Iniziare

NetApp Backup and Recovery

NetApp
February 11, 2026

Sommario

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)

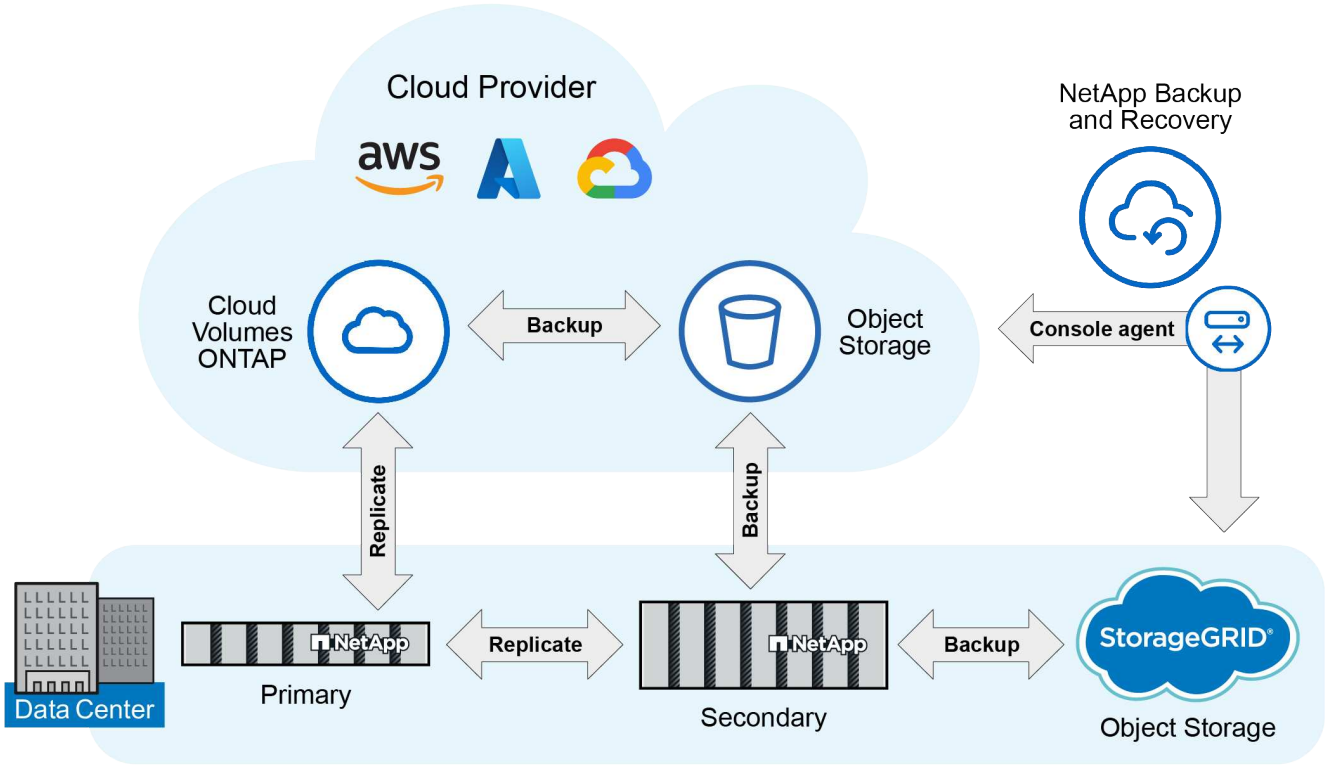
Destinazioni di backup supportate

- 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".

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".

Informazioni sul copyright

Informazioni sul marchio commerciale