Riferimento

NetApp Backup and Recovery

NetApp
February 11, 2026

Sommario

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.

Informazioni sul copyright

Informazioni sul marchio commerciale