operativo**, ma non disponibile per il ripristino di ulteriori registri delle transazioni. In questo modo il database torna online dopo l'applicazione dei backup del registro delle transazioni.
        - **Non operativo**, ma disponibile per il ripristino di ulteriori registri delle transazioni. Mantiene il database in uno stato non operativo dopo l'operazione di ripristino durante il ripristino dei backup

del registro delle transazioni. Questa opzione è utile per ripristinare ulteriori registri delle transazioni.

- **Modalità di sola lettura** e disponibile per il ripristino di registri di transazioni aggiuntivi. Ripristina il database in modalità di sola lettura e applica i backup del registro delle transazioni.
- **Postscript**: immettere il percorso completo di uno script che deve essere eseguito dopo l'operazione di ripristino e tutti gli argomenti accettati dallo script.

8. Selezionare **Ripristina**.

Ripristina l'ultimo backup

Questa opzione utilizza gli ultimi backup completi e di registro per ripristinare i dati all'ultimo stato valido. Il sistema esegue la scansione dei registri dall'ultimo snapshot fino al presente. Il processo tiene traccia delle modifiche e delle attività per ripristinare la versione più recente e accurata dei dati.

1. Proseguendo dalla pagina Opzioni di ripristino, seleziona **Ripristina all'ultimo backup**.

   NetApp Backup and Recovery mostra gli snapshot disponibili per l'operazione di ripristino.

2. Nella pagina Ripristina allo stato più recente, seleziona la posizione dello snapshot dell'archiviazione locale, secondaria o dell'archiviazione oggetti.
3. Selezionare **Avanti**.
4. Nella pagina Dettagli destinazione, inserisci le seguenti informazioni:
   - **Impostazioni di destinazione**: scegli se desideri ripristinare i dati nella posizione originale o in una posizione alternativa. Per una posizione alternativa, seleziona il nome host e l'istanza, inserisci il nome del database e inserisci il percorso di destinazione.
   - **Opzioni pre-ripristino**:
     - **Sovrascrivi il database con lo stesso nome durante il ripristino**: durante il ripristino, il nome originale del database viene mantenuto.
     - **Mantieni impostazioni di replica del database SQL**: conserva le impostazioni di replica per il database SQL dopo l'operazione di ripristino.
     - **Crea backup del registro delle transazioni prima del ripristino**: crea un backup del registro delle transazioni prima dell'operazione di ripristino.
     - **Interrompi il ripristino se il backup del registro delle transazioni prima del ripristino non riesce**: interrompe l'operazione di ripristino se il backup del registro delle transazioni non riesce.
     - **Prescript**: immettere il percorso completo di uno script che deve essere eseguito prima dell'operazione di ripristino, eventuali argomenti richiesti dallo script e il tempo di attesa per il completamento dello script.
   - **Opzioni post-ripristino**:
     - **Operativo**, ma non disponibile per il ripristino di ulteriori registri delle transazioni. In questo modo il database torna online dopo l'applicazione dei backup del registro delle transazioni.
     - **Non operativo**, ma disponibile per il ripristino di ulteriori registri delle transazioni. Mantiene il database in uno stato non operativo dopo l'operazione di ripristino durante il ripristino dei backup del registro delle transazioni. Questa opzione è utile per ripristinare ulteriori registri delle transazioni.
     - **Modalità di sola lettura** e disponibile per il ripristino di registri di transazioni aggiuntivi. Ripristina il database in modalità di sola lettura e applica i backup del registro delle transazioni.
     - **Postscript**: immettere il percorso completo di uno script che deve essere eseguito dopo

l'operazione di ripristino e tutti gli argomenti accettati dallo script.

5. Selezionare **Ripristina**.

Ripristina i dati del carico di lavoro dall'opzione Inventario

Ripristina i carichi di lavoro del database dalla pagina Inventario. Utilizzando l'opzione Inventario, è possibile ripristinare solo i database, non le istanze.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare l'host in cui si trova la risorsa che si desidera ripristinare.
3. Seleziona **Azioni*** **icona e seleziona *Visualizza dettagli**.
4. Nella pagina Microsoft SQL Server, selezionare la scheda **Database**.
5. Nel menu Database, seleziona un database con stato "Protetto".
6. Seleziona **Azioni*** **icona e seleziona *Ripristina**.

   Vengono visualizzate le stesse tre opzioni presenti quando si esegue il ripristino dalla pagina Ripristina:

   - Ripristina da snapshot
   - Ripristinare un punto specifico nel tempo
   - Ripristina l'ultimo backup
7. Continuare con gli stessi passaggi per l'opzione di ripristino dalla pagina Ripristina

Clona i carichi di lavoro di Microsoft SQL Server utilizzando NetApp Backup and Recovery

Clona i dati dell'applicazione Microsoft SQL Server su una macchina virtuale per lo sviluppo, il test o la protezione con NetApp Backup and Recovery. Crea cloni da snapshot istantanei o esistenti dei tuoi carichi di lavoro SQL Server.

Scegli tra i seguenti tipi di cloni:

- **Snapshot e clone istantanei**: puoi creare un clone dei tuoi carichi di lavoro di Microsoft SQL Server da uno snapshot istantaneo, ovvero una copia puntuale dei dati di origine creata da un backup. Il clone viene archiviato in un archivio oggetti nel tuo account cloud pubblico o privato. È possibile utilizzare il clone per ripristinare i carichi di lavoro in caso di perdita o danneggiamento dei dati.
- **Clona da uno snapshot esistente**: puoi scegliere uno snapshot esistente da un elenco di snapshot disponibili per il carico di lavoro. Questa opzione è utile se si desidera creare un clone da un punto specifico nel tempo. Clonazione su storage primario o secondario.

È possibile raggiungere i seguenti obiettivi di protezione:

- Crea un clone
- Aggiorna un clone
- Dividi un clone
- Elimina un clone

Ruolo di NetApp Console obbligatorio Ruolo di visualizzatore di storage, super amministratore di backup e

ripristino o amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Crea un clone

È possibile creare un clone dei carichi di lavoro di Microsoft SQL Server. Un clone è una copia dei dati di origine creata da un backup. Il clone viene archiviato in un archivio oggetti nel tuo account cloud pubblico o privato. È possibile utilizzare il clone per ripristinare i carichi di lavoro in caso di perdita o danneggiamento dei dati.

È possibile creare un clone da uno snapshot esistente o da uno snapshot istantaneo. Uno snapshot istantaneo è una copia puntuale dei dati di origine creata da un backup. È possibile utilizzare il clone per ripristinare i carichi di lavoro in caso di perdita o danneggiamento dei dati.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Clona**.
2. Seleziona **Crea nuovo clone**.
3. Seleziona il tipo di clone:
   - **Clona e aggiorna il database da uno snapshot esistente**: scegli uno snapshot e configura le opzioni di clonazione.
   - **Snapshot e clone istantanei**: acquisisci subito uno snapshot dei dati di origine e crea un clone da tale snapshot. Questa opzione è utile se si desidera creare un clone dai dati più recenti nel carico di lavoro di origine.
4. Completare la sezione **Origine del database**:
   - **Clone singolo o clone in blocco**: seleziona se creare un singolo clone o più cloni. Se selezioni **Clonazione in blocco**, puoi creare più cloni contemporaneamente utilizzando un gruppo di protezione già creato. Questa opzione è utile se si desidera creare più cloni per carichi di lavoro diversi.
   - **Host, istanza e nome del database di origine**: selezionare l'host, l'istanza e il nome del database di origine per il clone. Il database di origine è il database da cui verrà creato il clone.
5. Completare la sezione **Destinazione database**:
   - **Host, istanza e nome del database di destinazione**: selezionare l'host, l'istanza e il nome del database di destinazione per il clone. Il database di destinazione è la posizione in cui verrà creato il clone.

     Facoltativamente, selezionare **Suffisso** dall'elenco a discesa del nome di destinazione e aggiungere un suffisso al nome del database clonato. Se non si aggiunge un suffisso, il nome del database clonato sarà lo stesso del nome del database di origine.

   - **QoS (velocità massima)**: seleziona la velocità massima di trasmissione della qualità del servizio (QoS) in MBps per il clone. La QoS definisce le caratteristiche prestazionali del clone, come la velocità massima di trasmissione e gli IOPS.
6. Completa la sezione **Monte**:
   - **Assegnazione automatica del punto di montaggio**: assegna automaticamente un punto di montaggio per il clone nell'archivio oggetti.
   - **Definisci percorso punto di montaggio**: inserisci un punto di montaggio per il clone. Il punto di montaggio è la posizione in cui il clone verrà montato nell'archivio oggetti. Selezionare la lettera dell'unità, immettere il percorso del file di dati e immettere il percorso del file di registro.
7. Selezionare **Avanti**.

8. Seleziona il punto di ripristino:
    - **Snapshot esistenti**: seleziona uno snapshot esistente dall'elenco degli snapshot disponibili per il carico di lavoro. Questa opzione è utile se si desidera creare un clone da un punto specifico nel tempo.
    - **Snapshot e clone istantanei**: seleziona lo snapshot più recente dall'elenco degli snapshot disponibili per il carico di lavoro. Questa opzione è utile se si desidera creare un clone dai dati più recenti nel carico di lavoro di origine.
9. Se hai scelto di creare **Snapshot istantaneo e clone**, seleziona la posizione di archiviazione del clone:
    - **Archiviazione locale**: selezionare questa opzione per creare il clone nell'archiviazione locale del sistema ONTAP . L'archiviazione locale è l'archiviazione direttamente collegata al sistema ONTAP .
    - **Archiviazione secondaria**: selezionare questa opzione per creare il clone nell'archiviazione secondaria del sistema ONTAP . Lo storage secondario è lo storage utilizzato per i carichi di lavoro di backup e ripristino.
10. Selezionare la posizione di destinazione per i dati e i registri.
11. Selezionare **Avanti**.
12. Completa la sezione **Opzioni avanzate**.
13. Se hai scelto **Snapshot e clonazione istantanei**, completa le seguenti opzioni:
    - **Pianificazione e scadenza dell'aggiornamento del clone**: se hai scelto **Clonazione istantanea**, inserisci la data in cui iniziare ad aggiornare il clone. La pianificazione della clonazione definisce quando verrà creato il clone.
        - **Elimina il clone se la pianificazione scade**: se si desidera eliminare il clone alla data di scadenza.
        - **Aggiorna clone ogni**: seleziona la frequenza con cui il clone deve essere aggiornato. Puoi scegliere di aggiornare il clone ogni ora, ogni giorno, ogni settimana, ogni mese o ogni trimestre. Questa opzione è utile se si desidera mantenere il clone aggiornato con il carico di lavoro di origine.
    - **Prescript e postscript**: facoltativamente, aggiungi script da eseguire prima e dopo la creazione del clone. Questi script possono svolgere attività aggiuntive, come la configurazione del clone o l'invio di notifiche.
    - **Notifica**: facoltativamente, specificare gli indirizzi e-mail per ricevere notifiche sullo stato di creazione del clone insieme al report del lavoro. È anche possibile specificare un URL webhook per ricevere notifiche sullo stato di creazione del clone. È possibile specificare se si desiderano notifiche di successo e di fallimento oppure solo una o l'altra.
    - **Tag**: seleziona le etichette per aiutarti a cercare i gruppi di risorse in seguito e seleziona **Applica**. Ad esempio, se aggiungi "HR" come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag "HR".
14. Seleziona **Crea**.
15. Una volta creato il clone, puoi visualizzarlo nella pagina **Inventario**.

Aggiorna un clone

È possibile aggiornare un clone dei carichi di lavoro di Microsoft SQL Server. L'aggiornamento di un clone comporta l'aggiornamento del clone con i dati più recenti dal carico di lavoro di origine. Questa opzione è utile se si desidera mantenere il clone aggiornato con il carico di lavoro di origine.

È possibile modificare il nome del database, utilizzare l'ultimo snapshot istantaneo o aggiornare da uno snapshot di produzione esistente.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Clona**.
2. Seleziona il clone che vuoi aggiornare.
3. Seleziona l'icona Azioni ••• > **Aggiorna clone**.
4. Completa la sezione **Impostazioni avanzate**:
   - **Ambito di ripristino**: scegli se ripristinare tutti i backup del registro o solo i backup del registro fino a un punto specifico nel tempo. Questa opzione è utile se si desidera ripristinare il clone fino a un punto specifico nel tempo.
   - **Pianificazione e scadenza dell'aggiornamento del clone**: se hai scelto **Clonazione istantanea**, inserisci la data in cui iniziare ad aggiornare il clone. La pianificazione della clonazione definisce quando verrà creato il clone.
     - **Elimina il clone se la pianificazione scade**: se si desidera eliminare il clone alla data di scadenza.
     - **Aggiorna clone ogni**: seleziona la frequenza con cui il clone deve essere aggiornato. Puoi scegliere di aggiornare il clone ogni ora, ogni giorno, ogni settimana, ogni mese o ogni trimestre. Questa opzione è utile se si desidera mantenere il clone aggiornato con il carico di lavoro di origine.
   - **Impostazioni iGroup**: seleziona l'iGroup per il clone. L'iGroup è un raggruppamento logico di iniziatori utilizzati per accedere al clone. È possibile selezionare un iGroup esistente o crearne uno nuovo. Selezionare l'iGroup dal sistema di archiviazione ONTAP primario o secondario.
   - **Prescript e postscript**: facoltativamente, aggiungi script da eseguire prima e dopo la creazione del clone. Questi script possono svolgere attività aggiuntive, come la configurazione del clone o l'invio di notifiche.
   - **Notifica**: facoltativamente, specificare gli indirizzi e-mail per ricevere notifiche sullo stato di creazione del clone insieme al report del lavoro. È anche possibile specificare un URL webhook per ricevere notifiche sullo stato di creazione del clone. È possibile specificare se si desiderano notifiche di successo e di fallimento oppure solo una o l'altra.
   - **Tag**: inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse. Ad esempio, se aggiungi "HR" come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.
5. Nella finestra di dialogo di conferma Aggiorna, per continuare, seleziona **Aggiorna**.

Salta un aggiornamento clone

Salta l'aggiornamento del clone per mantenerlo invariato.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Clona**.
2. Seleziona il clone per il quale vuoi saltare l'aggiornamento.
3. Seleziona l'icona Azioni ••• > **Salta aggiornamento**.
4. Nella finestra di dialogo di conferma Ignora aggiornamento, procedere come segue:
   a. Per saltare solo la prossima pianificazione di aggiornamento, seleziona **Salta solo la prossima pianificazione di aggiornamento**.
   b. Per continuare, seleziona **Salta**.

Dividi un clone

È possibile suddividere un clone dei carichi di lavoro di Microsoft SQL Server. La divisione di un clone crea un nuovo backup dal clone. Il nuovo backup può essere utilizzato per ripristinare i carichi di lavoro.

È possibile scegliere di dividere un clone in cloni indipendenti o a lungo termine. Una procedura guidata mostra l'elenco degli aggregati che fanno parte dell'SVM, le loro dimensioni e dove risiede il volume clonato. NetApp Backup and Recovery indica anche se c'è abbastanza spazio per dividere il clone. Dopo essere stato diviso, il clone diventa un database indipendente a scopo di protezione.

Il lavoro di clonazione non può essere rimosso e può essere riutilizzato per altri cloni.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Clona**.
2. Seleziona un clone.
3. Seleziona l'icona Azioni ••• > **Clonazione divisa**.
4. Rivedi i dettagli del clone diviso e seleziona **Dividi**.
5. Una volta creato il clone diviso, è possibile visualizzarlo nella pagina **Inventario**.

Elimina un clone

È possibile eliminare un clone dei carichi di lavoro di Microsoft SQL Server. L'eliminazione di un clone rimuove il clone dall'archivio oggetti e libera spazio di archiviazione.

Se un criterio protegge il clone, sia il clone che il suo processo vengono eliminati.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Clona**.
2. Seleziona un clone.
3. Seleziona l'icona Azioni ••• > **Elimina clone**.
4. Nella finestra di dialogo di conferma dell'eliminazione del clone, rivedere i dettagli dell'eliminazione.
    a. Per eliminare le risorse clonate da SnapCenter anche se i cloni o il loro archivio non sono accessibili, selezionare **Forza eliminazione**.
    b. Seleziona **Elimina**.
5. Quando il clone viene eliminato, viene rimosso dalla pagina **Inventario**.

Gestisci l'inventario di Microsoft SQL Server con NetApp Backup and Recovery

NetApp Backup and Recovery ti aiuta a gestire gli host, i database e le istanze di Microsoft SQL Server. Puoi visualizzare, modificare o rimuovere le impostazioni di protezione per il tuo inventario.

Puoi svolgere le seguenti attività relative alla gestione del tuo inventario:

- Gestisci le informazioni dell'host
    - Sospendere gli orari
    - Modifica o elimina gli host

- Gestisci le informazioni sulle istanze
  - Associare le credenziali a una risorsa
  - Esegui subito il backup avviando un backup su richiesta
  - Modifica le impostazioni di protezione
- Gestire le informazioni del database
  - Proteggere i database
  - Ripristinare i database
  - Modifica le impostazioni di protezione
  - Esegui subito il backup avviando un backup su richiesta
- Configurare la directory dei registri (da **Inventario** > **Host**). Se si desidera eseguire il backup dei registri per gli host del database nello snapshot, configurare prima i registri in NetApp Backup and Recovery. Per i dettagli, fare riferimento a"Configurare le impostazioni NetApp Backup and Recovery" .

Gestisci le informazioni dell'host

È possibile gestire le informazioni sull'host per garantire che vengano protetti gli host giusti. È possibile visualizzare, modificare ed eliminare le informazioni sull'host.

*Ruolo richiesto NetApp Console * Ruolo di visualizzatore di storage, super amministratore di Backup and Recovery, amministratore di backup di Backup and Recovery, amministratore di ripristino di Backup and Recovery o amministratore di clone di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

- Configurare la directory dei registri. Per i dettagli, fare riferimento a"Configurare le impostazioni NetApp Backup and Recovery" .
- Sospendere gli orari
- Modifica un host
- Elimina un host

Gestisci gli host

Puoi gestire gli host rilevati nel tuo sistema. È possibile gestirli separatamente o in gruppo.

È possibile gestire gli host con stato "Non gestito" nella colonna Host. NetApp Backup and Recovery gestisce già gli host con stato "Gestito".

Dopo aver gestito gli host in NetApp Backup and Recovery, SnapCenter non gestisce più le risorse su tali host.

*Ruolo richiesto NetApp Console * Visualizzatore di storage o super amministratore di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu, seleziona **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Host**.

5. Seleziona uno o più host. Se selezioni più host, viene visualizzata l'opzione Azioni in blocco in cui puoi selezionare **Gestisci (fino a 5 host)**.
6. Seleziona l'icona Azioni ••• > **Gestisci**.
7. Esaminare le dipendenze dell'host:
   - Se vCenter non viene visualizzato, selezionare l'icona della matita per aggiungere o modificare i dettagli di vCenter.
   - Se si aggiunge un vCenter, è necessario anche registrarlo selezionando **Registra vCenter**.
8. Seleziona **Convalida impostazioni** per testare le tue impostazioni.
9. Selezionare **Gestisci** per gestire l'host.

Sospendere gli orari

Sospendi le pianificazioni per interrompere le operazioni di backup e ripristino durante la manutenzione dell'host.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona l'host su cui vuoi sospendere le pianificazioni.
3. Seleziona **Azioni*** ••• **icona e seleziona *Sospendi pianificazioni**.
4. Nella finestra di dialogo di conferma, seleziona **Sospendi**.

Modifica un host

È possibile modificare le informazioni del server vCenter, le credenziali di registrazione dell'host e le opzioni delle impostazioni avanzate.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona l'host che vuoi modificare.
3. Seleziona **Azioni*** ••• **icona e seleziona *Modifica host**.
4. Modifica le informazioni sull'host.
5. Selezionare **Fatto**.

Elimina un host

È possibile eliminare le informazioni dell'host per interrompere i costi del servizio.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona l'host che vuoi eliminare.
3. Seleziona **Azioni*** ••• **icona e seleziona *Elimina host**.
4. Rivedi le informazioni di conferma e seleziona **Elimina**.

Gestisci le informazioni sulle istanze

È possibile gestire le informazioni sulle istanze per assegnare le credenziali appropriate per la protezione delle risorse ed eseguire il backup delle risorse nei seguenti modi:

- Proteggere le istanze
- Credenziali associate
- Disassociare le credenziali
- Protezione dalle modifiche
- Esegui il backup ora

Ruolo NetApp Console obbligatorio Visualizzatore di storage, super amministratore di backup e ripristino, amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Proteggere le istanze del database

È possibile assegnare una policy a un'istanza di database utilizzando policy che regolano le pianificazioni e la conservazione della protezione delle risorse.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona il carico di lavoro che desideri visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Istanze**.
4. Selezionare l'istanza.
5. Seleziona **Azioni*** **icona e seleziona *Proteggi**.
6. Seleziona una policy o creane una nuova.

   Per i dettagli sulla creazione di una policy, fare riferimento a"Crea una politica" .

7. Fornire informazioni sugli script che si desidera eseguire prima e dopo il backup.
   - **Pre-script**: inserisci il nome del file e il percorso dello script per eseguirlo automaticamente prima che venga attivata l'azione di protezione. Ciò è utile per eseguire attività o configurazioni aggiuntive che devono essere eseguite prima del flusso di lavoro di protezione.
   - **Post-script**: inserisci il nome e il percorso del file dello script per eseguirlo automaticamente al termine dell'azione di protezione. Ciò è utile per eseguire attività o configurazioni aggiuntive che devono essere eseguite dopo il flusso di lavoro di protezione.
8. Fornisci informazioni su come desideri che venga verificato lo snapshot:
   - Posizione di archiviazione: seleziona la posizione in cui verrà archiviato lo snapshot di verifica.
   - Risorsa di verifica: seleziona se la risorsa che desideri verificare si trova nello snapshot locale e nell'archiviazione secondaria ONTAP .
   - Pianificazione della verifica: seleziona la frequenza oraria, giornaliera, settimanale, mensile o annuale.

Associare le credenziali a una risorsa

È possibile associare le credenziali a una risorsa in modo che possa essere garantita la protezione.

Per i dettagli, vedere"Configurare le impostazioni NetApp Backup and Recovery , incluse le credenziali" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona il carico di lavoro che desideri visualizzare e seleziona **Visualizza**.

3. Selezionare la scheda **Istanze**.
4. Selezionare l'istanza.
5. Seleziona **Azioni*** **icona e seleziona *Associa credenziali**.
6. Utilizza le credenziali esistenti o creane di nuove.

Modifica le impostazioni di protezione

È possibile modificare la policy, crearne una nuova, impostare una pianificazione e definire le impostazioni di conservazione.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona il carico di lavoro che desideri visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Istanze**.
4. Selezionare l'istanza.
5. Seleziona **Azioni*** **icona e seleziona *Modifica protezione**.

   Per i dettagli sulla creazione di una policy, fare riferimento a"Crea una politica" .

Esegui il backup ora

Esegui subito il backup dei tuoi dati per proteggerli immediatamente.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona il carico di lavoro che desideri visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Istanze**.
4. Selezionare l'istanza.
5. Seleziona **Azioni*** **icona e seleziona *Esegui backup ora**.
6. Scegli il tipo di backup e imposta la pianificazione.

   Per i dettagli sulla creazione di un backup ad hoc, fare riferimento a"Crea una politica" .

Gestire le informazioni del database

È possibile gestire le informazioni del database nei seguenti modi:

- Proteggere i database
- Ripristinare i database
- Visualizza i dettagli della protezione
- Modifica le impostazioni di protezione
- Esegui il backup ora

Proteggere i database

È possibile modificare la policy, crearne una nuova, impostare una pianificazione e definire le impostazioni di

conservazione.

Ruolo NetApp Console obbligatorio Visualizzatore di storage, super amministratore di backup e ripristino, amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona il carico di lavoro che desideri visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Database**.
4. Selezionare il database.
5. Seleziona **Azioni*** **icona e seleziona *Proteggi**.

   Per i dettagli sulla creazione di una policy, fare riferimento a"Crea una politica" .

Ripristinare i database

Ripristina un database per proteggere i tuoi dati.

Ruolo NetApp Console obbligatorio Visualizzatore di storage, super amministratore di backup e ripristino, amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

1. Selezionare la scheda **Database**.
2. Selezionare il database.
3. Seleziona **Azioni*** **icona e seleziona *Ripristina**.

   Per informazioni sul ripristino dei carichi di lavoro, fare riferimento a"Ripristinare i carichi di lavoro" .

Modifica le impostazioni di protezione

È possibile modificare la policy, crearne una nuova, impostare una pianificazione e definire le impostazioni di conservazione.

Ruolo NetApp Console obbligatorio Visualizzatore di storage, super amministratore di backup e ripristino, amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona il carico di lavoro che desideri visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Database**.
4. Selezionare il database.
5. Seleziona **Azioni*** **icona e seleziona *Modifica protezione**.

   Per i dettagli sulla creazione di una policy, fare riferimento a"Crea una politica" .

Esegui il backup ora

Puoi eseguire subito il backup delle istanze e dei database di Microsoft SQL Server per proteggere immediatamente i tuoi dati.

Ruolo NetApp Console obbligatorio Visualizzatore di storage, super amministratore di backup e ripristino, amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Seleziona il carico di lavoro che desideri visualizzare e seleziona **Visualizza**.
3. Selezionare la scheda **Istanze** o **Database**.
4. Selezionare l'istanza o il database.
5. Seleziona **Azioni*** **icona e seleziona *Esegui backup ora**.

Gestisci gli snapshot di Microsoft SQL Server con NetApp Backup and Recovery

È possibile gestire gli snapshot di Microsoft SQL Server eliminandoli da NetApp Backup and Recovery.

Elimina uno snapshot

È possibile eliminare solo gli snapshot locali.

Ruolo NetApp Console obbligatorio Visualizzatore di storage, super amministratore di backup e ripristino, amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Selezionare il carico di lavoro e selezionare **Visualizza**.
3. Selezionare la scheda **Database**.
4. Selezionare il database per il quale si desidera eliminare uno snapshot.
5. Dal menu Azioni, seleziona **Visualizza dettagli protezione**.
6. Selezionare lo snapshot locale che si desidera eliminare.

> Verificare che l'icona dello snapshot locale nella colonna **Posizione** su quella riga appaia in blu.

7. Seleziona **Azioni*** **icona e seleziona *Elimina snapshot locale**.
8. Nella finestra di dialogo di conferma, seleziona **Rimuovi**.

Crea report per i carichi di lavoro di Microsoft SQL Server in NetApp Backup and Recovery

In NetApp Backup and Recovery, crea report per i carichi di lavoro di Microsoft SQL Server per visualizzare lo stato e i dettagli del backup, inclusi i conteggi dei backup

riusciti e non riusciti, i tipi di backup, i sistemi di archiviazione e i timestamp.

Crea un report

*Ruolo richiesto NetApp Console * Visualizzatore di storage, Super amministratore di Backup e ripristino, Amministratore di backup di Backup e ripristino, Amministratore di ripristino di Backup e ripristino, Amministratore di clone di Backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

1. Dal menu NetApp Backup and Recovery , selezionare l'opzione **Report**.
2. Seleziona **Crea report**.
3. Inserisci i dettagli dell'ambito del report:
   - **Nome del report**: immettere un nome univoco per il report.
   - **Tipo di report**: scegli se desideri un report per account o per carico di lavoro (Microsoft SQL Server).
   - **Seleziona host**: se hai selezionato in base al carico di lavoro, seleziona l'host per il quale desideri generare il report.
   - **Seleziona contenuto**: scegli se desideri che il report includa un riepilogo di tutti i backup o i dettagli di ciascun backup. (Se hai scelto "Per account")
4. Inserisci l'intervallo di reporting: scegli se desideri che il report includa i dati dell'ultimo giorno, degli ultimi 7 giorni, degli ultimi 30 giorni, dell'ultimo trimestre o dell'ultimo anno.
5. Inserisci i dettagli di consegna del report: se desideri che il report venga consegnato via e-mail, seleziona **Invia report tramite e-mail**. Inserisci l'indirizzo email a cui desideri che venga inviato il report.

   Configura le notifiche e-mail nella pagina Impostazioni. Per i dettagli sulla configurazione delle notifiche e-mail, vedere"Configurare le impostazioni" .

Proteggi i carichi di lavoro VMware

Proteggi i carichi di lavoro VMware con la panoramica NetApp Backup and Recovery

Proteggi le tue VM VMware e i tuoi datastore con NetApp Backup and Recovery. NetApp Backup and Recovery offre operazioni di backup e ripristino rapide, efficienti in termini di spazio, coerenti con gli arresti anomali e con la VM. È possibile eseguire il backup dei carichi di lavoro VMware su Amazon Web Services S3 o StorageGRID e ripristinarli su un host VMware locale.

Questa versione di NetApp Backup and Recovery supporta solo VMware vCenter e non rileva vVols o VM su vVols.

Utilizza NetApp Backup and Recovery per implementare una strategia 3-2-1, in cui hai 3 copie dei tuoi dati di origine su 2 sistemi di archiviazione diversi, oltre a 1 copia nel cloud. I vantaggi dell'approccio 3-2-1 includono:

- Più copie di dati proteggono dalle minacce informatiche interne ed esterne.
- L'utilizzo di diversi tipi di supporto aiuta a recuperare i dati se un tipo non funziona.
- È possibile ripristinare rapidamente dalla copia in loco e utilizzare le copie fuori sede se la copia in loco è compromessa.

Per passare da una versione all'altra dell'interfaccia utente NetApp Backup and Recovery , fare riferimento a"Passa alla precedente interfaccia utente NetApp Backup and Recovery" .

È possibile utilizzare NetApp Backup and Recovery per eseguire le seguenti attività relative ai carichi di lavoro VMware:

- "Scopri i carichi di lavoro VMware"
- "Crea e gestisci gruppi di protezione per carichi di lavoro VMware"
- "Eseguire il backup dei carichi di lavoro VMware"
- "Ripristinare i carichi di lavoro VMware"

Scopri i carichi di lavoro VMware con NetApp Backup and Recovery

Per poter utilizzare il servizio NetApp Backup and Recovery, è necessario innanzitutto rilevare i datastore VMware e le VM in esecuzione sui sistemi ONTAP . Facoltativamente, puoi importare dati di backup e policy dal SnapCenter Plug-in for VMware vSphere se è già installato.

Ruolo di console obbligatorio Super amministratore di backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Scopri i carichi di lavoro VMware e, facoltativamente, importa le risorse SnapCenter

Durante la fase di individuazione, NetApp Backup and Recovery analizza i carichi di lavoro VMware all'interno dell'organizzazione e valuta e importa le policy di protezione, gli snapshot e le opzioni di backup e ripristino esistenti.

È possibile importare datastore e VM VMware NFS e VMFS dal SnapCenter Plug-in for VMware vSphere nell'inventario NetApp Backup and Recovery .

Questa versione di NetApp Backup and Recovery supporta solo VMware vCenter e non rileva vVols o VM su vVols.

Durante il processo di importazione, NetApp Backup and Recovery esegue le seguenti attività:

- Abilita l'accesso SSH sicuro al server vCenter.
- Attiva la modalità di manutenzione su tutti i gruppi di risorse nel server vCenter.
- Prepara i metadati del vCenter e lo contrassegna come non gestito nella NetApp Console.
- Configura l'accesso al database.
- Rileva VMware vCenter, datastore e VM.
- Importa criteri di protezione, snapshot e opzioni di backup e ripristino esistenti dal SnapCenter Plug-in for VMware vSphere.
- Visualizza le risorse rilevate nella pagina Inventario NetApp Backup and Recovery .

La scoperta avviene nei seguenti modi:

- Se disponi già SnapCenter Plug-in for VMware vSphere, importa le risorse SnapCenter in NetApp Backup and Recovery utilizzando l'interfaccia utente NetApp Backup and Recovery .

Se disponi già del plug-in SnapCenter , assicurati di soddisfare i prerequisiti prima di importare da SnapCenter. Ad esempio, dovresti creare prima i sistemi in NetApp Console per tutti gli storage cluster SnapCenter locali prima di importare da SnapCenter. Vedere"Prerequisiti per l'importazione di risorse da SnapCenter" .

- Se non disponi ancora del plug-in SnapCenter , puoi comunque individuare i carichi di lavoro nei tuoi sistemi aggiungendo manualmente un vCenter ed eseguendo l'individuazione.

Se il plug-in SnapCenter non è già installato, aggiungi un vCenter e scopri le risorse

Se non hai ancora installato il plug-in SnapCenter per VMware, aggiungi le informazioni di vCenter e fai in modo che NetApp Backup and Recovery rilevi i carichi di lavoro. All'interno di ciascun agente della console, seleziona i sistemi in cui desideri rilevare i carichi di lavoro.

Passi

1. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Backup e ripristino**.

   Se si accede a Backup and Recovery per la prima volta e si ha un sistema nella Console ma non sono state rilevate risorse, viene visualizzata la pagina *Benvenuti nel nuovo NetApp Backup and Recovery* con l'opzione **Rileva risorse**.

2. Seleziona **Scopri risorse**.
3. Inserisci le seguenti informazioni:
   a. **Tipo di carico di lavoro**: seleziona **VMware**.
   b. **Impostazioni vCenter**: aggiungi un nuovo vCenter. Per aggiungere un nuovo vCenter, immettere l'FQDN o l'indirizzo IP del vCenter, il nome utente, la password, la porta e il protocollo.

      Se si inseriscono informazioni su vCenter, immettere le informazioni sia per le impostazioni di vCenter sia per la registrazione dell'host. Se hai aggiunto o inserito informazioni su vCenter qui, devi aggiungere anche le informazioni sul plugin nelle Impostazioni avanzate.

   c. **Registrazione host**: non richiesta per VMware.
4. Seleziona **Scopri**.

   Questo processo potrebbe richiedere alcuni minuti.

5. Continua con Impostazioni avanzate.

Se il plug-in SnapCenter è già installato, importare le risorse del plug-in SnapCenter per VMware in NetApp Backup and Recovery

Se hai già installato il plug-in SnapCenter per VMware, importa le risorse del plug-in SnapCenter in NetApp Backup and Recovery seguendo questi passaggi. La console rileva gli host ESXi, i datastore e le VM nei vCenter e pianifica dal plug-in; non è necessario ricreare tutte queste informazioni.

Puoi farlo nei seguenti modi:

- Durante la scoperta, seleziona un'opzione per importare le risorse dal plug-in SnapCenter .
- Dopo la scoperta, dalla pagina Inventario, seleziona un'opzione per importare le risorse del plug-in SnapCenter .

- Dopo l'individuazione, dal menu Impostazioni, seleziona un'opzione per importare le risorse del plug-in SnapCenter . Per i dettagli, vedere"Configurare NetApp Backup and Recovery" . Questa funzionalità non è supportata per VMware.

Si tratta di un processo in due parti descritto in questa sezione:

1. Importa i metadati di vCenter dal plug-in SnapCenter . Le risorse di vCenter importate non sono ancora gestite da NetApp Backup and Recovery.
2. Avvia la gestione di vCenter, VM e datastore selezionati in NetApp Backup and Recovery. Dopo aver avviato la gestione, NetApp Backup and Recovery etichetta vCenter come "Gestito" nella pagina Inventario ed è in grado di eseguire il backup e il ripristino delle risorse importate. Dopo aver avviato la gestione in NetApp Backup and Recovery, non sarà più possibile gestire tali risorse nel plug-in SnapCenter .

Importa metadati vCenter dal plug-in SnapCenter

Questo primo passaggio importa i metadati di vCenter dal plug-in SnapCenter . A quel punto, le risorse non sono ancora gestite da NetApp Backup and Recovery.

Dopo aver importato i metadati di vCenter dal plug-in SnapCenter , NetApp Backup and Recovery non assume automaticamente la gestione della protezione. Per farlo, è necessario selezionare esplicitamente la gestione delle risorse importate in NetApp Backup and Recovery. In questo modo sarai pronto a sottoporre tali risorse a backup tramite NetApp Backup and Recovery.

Passi

1. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Backup e ripristino**.
2. Selezionare **Inventario**.
3. Dalla pagina delle risorse del carico di lavoro NetApp Backup and Recovery Discover, seleziona **Importa da SnapCenter**.
4. Nel campo Importa da, seleziona * SnapCenter Plug-in per VMware*.
5. Inserisci **credenziali VMware vCenter**:
   a. **IP/nome host vCenter**: immettere l'FQDN o l'indirizzo IP del vCenter che si desidera importare in NetApp Backup and Recovery.
   b. **Numero porta vCenter**: immettere il numero di porta per vCenter.
   c. **Nome utente vCenter** e **Password**: immettere il nome utente e la password per vCenter.
   d. **Connettore**: seleziona l'agente della console per vCenter.
6. Inserisci * Credenziali host del plug-in SnapCenter *:
   a. **Credenziali esistenti**: se selezioni questa opzione, puoi utilizzare le credenziali esistenti che hai già aggiunto. Scegli il nome delle credenziali.
   b. **Aggiungi nuove credenziali**: se non disponi di credenziali host per il plug-in SnapCenter , puoi aggiungerne di nuove. Immettere il nome delle credenziali, la modalità di autenticazione, il nome utente e la password.
7. Selezionare **Importa** per convalidare le voci e registrare il plug-in SnapCenter .

Se il plug-in SnapCenter è già registrato, è possibile aggiornare i dettagli di registrazione esistenti.

Risultato

Nella pagina Inventario, vCenter viene visualizzato come non gestito in NetApp Backup and Recovery finché non si seleziona esplicitamente di gestirlo.

Gestisci le risorse importate dal plug-in SnapCenter

Dopo aver importato i metadati vCenter dal plug-in SnapCenter per VMware, gestire le risorse in NetApp Backup and Recovery. Dopo aver scelto di gestire tali risorse, NetApp Backup and Recovery è in grado di eseguire il backup e il ripristino delle risorse importate. Dopo aver avviato la gestione in NetApp Backup and Recovery, non sarà più possibile gestire tali risorse nel plug-in SnapCenter .

Dopo aver scelto di gestire le risorse, le risorse, le VM e i criteri vengono importati dal plug-in SnapCenter per VMware. I gruppi di risorse, le policy e gli snapshot vengono migrati dal plug-in e gestiti in NetApp Backup and Recovery.

Passi

1. Dopo aver importato le risorse VMware dal plug-in SnapCenter , dal menu Backup e ripristino, selezionare **Inventario**.
2. Dalla pagina Inventario, seleziona il vCenter importato che da ora in poi desideri venga gestito da NetApp Backup and Recovery .
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli** per visualizzare i dettagli del carico di lavoro.
4. Dalla pagina Inventario > carico di lavoro, seleziona l'icona Azioni ••• > **Gestisci** per visualizzare la pagina Gestisci vCenter.
5. Seleziona la casella "Vuoi continuare con la migrazione?" e seleziona **Migra**.

Risultato

La pagina Inventario mostra le risorse vCenter appena gestite.

Continua alla dashboard NetApp Backup and Recovery

1. Per visualizzare la Dashboard, dal menu Backup e ripristino, selezionare **Dashboard**.
2. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai carichi di lavoro appena scoperti, protetti e sottoposti a backup.

   "Scopri cosa ti mostra la Dashboard".

Crea e gestisci gruppi di protezione per carichi di lavoro VMware con NetApp Backup and Recovery

Creare gruppi di protezione per gestire le operazioni di backup e ripristino per un set di carichi di lavoro. Un gruppo di protezione è un raggruppamento logico di risorse, quali VM e datastore, che si desidera proteggere insieme.

È possibile eseguire le seguenti attività relative ai gruppi di protezione:

- Crea un gruppo di protezione.
- Visualizza i dettagli della protezione.
- Crea subito un gruppo di protezione. Vedere"Esegui subito il backup dei carichi di lavoro VMware" .
- Sospendere e riprendere la pianificazione del backup di un gruppo di protezione.

- Elimina un gruppo di protezione.

Crea un gruppo di protezione

Raggruppa i carichi di lavoro che desideri proteggere in un gruppo di protezione per eseguirne il backup e il ripristino insieme.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup and Recovery o di amministratore di backup di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare **Crea gruppo di protezione**.
6. Fornire un nome per il gruppo di protezione.
7. Selezionare le VM o i database che si desidera includere nel gruppo di protezione.
8. Selezionare **Avanti**.
9. Selezionare il **criterio di backup** che si desidera applicare al gruppo di protezione.

   Se si desidera creare una policy, selezionare **Crea nuova policy** e seguire le istruzioni per creare una policy. Vedere"Creare politiche" per maggiori informazioni.

10. Selezionare **Avanti**.
11. Rivedere la configurazione.
12. Selezionare **Crea** per creare il gruppo di protezione.

Sospendere la pianificazione del backup di un gruppo di protezione

Sospendere un gruppo di protezione per sospendere i backup pianificati.

Quando si sospende un gruppo di protezione, lo stato di protezione cambia in "In manutenzione". È possibile riprendere la pianificazione del backup in qualsiasi momento.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Seleziona l'icona Azioni ••• > **Sospendi gruppo di protezione**.
6. Rivedi il messaggio di conferma e seleziona **Sospendi**.

Riprendi la pianificazione del backup di un gruppo di protezione

La ripresa di un gruppo di protezione sospeso riavvia i backup pianificati per il gruppo di protezione.

Lo stato di protezione cambia da "In manutenzione" quando si sospende un gruppo di protezione a "Protetto" quando lo si riprende. È possibile riprendere la pianificazione del backup in qualsiasi momento.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Seleziona l'icona Azioni ••• > **Riprendi gruppo di protezione**.
6. Rivedi il messaggio di conferma e seleziona **Riprendi**.

Risultato

Il sistema convalida le pianificazioni e modifica lo stato di protezione in "Protetto" se le pianificazioni sono valide. Se le pianificazioni non sono valide, il sistema visualizza un messaggio di errore e non riprende il gruppo di protezione.

Elimina un gruppo di protezione

Quando si elimina un gruppo di protezione, si rimuovono sia il gruppo stesso che tutte le pianificazioni di backup per il gruppo. Elimina un gruppo di protezione se non ti serve più.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare il gruppo di protezione che si desidera eliminare.
6. Seleziona l'icona Azioni ••• > **Elimina**.
7. Rivedere il messaggio di conferma relativo all'eliminazione dei backup associati e confermare l'eliminazione.

Esegui il backup dei carichi di lavoro VMware con NetApp Backup and Recovery

Esegui il backup delle VM VMware e degli archivi dati dai sistemi ONTAP locali ad Amazon Web Services, Azure NetApp Files o StorageGRID per garantire la protezione dei tuoi dati. I backup vengono generati automaticamente e archiviati in un archivio oggetti nel tuo account cloud pubblico o privato.

- Per eseguire il backup dei carichi di lavoro in base a una pianificazione, creare criteri che governino le operazioni di backup e ripristino. Vedere"Creare politiche" per istruzioni.
- Creare gruppi di protezione per gestire le operazioni di backup e ripristino per un set di risorse. Vedere"Crea e gestisci gruppi di protezione per carichi di lavoro VMware con NetApp Backup and Recovery" per maggiori informazioni.
- Esegui subito il backup dei carichi di lavoro (crea subito un backup su richiesta).

Esegui subito il backup dei carichi di lavoro con un backup on-demand

Crea subito un backup su richiesta. Se stai per apportare modifiche al tuo sistema e vuoi assicurarti di avere un backup prima di iniziare, potresti voler eseguire un backup su richiesta.

Ruolo di NetApp Console obbligatorio Ruolo di visualizzatore di storage, super amministratore di backup e ripristino o amministratore di backup di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu Backup e ripristino, selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**, **Datastore** o **Macchine virtuali**.
5. Selezionare il gruppo di protezione, gli archivi dati o le macchine virtuali di cui si desidera eseguire il backup.
6. Seleziona l'icona Azioni ••• > **Esegui il backup ora**.

   Il criterio applicato al backup è lo stesso criterio assegnato al gruppo di protezione, al datastore o alla macchina virtuale.

7. Selezionare il livello di pianificazione.
8. Seleziona **Esegui backup ora**.

Ripristinare i carichi di lavoro VMware

Ripristina i carichi di lavoro VMware con NetApp Backup and Recovery

Ripristina i carichi di lavoro VMware da snapshot, da un backup del carico di lavoro replicato su un archivio secondario o da backup archiviati in un archivio di oggetti utilizzando NetApp Backup and Recovery.

Ripristina da queste posizioni

È possibile ripristinare i carichi di lavoro da diverse posizioni di partenza:

- Ripristina da una posizione primaria (snapshot locale)
- Ripristina da una risorsa replicata su un archivio secondario
- Ripristina da un backup di archiviazione di oggetti

Ripristinare questi punti

È possibile ripristinare i dati in questi punti:

- **Ripristina nella posizione originale**: la VM viene ripristinata nella posizione originale, nella stessa distribuzione vCenter, nello stesso host ESXi e nello stesso datastore. La VM e tutti i suoi dati vengono sovrascritti.
- **Ripristina in una posizione alternativa**: puoi scegliere un vCenter, un host ESXi o un datastore diverso come destinazione di ripristino per la VM. Questa funzionalità è utile per gestire copie diverse della stessa VM in posizioni e stati diversi.

Considerazioni sul ripristino da storage di oggetti

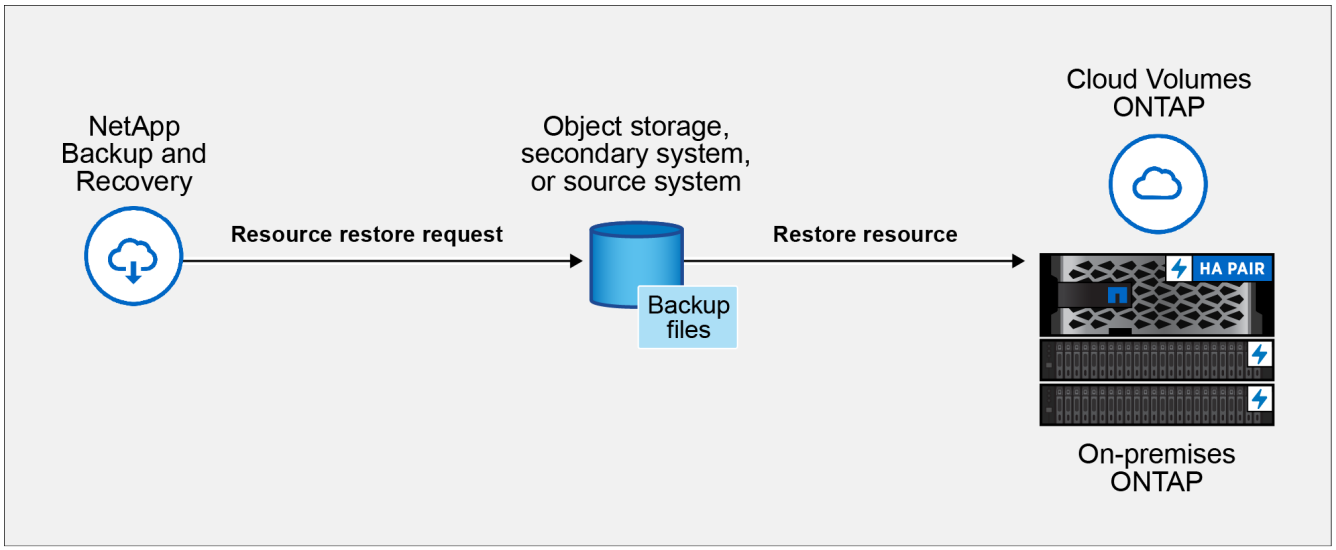
Se Ransomware Resilience è abilitato per un file di backup nell'archiviazione di oggetti, ti verrà chiesto di eseguire un controllo aggiuntivo prima del ripristino. Si consiglia di eseguire la scansione.

Potresti dover pagare costi aggiuntivi al tuo provider cloud per accedere al file di backup.

Come funziona il ripristino dei carichi di lavoro

Quando si ripristinano i carichi di lavoro, si verifica quanto segue:

- Quando si ripristina un carico di lavoro da uno snapshot locale o da un backup remoto, NetApp Backup and Recovery sovrascrive la VM originale se si esegue il ripristino nella posizione originale e crea una *nuova* risorsa se si esegue il ripristino in una posizione alternativa.
- Quando si esegue il ripristino da un carico di lavoro replicato, è possibile ripristinare il carico di lavoro sul sistema ONTAP locale originale o su un sistema ONTAP locale diverso.



- Quando si ripristina un backup da un archivio di oggetti, è possibile ripristinare i dati nel sistema originale o in un sistema ONTAP locale.

Dalla pagina Ripristina (Cerca e ripristina), puoi ripristinare una risorsa cercando lo snapshot con i filtri, anche se non ne ricordi il nome esatto, la posizione o l'ultima data nota.

Ripristina i dati del carico di lavoro dall'opzione Ripristina (Cerca e ripristina)

Ripristina i carichi di lavoro VMware utilizzando l'opzione Ripristina. È possibile cercare l'istantanea in base al nome o utilizzando i filtri.

*Ruolo richiesto NetApp Console * Ruolo di visualizzatore di storage, super amministratore di backup e ripristino, amministratore di ripristino di backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Ripristina**.
2. Dall'elenco a discesa a destra del campo di ricerca del nome, seleziona **VMware**.
3. Immettere il nome della risorsa che si desidera ripristinare oppure filtrare in base al vCenter, al datacenter o al datastore in cui si trova la risorsa da ripristinare.

Viene visualizzato un elenco di macchine virtuali che corrispondono ai criteri di ricerca.

4. Trova la macchina virtuale da cui desideri effettuare il ripristino nell'elenco e seleziona il pulsante del menu delle opzioni per quella macchina virtuale.
5. Nel menu visualizzato, seleziona **Ripristina macchina virtuale**.

   Viene visualizzato un elenco di snapshot (punti di ripristino) creati su quella macchina virtuale. Per impostazione predefinita, vengono mostrati gli snapshot più recenti per l'intervallo di tempo selezionato nel menu a discesa **Intervallo di tempo**.

   Per ogni snapshot, le icone illuminate nella colonna **Posizione** indicano le posizioni di archiviazione in cui è disponibile lo snapshot (archiviazione primaria, secondaria o di oggetti).

6. Abilita il pulsante di opzione per lo snapshot che desideri ripristinare.
7. Selezionare **Avanti**.

   Vengono visualizzate le opzioni per la posizione dello snapshot.

8. Selezionare la destinazione di ripristino per lo snapshot:
   - **Locale**: ripristina lo snapshot dalla posizione locale.
   - **Secondario**: ripristina lo snapshot da una posizione di archiviazione remota.
   - **Archivio oggetti**: ripristina lo snapshot dall'archivio oggetti.

     Se si sceglie l'archiviazione secondaria, selezionare la posizione di destinazione dall'elenco a discesa.

9. Selezionare **Avanti** per continuare.
10. Scegli la destinazione e le impostazioni di ripristino:

Selezione della destinazione

Ripristina nella posizione originale

Quando si esegue il ripristino nella posizione originale, non è possibile modificare il vCenter di destinazione, l'host ESXi, il datastore o il nome della VM. La VM originale viene sovrascritta con l'operazione di ripristino.

1. Selezionare il riquadro **Posizione originale**.
2. Scegli tra le seguenti opzioni:
   - Sezione **Opzioni pre-ripristino**:
     - **Prescript**: abilita questa opzione per automatizzare attività aggiuntive eseguendo uno script personalizzato prima dell'inizio dell'operazione di ripristino. Immettere il percorso completo dello script da eseguire e tutti gli argomenti accettati dallo script.
   - Sezione **Opzioni post-ripristino**:
     - **Riavvia macchina virtuale**: abilita questa opzione per riavviare la macchina virtuale dopo il completamento dell'operazione di ripristino e dopo l'applicazione dello script post-ripristino.
     - **Postscript**: abilita questa opzione per automatizzare attività aggiuntive eseguendo uno script personalizzato al termine del ripristino. Immettere il percorso completo dello script da eseguire e tutti gli argomenti accettati dallo script.
3. Selezionare **Ripristina**.

Ripristina in posizione alternativa

Quando si esegue il ripristino in una posizione alternativa, è possibile modificare il vCenter di destinazione, l'host ESXi, il datastore e il nome della VM per creare una nuova copia della VM in una posizione diversa o con un nome diverso.

1. Selezionare il riquadro **Posizione alternativa**.
2. Inserisci le seguenti informazioni:
   - Sezione **Impostazioni di destinazione**:
     - **FQDN o indirizzo IP vCenter**: seleziona il server vCenter in cui desideri ripristinare lo snapshot.
     - **Host ESXi**: seleziona l'host in cui desideri ripristinare lo snapshot.
     - **Rete**: seleziona la rete in cui desideri ripristinare lo snapshot.
     - **Datastore**: dall'elenco a discesa, seleziona il nome del datastore in cui desideri ripristinare lo snapshot.
     - **Nome macchina virtuale**: immettere il nome della macchina virtuale in cui si desidera ripristinare lo snapshot. Se il nome corrisponde a una VM già esistente nel datastore, Backup and Recovery rende il nome univoco aggiungendo un timestamp corrente.
   - Sezione **Opzioni pre-ripristino**:
     - **Prescript**: abilita questa opzione per automatizzare attività aggiuntive eseguendo uno script personalizzato prima dell'inizio dell'operazione di ripristino. Immettere il percorso completo dello script da eseguire e tutti gli argomenti accettati dallo script.
   - Sezione **Opzioni post-ripristino**:
     - **Riavvia macchina virtuale**: abilita questa opzione per riavviare la macchina virtuale dopo il completamento dell'operazione di ripristino e dopo l'applicazione dello script post-ripristino.
     - **Postscript**: abilita questa opzione per automatizzare attività aggiuntive eseguendo uno script

personalizzato al termine del ripristino. Immettere il percorso completo dello script da eseguire e tutti gli argomenti accettati dallo script.

3. Selezionare **Ripristina**.

Ripristina dischi virtuali specifici dai backup

È possibile ripristinare dischi virtuali esistenti (VMDK) oppure dischi virtuali eliminati o scollegati da backup primari o secondari di VM tradizionali. Ciò consente di ripristinare solo dati o applicazioni specifici della VM, in modo da non dover ripristinare l'intera VM e tutti i dischi virtuali associati in situazioni in cui sono interessati solo dati specifici. Dopo il ripristino, il disco virtuale viene collegato alla sua VM originale ed è pronto per l'uso.

È possibile ripristinare uno o più dischi di macchine virtuali (VMDK) su una VM nello stesso datastore o in datastore diversi.

Per migliorare le prestazioni delle operazioni di ripristino negli ambienti NFS, abilitare l'API vStorage dell'applicazione VMware per l'integrazione di array (VAAI).

Prima di iniziare

- Deve esistere un backup.
- La VM non deve essere in transito.

  La VM che si desidera ripristinare non deve essere in stato vMotion o Storage vMotion.

Informazioni su questo compito

- Se il VMDK viene eliminato o scollegato dalla VM, l'operazione di ripristino collega il VMDK alla VM.
- Un'operazione di ripristino potrebbe non riuscire se il livello di archiviazione del FabricPool in cui si trova la VM non è disponibile.
- Le operazioni di collegamento e ripristino collegano i VMDK utilizzando il controller SCSi predefinito. Tuttavia, quando si esegue il backup dei VMDK collegati a una VM con un disco NVMe, le operazioni di collegamento e ripristino utilizzano il controller NVMe, se disponibile.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Ripristina**.
2. Dall'elenco a discesa a destra del campo di ricerca del nome, seleziona **VMware**.
3. Immettere il nome della risorsa che si desidera ripristinare oppure filtrare in base al vCenter, al datacenter o al datastore in cui si trova la risorsa da ripristinare.

   Viene visualizzato un elenco di macchine virtuali che corrispondono ai criteri di ricerca.

4. Trova la macchina virtuale da cui desideri effettuare il ripristino nell'elenco e seleziona il pulsante del menu delle opzioni per quella macchina virtuale.
5. Nel menu visualizzato, seleziona **Ripristina dischi virtuali**.

   Viene visualizzato un elenco di snapshot (punti di ripristino) creati su quella macchina virtuale. Per impostazione predefinita, vengono mostrati gli snapshot più recenti per l'intervallo di tempo selezionato nel menu a discesa **Intervallo di tempo**.

Per ogni snapshot, le icone illuminate nella colonna **Posizione** indicano le posizioni di archiviazione in cui è disponibile lo snapshot (archiviazione primaria, secondaria o di oggetti).

6. Abilita il pulsante di opzione per lo snapshot che desideri ripristinare.
7. Selezionare **Avanti**.

   Vengono visualizzate le opzioni per la posizione dello snapshot.

8. Selezionare la destinazione di ripristino per lo snapshot:
   - **Locale**: ripristina lo snapshot dalla posizione locale.
   - **Secondario**: ripristina lo snapshot da una posizione di archiviazione remota.
   - **Archivio oggetti**: ripristina lo snapshot dall'archivio oggetti.

     Se si sceglie l'archiviazione secondaria, selezionare la posizione di destinazione dall'elenco a discesa.

9. Selezionare **Avanti** per continuare.
10. Scegli la destinazione e le impostazioni di ripristino:

Selezione della destinazione

Ripristina nella posizione originale

Quando si esegue il ripristino nella posizione originale, non è possibile modificare il vCenter di destinazione, l'host ESXi, il datastore o il nome del disco virtuale. Il disco virtuale originale viene sovrascritto.

1. Selezionare il riquadro **Posizione originale**.
2. Nella sezione **Impostazioni di destinazione**, seleziona la casella di controllo per tutti i dischi virtuali che desideri ripristinare.
3. Scegli tra le seguenti opzioni:
   - Sezione **Opzioni pre-ripristino**:
     - **Prescript**: abilita questa opzione per automatizzare attività aggiuntive eseguendo uno script personalizzato prima dell'inizio dell'operazione di ripristino. Immettere il percorso completo dello script da eseguire e tutti gli argomenti accettati dallo script.
   - Sezione **Opzioni post-ripristino**:
     - **Postscript**: abilita questa opzione per automatizzare attività aggiuntive eseguendo uno script personalizzato al termine del ripristino. Immettere il percorso completo dello script da eseguire e tutti gli argomenti accettati dallo script.
4. Selezionare **Ripristina**.

Ripristina in posizione alternativa

Quando si esegue il ripristino in una posizione alternativa, è possibile modificare il datastore di destinazione. Dopo l'operazione di ripristino, il disco virtuale viene collegato alla VM originale, indipendentemente dal datastore scelto.

1. Selezionare il riquadro **Posizione alternativa**.
2. Nella sezione **Impostazioni di destinazione**, seleziona la casella di controllo per tutti i dischi virtuali che desideri ripristinare.
3. Per tutti i dischi virtuali selezionati:
   a. Selezionare **Seleziona datastore** per scegliere una destinazione di ripristino del datastore diversa per il disco virtuale.
   b. Selezionare **Seleziona** per confermare la scelta e chiudere la finestra di selezione.
4. Scegli tra le seguenti opzioni:
   - Sezione **Opzioni pre-ripristino**:
     - **Prescript**: abilita questa opzione per automatizzare attività aggiuntive eseguendo uno script personalizzato prima dell'inizio dell'operazione di ripristino. Immettere il percorso completo dello script da eseguire e tutti gli argomenti accettati dallo script.
   - Sezione **Opzioni post-ripristino**:
     - **Postscript**: abilita questa opzione per automatizzare attività aggiuntive eseguendo uno script personalizzato al termine del ripristino. Immettere il percorso completo dello script da eseguire e tutti gli argomenti accettati dallo script.
5. Selezionare **Ripristina**.

Ripristina file e cartelle degli ospiti

Requisiti e limitazioni durante il ripristino di file e cartelle guest

È possibile ripristinare file o cartelle da un disco di macchina virtuale (VMDK) su un sistema operativo guest Windows.

Flusso di lavoro di ripristino degli ospiti

Le operazioni di ripristino del sistema operativo guest includono i seguenti passaggi:

1. Allegare

   Collegare un disco virtuale a una macchina virtuale guest e avviare una sessione di ripristino dei file guest.

2. Aspettare

   Attendi il completamento dell'operazione di collegamento prima di poter esplorare e ripristinare. Al termine dell'operazione di collegamento, viene creata automaticamente una sessione di ripristino del file guest.

3. Seleziona file o cartelle

   Sfoglia i file VMDK e seleziona uno o più file o cartelle da ripristinare.

4. Ripristinare

   Ripristina i file o le cartelle selezionati in una posizione specificata.

Prerequisiti per il ripristino di file e cartelle guest

Esaminare tutti i requisiti prima di ripristinare file o cartelle da un VMDK su un sistema operativo guest Windows.

- Gli strumenti VMware devono essere installati e in esecuzione.

  NetApp Backup and Recovery utilizza le informazioni degli strumenti VMware per stabilire una connessione al sistema operativo guest VMware.

- Il sistema operativo guest Windows deve eseguire Windows Server 2008 R2 o versione successiva.

  Per le informazioni più recenti sulle versioni supportate, fare riferimento a "Strumento matrice di interoperabilità NetApp (IMT)" .

- Le credenziali per la macchina virtuale di destinazione utilizzano il dominio predefinito o l'account amministratore locale con nome utente "Amministratore". Prima di avviare l'operazione di ripristino, configurare le credenziali per la macchina virtuale a cui si desidera collegare il disco virtuale. Le credenziali sono necessarie sia per le operazioni di collegamento che di ripristino. Gli utenti del gruppo di lavoro possono utilizzare l'account amministratore locale integrato.

  Se è necessario utilizzare un account che non è l'account amministratore predefinito, ma dispone di privilegi amministrativi all'interno della VM, è necessario disabilitare UAC sulla VM guest.

- È necessario conoscere lo snapshot di backup e il VMDK da cui eseguire il ripristino.

NetApp Backup and Recovery non supporta la ricerca di file o cartelle da ripristinare. Prima di iniziare è necessario sapere dove si trovano i file o le cartelle nello snapshot e il VMDK corrispondente.

- Il disco virtuale da collegare deve trovarsi in un backup NetApp Backup and Recovery .

  Il disco virtuale che contiene il file o la cartella che si desidera ripristinare deve trovarsi in un backup della VM eseguito tramite NetApp Backup and Recovery.

- Per i file con nomi in un alfabeto diverso dall'inglese, è necessario ripristinarli in una directory e non come un singolo file.

  È possibile ripristinare i file con nomi non alfabetici, come i Kanji giapponesi, ripristinando la directory in cui si trovano i file.

Limitazioni del ripristino dei file guest

Prima di ripristinare un file o una cartella da un sistema operativo guest, è necessario essere a conoscenza delle limitazioni della funzionalità.

- Non è possibile ripristinare tipi di dischi dinamici all'interno di un sistema operativo guest.
- Se si ripristina un file o una cartella crittografati, l'attributo di crittografia non viene mantenuto.
- Non è possibile ripristinare file o cartelle in una cartella crittografata.
- I file e le cartelle nascosti vengono visualizzati nella pagina di esplorazione dei file e non è possibile filtrarli.
- Non è possibile effettuare il ripristino da un sistema operativo guest Linux.

  Non è possibile ripristinare file e cartelle da una macchina virtuale che esegue il sistema operativo guest Linux. Tuttavia, è possibile allegare un VMDK e quindi ripristinare manualmente i file e le cartelle. Per le informazioni più recenti sui sistemi operativi guest supportati, fare riferimento a "Strumento matrice di interoperabilità NetApp (IMT)" .

- Non è possibile ripristinare da un file system NTFS a un file system FAT.

  Quando si tenta di ripristinare dal formato NTFS al formato FAT, il descrittore di sicurezza NTFS non viene copiato perché il file system FAT non supporta gli attributi di sicurezza di Windows.

- Non è possibile ripristinare i file guest da un VMDK clonato o da un VMDK non inizializzato.
- Non è possibile ripristinare la struttura della directory di un file.

  Quando si ripristina un file da una directory nidificata, il sistema ripristina solo il file, non la struttura della directory. Per ripristinare l'intero albero delle directory, copiare la directory di livello superiore.

- Non è possibile ripristinare i file guest da una VM vVol a un host alternativo.
- Non è possibile ripristinare i file guest crittografati.

Ripristinare file e cartelle guest da VMDK

È possibile ripristinare uno o più file o cartelle da un VMDK su un sistema operativo guest Windows.

Prima di iniziare

È necessario creare le credenziali per la VM guest in NetApp Backup and Recovery prima di poter ripristinare

file e cartelle da essa. NetApp Backup and Recovery utilizza queste credenziali per l'autenticazione con la VM guest quando si collega il disco virtuale.

Informazioni su questo compito

Le prestazioni del ripristino di file o cartelle guest dipendono da due fattori: la dimensione dei file o delle cartelle da ripristinare e il numero di file o cartelle da ripristinare. Il ripristino di un gran numero di file di piccole dimensioni potrebbe richiedere più tempo del previsto rispetto al ripristino di un piccolo numero di file di grandi dimensioni, se il set di dati da ripristinare ha le stesse dimensioni.

Su una VM è possibile eseguire solo un'operazione di collegamento o ripristino alla volta. Non è possibile eseguire operazioni di collegamento o ripristino parallele sulla stessa VM.

Grazie alla funzionalità di ripristino guest, è possibile visualizzare e ripristinare i file di sistema e nascosti, nonché visualizzare i file crittografati. Non sovrascrivere un file di sistema esistente né ripristinare i file crittografati in una cartella crittografata. Durante l'operazione di ripristino, gli attributi nascosti, di sistema e crittografati dei file guest non vengono mantenuti nel file ripristinato. La visualizzazione o l'esplorazione delle partizioni riservate potrebbe causare un errore.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare il menu **Macchine virtuali**.
3. Selezionare dall'elenco una macchina virtuale contenente i file che si desidera ripristinare.
4. Seleziona l'icona Azioni ••• per quella VM.
5. Seleziona **Ripristina file e cartelle**.
6. Selezionare uno snapshot da cui effettuare il ripristino, quindi selezionare **Avanti**.
7. Selezionare la posizione dello snapshot da cui effettuare il ripristino. Se si sceglie una posizione secondaria, selezionare lo snapshot secondario dall'elenco.
8. Selezionare **Avanti**.
9. Selezionare il disco virtuale dall'elenco da collegare alla VM, quindi selezionare **Avanti**.
10. Nella pagina *Seleziona credenziali macchina virtuale*, se non hai ancora memorizzato le credenziali per la VM guest, seleziona **Aggiungi credenziali** ed esegui le seguenti operazioni:
    a. **Nome credenziali**: immettere un nome per le credenziali.
    b. **Modalità di autenticazione**: selezionare **Windows**.
    c. **Agenti**: selezionare dall'elenco un agente della console che gestirà la comunicazione tra NetApp Backup and Recovery e questo host.
    d. **Dominio e nome utente**: immettere il NetBIOS o il nome di dominio completo (FQDN) e il nome utente per le credenziali.
    e. **Password**: Inserisci una password per le credenziali.
    f. Selezionare **Aggiungi**.
11. Scegliere le credenziali della macchina virtuale da utilizzare per l'autenticazione con la VM guest.

    NetApp Backup and Recovery collega il disco virtuale alla VM e visualizza tutti i file e le cartelle, compresi quelli nascosti. Assegna una lettera di unità a ogni partizione, comprese le partizioni riservate al sistema.

    I file e le cartelle selezionati vengono elencati nel riquadro destro dello schermo.

12. Selezionare **Avanti**.
13. Immettere il percorso di condivisione UNC per l'ospite in cui verranno ripristinati i file selezionati.
    - Esempio di indirizzo IPv4: `\\10.60.136.65\c$`
    - Esempio di indirizzo IPv6: `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`

    Se sono già presenti file con lo stesso nome, puoi scegliere di sovrascriverli o ignorarli.
14. Selezionare **Ripristina**.

    È possibile visualizzare l'avanzamento del ripristino nella pagina Monitoraggio processi.

Risoluzione dei problemi di ripristino dei file guest

Quando si tenta di ripristinare un file guest, è possibile che si verifichi uno dei seguenti scenari.

La sessione di ripristino dei file guest è vuota

Questo problema si verifica se si crea una sessione di ripristino file guest e il sistema operativo guest si riavvia durante la sessione. I VMDK nel sistema operativo guest potrebbero rimanere offline, pertanto l'elenco delle sessioni di ripristino dei file guest è vuoto.

Per correggere il problema, rimettere manualmente online i VMDK nel sistema operativo guest. Quando i VMDK sono online, la sessione di ripristino dei file guest visualizzerà il contenuto corretto.

L'operazione di collegamento del disco al ripristino del file guest non riesce

Questo problema si verifica quando si avvia un'operazione di ripristino di file guest, ma l'operazione di collegamento del disco non riesce anche se VMware Tools è in esecuzione e le credenziali del sistema operativo guest sono corrette. Se ciò si verifica, viene restituito il seguente errore:

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMWare tools is running properly on system and account used is Administrator account, Error is SystemError vix error codes = (3016, 0).
```

Per correggere il problema, riavviare il servizio VMware Tools Windows sul sistema operativo guest, quindi riprovare l'operazione di ripristino del file guest.

I backup non vengono scollegati dopo l'interruzione della sessione di ripristino dei file guest

Questo problema si verifica quando si esegue un'operazione di ripristino di file guest da un backup coerente con la VM. Mentre la sessione di ripristino dei file guest è attiva, viene eseguito un altro backup coerente con la VM per la stessa VM. Quando la sessione di ripristino dei file guest viene disconnessa, manualmente o automaticamente dopo 24 ore, i backup per la sessione non vengono scollegati.

Per correggere il problema, scollegare manualmente i VMDK collegati alla sessione di ripristino dei file guest attiva.

Protezione dei carichi di lavoro KVM (anteprima)

Panoramica sulla protezione dei carichi di lavoro KVM

Proteggi le tue VM KVM gestite e i pool di storage con NetApp Backup and Recovery. NetApp Backup and Recovery offre operazioni di backup e ripristino rapide, efficienti in termini di spazio, coerenti con gli arresti anomali e con la VM. Gli host KVM e le VM devono essere gestiti da una piattaforma di gestione come Apache CloudStack prima di poterli proteggere tramite Backup e ripristino.

È possibile eseguire il backup dei carichi di lavoro KVM su Amazon Web Services S3, Azure NetApp Files o StorageGRID e ripristinare i carichi di lavoro KVM su un host KVM locale.

Utilizza NetApp Backup and Recovery per implementare una strategia di protezione 3-2-1, in cui hai 3 copie dei tuoi dati di origine su 2 sistemi di archiviazione diversi, oltre a 1 copia nel cloud. I vantaggi dell'approccio 3-2-1 includono:

- Più copie di dati proteggono dalle minacce informatiche interne ed esterne.
- L'utilizzo di diversi tipi di supporto aiuta a recuperare i dati se un tipo non funziona.
- È possibile ripristinare rapidamente dalla copia in loco e utilizzare le copie fuori sede se la copia in loco è compromessa.

Per passare da una versione all'altra dell'interfaccia utente NetApp Backup and Recovery , fare riferimento a"Passa alla precedente interfaccia utente NetApp Backup and Recovery" .

È possibile utilizzare NetApp Backup and Recovery per eseguire le seguenti attività relative ai carichi di lavoro KVM:

- "Scopri i carichi di lavoro KVM"
- "Crea e gestisci gruppi di protezione per carichi di lavoro KVM"
- "Eseguire il backup dei carichi di lavoro KVM"
- "Ripristinare i carichi di lavoro KVM"

Scopri i carichi di lavoro KVM in NetApp Backup and Recovery

NetApp Backup and Recovery deve rilevare gli host KVM e le macchine virtuali prima di proteggerli. Gli host KVM e le VM devono essere gestiti da una piattaforma di gestione come Apache CloudStack prima di poterli aggiungere a Backup e ripristino.

Ruolo di console obbligatorio Super amministratore di backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Aggiungi una piattaforma di gestione, un host KVM e scopri le risorse

Aggiungi informazioni sulla piattaforma di gestione e sull'host KVM e lascia che NetApp Backup and Recovery rilevi i carichi di lavoro.

Passi

1. Dal menu NetApp Console , selezionare **Protezione > Backup e ripristino**.

2. In **Carichi di lavoro**, seleziona il riquadro **KVM**.

   Se si accede a Backup and Recovery per la prima volta e si ha un sistema nella Console ma non sono state rilevate risorse, viene visualizzata la pagina *Benvenuti nel nuovo NetApp Backup and Recovery* con l'opzione **Rileva risorse**.

3. Seleziona **Scopri risorse**.
4. Inserisci le seguenti informazioni:
   a. **Tipo di carico di lavoro**: selezionare **KVM**.
   b. Se non hai ancora integrato la tua piattaforma di gestione con Backup e Ripristino, seleziona **Aggiungi piattaforma di gestione**.
      i. Inserisci le seguenti informazioni:
         - **Indirizzo IP o FQDN della piattaforma di gestione**: immettere l'indirizzo IP o il nome di dominio completo della piattaforma di gestione.
         - **Chiave API**: inserisci la chiave API da utilizzare per autenticare le richieste API.
         - **Chiave segreta**: inserisci la chiave segreta da utilizzare per autenticare le richieste API.
         - **Porta**: immettere la porta da utilizzare per la comunicazione tra Backup and Recovery e la piattaforma di gestione.
         - **Agenti**: selezionare un agente della console da utilizzare per facilitare la comunicazione tra Backup and Recovery e la piattaforma di gestione.
      ii. Al termine, seleziona **Aggiungi**.
   c. **Impostazioni KVM**: aggiungi un nuovo host KVM immettendo le seguenti informazioni:
      - **FQDN o indirizzo IP KVM**: immettere l'FQDN o l'indirizzo IP dell'host.
      - **Credenziali**: immettere il nome utente e la password per l'host KVM.
      - **Agente console**: seleziona l'agente console da utilizzare per la comunicazione tra Backup and Recovery e l'host KVM.
      - **Numero porta**: immettere la porta da utilizzare per la comunicazione tra Backup and Recovery e l'host KVM.
      - **Piattaforma di gestione**: se l'host KVM è gestito e hai aggiunto la piattaforma di gestione a Backup e ripristino, seleziona la piattaforma di gestione dall'elenco.
5. Seleziona **Scopri**.

   Questo processo potrebbe richiedere alcuni minuti.

Risultato

Il carico di lavoro KVM viene visualizzato nell'elenco dei carichi di lavoro nella pagina Inventario.

Continua alla dashboard NetApp Backup and Recovery

Passi

1. Dal menu NetApp Console , selezionare **Protezione** > **Backup e ripristino**.
2. Selezionare un riquadro del carico di lavoro (ad esempio, Microsoft SQL Server).
3. Dal menu Backup e ripristino, seleziona **Dashboard**.

4. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai carichi di lavoro appena scoperti, protetti e sottoposti a backup.

Crea e gestisci gruppi di protezione per carichi di lavoro KVM con NetApp Backup and Recovery

Creare gruppi di protezione per gestire le operazioni di backup per un set di risorse KVM. Un gruppo di protezione è un raggruppamento logico di risorse, quali macchine virtuali e pool di archiviazione, che si desidera proteggere insieme. È necessario creare un gruppo di protezione per eseguire il backup delle macchine virtuali KVM o dei pool di archiviazione.

È possibile eseguire le seguenti attività relative ai gruppi di protezione:

- Crea un gruppo di protezione.
- Visualizza i dettagli della protezione.
- Crea subito un gruppo di protezione. Vedere"Esegui subito il backup dei carichi di lavoro KVM" .
- Elimina un gruppo di protezione.

Crea un gruppo di protezione

Raggruppa le VM e i pool di archiviazione che desideri proteggere in un gruppo di protezione.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup and Recovery o di amministratore di backup di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare **Crea gruppo di protezione**.
6. Fornire un nome per il gruppo di protezione.
7. Selezionare le VM o i pool di archiviazione che si desidera includere nel gruppo di protezione.
8. Selezionare **Avanti**.
9. Selezionare il **criterio di backup** che si desidera applicare al gruppo di protezione.

   Per ulteriori informazioni sulla creazione di una policy di backup, fare riferimento a"Creare e gestire policy" .
10. Selezionare **Avanti**.
11. Rivedere la configurazione.
12. Selezionare **Crea** per creare il gruppo di protezione.

Elimina un gruppo di protezione

L'eliminazione di un gruppo di protezione comporta la rimozione del gruppo stesso e di tutte le pianificazioni di backup associate. Potrebbe essere necessario eliminare un gruppo di protezione se non è più necessario.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare il gruppo di protezione che si desidera eliminare.
6. Seleziona l'icona Azioni ••• > **Elimina**.
7. Rivedere il messaggio di conferma relativo all'eliminazione dei backup associati e confermare l'eliminazione.

Esegui il backup dei carichi di lavoro KVM con NetApp Backup and Recovery

Esegui il backup dei gruppi di protezione KVM dai sistemi ONTAP locali ad Amazon Web Services, Azure NetApp Files o StorageGRID per garantire la protezione dei dati. Quando si esegue il backup di un gruppo di protezione, la NetApp Console esegue il backup delle VM e dei pool di archiviazione contenuti nel gruppo di protezione. I backup vengono generati automaticamente e archiviati in un archivio oggetti nel tuo account cloud pubblico o privato.

Per eseguire il backup dei gruppi di protezione in base a una pianificazione, creare criteri che governino le operazioni di backup e ripristino. Vedere"Creare politiche" per istruzioni.

- Creare gruppi di protezione per gestire le operazioni di backup e ripristino per un set di risorse. Vedere"Crea e gestisci gruppi di protezione per carichi di lavoro KVM con NetApp Backup and Recovery" per maggiori informazioni.

Esegui subito il backup dei gruppi di protezione con un backup su richiesta

È possibile eseguire immediatamente un backup su richiesta. Questa funzione è utile se stai per apportare modifiche al tuo sistema e vuoi assicurarti di avere un backup prima di iniziare.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup and Recovery o di amministratore di backup di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Console , selezionare **Protezione > Backup e ripristino**.
2. Nel riquadro KVM, seleziona **Scopri e gestisci**.
3. Selezionare **Inventario**.
4. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
5. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
6. Selezionare la scheda **Gruppi di protezione**, **Datastore** o **Macchine virtuali**.

7. Selezionare il gruppo di protezione di cui si desidera eseguire il backup.
8. Seleziona l'icona Azioni ••• > **Esegui il backup ora**.

   Il criterio applicato al backup è lo stesso criterio assegnato al gruppo di protezione.

9. Selezionare il livello di pianificazione.
10. Selezionare **Backup**.

Ripristinare le macchine virtuali KVM con NetApp Backup and Recovery

Ripristina le macchine virtuali KVM da snapshot, da un backup del gruppo di protezione replicato su un archivio secondario o da backup archiviati nell'archivio oggetti utilizzando NetApp Backup and Recovery.

Ripristina da queste posizioni

È possibile ripristinare le macchine virtuali da diverse posizioni di partenza:

- Ripristina da una posizione primaria (snapshot locale)
- Ripristina da una risorsa replicata su un archivio secondario
- Ripristina da un backup di archiviazione di oggetti

Ripristinare questi punti

È possibile ripristinare i dati in questi punti:

- Ripristina la posizione originale

Considerazioni sul ripristino da storage di oggetti

Se selezioni un file di backup nell'archiviazione oggetti e per quel backup è attiva la protezione ransomware (se hai abilitato DataLock e Ransomware Resilience nei criteri di backup), ti verrà richiesto di eseguire un ulteriore controllo di integrità sul file di backup prima di ripristinare i dati. Ti consigliamo di eseguire la scansione.

Per accedere al contenuto del file di backup, dovrai sostenere costi di uscita aggiuntivi da parte del tuo provider cloud.

Come funziona il ripristino delle macchine virtuali

Quando si ripristinano macchine virtuali, si verifica quanto segue:

- Quando si ripristina un carico di lavoro da un file di backup locale, NetApp Backup and Recovery crea una *nuova* risorsa utilizzando i dati del backup.
- Quando si esegue il ripristino da una VM replicata, è possibile ripristinarla nel sistema originale o in un sistema ONTAP locale.
- Quando si ripristina un backup da un archivio di oggetti, è possibile ripristinare i dati nel sistema originale o in un sistema ONTAP locale.

Dalla pagina Ripristina (nota anche come Cerca e ripristina), puoi ripristinare una VM anche se non ricordi il nome esatto, la posizione in cui si trova o la data dell'ultima volta in cui era in buone condizioni. È possibile cercare l'istantanea utilizzando i filtri.

Ripristina le VM dall'opzione Ripristina (Cerca e ripristina)

Ripristinare le macchine virtuali KVM utilizzando l'opzione Ripristina. È possibile cercare l'istantanea in base al nome o utilizzando i filtri.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup e ripristino o di amministratore di ripristino di Backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Console , selezionare **Protezione > Backup e ripristino**.
2. Dal menu NetApp Backup and Recovery , selezionare **Ripristina**.
3. Dall'elenco a discesa a destra del campo di ricerca del nome, selezionare **KVM**.
4. Immettere il nome della macchina virtuale che si desidera ripristinare oppure filtrare in base all'host della macchina virtuale o al pool di archiviazione in cui si trova la risorsa da ripristinare.

   Viene visualizzato un elenco di snapshot che corrispondono ai criteri di ricerca.

5. Selezionare il pulsante **Ripristina** per lo snapshot che si desidera ripristinare.

   Viene visualizzato un elenco di possibili punti di ripristino.

6. Seleziona il punto di ripristino che desideri utilizzare.
7. Selezionare una posizione di origine dello snapshot.
8. Selezionare **Avanti** per continuare.
9. Scegli la destinazione e le impostazioni di ripristino:

Selezione della destinazione

Ripristina nella posizione originale

1. **Abilita ripristino rapido**: seleziona questa opzione per eseguire un'operazione di ripristino rapido. I volumi e i dati ripristinati saranno disponibili immediatamente. Non utilizzare questa opzione su volumi che richiedono prestazioni elevate perché durante il processo di ripristino rapido l'accesso ai dati potrebbe essere più lento del solito.
2. **Opzioni pre-ripristino**: immettere il percorso completo di uno script che deve essere eseguito prima dell'operazione di ripristino e tutti gli argomenti accettati dallo script.
3. **Opzioni post-ripristino**:
   - **Riavvia VM**: selezionare questa opzione per riavviare la VM al termine dell'operazione di ripristino e dopo l'applicazione dello script post-ripristino.
   - **Postscript**: immettere il percorso completo di uno script che deve essere eseguito dopo l'operazione di ripristino e tutti gli argomenti accettati dallo script.
4. Sezione **Notifiche**:
   - **Abilita notifiche e-mail**: seleziona questa opzione per ricevere notifiche e-mail sull'operazione di ripristino e indica il tipo di notifiche che desideri ricevere.
5. Selezionare **Ripristina**.

Ripristina in posizione alternativa

Non disponibile per l'anteprima dei carichi di lavoro KVM.

Proteggere i carichi di lavoro Hyper-V

Panoramica sulla protezione dei carichi di lavoro Hyper-V

Proteggi le tue VM Hyper-V con NetApp Backup and Recovery. NetApp Backup and Recovery fornisce operazioni di backup e ripristino rapide, efficienti in termini di spazio, coerenti con gli arresti anomali e con la VM, sia per istanze standalone che per istanze cluster FCI. È anche possibile proteggere le macchine virtuali Hyper-V fornite da System Center Virtual Machine Manager (SCVMM) e ospitate su una condivisione CIFS.

È possibile eseguire il backup dei carichi di lavoro Hyper-V su Amazon Web Services S3 o StorageGRID e ripristinarli su un host Hyper-V locale.

Utilizza NetApp Backup and Recovery per implementare una strategia di protezione 3-2-1, in cui hai 3 copie dei tuoi dati di origine su 2 sistemi di archiviazione diversi, oltre a 1 copia nel cloud. I vantaggi dell'approccio 3-2-1 includono:

- Più copie di dati proteggono dalle minacce informatiche interne ed esterne.
- Diversi tipi di supporto garantiscono la fattibilità del failover in caso di guasto fisico o logico di un tipo di supporto.
- La copia in loco consente di ripristinare rapidamente i dati e, se la copia in loco è compromessa, è possibile utilizzare le copie fuori sede.

Quando si aggiungono host Hyper-V e si individuano risorse, NetApp Backup and Recovery installa il plug-in NetApp Hyper-V e il plug-in NetApp SnapCenter Windows FileSystem sull'host Hyper-V per facilitare la gestione e la protezione delle macchine virtuali.

Per passare da una versione all'altra dell'interfaccia utente NetApp Backup and Recovery , fare riferimento a"Passa alla precedente interfaccia utente NetApp Backup and Recovery" .

È possibile utilizzare NetApp Backup and Recovery per eseguire le seguenti attività relative ai carichi di lavoro Hyper-V:

- "Scopri i carichi di lavoro Hyper-V"
- "Crea e gestisci gruppi di protezione per carichi di lavoro Hyper-V"
- "Eseguire il backup dei carichi di lavoro Hyper-V"
- "Ripristinare i carichi di lavoro Hyper-V"

Scopri i carichi di lavoro Hyper-V in NetApp Backup and Recovery

NetApp Backup and Recovery deve rilevare le macchine virtuali Hyper-V prima di poterle proteggere.

Ruolo di console obbligatorio Super amministratore di backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Aggiungi un host Hyper-V e scopri le risorse

Aggiungi le informazioni sull'host Hyper-V e lascia che NetApp Backup and Recovery rilevi le macchine virtuali. All'interno di ciascun agente della Console, seleziona i sistemi in cui desideri scoprire le risorse.

Quando si aggiungono host Hyper-V e si individuano risorse, NetApp Backup and Recovery installa il plug-in NetApp Hyper-V e il plug-in NetApp SnapCenter Windows FileSystem sull'host Hyper-V per facilitare la gestione e la protezione delle macchine virtuali.

Passi

1. Dal menu NetApp Console , selezionare **Protezione** > **Backup e ripristino**.

   Se è la prima volta che accedi a NetApp Backup and Recovery, hai già un sistema nella Console ma non hai ancora individuato alcuna risorsa, viene visualizzata la pagina di destinazione "Benvenuti nel nuovo NetApp Backup and Recovery" che mostra un'opzione per **Individuare risorse**.

2. Seleziona **Scopri risorse**.
3. Inserisci le seguenti informazioni:
   a. **Tipo di carico di lavoro**: selezionare **Hyper-V**.
   b. Se non hai ancora memorizzato le credenziali per questo host Hyper-V, seleziona **Aggiungi credenziali**.
      i. Selezionare l'agente della console da utilizzare con questo host.
      ii. Inserisci un nome per questa credenziale.
      iii. Inserisci il nome utente e la password per l'account.
      iv. Selezionare **Fatto**.
   c. **Registrazione host**: aggiungi un nuovo host Hyper-V immettendo l'FQDN o l'indirizzo IP dell'host, le credenziali, l'agente della console e il numero di porta. Se l'FQDN non è risolvibile dall'agente della console, utilizzare invece l'indirizzo IP. Per i cluster FCI, immettere l'indirizzo IP di gestione del cluster FCI.

4. Seleziona **Scopri**.

Questo processo potrebbe richiedere alcuni minuti.

Risultato

Dopo che NetApp Backup and Recovery rileva le risorse, la pagina Inventario visualizza il carico di lavoro Hyper-V nell'elenco dei carichi di lavoro.

Continua alla dashboard NetApp Backup and Recovery

Passi

1. Dal menu NetApp Console , selezionare **Protezione** > **Backup e ripristino**.
2. Selezionare un riquadro del carico di lavoro (ad esempio, Microsoft SQL Server).
3. Dal menu Backup e ripristino, seleziona **Dashboard**.
4. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai carichi di lavoro appena scoperti, protetti e sottoposti a backup.

Crea e gestisci gruppi di protezione per carichi di lavoro Hyper-V con NetApp Backup and Recovery

Creare gruppi di protezione per gestire le operazioni di backup per un set di macchine virtuali. Un gruppo di protezione è un raggruppamento logico di risorse, ad esempio macchine virtuali, che si desidera proteggere insieme.

È possibile eseguire le seguenti attività relative ai gruppi di protezione:

- Crea un gruppo di protezione.
- Visualizza i dettagli della protezione.
- Crea subito un gruppo di protezione. Vedere"Esegui subito il backup dei carichi di lavoro Hyper-V" .
- Elimina un gruppo di protezione.

Crea un gruppo di protezione

Raggruppa i carichi di lavoro che desideri proteggere in un gruppo di protezione. Crea un gruppo di protezione per eseguire il backup e il ripristino dei carichi di lavoro insieme.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup and Recovery o di amministratore di backup di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare il menu **Gruppi di protezione**.
5. Selezionare **Crea gruppo di protezione**.
6. Fornire un nome per il gruppo di protezione.

7. Selezionare le VM che si desidera includere nel gruppo di protezione.
8. Selezionare **Avanti**.
9. Selezionare il **criterio di backup** che si desidera applicare al gruppo di protezione.
10. Selezionare **Avanti**.
11. Rivedere la configurazione.
12. Selezionare **Crea** per creare il gruppo di protezione.

Modifica un gruppo di protezione

Modifica un gruppo di protezione per cambiarne il nome o le impostazioni. Potrebbe essere necessario modificare un gruppo di protezione se le risorse al suo interno sono cambiate.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare il gruppo di protezione che si desidera modificare.
6. Seleziona l'icona Azioni ••• > **Modifica**.
7. Modificare le impostazioni del gruppo di protezione, ad esempio il nome o le macchine virtuali presenti nel gruppo.
8. Selezionare **Avanti**.
9. Se necessario, modificare la politica di protezione. Al termine, seleziona **Avanti**.
10. Rivedi la configurazione e seleziona **Invia**.

Elimina un gruppo di protezione

L'eliminazione di un gruppo di protezione comporta la rimozione del gruppo stesso e di tutte le pianificazioni di backup associate. Potrebbe essere necessario eliminare un gruppo di protezione se non è più necessario.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare il gruppo di protezione che si desidera eliminare.
6. Seleziona l'icona Azioni ••• > **Elimina**.
7. Rivedere il messaggio di conferma relativo all'eliminazione dei backup associati e confermare l'eliminazione.

Esegui il backup dei carichi di lavoro Hyper-V con NetApp Backup and Recovery

Esegui il backup delle VM Hyper-V dai sistemi ONTAP locali ad Amazon Web Services, Azure NetApp Files o StorageGRID per garantire la protezione dei tuoi dati. I backup

vengono generati automaticamente e archiviati in un archivio oggetti nel tuo account cloud pubblico o privato.

- Per eseguire il backup dei carichi di lavoro in base a una pianificazione, creare criteri che governino le operazioni di backup e ripristino. Vedere"Creare politiche" per istruzioni.
- Creare gruppi di protezione per gestire le operazioni di backup e ripristino per un set di risorse. Vedere"Crea e gestisci gruppi di protezione per carichi di lavoro Hyper-V con NetApp Backup and Recovery" per maggiori informazioni.
- Esegui subito il backup dei carichi di lavoro (crea subito un backup su richiesta).

Esegui subito il backup dei carichi di lavoro con un backup on-demand

Utilizza il backup su richiesta in modo che i tuoi dati siano protetti prima di apportare modifiche al sistema.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup and Recovery o di amministratore di backup di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu, seleziona **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**, **Datastore** o **Macchine virtuali**.
5. Selezionare il gruppo di protezione o le macchine virtuali di cui si desidera eseguire il backup.
6. Seleziona l'icona Azioni ••• > **Esegui il backup ora**.

   Il backup utilizza lo stesso criterio assegnato al gruppo di protezione o alla macchina virtuale.

7. Selezionare il livello di pianificazione.
8. Selezionare **Backup**.

Ripristina i carichi di lavoro Hyper-V con NetApp Backup and Recovery

Ripristina i carichi di lavoro Hyper-V da snapshot, da un backup del carico di lavoro replicato su un archivio secondario o da backup archiviati nell'archivio oggetti utilizzando NetApp Backup and Recovery.

Ripristina da queste posizioni

È possibile ripristinare i carichi di lavoro da diverse posizioni di partenza:

- Ripristina da una posizione primaria (snapshot locale)
- Ripristina da una risorsa replicata su un archivio secondario
- Ripristina da un backup di archiviazione di oggetti

Ripristinare questi punti

È possibile ripristinare i dati in questi punti:

- Ripristina la posizione originale
- Ripristina in una posizione alternativa

Considerazioni sul ripristino da storage di oggetti

Se selezioni un file di backup nell'archiviazione oggetti e per quel backup è attiva la protezione ransomware (se hai abilitato DataLock e Ransomware Resilience nei criteri di backup), ti verrà richiesto di eseguire un ulteriore controllo di integrità sul file di backup prima di ripristinare i dati. Ti consigliamo di eseguire la scansione.

Per accedere al contenuto del file di backup, dovrai sostenere costi di uscita aggiuntivi da parte del tuo provider cloud.

Come funziona il ripristino dei carichi di lavoro

Quando si ripristinano i carichi di lavoro, si verifica quanto segue:

- Quando si ripristina un carico di lavoro da un file di backup locale, NetApp Backup and Recovery crea una *nuova* risorsa utilizzando i dati del backup.
- Quando si esegue il ripristino da un carico di lavoro replicato, è possibile ripristinare il carico di lavoro sul sistema originale o su un sistema ONTAP locale.

Dalla pagina Ripristina (nota anche come Cerca e ripristina), puoi ripristinare una risorsa anche se non ricordi il nome esatto, la posizione in cui si trova o la data dell'ultima volta in cui era in buone condizioni. È possibile cercare l'istantanea utilizzando i filtri.

Ripristina i dati del carico di lavoro dall'opzione Ripristina (Cerca e ripristina)

Ripristinare i carichi di lavoro Hyper-V utilizzando l'opzione Ripristina. È possibile cercare l'istantanea in base al nome o utilizzando i filtri.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup e ripristino o di amministratore di ripristino di Backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Ripristina**.
2. Dall'elenco a discesa a destra del campo di ricerca del nome, selezionare **Hyper-V**.
3. Immettere il nome della risorsa che si desidera ripristinare oppure filtrare in base al nome della VM, all'host della VM o al pool di archiviazione in cui si trova la risorsa che si desidera ripristinare.

   Viene visualizzato un elenco di snapshot che corrispondono ai criteri di ricerca.

4. Selezionare il pulsante **Ripristina** per lo snapshot che si desidera ripristinare.

   Viene visualizzato un elenco di possibili punti di ripristino.

5. Seleziona il punto di ripristino che desideri utilizzare.
6. Selezionare una posizione di origine dello snapshot.
7. Selezionare **Avanti** per continuare.
8. Scegli la destinazione e le impostazioni di ripristino:

Selezione della destinazione

Ripristina nella posizione originale

Quando si ripristina la posizione originale, è possibile visualizzare le impostazioni di destinazione espandendo la sezione **Impostazioni di destinazione**, ma non è possibile modificarle.

1. Nella sezione **Opzioni post-ripristino**, prendere in considerazione la seguente opzione:
   - **Avvia la macchina virtuale**: abilita questa opzione per avviare la nuova macchina virtuale dopo il ripristino.
2. Selezionare **Ripristina**.

Ripristina in posizione alternativa

1. Nella sezione **Impostazioni destinazione**: inserisci le seguenti informazioni:
   - **FQDN o indirizzo IP Hyper-V**: immettere il nome di dominio completo o l'indirizzo IP dell'host Hyper-V di destinazione.
   - **Rete**: seleziona la rete di destinazione in cui desideri ripristinare lo snapshot.
   - **Nome macchina virtuale**: immettere il nome della VM che si desidera ripristinare.
   - **Posizione di destinazione**: immettere la cartella di destinazione o la condivisione CIFS che deve contenere i dati ripristinati.
2. Nella sezione **Opzioni pre-ripristino**, prendi in considerazione le seguenti opzioni:
   - **Ripristino rapido**: abilita questa opzione per rendere immediatamente disponibile la VM ripristinata. Dall'archivio oggetti vengono ripristinati solo i file necessari per eseguire la macchina virtuale, anziché l'intero volume.
3. Nella sezione **Opzioni di ripristino post**, prendi in considerazione le seguenti opzioni:
   - **Avvia la macchina virtuale**: abilita questa opzione per avviare la nuova macchina virtuale dopo il ripristino.
4. Selezionare **Ripristina**.

Proteggi i carichi di lavoro Oracle Database (Preview)

Panoramica sulla protezione dei carichi di lavoro del database Oracle

Proteggi i database e i log Oracle utilizzando NetApp Backup and Recovery. Ottieni backup e ripristini rapidi, efficienti in termini di spazio, coerenti con gli arresti anomali e coerenti con il database. Esegui il backup dei carichi di lavoro di Oracle Database su AWS S3, NetApp StorageGRID, Azure Blob Storage o ONTAP S3. Ripristina i backup su un host Oracle on-premises.

Utilizza NetApp Backup and Recovery per implementare una strategia di protezione 3-2-1, in cui hai 3 copie dei tuoi dati di origine su 2 sistemi di archiviazione diversi, oltre a 1 copia nel cloud. I vantaggi dell'approccio 3-2-1 includono:

- Più copie di dati proteggono dalle minacce informatiche interne ed esterne.
- L'utilizzo di diversi tipi di supporto aiuta a recuperare i dati se un tipo non funziona.

- È possibile ripristinare rapidamente dalla copia in loco e utilizzare le copie fuori sede se la copia in loco è compromessa.

> Per passare da una versione all'altra dell'interfaccia utente NetApp Backup and Recovery , fare riferimento a"Passa alla precedente interfaccia utente NetApp Backup and Recovery" .

È possibile utilizzare NetApp Backup and Recovery per eseguire le seguenti attività relative ai carichi di lavoro di Oracle Database:

- "Scopri i carichi di lavoro Oracle Database"
- "Crea e gestisci gruppi di protezione per i carichi di lavoro Oracle Database"
- "Esegui il backup dei carichi di lavoro Oracle Database"
- "Ripristina i carichi di lavoro del database Oracle"

Scopri i carichi di lavoro di Oracle Database in NetApp Backup and Recovery

NetApp Backup and Recovery deve prima rilevare i database Oracle per poterli proteggere.

Ruolo di console obbligatorio Super amministratore di backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Aggiungi un host Oracle e scopri le risorse

Aggiungi le informazioni sull'host Oracle e lascia che NetApp Backup and Recovery rilevi i carichi di lavoro. All'interno di ciascun agente della console, seleziona i sistemi in cui desideri rilevare i carichi di lavoro.

Passi

1. Dal menu NetApp Console , selezionare **Protezione > Backup e ripristino**.
2. In **Carichi di lavoro**, seleziona il riquadro **Oracle**.

   Se si accede a Backup and Recovery per la prima volta e si ha un sistema nella Console ma non sono state rilevate risorse, viene visualizzata la pagina *Benvenuti nel nuovo NetApp Backup and Recovery* con l'opzione **Rileva risorse**.

3. Seleziona **Scopri risorse**.
4. Inserisci le seguenti informazioni:
   a. **Tipo di carico di lavoro**: seleziona **Oracle**.
   b. Se non hai ancora memorizzato le credenziali per questo host Oracle, seleziona **Aggiungi credenziali**.
      i. Selezionare l'agente della console da utilizzare con questo host.
      ii. Inserisci un nome per questa credenziale.
      iii. Inserisci il nome utente e la password per l'account.
      iv. Selezionare **Fatto**.
   c. **Registrazione host**: aggiungi un nuovo host Oracle. Immettere l'FQDN o l'indirizzo IP dell'host, le credenziali, l'agente della console e il numero di porta.
5. Seleziona **Scopri**.

Questo processo potrebbe richiedere alcuni minuti.

Risultato

Il carico di lavoro Oracle viene visualizzato nell'elenco dei carichi di lavoro nella pagina Inventario.

Continua alla dashboard NetApp Backup and Recovery

1. Dal menu NetApp Console , selezionare **Protezione** > **Backup e ripristino**.
2. Selezionare un riquadro del carico di lavoro (ad esempio, Microsoft SQL Server).
3. Dal menu Backup e ripristino, seleziona **Dashboard**.
4. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai carichi di lavoro appena scoperti, protetti e sottoposti a backup.

Crea e gestisci gruppi di protezione per i carichi di lavoro di Oracle Database con NetApp Backup and Recovery

Creare gruppi di protezione per gestire le operazioni di backup per un set di risorse di Oracle Database. Un gruppo di protezione è un raggruppamento logico di risorse, ad esempio database, che si desidera proteggere insieme. È necessario creare un gruppo di protezione per eseguire il backup dei database Oracle.

È possibile eseguire le seguenti attività relative ai gruppi di protezione:

- Crea un gruppo di protezione.
- Visualizza i dettagli della protezione.
- Esegui subito il backup di un gruppo di protezione. Vedi "Esegui subito il backup dei carichi di lavoro Oracle Database".
- Elimina un gruppo di protezione.

Crea un gruppo di protezione

Raggruppa le VM e i pool di archiviazione che desideri proteggere in un gruppo di protezione.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup and Recovery o di amministratore di backup di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare **Crea gruppo di protezione**.
6. Fornire un nome per il gruppo di protezione.
7. Selezionare le VM o i pool di archiviazione che si desidera includere nel gruppo di protezione.
8. Selezionare **Avanti**.

9. Selezionare il **criterio di backup** che si desidera applicare al gruppo di protezione.

   Se si desidera creare una policy, selezionare **Crea nuova policy** e seguire le istruzioni per creare una policy. Vedere"Creare politiche" per maggiori informazioni.

10. Selezionare **Avanti**.
11. Rivedere la configurazione.
12. Selezionare **Crea** per creare il gruppo di protezione.

Elimina un gruppo di protezione

L'eliminazione di un gruppo di protezione comporta la rimozione del gruppo stesso e di tutte le pianificazioni di backup associate. Potrebbe essere necessario eliminare un gruppo di protezione se non è più necessario.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Inventario**.
2. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
3. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
4. Selezionare la scheda **Gruppi di protezione**.
5. Selezionare il gruppo di protezione che si desidera eliminare.
6. Seleziona l'icona Azioni ••• > **Rimuovi protezione**.
7. Rivedere il messaggio di conferma relativo all'eliminazione dei backup associati e confermare l'eliminazione.

Esegui il backup dei carichi di lavoro di Oracle Database utilizzando NetApp Backup and Recovery

Utilizza NetApp Backup and Recovery per eseguire il backup di gruppi di protezione o database Oracle Database da sistemi ONTAP locali a storage cloud, tra cui Amazon S3, NetApp StorageGRID, Microsoft Azure Blob Storage o ONTAP S3. NetApp Backup and Recovery esegue il backup dei database e dei dati di registro in ciascun gruppo di protezione.

Per eseguire il backup di gruppi di protezione o singoli database in base a una pianificazione, creare policy che gestiscano le operazioni di backup e ripristino. Vedere"Creare politiche" per istruzioni.

- Crea gruppi di protezione per gestire le operazioni di backup e ripristino per un set di risorse. Vedi "Crea e gestisci gruppi di protezione per i carichi di lavoro di Oracle Database con NetApp Backup and Recovery" per ulteriori informazioni.
- Esegui subito il backup di un gruppo di protezione (crea subito un backup su richiesta).
- Esegui subito il backup di un database.

Esegui subito il backup dei gruppi di protezione con un backup su richiesta

Esegui un backup su richiesta prima di apportare modifiche al sistema per garantire la protezione dei dati.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup and Recovery o di amministratore di

backup di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Console , selezionare **Protezione > Backup e ripristino**.
2. In **Carichi di lavoro**, seleziona il riquadro **Oracle**.
3. Selezionare **Inventario**.
4. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
5. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
6. Selezionare la scheda **Gruppi di protezione**, **Datastore** o **Macchine virtuali**.
7. Selezionare il gruppo di protezione di cui si desidera eseguire il backup.
8. Seleziona l'icona Azioni ••• > **Esegui il backup ora**.

   NetApp Backup and Recovery utilizza la stessa policy sia per il gruppo di backup che per quello di protezione.

9. Selezionare il livello di pianificazione.
10. Selezionare **Backup**.

Esegui subito il backup di un database con un backup su richiesta

È possibile eseguire un backup su richiesta di un singolo database.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup and Recovery o di amministratore di backup di Backup and Recovery. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Console , selezionare **Protezione > Backup e ripristino**.
2. In **Carichi di lavoro**, seleziona il riquadro **Oracle**.
3. Selezionare **Inventario**.
4. Selezionare un carico di lavoro per visualizzare i dettagli della protezione.
5. Seleziona l'icona Azioni ••• > **Visualizza dettagli**.
6. Selezionare la scheda **Database**.
7. Selezionare il database di cui si desidera eseguire il backup.
8. Seleziona l'icona Azioni ••• > **Esegui il backup ora**.
9. Selezionare il livello di pianificazione.
10. Selezionare **Backup**.

Ripristina i database Oracle con NetApp Backup and Recovery

Ripristina i database Oracle da snapshot, da un backup replicato su un archivio secondario o da backup archiviati in un archivio oggetti utilizzando NetApp Backup and Recovery.

Ripristina da queste posizioni

È possibile ripristinare i database da diverse posizioni di partenza:

- Ripristina da una posizione primaria (snapshot locale)
- Ripristina da una risorsa replicata su un archivio secondario
- Ripristina da un backup di archiviazione di oggetti

Ripristinare questi punti

È possibile ripristinare i dati nella posizione originale; il ripristino in una posizione alternativa non è disponibile in questa versione di anteprima privata.

- Ripristina la posizione originale

Come funziona il ripristino dei database Oracle

Quando si ripristinano i database Oracle, si verifica quanto segue:

- Quando si ripristina un database da uno snapshot locale, NetApp Backup and Recovery crea una *nuova* risorsa utilizzando i dati del backup.
- Quando si esegue il ripristino da un archivio replicato, è possibile ripristinarlo nella posizione originale.
- Quando si ripristina un backup da un archivio oggetti, è possibile ripristinare i dati nell'archivio di origine o in un sistema ONTAP locale e recuperare il database da lì.

Dalla pagina Ripristina (nota anche come Cerca e ripristina), puoi ripristinare un database anche se non ricordi il nome esatto, la posizione in cui si trova o la data dell'ultima volta in cui era in buone condizioni. È possibile effettuare ricerche nel database utilizzando i filtri.

Ripristinare un database Oracle

A seconda delle esigenze, è possibile ripristinare un database Oracle a un punto specifico nel tempo, a un numero di modifica del sistema (SCN) specifico o all'ultimo stato valido. È anche possibile ripristinare semplicemente il database dagli snapshot e saltare il processo di ripristino automatico. Se si desidera eseguire il ripristino manualmente, è consigliabile saltare il processo di ripristino automatico. È possibile effettuare la ricerca nel database tramite il nome oppure tramite filtri specifici.

Ruolo di console obbligatorio Ruolo di super amministratore di Backup e ripristino o di amministratore di ripristino di Backup e ripristino. "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Dal menu NetApp Console , selezionare **Protezione > Backup e ripristino**.
2. Dal menu NetApp Backup and Recovery , selezionare **Ripristina**.
3. Dall'elenco a discesa a destra del campo di ricerca del nome, seleziona **Oracle**.
4. Immettere il nome del database che si desidera ripristinare oppure filtrare in base all'host del database in cui si trova il database che si desidera ripristinare.

   Viene visualizzato un elenco di snapshot che corrispondono ai criteri di ricerca.

5. Selezionare il pulsante **Ripristina** per il database che si desidera ripristinare.
6. Scegli un'opzione di ripristino:

Ripristinare un punto specifico nel tempo

a. Seleziona **Ripristina a un punto specifico nel tempo**.
b. Selezionare **Avanti**.
c. Scegli una data dal menu a discesa e seleziona **Cerca**.

   Viene visualizzato un elenco di snapshot corrispondenti alla data specificata.

Ripristinare un numero di modifica del sistema specifico (SCN)

a. Selezionare **Ripristina a un numero di modifica del sistema (SCN) specifico**.
b. Selezionare **Avanti**.
c. Inserisci l'SCN da utilizzare come punto di ripristino e seleziona **Cerca**.

   Viene visualizzato un elenco di snapshot corrispondenti per l'SCN specificato.

Ripristina l'ultimo backup (ultimo stato valido)

a. Seleziona **Ripristina all'ultimo backup**.
b. Selezionare **Avanti**.

   Vengono visualizzati gli ultimi backup completi e di registro.

Ripristina da snapshot senza recupero

a. Seleziona **Ripristina da snapshot senza ripristino**.
b. Selezionare **Avanti**.

   Vengono visualizzate le istantanee corrispondenti.

7. Selezionare una posizione di origine dello snapshot.
8. Selezionare **Avanti** per continuare.
9. Scegli la destinazione e le impostazioni di ripristino:

Selezione della destinazione

Ripristina nella posizione originale

1. **Impostazioni di destinazione**:
   - Scegliere se ripristinare l'intero database o solo i tablespace del database.
   - **File di controllo**: facoltativamente, abilitare questa opzione per ripristinare anche i file di controllo del database.
2. **Opzioni pre-ripristino**:
   - Facoltativamente, abilitare questa opzione e immettere il percorso completo di uno script che deve essere eseguito prima dell'operazione di ripristino e tutti gli argomenti accettati dallo script.
   - Scegliere un valore di timeout per lo script. Se lo script non riesce a essere eseguito entro questo periodo di tempo, il ripristino verrà comunque eseguito.
3. **Opzioni post-ripristino**:
   - **Postscript**: facoltativamente, abilitare questa opzione e immettere il percorso completo di uno script che deve essere eseguito dopo l'operazione di ripristino e tutti gli argomenti accettati dallo script.
   - **Aprire il database o il database contenitore in modalità LETTURA-SCRITTURA dopo il ripristino**: una volta completata l'operazione di ripristino, Backup and Recovery abiliterà la modalità LETTURA-SCRITTURA per il database.
4. Sezione **Notifiche**:
   - **Abilita notifiche e-mail**: seleziona questa opzione per ricevere notifiche e-mail sull'operazione di ripristino e indica il tipo di notifiche che desideri ricevere.
5. Selezionare **Ripristina**.

Ripristina in posizione alternativa

Non disponibile per l'anteprima dei carichi di lavoro Oracle Database.

Montare e smontare i punti di ripristino del database Oracle con NetApp Backup and Recovery

Potrebbe essere necessario montare un punto di ripristino di Oracle Database se è necessario accedere al database in uno stato controllato per eseguire operazioni di ripristino.

Montare un punto di ripristino del database Oracle

Se si configura il criterio di protezione per un database in modo che conservi i log di archivio, è possibile montare punti di ripristino per visualizzare la cronologia delle modifiche del database.

Passi

1. Dal menu NetApp Console , selezionare **Protezione > Backup e ripristino**.
2. Seleziona la tessera Oracle.
3. Nel menu Backup e ripristino, selezionare **Inventario**.
4. Per il carico di lavoro Oracle Database nell'elenco, selezionare **Visualizza**.
5. Selezionare il menu **Database**.

6. Scegli un database dall'elenco e seleziona l'icona Azioni ••• > **Visualizza i dettagli della protezione**.

   Viene visualizzato un elenco di punti di ripristino per quel database.

7. Scegli un punto di ripristino dall'elenco e seleziona l'icona Azioni ••• > **Monte**.
8. Nella finestra di dialogo che appare, procedi come segue:
   a. Selezionare dall'elenco l'host che deve montare il punto di ripristino.
   b. Selezionare la posizione che Backup e Ripristino devono utilizzare per montare il punto di ripristino. Per la versione di anteprima, il montaggio dall'archivio oggetti non è supportato.

      Viene visualizzato il percorso di montaggio che Backup e Ripristino devono utilizzare.

9. Selezionare **Monta**.

   Il punto di ripristino è montato sull'host Oracle.

Smontare un punto di ripristino del database Oracle

Smontare il punto di ripristino quando non è più necessario visualizzare le modifiche apportate al database.

Passi

1. Dal menu NetApp Console , selezionare **Protezione > Backup e ripristino**.
2. Seleziona la tessera Oracle.
3. Nel menu Backup e ripristino, selezionare **Inventario**.
4. Per il carico di lavoro Oracle nell'elenco, selezionare **Visualizza**.
5. Selezionare il menu **Database**.
6. Scegli un database dall'elenco e seleziona l'icona Azioni ••• > **Visualizza i dettagli della protezione**.

   Viene visualizzato un elenco di punti di ripristino per quel database.

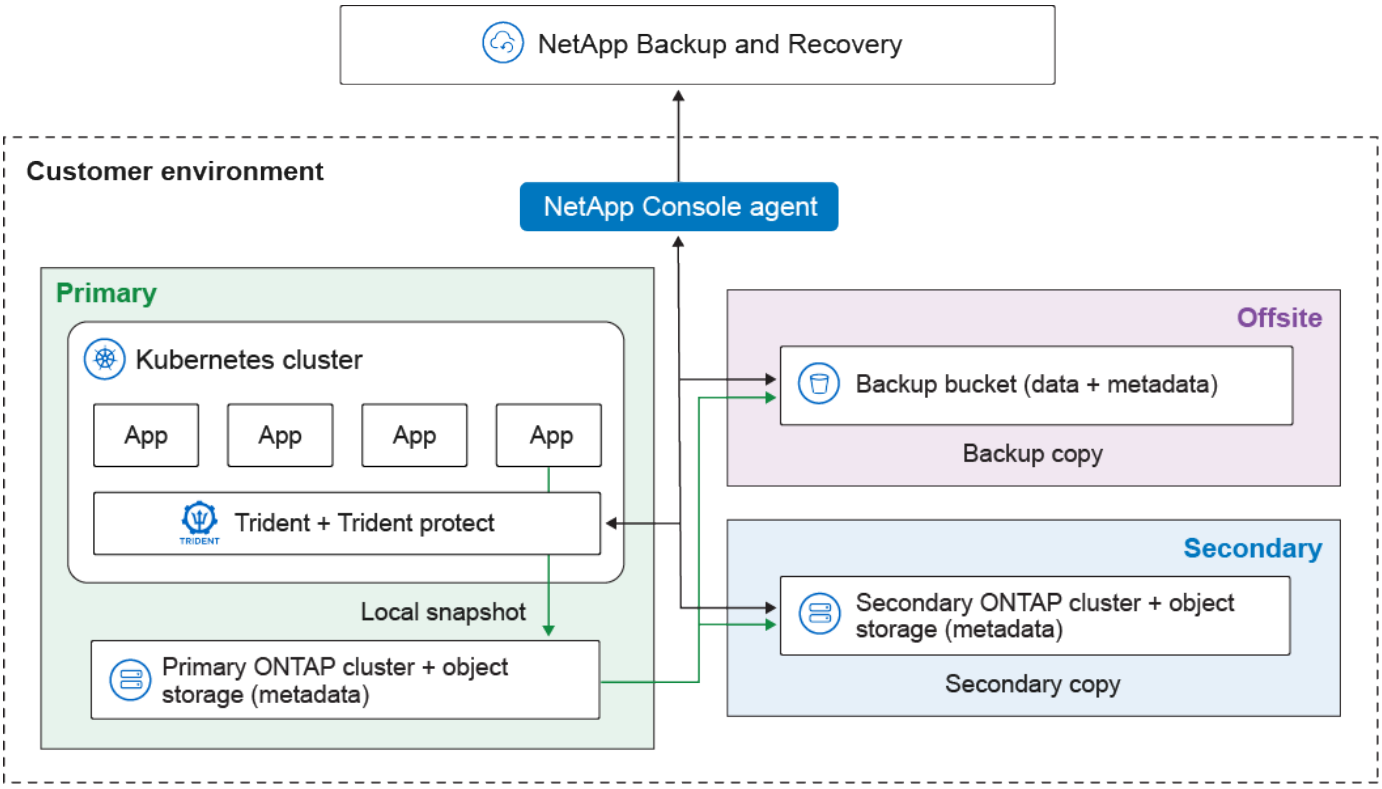
7. Scegli un punto di ripristino dall'elenco e seleziona l'icona Azioni ••• > **Smonta**.
8. Confermare l'azione selezionando **Smonta**.

Proteggi i carichi di lavoro di Kubernetes (anteprima)

Panoramica sulla gestione dei carichi di lavoro Kubernetes

La gestione dei carichi di lavoro Kubernetes in NetApp Backup and Recovery consente di individuare, gestire e proteggere i cluster e le applicazioni Kubernetes, il tutto in un unico posto. Puoi gestire risorse e applicazioni ospitate sui tuoi cluster Kubernetes. Puoi anche creare e associare policy di protezione ai tuoi carichi di lavoro Kubernetes, il tutto utilizzando un'unica interfaccia.

Il diagramma seguente mostra i componenti e l'architettura di base del backup e del ripristino per i carichi di lavoro Kubernetes e come diverse copie dei dati possono essere archiviate in posizioni diverse:



NetApp Backup and Recovery offre i seguenti vantaggi per la gestione dei carichi di lavoro Kubernetes:

- Un unico piano di controllo per proteggere le applicazioni in esecuzione su più cluster Kubernetes. Queste applicazioni possono includere container o macchine virtuali in esecuzione sui cluster Kubernetes.
- Integrazione nativa con NetApp SnapMirror, che consente funzionalità di offload dello storage per tutti i flussi di lavoro di backup e ripristino.
- Backup incrementali permanenti per le applicazioni Kubernetes, che si traducono in Recovery Point Objectives (RPO) e Recovery Time Objectives (RTO) inferiori.

> La presente documentazione viene fornita come anteprima tecnologica. Durante l'anteprima, la funzionalità Kubernetes non è consigliata per i carichi di lavoro di produzione. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli, i contenuti e la tempistica dell'offerta prima della disponibilità generale.

È possibile svolgere le seguenti attività relative alla gestione dei carichi di lavoro Kubernetes:

- "Scopri i carichi di lavoro di Kubernetes".
- "Gestire i cluster Kubernetes".
- "Aggiungi e proteggi le applicazioni Kubernetes".
- "Gestire le applicazioni Kubernetes".
- "Ripristina le applicazioni Kubernetes".

Scopri i carichi di lavoro Kubernetes in NetApp Backup and Recovery

NetApp Backup and Recovery deve rilevare i carichi di lavoro Kubernetes prima di proteggerli.

*Ruolo richiesto NetApp Console * Super amministratore di backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Scopri i carichi di lavoro di Kubernetes

Nell'inventario di backup e ripristino, scopri i carichi di lavoro Kubernetes nel tuo ambiente. L'aggiunta di un carico di lavoro aggiunge un cluster Kubernetes a NetApp Backup and Recovery. È quindi possibile aggiungere applicazioni e proteggere le risorse del cluster.

> Quando si rileva un cluster attualmente protetto con Trident Protect, tutte le pianificazioni di backup utilizzate con Trident Protect vengono disabilitate durante il processo di rilevamento (le pianificazioni di backup di Trident Protect non sono compatibili con Backup and Recovery). Per proteggere le applicazioni del cluster, "crea una nuova policy di protezione" oppure associare le applicazioni a una policy esistente. È quindi possibile rimuovere le pianificazioni di backup di Trident Protect, se necessario.

Passi

1. Eseguire una delle seguenti operazioni:
   - Se stai rilevando carichi di lavoro Kubernetes per la prima volta, in NetApp Backup and Recovery, in **Carichi di lavoro**, seleziona il riquadro **Kubernetes**.
   - Se hai già individuato i carichi di lavoro Kubernetes, in NetApp Backup and Recovery seleziona **Inventario** > **Carichi di lavoro** e quindi seleziona **Individuazione risorse**.
2. Selezionare il tipo di carico di lavoro **Kubernetes**.
3. Inserisci un nome per il cluster e scegli un connettore da utilizzare con il cluster.
4. Seguire le istruzioni della riga di comando che appaiono:
   - Crea uno spazio dei nomi Trident Protect
   - Crea un segreto Kubernetes
   - Aggiungi un repository Helm
   - Installa o aggiorna Trident Protect e il connettore Trident Protect

     Questi passaggi garantiscono che NetApp Backup and Recovery possa interagire con il cluster.
5. Dopo aver completato i passaggi, seleziona **Scopri**.

   Il cluster viene aggiunto all'inventario.
6. Selezionare **Visualizza** nel carico di lavoro Kubernetes associato per visualizzare l'elenco di applicazioni, cluster e namespace per quel carico di lavoro.

Continua alla dashboard NetApp Backup and Recovery

Per visualizzare la dashboard NetApp Backup and Recovery , seguire questi passaggi.

1. Dal menu NetApp Console , selezionare **Protezione** > **Backup e ripristino**.
2. Selezionare un riquadro del carico di lavoro (ad esempio, Microsoft SQL Server).
3. Dal menu Backup e ripristino, seleziona **Dashboard**.
4. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai carichi di lavoro appena scoperti, protetti e sottoposti a backup.

"Scopri cosa ti mostra la Dashboard".

Aggiungi e proteggi le applicazioni Kubernetes

Aggiungi e proteggi le applicazioni Kubernetes

NetApp Backup and Recovery ti consente di individuare facilmente i tuoi cluster Kubernetes, senza dover generare e caricare file kubeconfig. È possibile connettere i cluster Kubernetes e installare il software necessario utilizzando semplici comandi copiati dall'interfaccia utente NetApp Console .

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Aggiungi e proteggi una nuova applicazione Kubernetes

Il primo passo per proteggere le applicazioni Kubernetes è creare un'applicazione all'interno NetApp Backup and Recovery. Quando si crea un'applicazione, si fa in modo che la Console sia a conoscenza dell'applicazione in esecuzione sul cluster Kubernetes.

Prima di iniziare

Prima di poter aggiungere e proteggere un'applicazione Kubernetes, è necessario"scopri i carichi di lavoro di Kubernetes" .

Aggiungi un'applicazione utilizzando l'interfaccia utente web

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Seleziona **Crea applicazione**.
5. Inserisci un nome per l'applicazione.
6. Facoltativamente, seleziona uno dei seguenti campi per cercare le risorse che desideri proteggere:
   - Cluster associato
   - Spazi dei nomi associati
   - Tipi di risorse
   - Selettori di etichette
7. Facoltativamente, seleziona **Risorse con ambito cluster** per scegliere tutte le risorse con ambito a livello di cluster. Se le includi, verranno aggiunte all'applicazione al momento della creazione.
8. Facoltativamente, seleziona **Cerca** per trovare le risorse in base ai tuoi criteri di ricerca.

   La console non memorizza i parametri o i risultati della ricerca; i parametri vengono utilizzati per cercare nel cluster Kubernetes selezionato le risorse che possono essere incluse nell'applicazione.

9. La Console visualizza un elenco di risorse che corrispondono ai criteri di ricerca.
10. Se l'elenco contiene le risorse che si desidera proteggere, selezionare **Avanti**.
11. Facoltativamente, nell'area **Criterio**, seleziona un criterio di protezione esistente per proteggere l'applicazione o creane uno nuovo. Se non selezioni un criterio, l'applicazione verrà creata senza criterio di protezione. Puoi"aggiungere una politica di protezione" Dopo.
12. Nell'area **Prescript e postscript**, abilitare e configurare tutti gli hook di esecuzione prescript o postscript che si desidera eseguire prima o dopo le operazioni di backup. Per abilitare prescript o postscript, devi averne già creato almeno uno"modello di gancio di esecuzione" .
13. Seleziona **Crea**.

Risultato

L'applicazione viene creata e appare nell'elenco delle applicazioni nella scheda **Applicazioni** dell'inventario Kubernetes. La NetApp Console consente la protezione dell'applicazione in base alle impostazioni e puoi monitorare l'avanzamento nell'area **Monitoraggio** del backup e del ripristino.

Aggiungi un'applicazione utilizzando un CR

Passi

1. Crea il file CR dell'applicazione di destinazione:
   a. Creare il file custom resource (CR) e assegnargli un nome (ad esempio `my-app-name.yaml`).
   b. Configura i seguenti attributi:
      - **metadata.name**: (*Obbligatorio*) Il nome della risorsa personalizzata dell'applicazione. Nota il nome che scegli perché altri file CR necessari per le operazioni di protezione fanno

riferimento a questo valore.

- **spec.includedNamespaces**: (*Obbligatorio*) Utilizzare il selettore di namespace e di etichetta per specificare i namespace e le risorse che l'applicazione utilizza. Il namespace dell'applicazione deve essere parte di questo elenco. Il selettore di etichetta è facoltativo e può essere utilizzato per filtrare le risorse all'interno di ciascun namespace specificato.
- **spec.includedClusterScopedResources**: (*Facoltativo*) Utilizzare questo attributo per specificare le risorse con ambito cluster da includere nella definizione dell'applicazione. Questo attributo consente di selezionare queste risorse in base al gruppo, alla versione, al tipo e alle etichette.
  - **groupVersionKind**: (*Obbligatorio*) Specifica il gruppo API, la versione e il tipo di risorsa con ambito cluster.
  - **labelSelector**: (*Facoltativo*) Filtra le risorse con ambito cluster in base alle loro etichette.

c. Configurare le seguenti annotazioni, se necessario:

- **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze**: (*Facoltativo*) Questa annotazione è applicabile solo alle applicazioni definite da macchine virtuali, ad esempio in ambienti KubeVirt, in cui si verificano blocchi del file system prima degli snapshot. Specificare se l'applicazione può scrivere sul file system durante uno snapshot. Se impostato su true, l'applicazione ignora l'impostazione globale e può scrivere sul file system durante uno snapshot. Se impostato su false, l'applicazione ignora l'impostazione globale e il file system viene bloccato durante uno snapshot. Se specificato ma l'applicazione non ha macchine virtuali nella definizione dell'applicazione, l'annotazione viene ignorata. Se non specificato, l'applicazione segue "impostazione di congelamento del filesystem globale".
- **protect.trident.netapp.io/protection-command**: (*Facoltativo*) Utilizzare questa annotazione per indicare a NetApp Backup and Recovery di proteggere o interrompere la protezione dell'applicazione. I valori possibili sono `protect` o `unprotect`.
- **protect.trident.netapp.io/protection-policy-name**: (*Facoltativo*) Utilizzare questa annotazione per specificare il nome della policy di protezione di NetApp Backup and Recovery che si desidera utilizzare per proteggere questa applicazione. Questa policy di protezione deve essere già presente in NetApp Backup and Recovery.

Se è necessario applicare questa annotazione dopo che un'applicazione è già stata creata, è possibile utilizzare il seguente comando:

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```

+
Esempio YAML:

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
    protect.trident.netapp.io/protection-command: "protect"
    protect.trident.netapp.io/protection-policy-name: "policy-name"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. (*Facoltativo*) Aggiungi il filtraggio che include o esclude le risorse contrassegnate con etichette particolari:

   - **resourceFilter.resourceSelectionCriteria**: (Obbligatorio per il filtraggio) Utilizzare `Include` o `Exclude` per includere o escludere una risorsa definita in resourceMatchers. Aggiungere i seguenti parametri resourceMatchers per definire le risorse da includere o escludere:

     - **resourceFilter.resourceMatchers**: Un array di resourceMatcher oggetti. Se si definiscono più elementi in questo array, la corrispondenza avviene tramite un'operazione OR, e i campi all'interno di ciascun elemento (group, kind, version) corrispondono tramite un'operazione AND.

       - **resourceMatchers[].group**: (*Facoltativo*) Gruppo della risorsa da filtrare.
       - **resourceMatchers[].kind**: (*Facoltativo*) Tipo di risorsa da filtrare.

- **resourceMatchers[].version**: (*Facoltativo*) Versione della risorsa da filtrare.
- **resourceMatchers[].names**: (*Facoltativo*) Nomi nel campo metadata.name di Kubernetes della risorsa da filtrare.
- **resourceMatchers[].namespaces**: (*Facoltativo*) Namespace nel campo metadata.name di Kubernetes della risorsa da filtrare.
- **resourceMatchers[].labelSelectors**: (*Facoltativo*) Stringa del selettore di etichetta nel campo metadata.name dei metadati Kubernetes della risorsa come definito in "Documentazione Kubernetes". Ad esempio: `"trident.netapp.io/os=linux"`.

> Quando sia `resourceFilter` che `labelSelector` vengono utilizzati, `resourceFilter` viene eseguito per primo e poi `labelSelector` viene applicato alle risorse risultanti.

Ad esempio:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

2. Dopo aver creato la CR dell'applicazione adatta al tuo ambiente, applica la CR. Ad esempio:

```
kubectl apply -f my-app-name.yaml
```

Esegui ora il backup delle applicazioni Kubernetes utilizzando l'interfaccia utente Web di Backup and Recovery

NetApp Backup and Recovery consente di eseguire manualmente il backup delle applicazioni Kubernetes utilizzando l'interfaccia web.

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp

Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Esegui subito il backup di un'applicazione Kubernetes utilizzando la web UI

Crea manualmente un backup di un'applicazione Kubernetes per stabilire una base di riferimento per backup e snapshot futuri o per garantire la protezione dei dati più recenti.

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione di cui vuoi eseguire il backup e seleziona il menu Azioni associato.
5. Seleziona **Esegui backup ora**.
6. Assicurarsi che sia selezionato il nome corretto dell'applicazione.
7. Selezionare **Backup**.

Risultato

La Console crea un backup dell'applicazione e visualizza l'avanzamento nell'area **Monitoraggio** di Backup e Ripristino. Il backup viene creato in base ai criteri di protezione associati all'applicazione.

Esegui ora il backup delle applicazioni Kubernetes utilizzando risorse personalizzate in Backup and Recovery

NetApp Backup and Recovery consente di eseguire manualmente il backup delle applicazioni Kubernetes utilizzando risorse personalizzate (CR).

Esegui subito il backup di un'applicazione Kubernetes utilizzando risorse personalizzate

Crea manualmente un backup di un'applicazione Kubernetes per stabilire una base di riferimento per backup e snapshot futuri o per garantire la protezione dei dati più recenti.

> Le risorse con ambito cluster vengono incluse in un backup, snapshot o clone se sono esplicitamente referenziate nella definizione dell'applicazione o se hanno riferimenti a uno qualsiasi degli spazi dei nomi dell'applicazione.

Prima di iniziare

Assicurarsi che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di backup s3 di lunga durata. Se il token scade durante l'operazione di backup, l'operazione può fallire.

- Fare riferimento a "Documentazione API AWS" per ulteriori informazioni sulla verifica della scadenza del token della sessione corrente.
- Fare riferimento a "Documentazione AWS IAM" per ulteriori informazioni sulle credenziali con le risorse AWS.

Crea uno snapshot locale utilizzando una risorsa personalizzata

Per creare uno snapshot della tua applicazione Kubernetes e archiviarlo localmente, usa la risorsa personalizzata Snapshot con attributi specifici.

Passi

1. Crea il file di risorsa personalizzata (CR) e assegnagli il nome `local-snapshot-cr.yaml`.
2. Nel file che hai creato, configura i seguenti attributi:
   - **metadata.name**: (*Obbligatorio*) Il nome di questa risorsa personalizzata; scegli un nome univoco e sensato per il tuo ambiente.
   - **spec.applicationRef**: Nome Kubernetes dell'applicazione di cui eseguire lo Snapshot.
   - **spec.appVaultRef**: (*Obbligatorio*) Il nome del AppVault in cui i contenuti dello snapshot (metadati) devono essere archiviati.
   - **spec.reclaimPolicy**: (*Facoltativo*) Definisce cosa succede all'AppArchive di uno snapshot quando il CR dello snapshot viene eliminato. Ciò significa che anche quando impostato su `Retain`, lo snapshot verrà eliminato. Opzioni valide:
     - `Retain` (predefinito)
     - `Delete`

```
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  namespace: my-app-namespace
  name: local-snapshot-cr
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  reclaimPolicy: Retain
```

3. Dopo aver popolato il `local-snapshot-cr.yaml` file con i valori corretti, applica la CR:

```
kubectl apply -f local-snapshot-cr.yaml
```

Eseguire il backup di un'applicazione in un archivio di oggetti utilizzando una risorsa personalizzata

Crea un CR di backup con attributi specifici per eseguire il backup della tua applicazione su un archivio di oggetti.

Passi

1. Crea il file custom resource (CR) e assegnagli il nome `object-store-backup-cr.yaml`.
2. Nel file che hai creato, configura i seguenti attributi:
   - **metadata.name**: (*Obbligatorio*) Il nome di questa risorsa personalizzata; scegli un nome univoco e sensato per il tuo ambiente.
   - **spec.applicationRef**: (*Obbligatorio*) Il nome Kubernetes dell'applicazione di cui eseguire il backup.
   - **spec.appVaultRef**: (*Obbligatorio, mutuamente esclusivo con spec.appVaultTargetsRef*) Se si utilizza lo stesso bucket per archiviare lo snapshot e il backup, questo è il nome del AppVault in cui devono essere archiviati i contenuti del backup.

- **spec.appVaultTargetsRef**: (*Obbligatorio, mutuamente esclusivo con spec.appVaultRef*) Se si utilizzano bucket diversi per archiviare lo snapshot e il backup, questo è il nome del AppVault dove devono essere archiviati i contenuti del backup.
- **spec.dataMover**: (*Facoltativo*) Una stringa che indica quale strumento di backup utilizzare per l'operazione di backup. Il valore distingue tra maiuscole e minuscole e deve essere `CBS`.
- **spec.reclaimPolicy**: (*Facoltativo*) Definisce cosa succede al contenuto del backup (metadati/dati del volume) quando il Backup CR viene eliminato. Valori possibili:
  - `Delete`
  - `Retain` (predefinito)
- **spec.cleanupSnapshot**: (*Obbligatorio*) Garantisce che lo snapshot temporaneo creato dal Backup CR non venga eliminato al termine dell'operazione di backup. Valore consigliato: `false`.

  Esempio di YAML quando si utilizza lo stesso bucket per archiviare la Snapshot e il backup:

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

  Esempio di YAML quando si utilizzano bucket diversi per archiviare lo snapshot e il backup:

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: object-store-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

3. Dopo aver popolato il `object-store-backup-cr.yaml` file con i valori corretti, applica la CR:

```
kubectl apply -f object-store-backup-cr.yaml
```

Crea un backup 3-2-1 fanout utilizzando una risorsa personalizzata

Il backup con architettura fanout 3-2-1 copia un backup sia su storage secondario che su un archivio di oggetti. Per creare un backup fanout 3-2-1, crea un Backup CR con attributi specifici.

Passi

1. Crea il file custom resource (CR) e assegnagli il nome `3-2-1-fanout-backup-cr.yaml`.
2. Nel file che hai creato, configura i seguenti attributi:

   - **metadata.name**: (*Obbligatorio*) Il nome di questa risorsa personalizzata; scegli un nome univoco e sensato per il tuo ambiente.
   - **spec.applicationRef**: (*Obbligatorio*) Il nome Kubernetes dell'applicazione di cui eseguire il backup.
   - **spec.appVaultTargetsRef**: (*Obbligatorio*) Il nome del AppVault in cui devono essere archiviati i contenuti del backup.
   - **spec.dataMover**: (*Facoltativo*) Una stringa che indica quale strumento di backup utilizzare per l'operazione di backup. Il valore distingue tra maiuscole e minuscole e deve essere `CBS`.
   - **spec.reclaimPolicy**: (*Facoltativo*) Definisce cosa succede al contenuto del backup (metadati/dati del volume) quando il Backup CR viene eliminato. Valori possibili:
     - `Delete`
     - `Retain` (predefinito)
   - **spec.cleanupSnapshot**: (*Obbligatorio*) Garantisce che lo snapshot temporaneo creato dal Backup CR non venga eliminato al termine dell'operazione di backup. Valore consigliato: `false`.
   - **spec.replicateSnapshot**: (*Obbligatorio*) Indica a Backup and Recovery di replicare lo snapshot nello storage secondario. Valore obbligatorio: `true`.
   - **spec.replicateSnapshotReclaimPolicy**: (*Facoltativo*) Definisce cosa succede allo snapshot replicato quando viene eliminato. Valori possibili:
     - `Delete`
     - `Retain` (predefinito)

     Esempio YAML:

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: 3-2-1-fanout-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
  replicateSnapshot: true
  replicateSnapshotReclaimPolicy: Retain
```

3. Dopo aver popolato il `3-2-1-fanout-backup-cr.yaml` file con i valori corretti, applica la CR:

```
kubectl apply -f 3-2-1-fanout-backup-cr.yaml
```

Annotazioni di backup supportate

La tabella seguente descrive le annotazioni che è possibile utilizzare quando si crea un CR di backup.

Annotazione	Tipo	Descrizione	Valore predefinito
protect.trident.netapp.io/full-backup	stringa	Specifica se un backup deve essere non incrementale. Impostare su `true` per creare un backup non incrementale. È best practice eseguire periodicamente un backup completo e poi eseguire backup incrementali tra un backup completo e l'altro per ridurre al minimo il rischio associato ai ripristini.	"false"
protect.trident.netapp.io/snapshot-completion-timeout	stringa	Il tempo massimo consentito per il completamento dell'operazione di snapshot complessiva.	"60m"
protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout	stringa	Tempo massimo consentito affinché gli snapshot del volume raggiungano lo stato pronto all'uso.	"30m"
protect.trident.netapp.io/volume-snapshots-created-timeout	stringa	Il tempo massimo consentito per la creazione di snapshot del volume.	"5m"
protect.trident.netapp.io/pvc-bind-timeout-sec	stringa	Tempo massimo (in secondi) di attesa affinché i nuovi PersistentVolumeClaims (PVC) creati raggiungano la `Bound` fase prima che l'operazione fallisca.	"1200" (20 minuti)

Ripristina le applicazioni Kubernetes

Ripristina le applicazioni Kubernetes utilizzando l'interfaccia utente web

NetApp Backup and Recovery consente di ripristinare le applicazioni protette tramite una policy di protezione. Per ripristinare un'applicazione, è necessario che quest'ultima disponga di almeno un punto di ripristino. Un punto di ripristino può essere costituito dallo snapshot locale o dal backup nell'archivio oggetti (o da entrambi). È possibile ripristinare un'applicazione utilizzando l'archivio locale, secondario o dell'archivio oggetti.

Prima di iniziare

Se si sta ripristinando un'applicazione di cui è stato eseguito il backup utilizzando Trident Protect, assicurarsi che Trident Protect sia installato sia sul cluster di origine che sul cluster di destinazione.

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. Nel menu NetApp Backup e ripristino, seleziona **Ripristina**.
2. Scegli un'applicazione Kubernetes dall'elenco e seleziona **Visualizza e ripristina** per quell'applicazione.

   Viene visualizzato l'elenco dei punti di ripristino.
3. Seleziona il pulsante **Ripristina** per il punto di ripristino che si desidera utilizzare.

Impostazioni generali

1. Scegli la posizione di origine da cui eseguire il ripristino.
2. Selezionare il cluster di destinazione dall'elenco **Cluster**.

   Al momento non è supportato il ripristino di uno snapshot locale creato da Trident Protect su un cluster diverso.
3. Scegli se ripristinare negli spazi dei nomi originali o in nuovi spazi dei nomi.
4. Se si sceglie di ripristinare su nuovi namespace, immettere il namespace di destinazione o i namespace di destinazione da utilizzare.
5. Selezionare **Avanti**.

Selezione delle risorse

1. Scegli se desideri ripristinare tutte le risorse associate all'applicazione oppure utilizzare un filtro per selezionare risorse specifiche da ripristinare:

Ripristina tutte le risorse

1. Seleziona **Ripristina tutte le risorse**.
2. Selezionare **Avanti**.

Ripristina risorse specifiche

1. Seleziona **Risorse selettive**.
2. Scegli il comportamento del filtro delle risorse. Se scegli **Includi**, le risorse selezionate verranno ripristinate. Se si sceglie **Escludi**, le risorse selezionate non verranno ripristinate.
3. Selezionare **Aggiungi regole** per aggiungere regole che definiscono i filtri per la selezione delle risorse. Per filtrare le risorse è necessaria almeno una regola.

   Ogni regola può filtrare in base a criteri quali lo spazio dei nomi della risorsa, le etichette, il gruppo, la versione e il tipo.
4. Selezionare **Salva** per salvare ciascuna regola.
5. Dopo aver aggiunto tutte le regole necessarie, seleziona **Cerca** per visualizzare le risorse disponibili nell'archivio di backup che corrispondono ai criteri di filtro.

   Le risorse mostrate sono le risorse attualmente presenti nel cluster.
6. Una volta soddisfatti dei risultati, selezionare **Avanti**.

Impostazioni di destinazione

1. Espandi la sezione **Impostazioni di destinazione** e scegli se ripristinare sulla classe di archiviazione predefinita, su una classe di archiviazione diversa oppure, se stai eseguendo il ripristino su un cluster diverso, di mappare le classi di archiviazione sul cluster di destinazione.
2. Se si sceglie di ripristinare in una classe di archiviazione diversa, selezionare una classe di archiviazione di destinazione che corrisponda a ciascuna classe di archiviazione di origine.
3. Facoltativamente, se si sta ripristinando un backup o uno snapshot creato con Trident Protect, visualizzare i dettagli del AppVault utilizzato come bucket di archiviazione per l'operazione di ripristino. Se vi è una modifica nell'ambiente o nello stato di AppVault, selezionare **Sync App Vault** per aggiornare i dettagli.

   Se è necessario creare un AppVault su un cluster Kubernetes per facilitare il ripristino di un backup o di uno snapshot creato utilizzando Trident Protect, fare riferimento a "Utilizzare gli oggetti Trident Protect AppVault per gestire i bucket".
4. Facoltativamente, espandi la sezione **Script di ripristino** e abilita l'opzione **Postscript** per scegliere un modello di hook di esecuzione che verrà eseguito al termine dell'operazione di ripristino. Se necessario, inserisci gli argomenti di cui lo script ha bisogno e aggiungi selettori di etichetta per filtrare le risorse in base alle etichette delle risorse.
5. Selezionare **Ripristina**.

Ripristina le applicazioni Kubernetes utilizzando una risorsa personalizzata

È possibile utilizzare risorse personalizzate per ripristinare le applicazioni da uno snapshot o da un backup. Il ripristino da uno snapshot esistente sarà più rapido quando

si ripristina l'applicazione nello stesso cluster.

- Quando si ripristina un'applicazione, tutti gli hook di esecuzione configurati per l'applicazione vengono ripristinati con l'app. Se è presente un hook di esecuzione post-ripristino, viene eseguito automaticamente come parte dell'operazione di ripristino.
- Il ripristino da un backup a un namespace diverso o al namespace originale è supportato per i volumi qtree. Tuttavia, il ripristino da uno snapshot a un namespace diverso o al namespace originale non è supportato per i volumi qtree.
- È possibile utilizzare le impostazioni avanzate per personalizzare le operazioni di ripristino. Per ulteriori informazioni, consultare "Utilizza impostazioni avanzate di ripristino delle risorse personalizzate".

Ripristina un backup in un namespace diverso

Quando si ripristina un backup in un namespace diverso utilizzando una BackupRestore CR, NetApp Backup and Recovery ripristina l'applicazione in un nuovo namespace e crea una application CR per l'applicazione ripristinata. Per proteggere l'applicazione ripristinata, crea backup o snapshot on-demand oppure stabilisci una policy di protezione.

- Il ripristino di un backup in un namespace diverso con risorse esistenti non modificherà le risorse che condividono i nomi con quelle nel backup. Per ripristinare tutte le risorse nel backup, eliminare e ricreare il namespace di destinazione o ripristinare il backup in un nuovo namespace.
- Quando si utilizza una CR per ripristinare in un nuovo namespace, è necessario creare manualmente il namespace di destinazione prima di applicare la CR. NetApp Backup and Recovery crea automaticamente i namespace solo quando si utilizza la CLI.

Prima di iniziare

Assicurarsi che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino s3 di lunga durata. Se il token scade durante l'operazione di ripristino, l'operazione può non riuscire.

- Fare riferimento a "Documentazione API AWS" per ulteriori informazioni sulla verifica della scadenza del token della sessione corrente.
- Fare riferimento a "Documentazione AWS IAM" per ulteriori informazioni sulle credenziali con le risorse AWS.

Quando si ripristinano i backup utilizzando Kopia come data mover, è possibile specificare facoltativamente annotazioni nella CR per controllare il comportamento dello storage temporaneo utilizzato da Kopia. Consultare il "Documentazione Kopia" per ulteriori informazioni sulle opzioni che è possibile configurare.

Passi

1. Crea il file custom resource (CR) e assegnagli il nome `trident-protect-backup-restore-cr.yaml`.
2. Nel file che hai creato, configura i seguenti attributi:
   - **metadata.name**: (*Obbligatorio*) Il nome di questa risorsa personalizzata; scegli un nome univoco e sensato per il tuo ambiente.
   - **spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono archiviati i contenuti del backup. È possibile utilizzare il seguente comando per trovare questo percorso:

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.appVaultRef**: (*Obbligatorio*) Il nome del AppVault in cui sono archiviati i contenuti del backup.
- **spec.namespaceMapping**: Il mapping dello spazio dei nomi di origine dell'operazione di ripristino allo spazio dei nomi di destinazione. Sostituisci `my-source-namespace` e `my-destination-namespace` con le informazioni del tuo ambiente.

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. (*Facoltativo*) Se è necessario selezionare solo determinate risorse dell'applicazione da ripristinare, aggiungere un filtro che includa o escluda le risorse contrassegnate con etichette particolari:

> Trident Protect seleziona automaticamente alcune risorse in base alla loro relazione con le risorse che selezioni. Ad esempio, se selezioni una risorsa di richiesta di volume persistente e questa ha un pod associato, Trident Protect ripristinerà anche il pod associato.

- **resourceFilter.resourceSelectionCriteria**: (Obbligatorio per il filtraggio) Utilizzare `Include` o `Exclude` per includere o escludere una risorsa definita in resourceMatchers. Aggiungere i seguenti parametri resourceMatchers per definire le risorse da includere o escludere:
  - **resourceFilter.resourceMatchers**: Un array di resourceMatcher oggetti. Se si definiscono più elementi in questo array, la corrispondenza avviene tramite un'operazione OR, e i campi all'interno di ciascun elemento (group, kind, version) corrispondono tramite un'operazione AND.
    - **resourceMatchers[].group**: (*Facoltativo*) Gruppo della risorsa da filtrare.
    - **resourceMatchers[].kind**: (*Facoltativo*) Tipo di risorsa da filtrare.
    - **resourceMatchers[].version**: (*Facoltativo*) Versione della risorsa da filtrare.
    - **resourceMatchers[].names**: (*Facoltativo*) Nomi nel campo metadata.name di Kubernetes della risorsa da filtrare.
    - **resourceMatchers[].namespaces**: (*Facoltativo*) Namespace nel campo metadata.name di Kubernetes della risorsa da filtrare.
    - **resourceMatchers[].labelSelectors**: (*Facoltativo*) Stringa del selettore di etichetta nel campo metadata.name dei metadati Kubernetes della risorsa come definito in "Documentazione Kubernetes". Ad esempio: `"trident.netapp.io/os=linux"`.

      Ad esempio:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Dopo aver popolato il `trident-protect-backup-restore-cr.yaml` file con i valori corretti, applica la CR:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Ripristina un backup nello spazio dei nomi originale

È possibile ripristinare un backup nello spazio dei nomi originale in qualsiasi momento.

Prima di iniziare

Assicurarsi che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino s3 di lunga durata. Se il token scade durante l'operazione di ripristino, l'operazione può non riuscire.

- Fare riferimento a "Documentazione API AWS" per ulteriori informazioni sulla verifica della scadenza del token della sessione corrente.
- Fare riferimento a "Documentazione AWS IAM" per ulteriori informazioni sulle credenziali con le risorse AWS.

> Quando si ripristinano i backup utilizzando Kopia come data mover, è possibile specificare facoltativamente annotazioni nella CR per controllare il comportamento dello storage temporaneo utilizzato da Kopia. Consultare il "Documentazione Kopia" per ulteriori informazioni sulle opzioni che è possibile configurare.

Passi

1. Crea il file custom resource (CR) e assegnagli il nome `trident-protect-backup-ipr-cr.yaml`.
2. Nel file che hai creato, configura i seguenti attributi:
   - **metadata.name**: (*Obbligatorio*) Il nome di questa risorsa personalizzata; scegli un nome univoco e sensato per il tuo ambiente.

- **spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono archiviati i contenuti del backup. È possibile utilizzare il seguente comando per trovare questo percorso:

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.appVaultRef**: (*Obbligatorio*) Il nome del AppVault in cui sono archiviati i contenuti del backup.

  Ad esempio:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
```

3. (*Facoltativo*) Se è necessario selezionare solo determinate risorse dell'applicazione da ripristinare, aggiungere un filtro che includa o escluda le risorse contrassegnate con etichette particolari:

> Trident Protect seleziona automaticamente alcune risorse in base alla loro relazione con le risorse che selezioni. Ad esempio, se selezioni una risorsa di richiesta di volume persistente e questa ha un pod associato, Trident Protect ripristinerà anche il pod associato.

- **resourceFilter.resourceSelectionCriteria**: (Obbligatorio per il filtraggio) Utilizzare `Include` o `Exclude` per includere o escludere una risorsa definita in resourceMatchers. Aggiungere i seguenti parametri resourceMatchers per definire le risorse da includere o escludere:
  - **resourceFilter.resourceMatchers**: Un array di resourceMatcher oggetti. Se si definiscono più elementi in questo array, la corrispondenza avviene tramite un'operazione OR, e i campi all'interno di ciascun elemento (group, kind, version) corrispondono tramite un'operazione AND.
    - **resourceMatchers[].group**: (*Facoltativo*) Gruppo della risorsa da filtrare.
    - **resourceMatchers[].kind**: (*Facoltativo*) Tipo di risorsa da filtrare.
    - **resourceMatchers[].version**: (*Facoltativo*) Versione della risorsa da filtrare.
    - **resourceMatchers[].names**: (*Facoltativo*) Nomi nel campo metadata.name di Kubernetes della risorsa da filtrare.
    - **resourceMatchers[].namespaces**: (*Facoltativo*) Namespace nel campo metadata.name di Kubernetes della risorsa da filtrare.
    - **resourceMatchers[].labelSelectors**: (*Facoltativo*) Stringa del selettore di etichetta nel campo metadata.name dei metadati Kubernetes della risorsa come definito in "Documentazione Kubernetes". Ad esempio: `"trident.netapp.io/os=linux"`.

      Ad esempio:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Dopo aver popolato il `trident-protect-backup-ipr-cr.yaml` file con i valori corretti, applica la CR:

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

Ripristinare un backup su un cluster diverso

È possibile ripristinare un backup su un cluster diverso se si verifica un problema con il cluster originale.

- Quando si ripristinano i backup utilizzando Kopia come data mover, è possibile specificare facoltativamente annotazioni nella CR per controllare il comportamento dello storage temporaneo utilizzato da Kopia. Consultare il "Documentazione Kopia" per ulteriori informazioni sulle opzioni che è possibile configurare.
- Quando si utilizza una CR per ripristinare in un nuovo namespace, è necessario creare manualmente il namespace di destinazione prima di applicare la CR.

Prima di iniziare

Assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Il cluster di destinazione ha Trident Protect installato.
- Il cluster di destinazione ha accesso al percorso del bucket dello stesso AppVault del cluster di origine, dove è archiviato il backup.
- Assicurarsi che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino di lunga durata. Se il token scade durante l'operazione di ripristino, l'operazione può fallire.
  - Fare riferimento a "Documentazione API AWS" per ulteriori informazioni sulla verifica della scadenza del token della sessione corrente.
  - Fare riferimento a "Documentazione AWS" per ulteriori informazioni sulle credenziali con le risorse AWS.

Passi

1. Verificare la disponibilità del AppVault CR sul cluster di destinazione utilizzando il plug-in Trident Protect CLI:

```
tridentctl-protect get appvault --context <destination_cluster_name>
```

Assicurarsi che lo spazio dei nomi destinato al ripristino dell'applicazione esista nel cluster di destinazione.

2. Visualizza il contenuto del backup disponibile di AppVault dal cluster di destinazione:

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

L'esecuzione di questo comando visualizza i backup disponibili in AppVault, inclusi i cluster di origine, i nomi delle applicazioni corrispondenti, i timestamp e i percorsi di archivio.

Esempio di output:

```
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
|   CLUSTER   |    APP    |  TYPE  |      NAME       |         TIMESTAMP
|    PATH     |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
| production1 | wordpress | backup | wordpress-bkup-1| 2024-10-30
08:37:40 (UTC)| backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2| 2024-10-30
08:37:40 (UTC)| backuppath2 |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
```

3. Ripristina l'applicazione nel cluster di destinazione utilizzando il nome AppVault e il percorso di archivio:
4. Crea il file custom resource (CR) e assegnagli il nome `trident-protect-backup-restore-cr.yaml`.
5. Nel file che hai creato, configura i seguenti attributi:

   - **metadata.name**: (*Obbligatorio*) Il nome di questa risorsa personalizzata; scegli un nome univoco e sensato per il tuo ambiente.
   - **spec.appVaultRef**: (*Obbligatorio*) Il nome del AppVault in cui sono archiviati i contenuti del backup.
   - **spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono archiviati i contenuti del backup. È possibile utilizzare il seguente comando per trovare questo percorso:

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

Se BackupRestore CR non è disponibile, è possibile utilizzare il comando menzionato nel passaggio 2 per visualizzare il contenuto del backup.

- **spec.namespaceMapping**: Il mapping dello spazio dei nomi di origine dell'operazione di ripristino allo spazio dei nomi di destinazione. Sostituisci `my-source-namespace` e `my-destination-namespace` con le informazioni del tuo ambiente.

  Ad esempio:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

6. Dopo aver popolato il `trident-protect-backup-restore-cr.yaml` file con i valori corretti, applica la CR:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Ripristina uno snapshot in un namespace diverso

È possibile ripristinare i dati da uno snapshot utilizzando un file di risorsa personalizzata (CR) sia in un namespace diverso che nel namespace di origine. Quando si ripristina uno snapshot in un namespace diverso utilizzando una SnapshotRestore CR, NetApp Backup and Recovery ripristina l'applicazione in un nuovo namespace e crea una CR dell'applicazione per l'applicazione ripristinata. Per proteggere l'applicazione ripristinata, crea backup o snapshot su richiesta oppure stabilisci una policy di protezione.

- SnapshotRestore supporta l' `spec.storageClassMapping` attributo, ma solo quando le classi di archiviazione di origine e destinazione utilizzano lo stesso backend di archiviazione. Se si tenta di eseguire il ripristino su una `StorageClass` che utilizza un backend di archiviazione diverso, l'operazione di ripristino non riuscirà.
- Quando si utilizza una CR per ripristinare in un nuovo namespace, è necessario creare manualmente il namespace di destinazione prima di applicare la CR.

Prima di iniziare

Assicurarsi che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino s3

di lunga durata. Se il token scade durante l'operazione di ripristino, l'operazione può non riuscire.

- Fare riferimento a "Documentazione API AWS" per ulteriori informazioni sulla verifica della scadenza del token della sessione corrente.
- Fare riferimento a "Documentazione AWS IAM" per ulteriori informazioni sulle credenziali con le risorse AWS.

Passi

1. Crea il file di risorsa personalizzata (CR) e assegnagli il nome `trident-protect-snapshot-restore-cr.yaml`.
2. Nel file che hai creato, configura i seguenti attributi:
   - **metadata.name**: (*Obbligatorio*) Il nome di questa risorsa personalizzata; scegli un nome univoco e sensato per il tuo ambiente.
   - **spec.appVaultRef**: (*Obbligatorio*) Il nome del AppVault in cui sono archiviati i contenuti dello snapshot.
   - **spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono archiviati i contenuti dello snapshot. È possibile utilizzare il seguente comando per trovare questo percorso:

     ```
     kubectl get snapshots <SNAPHOT_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.namespaceMapping**: Il mapping dello spazio dei nomi di origine dell'operazione di ripristino allo spazio dei nomi di destinazione. Sostituisci `my-source-namespace` e `my-destination-namespace` con le informazioni del tuo ambiente.

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
       namespaceMapping: [{"source": "my-source-namespace", "destination":
     "my-destination-namespace"}]
     ```

3. (*Facoltativo*) Se è necessario selezionare solo determinate risorse dell'applicazione da ripristinare, aggiungere un filtro che includa o escluda le risorse contrassegnate con etichette particolari:

   > Trident Protect seleziona automaticamente alcune risorse in base alla loro relazione con le risorse che selezioni. Ad esempio, se selezioni una risorsa di richiesta di volume persistente e questa ha un pod associato, Trident Protect ripristinerà anche il pod associato.

   - **resourceFilter.resourceSelectionCriteria**: (Obbligatorio per il filtraggio) Utilizzare `Include` o `Exclude` per includere o escludere una risorsa definita in resourceMatchers. Aggiungere i seguenti parametri resourceMatchers per definire le risorse da includere o escludere:

- **resourceFilter.resourceMatchers**: Un array di resourceMatcher oggetti. Se si definiscono più elementi in questo array, la corrispondenza avviene tramite un'operazione OR, e i campi all'interno di ciascun elemento (group, kind, version) corrispondono tramite un'operazione AND.
  - **resourceMatchers[].group**: (*Facoltativo*) Gruppo della risorsa da filtrare.
  - **resourceMatchers[].kind**: (*Facoltativo*) Tipo di risorsa da filtrare.
  - **resourceMatchers[].version**: (*Facoltativo*) Versione della risorsa da filtrare.
  - **resourceMatchers[].names**: (*Facoltativo*) Nomi nel campo metadata.name di Kubernetes della risorsa da filtrare.
  - **resourceMatchers[].namespaces**: (*Facoltativo*) Namespace nel campo metadata.name di Kubernetes della risorsa da filtrare.
  - **resourceMatchers[].labelSelectors**: (*Facoltativo*) Stringa del selettore di etichetta nel campo metadata.name dei metadati Kubernetes della risorsa come definito in "Documentazione Kubernetes". Ad esempio: `"trident.netapp.io/os=linux"`.

    Ad esempio:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Dopo aver popolato il `trident-protect-snapshot-restore-cr.yaml` file con i valori corretti, applica la CR:

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

Ripristina uno snapshot nello spazio dei nomi originale

È possibile ripristinare uno snapshot nel namespace originale in qualsiasi momento.

Prima di iniziare

Assicurarsi che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino s3 di lunga durata. Se il token scade durante l'operazione di ripristino, l'operazione può non riuscire.

- Fare riferimento a "Documentazione API AWS" per ulteriori informazioni sulla verifica della scadenza del token della sessione corrente.
- Fare riferimento a "Documentazione AWS IAM" per ulteriori informazioni sulle credenziali con le risorse AWS.

Passi

1. Crea il file custom resource (CR) e assegnagli il nome `trident-protect-snapshot-ipr-cr.yaml`.
2. Nel file che hai creato, configura i seguenti attributi:
   - **metadata.name**: (*Obbligatorio*) Il nome di questa risorsa personalizzata; scegli un nome univoco e sensato per il tuo ambiente.
   - **spec.appVaultRef**: (*Obbligatorio*) Il nome del AppVault in cui sono archiviati i contenuti dello snapshot.
   - **spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono archiviati i contenuti dello snapshot. È possibile utilizzare il seguente comando per trovare questo percorso:

     ```
     kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o
     jsonpath='{.status.appArchivePath}'
     ```

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotInplaceRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
     ```

3. (*Facoltativo*) Se è necessario selezionare solo determinate risorse dell'applicazione da ripristinare, aggiungere un filtro che includa o escluda le risorse contrassegnate con etichette particolari:

   > Trident Protect seleziona automaticamente alcune risorse in base alla loro relazione con le risorse che selezioni. Ad esempio, se selezioni una risorsa di richiesta di volume persistente e questa ha un pod associato, Trident Protect ripristinerà anche il pod associato.

   - **resourceFilter.resourceSelectionCriteria**: (Obbligatorio per il filtraggio) Utilizzare `Include` o `Exclude` per includere o escludere una risorsa definita in resourceMatchers. Aggiungere i seguenti parametri resourceMatchers per definire le risorse da includere o escludere:
     - **resourceFilter.resourceMatchers**: Un array di resourceMatcher oggetti. Se si definiscono più elementi in questo array, la corrispondenza avviene tramite un'operazione OR, e i campi all'interno di ciascun elemento (group, kind, version) corrispondono tramite un'operazione AND.
       - **resourceMatchers[].group**: (*Facoltativo*) Gruppo della risorsa da filtrare.
       - **resourceMatchers[].kind**: (*Facoltativo*) Tipo di risorsa da filtrare.
       - **resourceMatchers[].version**: (*Facoltativo*) Versione della risorsa da filtrare.
       - **resourceMatchers[].names**: (*Facoltativo*) Nomi nel campo metadata.name di Kubernetes della risorsa da filtrare.

- **resourceMatchers[].namespaces**: (*Facoltativo*) Namespace nel campo metadata.name di Kubernetes della risorsa da filtrare.
- **resourceMatchers[].labelSelectors**: (*Facoltativo*) Stringa del selettore di etichetta nel campo metadata.name dei metadati Kubernetes della risorsa come definito in "Documentazione Kubernetes". Ad esempio: `"trident.netapp.io/os=linux"`.

  Ad esempio:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Dopo aver popolato il `trident-protect-snapshot-ipr-cr.yaml` file con i valori corretti, applica la CR:

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

Utilizza impostazioni avanzate di ripristino delle risorse personalizzate

È possibile personalizzare le operazioni di ripristino utilizzando impostazioni avanzate come annotazioni, impostazioni dello spazio dei nomi e opzioni di storage per soddisfare i requisiti specifici.

Annotazioni ed etichette dello spazio dei nomi durante le operazioni di ripristino e failover

Durante le operazioni di ripristino e failover, le etichette e le annotazioni nello spazio dei nomi di destinazione vengono rese corrispondenti alle etichette e alle annotazioni nello spazio dei nomi di origine. Le etichette o le annotazioni dello spazio dei nomi di origine che non esistono nello spazio dei nomi di destinazione vengono aggiunte e tutte le etichette o annotazioni già esistenti vengono sovrascritte per corrispondere al valore dello spazio dei nomi di origine. Le etichette o le annotazioni che esistono solo nello spazio dei nomi di destinazione rimangono invariate.

Se si utilizza Red Hat OpenShift, è importante tenere presente il ruolo fondamentale delle annotazioni dello spazio dei nomi negli ambienti OpenShift. Le annotazioni dello spazio dei nomi garantiscono che i pod ripristinati aderiscano alle autorizzazioni e alle configurazioni di sicurezza appropriate definite dai vincoli del contesto di sicurezza (SCC) di OpenShift e possano accedere ai volumi senza problemi di autorizzazione. Per ulteriori informazioni, consultare il "Documentazione sui vincoli del contesto di sicurezza di OpenShift".

È possibile impedire che specifiche annotazioni nello spazio dei nomi di destinazione vengano sovrascritte impostando la variabile di ambiente Kubernetes `RESTORE_SKIP_NAMESPACE_ANNOTATIONS` prima di eseguire l'operazione di ripristino o failover. Ad esempio:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k
ey_to_skip_2>}" \
  --reuse-values
```

Quando si esegue un'operazione di ripristino o failover, tutte le annotazioni e le etichette dello spazio dei nomi specificate in `restoreSkipNamespaceAnnotations` e `restoreSkipNamespaceLabels` sono escluse dall'operazione di ripristino o failover. Assicurarsi che queste impostazioni siano configurate durante l'installazione iniziale di Helm. Per ulteriori informazioni, consultare "Configura impostazioni aggiuntive dell'helm chart Trident Protect".

Se hai installato l'applicazione sorgente utilizzando Helm con il `--create-namespace` flag, viene riservato un trattamento speciale alla chiave dell'etichetta `name`. Durante il processo di ripristino o failover, Trident Protect copia questa etichetta nello spazio dei nomi di destinazione, ma aggiorna il valore a quello dello spazio dei nomi di destinazione se il valore della sorgente corrisponde allo spazio dei nomi di origine. Se questo valore non corrisponde allo spazio dei nomi di origine, viene copiato nello spazio dei nomi di destinazione senza modifiche.

Esempio

Il seguente esempio presenta uno spazio dei nomi di origine e uno di destinazione, ciascuno con annotazioni ed etichette diverse. Puoi vedere lo stato dello spazio dei nomi di destinazione prima e dopo l'operazione e come le annotazioni e le etichette vengono combinate o sovrascritte nello spazio dei nomi di destinazione.

Prima dell'operazione di ripristino o failover

La tabella seguente illustra lo stato degli spazi dei nomi di origine e di destinazione di esempio prima dell'operazione di ripristino o failover:

Spazio dei nomi	Annotazioni	Etichette
Namespace ns-1 (origine)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true"	• ambiente=produzione • compliance=hipaa • name=ns-1

Spazio dei nomi	Annotazioni	Etichette
Namespace ns-2 (destinazione)	• annotation.one/key: "true" • annotazione.tre/chiave: "false"	• role=database

Dopo l'operazione di ripristino

La tabella seguente illustra lo stato dello spazio dei nomi di destinazione di esempio dopo l'operazione di ripristino o failover. Alcune chiavi sono state aggiunte, alcune sono state sovrascritte e l' `name`etichetta è stata aggiornata per corrispondere allo spazio dei nomi di destinazione:

Spazio dei nomi	Annotazioni	Etichette
Namespace ns-2 (destinazione)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true" • annotazione.tre/chiave: "false"	• name=ns-2 • compliance=hipaa • ambiente=produzione • role=database

Campi supportati

Questa sezione descrive i campi aggiuntivi disponibili per le operazioni di ripristino.

Mappatura delle storage class

L' `spec.storageClassMapping`attributo definisce una mappatura da una classe di storage presente nell'applicazione di origine a una nuova classe di storage nel cluster di destinazione. Puoi utilizzare questa opzione quando migri applicazioni tra cluster con classi di storage diverse o quando cambi il backend di storage per le operazioni di BackupRestore.

Esempio:

```
storageClassMapping:
  - destination: "destinationStorageClass1"
    source: "sourceStorageClass1"
  - destination: "destinationStorageClass2"
    source: "sourceStorageClass2"
```

Annotazioni supportate

Questa sezione elenca le annotazioni supportate per la configurazione di vari comportamenti nel sistema. Se un'annotazione non viene impostata esplicitamente dall'utente, il sistema utilizzerà il valore predefinito.

Annotazione	Tipo	Descrizione	Valore predefinito
protect.trident.netapp.io/data-mover-timeout-sec	stringa	Il tempo massimo (in secondi) consentito per l'operazione di spostamento dei dati che può essere bloccata.	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	stringa	Limite massimo di dimensione (in megabyte) per la cache dei contenuti Kopia.	"1000"
protect.trident.netapp.io/pvc-bind-timeout-sec	stringa	Tempo massimo (in secondi) di attesa affinché eventuali nuove PersistentVolumeClaims (PVC) raggiungano la fase `Bound` prima che l'operazione fallisca. Si applica a tutti i tipi di restore CR (BackupRestore, BackupInplaceRestore, SnapshotRestore, SnapshotInplaceRestore). Utilizzare un valore più alto se il backend di storage o il cluster richiede spesso più tempo.	"1200" (20 minuti)

Gestire i cluster Kubernetes

NetApp Backup and Recovery ti consente di scoprire e gestire i tuoi cluster Kubernetes in modo da poter proteggere le risorse ospitate dai cluster.

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Per scoprire i cluster Kubernetes, fare riferimento a"Scopri i carichi di lavoro di Kubernetes" .

Modifica le informazioni del cluster Kubernetes

È possibile modificare un cluster se è necessario cambiarne il nome.

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario** > **Cluster**.
2. Nell'elenco dei cluster, seleziona il cluster che desideri modificare e seleziona il menu Azioni associato.
3. Seleziona **Modifica cluster**.
4. Apportare le modifiche necessarie al nome del cluster. Il nome del cluster deve corrispondere al nome utilizzato con il comando Helm durante il processo di individuazione.
5. Selezionare **Fatto**.

Rimuovere un cluster Kubernetes

Per interrompere la protezione di un cluster Kubernetes, disabilitare la protezione ed eliminare le applicazioni associate, quindi rimuovere il cluster da NetApp Backup and Recovery. NetApp Backup and Recovery non elimina il cluster o le sue risorse; rimuove solo il cluster dall'inventario della NetApp Console .

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario** > **Cluster**.
2. Nell'elenco dei cluster, seleziona il cluster che desideri modificare e seleziona il menu Azioni associato.
3. Selezionare **Rimuovi cluster**.
4. Rivedi le informazioni nella finestra di dialogo di conferma e seleziona **Rimuovi**.

Gestire le applicazioni Kubernetes

NetApp Backup and Recovery consente di rimuovere la protezione ed eliminare le applicazioni Kubernetes e le risorse associate.

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Rimuovere la protezione di un'applicazione Kubernetes

È possibile rimuovere la protezione da un'applicazione se non si desidera più proteggerla. Quando si rimuove la protezione di un'applicazione, NetApp Backup and Recovery interrompe la protezione dell'applicazione ma conserva tutti i backup e gli snapshot associati.

> Non è possibile rimuovere la protezione di un'applicazione mentre sono ancora in esecuzione operazioni di protezione. Attendere il completamento dell'operazione oppure, come soluzione alternativa, rimuovere il punto di ripristino che l'operazione di protezione in esecuzione sta utilizzando. A questo punto, è possibile rimuovere la protezione dell'applicazione.

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione di cui desideri rimuovere la protezione e seleziona il menu Azioni associato.
5. Selezionare **Rimuovi protezione**.
6. Leggi l'avviso e, quando sei pronto, seleziona **Rimuovi protezione**.

Eliminare un'applicazione Kubernetes

Elimina un'applicazione di cui non hai più bisogno. NetApp Backup and Recovery interrompe la protezione e rimuove tutti i backup e gli snapshot delle applicazioni eliminate.

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione che desideri eliminare e seleziona il menu Azioni associato.
5. Seleziona **Elimina**.

6. Abilita **Elimina snapshot e backup** per rimuovere tutti gli snapshot e i backup dell'applicazione.

   Non sarà più possibile ripristinare l'applicazione utilizzando questi snapshot e backup.

7. Confermare l'azione e selezionare **Elimina**.

Rimuovi un punto di ripristino per un'applicazione Kubernetes

Potrebbe essere necessario rimuovere un punto di ripristino per un'applicazione se è necessario rimuoverne la protezione e sono attualmente in esecuzione operazioni di protezione.

Passi

1. Nel menu NetApp Backup e ripristino, seleziona **Ripristina**.
2. Scegli un'applicazione Kubernetes dall'elenco e seleziona **Visualizza e ripristina** per quell'applicazione.

   Viene visualizzato l'elenco dei punti di ripristino.

3. Scegli il punto di ripristino che desideri eliminare e seleziona l'icona Azioni ••• > **Elimina punto di ripristino** per eliminarlo.

Gestisci i modelli di hook di esecuzione di NetApp Backup and Recovery per i carichi di lavoro Kubernetes

Un hook di esecuzione è un'azione personalizzata che viene eseguita con un'operazione di protezione dei dati in un'applicazione Kubernetes gestita. Ad esempio, è possibile creare snapshot coerenti con l'applicazione utilizzando un hook di esecuzione per mettere in pausa le transazioni del database prima di uno snapshot e riprenderle dopo. Quando si crea un modello di hook di esecuzione, specificare il tipo di hook, lo script da eseguire e i filtri per i contenitori di destinazione. Utilizza il modello per collegare gli hook di esecuzione alle tue applicazioni.

NetApp Backup and Recovery blocca e sblocca i filesystem per applicazioni come KubeVirt durante la protezione dei dati. Puoi disabilitare questo comportamento a livello globale o per applicazioni specifiche utilizzando la documentazione di Trident Protect:

- Per disattivare questo comportamento per tutte le applicazioni, fare riferimento a "Protezione dei dati con le VM KubeVirt" .
- Per disattivare questo comportamento per un'applicazione specifica, fare riferimento a "Definire un'applicazione" .

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Tipi di ganci di esecuzione

NetApp Backup and Recovery supporta i seguenti tipi di hook di esecuzione, in base al momento in cui possono essere eseguiti:

- Pre-istantanea

- Post-istantanea
- Pre-backup
- Post-backup
- Post-ripristino

Ordine di esecuzione

Quando viene eseguita un'operazione di protezione dei dati, gli eventi di hook di esecuzione si verificano nel seguente ordine:

1. Tutti gli hook di esecuzione pre-operazione personalizzati applicabili vengono eseguiti sui contenitori appropriati. È possibile creare più hook pre-operativi personalizzati, ma il loro ordine di esecuzione non è garantito né configurabile.
2. Se applicabile, si verificano blocchi del file system.
3. L'operazione di protezione dei dati è eseguita.
4. I file system congelati vengono sbloccati, se applicabile.
5. NetApp Backup and Recovery esegue tutti gli hook di esecuzione pre-operazione personalizzati applicabili sui contenitori appropriati. È possibile creare più hook post-operazione personalizzati, ma il loro ordine di esecuzione non è garantito né configurabile.

Se si creano più hook dello stesso tipo, il loro ordine di esecuzione non è garantito. I ganci di tipo diverso vengono sempre eseguiti nell'ordine specificato. Ad esempio, ecco l'ordine di esecuzione di una configurazione che presenta tutti i diversi tipi di hook:

1. Eseguiti i pre-snapshot hook
2. Eseguiti i ganci post-snapshot
3. Hook pre-backup eseguiti
4. Hook post-backup eseguiti

Testare gli script di hook di esecuzione prima di abilitarli in produzione. Utilizzare 'kubectl exec' per testare gli script, quindi verificare gli snapshot e i backup clonando l'app in uno spazio dei nomi temporaneo e ripristinandola.

Se un hook di esecuzione pre-snapshot aggiunge, modifica o rimuove risorse Kubernetes, tali modifiche vengono incluse nello snapshot o nel backup e in qualsiasi successiva operazione di ripristino.

Note importanti sui ganci di esecuzione personalizzati

Quando pianifichi gli hook di esecuzione per le tue app, tieni presente quanto segue.

- Un hook di esecuzione deve utilizzare uno script per eseguire azioni. Molti hook di esecuzione possono fare riferimento allo stesso script.
- Gli hook di esecuzione devono essere scritti nel formato degli script shell eseguibili.
- La dimensione dello script è limitata a 96 KB.
- Le impostazioni dell'hook di esecuzione e tutti i criteri corrispondenti vengono utilizzati per determinare quali hook sono applicabili a un'operazione di snapshot, backup o ripristino.

Gli hook di esecuzione possono ridurre o disabilitare la funzionalità dell'applicazione. Fai in modo che i tuoi hook personalizzati vengano eseguiti il più velocemente possibile. Se si avvia un'operazione di backup o snapshot con hook di esecuzione associati ma poi la si annulla, gli hook possono comunque essere eseguiti se l'operazione di backup o snapshot è già iniziata. Ciò significa che la logica utilizzata in un hook di esecuzione post-backup non può presumere che il backup sia stato completato.

Filtri di hook di esecuzione

Quando aggiungi o modifichi un hook di esecuzione per un'applicazione, puoi aggiungere filtri all'hook di esecuzione per gestire i contenitori a cui l'hook corrisponderà. I filtri sono utili per le applicazioni che utilizzano la stessa immagine contenitore su tutti i contenitori, ma potrebbero utilizzare ciascuna immagine per uno scopo diverso (ad esempio Elasticsearch). I filtri consentono di creare scenari in cui gli hook di esecuzione vengono eseguiti su alcuni contenitori identici, ma non necessariamente su tutti. Se si creano più filtri per un singolo hook di esecuzione, questi vengono combinati con un operatore logico AND. È possibile avere fino a 10 filtri attivi per ogni hook di esecuzione.

Ogni filtro aggiunto a un hook di esecuzione utilizza un'espressione regolare per abbinare i contenitori nel cluster. Quando un hook corrisponde a un contenitore, eseguirà lo script associato su quel contenitore. Le espressioni regolari per i filtri utilizzano la sintassi Regular Expression 2 (RE2), che non supporta la creazione di un filtro che escluda i contenitori dall'elenco delle corrispondenze. Per informazioni sulla sintassi supportata da NetApp Backup and Recovery per le espressioni regolari nei filtri di hook di esecuzione, vedere "Supporto della sintassi Regular Expression 2 (RE2)" .

Se si aggiunge un filtro namespace a un hook di esecuzione eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o della clonazione si trovano in namespace diversi, il filtro namespace viene applicato solo al namespace di destinazione.

Esempi di hook di esecuzione

Visita il "Progetto GitHub NetApp Verda" per scaricare veri e propri hook di esecuzione per app popolari come Apache Cassandra ed Elasticsearch. Puoi anche vedere esempi e trarre spunti per strutturare i tuoi hook di esecuzione personalizzati.

Creare un modello di hook di esecuzione

È possibile creare un modello di hook di esecuzione personalizzato da utilizzare per eseguire azioni prima o dopo un'operazione di protezione dei dati su un'applicazione.

I modelli che crei qui sono utilizzabili solo quando proteggi i carichi di lavoro Kubernetes.

Passi

1. Nella Console, vai a **Protezione** > **Backup e ripristino**.
2. Selezionare la scheda **Impostazioni**.
3. Espandi la sezione **Modello di hook di esecuzione**.
4. Selezionare **Crea modello di hook di esecuzione**.
5. Immettere un nome per l'hook di esecuzione.
6. Facoltativamente, scegli un tipo di hook. Ad esempio, un hook post-restore viene eseguito al termine dell'operazione di ripristino.

7. Nella casella di testo **Script**, immettere lo script shell eseguibile che si desidera eseguire come parte del modello di hook di esecuzione. Facoltativamente, puoi selezionare **Carica script** per caricare un file di script.
8. Seleziona **Crea**.

   Dopo aver creato il modello, questo viene visualizzato nell'elenco dei modelli nella sezione **Modello di hook di esecuzione**.

Monitorare i lavori in NetApp Backup and Recovery

Con NetApp Backup and Recovery puoi monitorare gli snapshot locali, le repliche e i processi di backup che avvii. Tieni traccia dei processi di ripristino che avvii. Visualizza i lavori completati, in corso o non riusciti per aiutare a diagnosticare i problemi. Abilita le notifiche e-mail nel Centro notifiche NetApp Console per rimanere informato sulle attività del sistema quando non hai effettuato l'accesso. Utilizza la cronologia della console per visualizzare i dettagli di tutte le azioni avviate dall'interfaccia utente o dall'API.

NetApp Backup and Recovery conserva le informazioni sui processi per 15 giorni, quindi le elimina e le rimuove da Job Monitor.

*Ruolo richiesto NetApp Console * Visualizzatore di storage, super amministratore di Backup and Recovery, amministratore di backup di Backup and Recovery, amministratore di ripristino di Backup and Recovery, amministratore di clonazione di Backup and Recovery o ruolo di visualizzatore di Backup and Recovery. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Visualizza lo stato del lavoro sul Job Monitor

È possibile visualizzare un elenco di tutte le operazioni di snapshot, replica, backup su storage di oggetti e ripristino, nonché il relativo stato corrente nella scheda **Monitoraggio processi**. Ciò include le operazioni da Cloud Volumes ONTAP, ONTAP locale, applicazioni e macchine virtuali. Ogni operazione o lavoro ha un ID univoco e uno stato.

Lo stato può essere:

- Successo
- In corso
- In coda
- Avvertimento
- Fallito

Nella scheda Monitoraggio processi sono disponibili snapshot, repliche, backup su storage di oggetti e operazioni di ripristino avviate dall'interfaccia utente e dall'API NetApp Backup and Recovery .

Se hai aggiornato i tuoi sistemi ONTAP alla versione 9.13.x e non vedi operazioni di backup pianificate in corso nel Job Monitor, riavvia NetApp Backup and Recovery. "Scopri come riavviare NetApp Backup and Recovery".

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Monitoraggio**.
2. Per visualizzare colonne aggiuntive (Sistema, SVM, Nome utente, Carico di lavoro, Nome policy, Etichetta snapshot), selezionare il segno più.

Cerca e filtra l'elenco dei lavori

È possibile filtrare le operazioni nella pagina Monitoraggio processi utilizzando diversi filtri, ad esempio criteri, etichetta snapshot, tipo di operazione (protezione, ripristino, conservazione o altro) e tipo di protezione (snapshot locale, replica o backup sul cloud).

Per impostazione predefinita, la pagina Monitoraggio processi mostra i processi di protezione e ripristino delle ultime 24 ore. È possibile modificare l'intervallo di tempo utilizzando il filtro Intervallo di tempo.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Monitoraggio**.
2. Per ordinare i risultati in modo diverso, seleziona ogni intestazione di colonna per ordinarli in base a Stato, Ora di inizio, Nome risorsa e altro ancora.
3. Se stai cercando lavori specifici, seleziona l'area **Ricerca avanzata e filtri** per aprire il pannello di ricerca.

   Utilizzare questo pannello per effettuare una ricerca di testo libero per qualsiasi risorsa, ad esempio "volume 1" o "applicazione 3". È anche possibile filtrare l'elenco dei lavori in base alle voci presenti nei menu a discesa.

   La maggior parte dei filtri sono autoesplicativi. Il filtro per "Carico di lavoro" consente di visualizzare i lavori nelle seguenti categorie:

   - Volumi ONTAP (Cloud Volumes ONTAP e volumi ONTAP on-premise)
   - Microsoft SQL Server
   - Macchine virtuali
   - Kubernetes

   - È possibile cercare dati all'interno di uno specifico "SVM" solo se prima è stato selezionato un sistema.
   - È possibile effettuare la ricerca utilizzando il filtro "Tipo di protezione" solo se è stato selezionato il "Tipo" di "Protezione".

4. Per aggiornare immediatamente la pagina, seleziona pulsante. Altrimenti, questa pagina si aggiorna ogni 15 minuti, così vedrai sempre i risultati più recenti sullo stato del lavoro.

Visualizza i dettagli del lavoro

È possibile visualizzare i dettagli corrispondenti a uno specifico lavoro completato. È possibile esportare i dettagli di un determinato lavoro in formato JSON.

È possibile visualizzare dettagli quali tipo di processo (pianificato o su richiesta), tipo di backup SnapMirror (iniziale o periodico), orari di inizio e fine, durata, quantità di dati trasferiti dal sistema all'archiviazione degli oggetti, velocità di trasferimento media, nome della policy, blocco di conservazione abilitato, scansione ransomware eseguita, dettagli sull'origine della protezione e dettagli sulla destinazione della protezione.

I processi di ripristino mostrano dettagli quali il provider di destinazione del backup (Amazon Web Services,

Microsoft Azure, Google Cloud, locale), il nome del bucket S3, il nome della SVM, il nome del volume di origine, il volume di destinazione, l'etichetta dello snapshot, il conteggio degli oggetti recuperati, i nomi dei file, le dimensioni dei file, la data dell'ultima modifica e il percorso completo del file.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Monitoraggio**.
2. Seleziona il nome del lavoro.
3. Seleziona il menu Azioni ••• e seleziona **Visualizza dettagli**.
4. Espandi ogni sezione per vedere i dettagli.

Scarica i risultati del monitoraggio dei lavori come report

È possibile scaricare il contenuto della pagina principale di Monitoraggio lavori come report dopo aver filtrato o ordinato i risultati. NetApp Backup and Recovery genera e scarica un file .CSV che puoi esaminare e inviare ad altri gruppi, se necessario. Il file .CSV include fino a 10.000 righe di dati.

Dalle informazioni sui dettagli del monitoraggio del lavoro, è possibile scaricare un file JSON contenente i dettagli per un singolo lavoro.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Monitoraggio**.
2. Per scaricare un file CSV per tutti i lavori, seleziona il pulsante Scarica e individua il file nella directory di download.
3. Per scaricare un file JSON per un singolo lavoro, seleziona il menu Azioni ••• per il lavoro, seleziona **Scarica file JSON** e individua il file nella directory di download.

Lavori di conservazione delle revisioni (ciclo di vita del backup)

Monitorare i flussi di conservazione (*ciclo di vita del backup*) per controllare i backup, mantenerli al sicuro e supportare gli audit. Identificare la scadenza delle copie di backup per monitorarne il ciclo di vita.

Un processo di backup del ciclo di vita tiene traccia di tutti gli snapshot eliminati o in coda per l'eliminazione. A partire da ONTAP 9.13, è possibile visualizzare tutti i tipi di lavoro denominati "Conservazione" nella pagina Monitoraggio lavori.

Il tipo di processo "Conservazione" acquisisce tutti i processi di eliminazione degli snapshot avviati su un volume protetto da NetApp Backup and Recovery.

Passi

1. Dal menu NetApp Backup and Recovery , selezionare **Monitoraggio**.
2. Selezionare l'area **Ricerca avanzata e filtro** per aprire il pannello Ricerca.
3. Selezionare "Conservazione" come tipo di lavoro.

Esaminare gli avvisi di backup e ripristino nel Centro notifiche NetApp Console

Il Centro notifiche NetApp Console tiene traccia dell'avanzamento dei processi di backup e ripristino avviati, consentendoti di verificare se l'operazione è riuscita o meno.

È possibile visualizzare gli avvisi nel Centro notifiche e configurare la Console in modo che invii avvisi tramite e-mail per attività di sistema importanti, anche quando non si è effettuato l'accesso. "Scopri di più sul Centro notifiche e su come inviare e-mail di avviso per i processi di backup e ripristino" .

Il Centro notifiche visualizza numerosi eventi di snapshot, replica, backup su cloud e ripristino, ma solo alcuni eventi attivano avvisi e-mail:

Tipo di operazione	Evento	Avviso generato	Email inviata
Attivazione	Attivazione del backup e del ripristino non riuscita per il sistema	SÌ	SÌ
Attivazione	Modifica di backup e ripristino non riuscita per il sistema	SÌ	SÌ
Attivazione	Volume ora associato al criterio snapshot	SÌ	SÌ
Attivazione	Backup del volume o stato modificato	SÌ	SÌ
Attivazione	Attivazione del backup e del ripristino riuscita per il sistema	SÌ	SÌ
Attivazione	Backup del volume ad hoc non riuscito	SÌ	SÌ
Attivazione	Backup del volume ad hoc riuscito	SÌ	NO
Attivazione	Backup multivolume non riuscito	SÌ	SÌ
Operazioni Cron	Controllo delle etichette snapshot mancanti	SÌ	SÌ
Operazioni Cron	Impossibile inviare il token di sicurezza a ONTAP per questo sistema	SÌ	SÌ
Eventi Pub/Sub	Errore di connessione	SÌ	NO
Eventi Pub/Sub	Impossibile eliminare uno snapshot pianificato	SÌ	NO
Eventi Pub/Sub	Backup pianificato del volume non riuscito	SÌ	NO
Eventi Pub/Sub	Ripristino del volume riuscito	SÌ	NO
Eventi Pub/Sub	Ripristino del volume non riuscito	SÌ	NO
Ransomware	Potenziale attacco ransomware identificato sulla copia di backup	SÌ	SÌ
Ransomware	Potenziale attacco ransomware identificato sulla copia di backup di questo sistema	SÌ	SÌ
Istantanea locale	Errore durante la creazione dello snapshot ad hoc NetApp Backup and Recovery	SÌ	SÌ
Replicazione	Modifica della relazione di replicazione del fallimento del volume	SÌ	SÌ
Replicazione	Errore del processo di replica ad hoc NetApp Backup and Recovery	SÌ	SÌ
Replicazione	Errore durante la pausa della replica NetApp Backup and Recovery	SÌ	NO
Replicazione	Errore durante l’interruzione della replica NetApp Backup and Recovery	SÌ	NO

Tipo di operazione	Evento	Avviso generato	Email inviata
Replicazione	Errore durante il processo di risincronizzazione della replica NetApp Backup and Recovery	SÌ	NO
Replicazione	Errore di interruzione del processo di replica NetApp Backup and Recovery	SÌ	NO
Replicazione	Errore nel processo di risincronizzazione inversa della replica NetApp Backup and Recovery	SÌ	SÌ
Replicazione	Errore di eliminazione della replica NetApp Backup and Recovery	SÌ	SÌ
Operazioni mirate	Errore di ripristino nella destinazione locale o cloud	SÌ	SÌ
Operazioni mirate	Errore di ripristino su richiesta	SÌ	SÌ
Operazioni di sistema	Errore nella creazione dello snapshot del volume ad hoc	SÌ	SÌ

A partire da ONTAP 9.13.0, tutti gli avvisi vengono visualizzati per i sistemi Cloud Volumes ONTAP e ONTAP locali. Per i sistemi con Cloud Volumes ONTAP 9.13.0 e ONTAP on-premises, viene visualizzato solo l'avviso relativo a "Ripristino attività completato, ma con avvisi".

Per impostazione predefinita, gli amministratori dell'organizzazione e dell'account NetApp Console ricevono e-mail per tutti gli avvisi "Critici" e "Raccomandati". Per impostazione predefinita, il sistema non configura altri utenti e destinatari per ricevere e-mail di notifica. Configura avvisi e-mail per tutti gli utenti della Console nel tuo account NetApp Cloud o per altri destinatari che devono essere informati sulle attività di backup e ripristino.

Per ricevere gli avvisi e-mail NetApp Backup and Recovery , è necessario selezionare i tipi di gravità della notifica "Critico", "Avviso" ed "Errore" nella pagina delle impostazioni Notifiche.

"Scopri come inviare email di avviso per i processi di backup e ripristino".

Passi

1. Dal menu Console, selezionare ( ).
2. Controlla le notifiche.

Esaminare l'attività operativa nella cronologia della console

È possibile visualizzare i dettagli delle operazioni di backup e ripristino per ulteriori indagini nella cronologia della console. La cronologia della console fornisce dettagli su ciascun evento, sia esso avviato dall'utente o dal sistema, e mostra le azioni avviate nell'interfaccia utente o tramite l'API.

"Scopri le differenze tra la Timeline e il Centro Notifiche".

Riavvia NetApp Backup and Recovery

Potrebbero verificarsi situazioni in cui sarà necessario riavviare NetApp Backup and Recovery.

L’agente Console include la funzionalità NetApp Backup and Recovery .

Passi

1. Connettersi al sistema Linux su cui è in esecuzione l’agente Console.

Posizione dell’agente della console	Procedura
Distribuzione cloud	Seguire le istruzioni per "connessione alla macchina virtuale Linux dell’agente Console" a seconda del provider cloud che stai utilizzando.
Installazione manuale	Accedi al sistema Linux.

2. Immettere il comando per riavviare il servizio.

Posizione dell’agente della console	Comando Docker	Comando Podman
Distribuzione cloud	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Installazione manuale con accesso a Internet	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Installazione manuale senza accesso a Internet	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`

Automatizza con le API REST di NetApp Backup and Recovery

Le funzionalità NetApp Backup and Recovery disponibili tramite l'interfaccia utente Web sono disponibili anche tramite l'API REST di backup e ripristino.

In NetApp Backup and Recovery sono definite dieci categorie di endpoint:

- `backup`- gestisce le operazioni di backup delle risorse cloud e on-premise e recupera i dettagli dei dati di backup
- `catalog`- gestisce la ricerca nel catalogo indicizzato dei file in base a una query (Cerca e Ripristina)
- `cloud`- recupera informazioni sulle varie risorse del provider cloud dalla NetApp Console
- `job`- gestisce le voci dei dettagli del lavoro sul database NetApp Console
- `license`- recupera la validità della licenza dei sistemi dalla NetApp Console
- `ransomware scan`- avvia una scansione ransomware su uno specifico file di backup
- `restore`- consente di eseguire operazioni di ripristino a livello di volume, file e cartella
- `sfr`- recupera i file da un file di backup per operazioni di ripristino a livello di singolo file (Sfoglia e ripristina)
- `storagegrid`- recupera i dettagli su un server StorageGRID e consente di scoprire un server StorageGRID
- `system`- gestisce le policy di backup e configura l'archivio oggetti di destinazione associato a un sistema

Riferimento API

La documentazione per ciascuna API NetApp Backup and Recovery è disponibile da "Automazione NetApp Console per NetApp Backup and Recovery" .

Iniziare

Per iniziare a utilizzare le API NetApp Backup and Recovery , è necessario ottenere un token utente, l'ID dell'account NetApp Console e l'ID dell'agente della console.

Quando si effettuano chiamate API, si aggiungerà il token utente nell'intestazione Authorization e l'ID agente della console nell'intestazione x-agent-id. Dovresti utilizzare l'ID account NetApp Console nelle API.

> Se si utilizza un account di servizio, è necessario utilizzare il token di accesso al servizio anziché un token utente. Il valore per "client_id" ("Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC") è un valore fisso e non può essere modificato. In questo caso, segui le istruzioni qui: "Crea un token di accesso al servizio" .

Passi

1. Ottieni un token utente dal sito Web NetApp NetApp Console .

   Assicurati di generare il token di aggiornamento dal seguente xref:./ https://services.cloud.netapp.com/refresh-token/. Il token di aggiornamento è una stringa alfanumerica che verrà utilizzata per generare un

token utente.

```
curl --location --request POST 'https://netapp-cloud-
account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
    "grant_type": "refresh_token",
    "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
    "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

Il token utente dal sito Web NetApp Console ha una data di scadenza. La risposta API include un campo "expires_in" che indica quando scade il token. Per aggiornare il token, dovrai richiamare nuovamente questa API.

2. Ottieni l'ID del tuo account NetApp Console .

```
GET 'https://api.bluexp.netapp.com/tenancy/account' -H 'authority:
api.bluexp.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR
```

Questa API restituirà una risposta simile alla seguente. È possibile recuperare l'ID dell'account analizzando l'output da **[0].[accountPublicId]**.

```
{
  "accountPublicId": "account-i6vJXvZW",
  "accountName": "rashidn",
  "isSaas": true,
  "isGov": false,
  "isPrivatePreviewEnabled": false,
  "is3rdPartyServicesEnabled": false,
  "accountSerial": "96064469711530003565",
  "userRole": "Role-1"
}
```

3. Ottieni x-agent-id che contiene l'ID dell'agente della console.

```
GET 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
  -H 'authority: api.services.cloud.netapp.com' \
  -H 'accept: application/json' \
  -H 'accept-language: en-GB,en;q=0.9' \
  -H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5……
```

È possibile recuperare l'ID dell'agente dalla risposta analizzando l'output da **occm.[0].[agent].[agentId]**.

Esempio utilizzando le API

L'esempio seguente mostra una chiamata API per attivare NetApp Backup and Recovery su un sistema con una nuova policy che ha impostato etichette giornaliere, orarie e settimanali e l'archiviazione dopo giorni impostata su 180 giorni, nella regione East-US-2 nel cloud di Azure. Si noti che in questo modo viene abilitato solo il backup sul sistema, ma non viene eseguito il backup dei volumi.

Richiesta API

Vedrai che utilizziamo l'ID account NetApp Console `account-DpTFcxN3` , ID agente console `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients` e token utente `Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwkeMwHc4V alobjUmju2x0xUH48g` in questo comando.

```
curl --location --request POST
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
    "provider":"AZURE",
    "backup-policy": {
      "archive-after-days": 180,
      "rule": [
        {
          "label": "hourly",
          "retention": "2"
        },
        {
          "label": "daily",
          "retention": "30"
        },
        {
          "label": "weekly",
          "retention": "52"
        }
      ]
    },
    "ip-space": "Default",
    "region": "eastus2",
    "azure": {
      "resource-group": "rn-test-backup-rg",
      "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
    }
  }
```

La risposta è un ID di processo che puoi monitorare:

```
{
 "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}
```

Monitorare la risposta:

```
curl --location --request GET
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

Risposta:

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "PENDING",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

Monitorare finché lo "stato" non è "COMPLETO":

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "COMPLETED",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

Riferimento

Criteri in SnapCenter confrontati con quelli in NetApp Backup and Recovery

Esistono alcune differenze tra i criteri utilizzati in SnapCenter e quelli utilizzati in NetApp Backup and Recovery che potrebbero influire su ciò che viene visualizzato dopo l'importazione di risorse e criteri da SnapCenter.

Pianifica i livelli

SnapCenter utilizza i seguenti livelli di pianificazione:

- **Ogni ora**: più ore e minuti con qualsiasi ora (0-23) e qualsiasi minuto (0-60).
- **Giornaliero**: possibilità di ripetere ogni numero di giorni impostato, ad esempio ogni 3 giorni.
- **Settimanale**: da domenica a lunedì, con la possibilità di eseguire uno snapshot il primo giorno della settimana o in più giorni della settimana.
- **Mensile**: da gennaio a dicembre, con la possibilità di eseguire l'attività in giorni specifici o in più giorni del mese, ad esempio il 7.

NetApp Backup and Recovery utilizza i seguenti livelli di pianificazione, leggermente diversi:

- **Ogni ora**: esegue snapshot solo a intervalli di 15 minuti, ad esempio intervalli di 1 ora o 15 minuti inferiori a 60.
- **Giornaliero**: Ore del giorno (0-23) con inizio, ad esempio, alle 10:00, con la possibilità di eseguire l'attività ogni tot di ore.
- **Settimanale**: Giorno della settimana (da domenica a lunedì) con la possibilità di eseguire l'attività in 1 o più giorni. È lo stesso di SnapCenter.
- **Mensile**: Date del mese (0-30) con un orario di inizio in più date del mese.
- **Annuale**: Mensile. Ciò corrisponde al dato mensile di SnapCenter.

Più policy in SnapCenter con lo stesso livello di pianificazione

È possibile assegnare più policy con lo stesso livello di pianificazione a una risorsa in SnapCenter. Tuttavia, NetApp Backup and Recovery non supporta più policy su una risorsa che utilizza lo stesso livello di pianificazione.

Esempio: se si utilizzano tre policy (per dati, registro e registro degli snapshot) in SnapCenter, dopo la migrazione da SnapCenter, NetApp Backup and Recovery utilizza una singola policy anziché tutte e tre.

Pianificazioni giornaliere SnapCenter importate

NetApp Backup and Recovery regola le pianificazioni SnapCenter come segue:

- Se la pianificazione SnapCenter è impostata su un intervallo inferiore o uguale a 7 giorni, NetApp Backup and Recovery imposta la pianificazione su settimanale. Durante la settimana alcune istantanee vengono saltate.

Esempio: se si dispone di una policy giornaliera SnapCenter con un intervallo di ripetizione ogni 3 giorni a partire da lunedì, NetApp Backup and Recovery imposta la pianificazione su settimanale il lunedì, il giovedì e la domenica. Alcuni giorni verranno saltati perché non si verificano esattamente ogni 3 giorni.

- Se la pianificazione SnapCenter è impostata su un intervallo superiore a 7 giorni, NetApp Backup and Recovery imposta la pianificazione su mensile. Durante il mese alcune istantanee verranno saltate.

  Esempio: se si dispone di una policy giornaliera SnapCenter con un intervallo di ripetizione ogni 10 giorni a partire dal 2 del mese, NetApp Backup and Recovery, dopo la migrazione, imposta la pianificazione su mensile il 2, il 12 e il 22 del mese. NetApp Backup and Recovery salterà alcuni giorni nel prossimo mese.

Pianificazioni orarie SnapCenter importate

I criteri orari SnapCenter con intervalli ripetuti superiori a un'ora vengono convertiti in criteri giornalieri in NetApp Backup and Recovery.

Qualsiasi politica oraria con intervalli ripetuti che non siano un fattore di 24 (ad esempio 5, 7, ecc.) salterà alcuni snapshot in un giorno.

Esempio: se si dispone di una policy oraria SnapCenter con un intervallo ripetuto ogni 5 ore a partire dall'1:00, NetApp Backup and Recovery (dopo la migrazione) imposterà la pianificazione su giornaliera con intervalli di 5 ore all'1:00, alle 6:00, alle 11:00, alle 16:00 e alle 21:00. Alcune ore verranno saltate, dopo le 21:00 dovrebbe essere alle 2:00 del mattino per ripetere ogni 5 ore, ma sarà sempre all'1:00 del mattino.

Conservazione dei registri dalle policy SnapCenter

Se si dispone di una risorsa in SnapCenter con più policy, NetApp Backup and Recovery utilizza il seguente ordine di priorità per assegnare il valore di conservazione del registro:

- Per i criteri "Backup completo con backup del registro" più i criteri "solo registro" in SnapCenter, NetApp Backup and Recovery utilizza il valore di conservazione del criterio solo registro.
- Per i criteri "Backup completo solo con registro" e "Completo e registro" in SnapCenter, NetApp Backup and Recovery utilizza il valore di conservazione solo registro.
- Per "Backup completo e registro" più "Backup completo" in SnapCenter, NetApp Backup and Recovery utilizza il valore di conservazione "Backup completo e registro".
- Se in SnapCenter è presente solo un backup completo, NetApp Backup and Recovery non abilita il backup del registro.

Conservazione del backup del registro

SnapCenter supporta più valori di conservazione per i criteri su una risorsa. NetApp Backup and Recovery supporta un solo valore di conservazione per risorsa.

Conteggio della conservazione dai criteri di SnapCenter

Se si dispone di una risorsa con protezione secondaria abilitata in SnapCenter con più volumi di origine, più volumi di destinazione e più relazioni SnapMirror , NetApp Backup and Recovery utilizza solo il conteggio di conservazione del primo criterio.

Esempio: se si dispone di una policy SnapCenter con un conteggio di conservazione pari a 5 e di un'altra policy con un conteggio di conservazione pari a 10, NetApp Backup and Recovery utilizza il conteggio di conservazione pari a 5.

Etichette SnapMirror dalle policy SnapCenter

SnapCenter conserva le etichette SnapMirror per ogni policy dopo la migrazione, anche se cambia il livello.

Esempio: una policy oraria di SnapCenter potrebbe cambiare in giornaliera in NetApp Backup and Recovery. Tuttavia, le etichette SnapMirror rimangono le stesse dopo la migrazione.

Ruoli di gestione dell'identità e dell'accesso (IAM) NetApp Backup and Recovery

NetApp Backup and Recovery utilizza Identity and Access Management (IAM) per gestire l'accesso di ciascun utente a specifiche funzionalità e azioni.

Per informazioni sui ruoli IAM specifici di NetApp Backup and Recovery, fare riferimento a "Ruoli NetApp Backup and Recovery nella NetApp Console" .

Ripristinare i dati di configurazione di NetApp Backup and Recovery in un sito oscuro

Quando si utilizza NetApp Backup and Recovery in un sito senza accesso a Internet, noto come *modalità privata*, i dati di configurazione di NetApp Backup and Recovery vengono sottoposti a backup nel bucket StorageGRID o ONTAP S3 in cui vengono archiviati i backup. In caso di problemi con il sistema host dell'agente Console, è possibile distribuire un nuovo agente Console e ripristinare i dati critici NetApp Backup and Recovery .

Questa procedura si applica solo ai dati di volume ONTAP .

Quando si utilizza NetApp Backup and Recovery in un ambiente SaaS con l'agente Console distribuito presso il provider cloud o sul proprio host connesso a Internet, il sistema esegue il backup e protegge tutti i dati di configurazione importanti nel cloud. Se riscontri un problema con l'agente Console, crea un nuovo agente Console e aggiungi i tuoi sistemi. I dettagli del backup vengono ripristinati automaticamente.

Esistono due tipi di dati sottoposti a backup:

- Database NetApp Backup and Recovery : contiene un elenco di tutti i volumi, file di backup, policy di backup e informazioni di configurazione.
- File di catalogo indicizzati: contengono indici dettagliati utilizzati per la funzionalità di ricerca e ripristino, che rendono le ricerche molto rapide ed efficienti quando si cercano dati di volume che si desidera ripristinare.

Questi dati vengono sottoposti a backup una volta al giorno a mezzanotte e vengono conservate al massimo 7 copie di ciascun file. Se l'agente Console gestisce più sistemi ONTAP locali, i file NetApp Backup and Recovery vengono archiviati nel bucket del sistema attivato per primo.

Nessun dato di volume viene mai incluso nel database NetApp Backup and Recovery o nei file del catalogo indicizzato.

Ripristina i dati NetApp Backup and Recovery su un nuovo agente Console

Se l'agente della console locale smette di funzionare, sarà necessario installare un nuovo agente della console e quindi ripristinare i dati di NetApp Backup and Recovery sul nuovo agente della console.

Per ripristinare il funzionamento del sistema NetApp Backup and Recovery, è necessario eseguire le seguenti operazioni:

- Installa un nuovo agente Console
- Ripristinare il database NetApp Backup and Recovery
- Ripristina i file del catalogo indicizzato
- Riscopri tutti i tuoi sistemi ONTAP on-premise e i sistemi StorageGRID nell'interfaccia utente NetApp Console

Dopo aver verificato il funzionamento del sistema, crea nuovi file di backup.

Cosa ti servirà

Sarà necessario accedere ai backup più recenti del database e dell'indice dal bucket StorageGRID o ONTAP S3 in cui sono archiviati i file di backup:

- File del database MySQL NetApp Backup and Recovery

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/mysql_backup/` , e si chiama `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- File zip di backup del catalogo indicizzato

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/catalog_backup/` , e si chiama `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installa un nuovo agente Console su un nuovo host Linux locale

Quando si installa un nuovo agente Console, scaricare la stessa versione software dell'agente originale. Le modifiche apportate al database NetApp Backup and Recovery potrebbero impedire il funzionamento delle versioni software più recenti con i vecchi backup del database. Puoi "aggiornare il software dell'agente della console alla versione più recente dopo aver ripristinato il database di backup" .

1. "Installa l'agente Console su un nuovo host Linux locale"
2. Accedi alla Console utilizzando le credenziali utente amministratore appena create.

Ripristinare il database NetApp Backup and Recovery

1. Copiare il backup MySQL dalla posizione di backup al nuovo host dell'agente della console. Di seguito utilizzeremo il nome file di esempio "CBS_DB_Backup_23_05_2023.sql".
2. Copiare il backup nel contenitore Docker MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Accedere alla shell del contenitore MySQL utilizzando uno dei seguenti comandi, a seconda che si utilizzi un contenitore Docker o Podman:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Nella shell del contenitore, distribuire "env".
5. Ti servirà la password del database MySQL, quindi copia il valore della chiave "MYSQL_ROOT_PASSWORD".
6. Ripristinare il database MySQL NetApp Backup and Recovery utilizzando il seguente comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verificare che il database MySQL NetApp Backup and Recovery sia stato ripristinato correttamente utilizzando i seguenti comandi SQL:

```
mysql -u root -p cloud_backup
```

8. Inserisci la password.

```
mysql> show tables;
mysql> select * from volume;
```

9. Assicurarsi che i volumi visualizzati siano gli stessi presenti nell'ambiente originale.

Ripristina i file del catalogo indicizzato

1. Copiare il file zip di backup del catalogo indicizzato (utilizzeremo il nome file di esempio "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip") dalla posizione di backup al nuovo host dell'agente della console nella cartella "/opt/application/netapp/cbs".
2. Decomprimere il file "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" utilizzando il seguente comando:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Eseguire il comando **ls** per assicurarsi che sia stata creata la cartella "catalogdb1" con le sottocartelle "changes" e "snapshots".

Scopri i tuoi cluster ONTAP e i sistemi StorageGRID

1. "Scopri tutti i sistemi ONTAP on-prem"che erano disponibili nel tuo ambiente precedente. Ciò include il sistema ONTAP utilizzato come server S3.
2. "Scopri i tuoi sistemi StorageGRID".

Impostare i dettagli dell'ambiente StorageGRID

Aggiungere i dettagli del sistema StorageGRID associato ai sistemi ONTAP così come sono stati configurati nella configurazione originale dell'agente della console utilizzando "API NetApp Console" .

Le seguenti informazioni si applicano alle installazioni in modalità privata a partire da NetApp Console 3.9.xx. Per le versioni precedenti, utilizzare la seguente procedura: "DarkSite Cloud Backup: backup e ripristino di MySQL e catalogo indicizzato" .

Sarà necessario eseguire questi passaggi per ogni sistema che esegue il backup dei dati su StorageGRID.

1. Estrarre il token di autorizzazione utilizzando la seguente API oauth/token.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

   Mentre l'indirizzo IP, il nome utente e le password sono valori personalizzati, il nome dell'account non lo è. Il nome dell'account è sempre "account-DARKSITE1". Inoltre, il nome utente deve essere formattato come indirizzo email.

   Questa API restituirà una risposta simile alla seguente. È possibile recuperare il token di autorizzazione come mostrato di seguito.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Estrarre l'ID di sistema e l'X-Agent-Id utilizzando l'API tenancy/external/resource.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Questa API restituirà una risposta simile alla seguente. Il valore sotto "resourceIdentifier" indica *WorkingEnvironment Id* e il valore sotto "agentId" indica *x-agent-id*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. Aggiornare il database NetApp Backup and Recovery con i dettagli del sistema StorageGRID associato ai sistemi. Assicurarsi di immettere il nome di dominio completo di StorageGRID, nonché la chiave di accesso e la chiave di archiviazione come mostrato di seguito:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Verificare le impostazioni NetApp Backup and Recovery

1. Selezionare ciascun sistema ONTAP e fare clic su **Visualizza backup** accanto al servizio Backup e ripristino nel pannello di destra.

   Dovresti vedere tutti i backup creati per i tuoi volumi.

2. Nella Dashboard di ripristino, nella sezione Cerca e ripristina, fai clic su **Impostazioni di indicizzazione**.

   Assicurarsi che i sistemi in cui era abilitata in precedenza la catalogazione indicizzata rimangano abilitati.

3. Dalla pagina Cerca e ripristina, esegui alcune ricerche nel catalogo per confermare che il ripristino del catalogo indicizzato sia stato completato correttamente.

Livelli di archiviazione AWS supportati con NetApp Backup and Recovery

NetApp Backup and Recovery supporta due classi di archiviazione S3 e la maggior parte delle regioni.

Per passare da una versione all'altra dell'interfaccia utente NetApp Backup and Recovery , fare riferimento a"Passa alla precedente interfaccia utente NetApp Backup and Recovery" .

Classi di archiviazione S3 supportate per NetApp Backup and Recovery

Quando vengono creati inizialmente i file di backup, questi vengono archiviati nell'archiviazione S3 *Standard*. Questo livello è ottimizzato per l'archiviazione di dati a cui si accede raramente, ma consente anche di accedervi immediatamente. Dopo 30 giorni i backup passano alla classe di archiviazione S3 *Standard-Infrequent Access* per risparmiare sui costi.

Se i cluster di origine eseguono ONTAP 9.10.1 o versione successiva, è possibile scegliere di suddividere i backup in livelli di archiviazione *S3 Glacier* o *S3 Glacier Deep Archive* dopo un certo numero di giorni (in genere più di 30 giorni) per un'ulteriore ottimizzazione dei costi. È possibile impostarlo su "0" oppure su un valore compreso tra 1 e 999 giorni. Se imposti il valore su "0" giorni, non potrai modificarlo in seguito in 1-999 giorni.

I dati in questi livelli non sono accessibili immediatamente quando necessario e richiederanno un costo di recupero più elevato, quindi è necessario valutare la frequenza con cui potrebbe essere necessario ripristinare i dati da questi file di backup archiviati. Consultare la sezione di questa pagina sul ripristino dei dati dall'archivio.

- Se non selezioni alcun livello di archivio nella tua prima policy di backup quando attivi NetApp Backup and Recovery, *S3 Glacier* sarà la tua unica opzione di archiviazione per le policy future.
- Se selezioni *S3 Glacier* nella tua prima policy di backup, puoi passare al livello *S3 Glacier Deep Archive* per le future policy di backup per quel cluster.
- Se selezioni *S3 Glacier Deep Archive* nella tua prima policy di backup, quel livello sarà l'unico livello di archivio disponibile per le future policy di backup per quel cluster.

Tieni presente che quando configuri NetApp Backup and Recovery con questo tipo di regola del ciclo di vita, non devi configurare alcuna regola del ciclo di vita quando imposti il bucket nel tuo account AWS.

"Scopri di più sulle classi di archiviazione S3".

Ripristinare i dati dall'archivio

Sebbene l'archiviazione di file di backup più vecchi in un archivio sia molto meno costosa rispetto all'archiviazione Standard o Standard-IA, l'accesso ai dati da un file di backup in un archivio per le operazioni di ripristino richiederà più tempo e costi maggiori.

Quanto costa ripristinare i dati da Amazon S3 Glacier e Amazon S3 Glacier Deep Archive?

Quando si recuperano dati da Amazon S3 Glacier, è possibile scegliere tra 3 priorità di ripristino e 2 priorità di ripristino quando si recuperano dati da Amazon S3 Glacier Deep Archive. S3 Glacier Deep Archive costa meno di S3 Glacier:

Livello di archivio	Ripristina priorità e costi		
	Alto	**Standard**	**Basso**
Ghiacciaio S3	Recupero più veloce, costo più alto	Recupero più lento, costi inferiori	Recupero più lento, costo più basso
Archivio S3 Glacier Deep		Recupero più rapido, costi più elevati	Recupero più lento, costo più basso

Ogni metodo prevede una tariffa di recupero per GB e una tariffa per richiesta diverse. Per i prezzi dettagliati di S3 Glacier per regione AWS, visitare "Pagina dei prezzi di Amazon S3" .

Quanto tempo ci vorrà per ripristinare i miei oggetti archiviati in Amazon S3 Glacier?

Il tempo totale di ripristino è composto da 2 parti:

- **Tempo di recupero**: tempo necessario per recuperare il file di backup dall'archivio e posizionarlo nell'archiviazione standard. Questo è talvolta chiamato il periodo di "reidratazione". Il tempo di recupero varia a seconda della priorità di ripristino scelta.

Livello di archivio	Ripristina priorità e tempo di recupero		
	Alto	**Standard**	**Basso**
Ghiacciaio S3	3-5 minuti	3-5 ore	5-12 ore
Archivio S3 Glacier Deep		12 ore	48 ore

- **Tempo di ripristino**: tempo necessario per ripristinare i dati dal file di backup nell'archiviazione standard. Questa volta non c'è differenza rispetto alla tipica operazione di ripristino eseguita direttamente dall'archiviazione Standard, quando non si utilizza un livello di archiviazione.

Per ulteriori informazioni sulle opzioni di recupero di Amazon S3 Glacier e S3 Glacier Deep Archive, fare riferimento a "le FAQ di Amazon su queste classi di archiviazione" .

Livelli di accesso all'archivio di Azure supportati con NetApp Backup and Recovery

NetApp Backup and Recovery supporta un livello di accesso all'archivio di Azure e la maggior parte delle regioni.

Per passare da una versione all'altra dell'interfaccia utente NetApp Backup and Recovery , fare riferimento a"Passa alla precedente interfaccia utente NetApp Backup and Recovery" .

Livelli di accesso Azure Blob supportati per NetApp Backup and Recovery

Quando vengono creati inizialmente i file di backup, questi vengono archiviati nel livello di accesso *Cool*. Questo livello è ottimizzato per l'archiviazione di dati a cui si accede raramente, ma che, quando necessario, sono immediatamente accessibili.

Se i cluster di origine eseguono ONTAP 9.10.1 o versione successiva, è possibile scegliere di suddividere i backup da *Cool* ad *Azure Archive* dopo un certo numero di giorni (in genere più di 30 giorni) per un'ulteriore ottimizzazione dei costi. I dati in questo livello non sono accessibili immediatamente quando necessario e richiederanno un costo di recupero più elevato, quindi è necessario valutare la frequenza con cui potrebbe essere necessario ripristinare i dati da questi file di backup archiviati. Consultare la sezione di questa pagina sul ripristino dei dati dall'archivio.

Tieni presente che quando configuri NetApp Backup and Recovery con questo tipo di regola del ciclo di vita, non devi configurare alcuna regola del ciclo di vita quando imposti il contenitore nel tuo account Azure.

"Scopri di più sui livelli di accesso di Azure Blob".

Ripristinare i dati dall'archivio

Sebbene l'archiviazione di file di backup più vecchi in un archivio sia molto meno costosa rispetto all'archiviazione Cool, l'accesso ai dati da un file di backup in Azure Archive per le operazioni di ripristino richiederà più tempo e avrà un costo maggiore.

Quanto costa ripristinare i dati da Azure Archive?

Quando si recuperano dati da Azure Archive, è possibile scegliere tra due priorità di ripristino:

- **Alto**: Recupero più rapido, costo più elevato
- **Standard**: Recupero più lento, costo inferiore

Ogni metodo prevede una tariffa di recupero per GB e una tariffa per richiesta diverse. Per i prezzi dettagliati di Azure Archive per regione di Azure, visitare il sito "Pagina dei prezzi di Azure" .

La priorità Alta non è supportata durante il ripristino dei dati da Azure ai sistemi StorageGRID .

Quanto tempo ci vorrà per ripristinare i miei dati archiviati in Azure Archive?

Il tempo di ripristino è composto da 2 parti:

- **Tempo di recupero**: tempo necessario per recuperare il file di backup archiviato da Azure Archive e posizionarlo nell'archivio Cool. Questo è talvolta chiamato il periodo di "reidratazione". Il tempo di recupero varia a seconda della priorità di ripristino scelta:
  - **Alto**: < 1 ora
  - **Standard**: < 15 ore
- **Tempo di ripristino**: tempo necessario per ripristinare i dati dal file di backup nell'archivio Cool. Questa volta non c'è differenza rispetto alla tipica operazione di ripristino eseguita direttamente dall'archiviazione Cool, quando non si utilizza un livello di archiviazione.

Per ulteriori informazioni sulle opzioni di recupero di Azure Archive, fare riferimento a "queste FAQ di Azure" .

Livelli di archiviazione di Google supportati con NetApp Backup and Recovery

NetApp Backup and Recovery supporta una classe di archiviazione Google e la maggior parte delle regioni.

Per passare da una versione all'altra dell'interfaccia utente NetApp Backup and Recovery , fare riferimento a"Passa alla precedente interfaccia utente NetApp Backup and Recovery" .

Classi di archiviazione Google supportate per NetApp Backup and Recovery

Quando vengono creati inizialmente i file di backup, questi vengono archiviati nella memoria *Standard*. Questo livello è ottimizzato per l'archiviazione di dati a cui si accede raramente, ma consente anche di accedervi immediatamente.

Se il cluster on-prem utilizza ONTAP 9.12.1 o versione successiva, è possibile scegliere di suddividere i

backup più vecchi nello storage *Archive* nell'interfaccia utente NetApp Backup and Recovery dopo un certo numero di giorni (in genere più di 30 giorni) per un'ulteriore ottimizzazione dei costi. I dati in questo livello richiederanno un costo di recupero più elevato, quindi è necessario valutare la frequenza con cui potrebbe essere necessario ripristinare i dati da questi file di backup archiviati. Consultare la sezione di questa pagina sul ripristino dei dati dall'archivio.

Tieni presente che quando configuri NetApp Backup and Recovery con questo tipo di regola del ciclo di vita, non devi configurare alcuna regola del ciclo di vita quando imposti il bucket nel tuo account Google.

"Scopri di più sulle classi di archiviazione di Google".

Ripristinare i dati dall'archivio

Sebbene l'archiviazione di file di backup più vecchi in un archivio sia molto meno costosa rispetto all'archiviazione standard, l'accesso ai dati da un file di backup in un archivio per le operazioni di ripristino richiederà un tempo leggermente più lungo e avrà un costo maggiore.

Quanto costa ripristinare i dati da Google Archive?

Per i prezzi dettagliati di Google Cloud Storage per regione, visita "Pagina dei prezzi di Google Cloud Storage" .

Quanto tempo ci vorrà per ripristinare i miei oggetti archiviati in Google Archive?

Il tempo totale di ripristino è composto da 2 parti:

- **Tempo di recupero**: tempo necessario per recuperare il file di backup dall'archivio e posizionarlo nell'archiviazione standard. Questo è talvolta chiamato il periodo di "reidratazione". A differenza delle soluzioni di archiviazione "più fredde" offerte da altri provider cloud, i tuoi dati sono accessibili in pochi millisecondi.
- **Tempo di ripristino**: tempo necessario per ripristinare i dati dal file di backup nell'archiviazione standard. Questa volta non c'è differenza rispetto alla tipica operazione di ripristino eseguita direttamente dall'archiviazione Standard, quando non si utilizza un livello di archiviazione.

Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi commerciali, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina Marchi NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politica sulla riservatezza

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp .

- "Avviso per NetApp Console"
- "Avviso per NetApp Backup and Recovery"
- "Avviso per il ripristino di un singolo file"