Iniziare

NetApp Console setup and administration

NetApp
January 27, 2026

Sommario

Iniziare

Impara le basi

Scopri di più su NetApp Console

La console unifica la gestione e la protezione dello storage su cloud multi-ibridi con servizi dati integrati per proteggere e ottimizzare i dati.

È disponibile come piattaforma di servizi (SaaS) o come opzione self-hosted che puoi installare nel tuo cloud sovrano. Fornisce gestione dell'archiviazione, mobilità dei dati, protezione dei dati, analisi e controllo dei dati. Le funzionalità di gestione sono fornite tramite una console basata sul Web e API.

Gestione centralizzata dell'archiviazione

Scopri, distribuisci e gestisci l'archiviazione cloud e on-premise con la Console.

Archiviazione cloud e on-premise supportata

Dalla Console è possibile gestire i seguenti tipi di archiviazione:

Soluzioni di archiviazione cloud

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

Archiviazione flash e di oggetti in sede

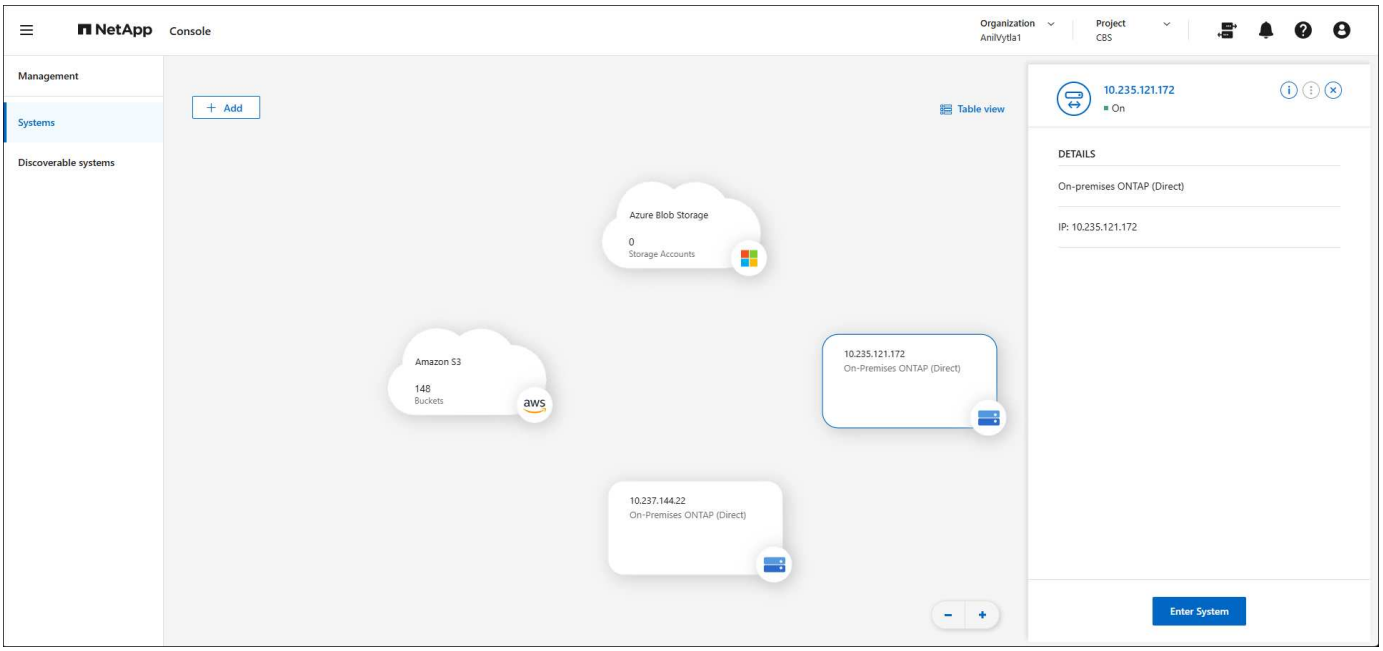
- Sistemi della serie E
- Cluster ONTAP
- Sistemi StorageGRID

Archiviazione di oggetti nel cloud

- Archiviazione Amazon S3
- Archiviazione BLOB di Azure
- Google Cloud Storage

Gestione dello storage

All'interno della Console, i *sistemi* rappresentano lo storage scoperto o distribuito. È possibile selezionare un *sistema* per integrarlo con i servizi dati NetApp o per gestire l'archiviazione, ad esempio aggiungendo volumi.



Servizi dati integrati e gestione dell'archiviazione per proteggere, proteggere e ottimizzare i dati

La Console fornisce servizi dati per proteggere e mantenere la disponibilità dell'archiviazione.

Avvisi di archiviazione

Visualizza i problemi relativi a capacità, disponibilità, prestazioni, protezione e sicurezza nel tuo ambiente ONTAP .

Hub di automazione

Utilizzare soluzioni con script per automatizzare la distribuzione e l'integrazione dei prodotti e dei servizi NetApp .

NetApp Backup and Recovery

Esegui il backup e il ripristino dei dati nel cloud e in locale.

NetApp Data Classification

Proteggi la privacy dei dati delle tue applicazioni e degli ambienti cloud.

NetApp Copy and Sync

Sincronizza i dati tra archivi dati locali e cloud.

Consulente digitale NetApp (Active IQ)

Utilizza analisi predittive e supporto proattivo per ottimizzare la tua infrastruttura dati.

Licenses and subscriptions

Gestisci e monitora le tue licenze e i tuoi abbonamenti.

NetApp Disaster Recovery

Proteggi i carichi di lavoro VMware on-premise utilizzando VMware Cloud su Amazon FSx per ONTAP come sito di disaster recovery.

Pianificazione del ciclo di vita

Identificare i cluster con capacità attuale o prevista bassa e implementare la suddivisione in livelli dei dati o raccomandazioni sulla capacità aggiuntiva.

NetApp Ransomware Resilience

Rileva anomalie che potrebbero causare attacchi ransomware. Proteggere e ripristinare i carichi di lavoro.

NetApp Replication

Replicare i dati tra i sistemi di archiviazione per supportare il backup e il ripristino di emergenza.

Aggiornamenti software

Automatizzare la valutazione, la pianificazione e l'esecuzione degli aggiornamenti ONTAP .

Dashboard della sostenibilità

Analizza la sostenibilità dei tuoi sistemi di storage.

NetApp Cloud Tiering

Estendi il tuo storage ONTAP on-premise al cloud.

NetApp Volume Caching

Crea un volume di cache scrivibile per velocizzare l'accesso ai dati o per scaricare il traffico dai volumi a cui si accede più frequentemente.

Carichi di lavoro NetApp

Progetta, configura e gestisci carichi di lavoro chiave utilizzando Amazon FSx for NetApp ONTAP.

"Scopri di più sulla NetApp Console e sui servizi dati disponibili"

Fornitori cloud supportati

La Console consente di gestire l'archiviazione cloud e di utilizzare i servizi cloud in Amazon Web Services, Microsoft Azure e Google Cloud.

Costo

L'utilizzo della NetApp Console è gratuito. Se distribuisci agenti Console nel cloud o utilizzi la modalità con restrizioni distribuita nel cloud, verranno addebitati dei costi. Alcuni servizi dati NetApp prevedono dei costi.https://bluexp.netapp.com/pricing["Scopri i prezzi dei servizi dati NetApp"^]

Come funziona NetApp Console

NetApp Console è una console basata sul Web fornita tramite il livello SaaS, un sistema di gestione delle risorse e degli accessi, agenti della console che gestiscono i sistemi di storage e abilitano i servizi dati NetApp e diverse modalità di distribuzione per soddisfare i requisiti aziendali.

Software come servizio

Si accede alla Console tramite un "interfaccia basata sul web" e API. Questa esperienza SaaS ti consente di accedere automaticamente alle funzionalità più recenti non appena vengono rilasciate.

Gestione dell'identità e dell'accesso (IAM)

La Console fornisce la gestione delle identità e degli accessi (IAM) per la gestione delle risorse e degli accessi.

Questo modello IAM fornisce una gestione granulare delle risorse e delle autorizzazioni:

- Un'organizzazione di primo livello ti consente di gestire l'accesso tra i tuoi vari progetti
- Le *cartelle* consentono di raggruppare insieme progetti correlati
- La gestione delle risorse consente di associare una risorsa a una o più cartelle o progetti
- La gestione degli accessi consente di assegnare un ruolo ai membri a diversi livelli della gerarchia dell'organizzazione
- "Scopri di più su IAM nella NetApp Console"

Agenti della console

Per alcune funzionalità e servizi dati aggiuntivi è necessario un agente Console. Ti consente di gestire risorse e processi nei tuoi ambienti on-premise e cloud. È necessario per gestire alcuni sistemi (ad esempio, Cloud Volumes ONTAP) e per utilizzare alcuni servizi dati NetApp .

"Scopri di più sugli agenti della console" .

Distribuzione SaaS rispetto a cloud sovrano

Puoi iniziare a utilizzare NetApp Console sottoscrivendo l'offerta SaaS o distribuendola nel tuo cloud sovrano. Quando distribuisci NetApp Console in un cloud sovrano, NetApp limita la connettività in uscita per soddisfare i requisiti di sicurezza e conformità della tua organizzazione. Non tutte le funzionalità e i servizi sono disponibili quando la Console viene distribuita in un cloud sovrano.

NetApp continua a offrire BlueXP per i siti che non desiderano connettività in uscita. BlueXP può essere installato sulla tua rete senza connettività in uscita. "Scopri di più su BlueXP (modalità privata) per i siti senza connettività Internet."

"Scopri di più sulle modalità di distribuzione" .

Certificazione SOC 2 Tipo 2

Uno studio contabile certificato indipendente e un revisore dei servizi hanno esaminato la Console e hanno confermato che ha ottenuto i report SOC 2 Tipo 2 in base ai criteri applicabili ai servizi fiduciari.

"Visualizza i report SOC 2 di NetApp"

Scopri di più sulle modalità di distribuzione NetApp Console

NetApp Console offre diverse *modalità di distribuzione* che ti consentono di soddisfare i requisiti aziendali e di sicurezza.

- La *modalità standard* sfrutta un livello di software come servizio (SaaS) per fornire funzionalità complete. Gli utenti accedono alla Console tramite un'interfaccia ospitata basata sul Web
- La *Modalità limitata* è disponibile per le organizzazioni con restrizioni di connettività che desiderano installare NetApp Console nel proprio cloud pubblico. Gli utenti accedono alla Console tramite un'interfaccia basata sul Web ospitata su un agente Console nel loro ambiente cloud.

  NetApp Console limita il traffico, le comunicazioni e i dati in modalità limitata, ed è necessario assicurarsi che l'ambiente (in sede e nel cloud) sia conforme alle normative richieste.

Panoramica

Ogni modalità di distribuzione differisce in termini di connettività in uscita, posizione, installazione, autenticazione, servizi dati e metodi di addebito.

Modalità standard

Si utilizza un servizio SaaS dalla console basata sul Web. A seconda dei servizi dati e delle funzionalità che intendi utilizzare, un amministratore dell'organizzazione Console crea uno o più agenti Console per gestire i dati all'interno del tuo ambiente cloud ibrido.

Questa modalità utilizza la trasmissione crittografata dei dati tramite la rete Internet pubblica.

Modalità limitata

Si installa un agente Console nel cloud (in una regione governativa, sovrana o commerciale) e ha una connettività in uscita limitata al livello SaaS NetApp Console .

Questa modalità è solitamente utilizzata dagli enti governativi statali e locali e dalle aziende regolamentate.

Scopri di più sulla connettività in uscita al livello SaaS .

Modalità privata BlueXP (solo interfaccia BlueXP legacy)

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

La tabella seguente fornisce un confronto della console NetApp .

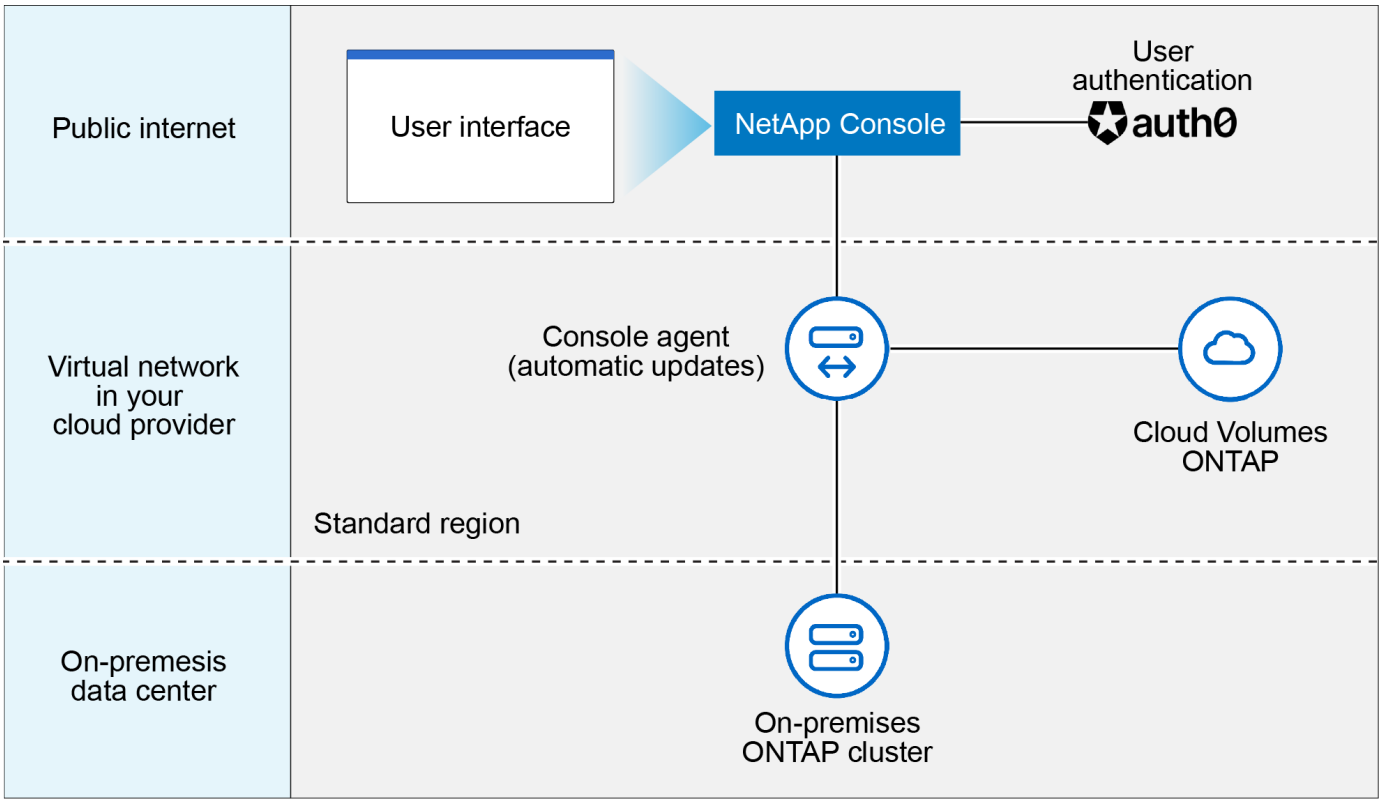
	Modalità standard	Modalità limitata
È richiesta la connessione al livello SaaS NetApp Console ?	SÌ	Solo in uscita
È richiesta la connessione al tuo provider cloud?	SÌ	Sì, all'interno della regione
Installazione dell'agente della console	Dalla console, dal cloud marketplace o dall'installazione manuale	Marketplace cloud o installazione manuale
Aggiornamenti dell'agente della console	Aggiornamenti automatici	Aggiornamenti automatici
Accesso UI	Dal livello SaaS della console	Localmente da una VM agente
Punto finale dell'API	Il livello SaaS della console	Un agente della console
Autenticazione	Tramite SaaS utilizzando auth0, login NSS o federazione delle identità	Tramite SaaS utilizzando auth0 o federazione delle identità
Autenticazione multifattoriale	Disponibile per gli utenti locali	Non disponibile

	Modalità standard	Modalità limitata
Servizi di archiviazione e dati	Tutti sono supportati	Molti sono supportati
Opzioni di licenza del servizio dati	Abbonamenti al Marketplace e BYOL	Abbonamenti al Marketplace e BYOL

Per saperne di più su queste modalità, comprese le funzionalità e i servizi NetApp Console supportati, leggere le sezioni seguenti.

Modalità standard

L'immagine seguente è un esempio di distribuzione in modalità standard.



In modalità standard la console funziona come segue:

Comunicazione in uscita

È richiesta la connettività da un agente della console al livello SaaS della console, alle risorse pubbliche del tuo provider cloud e ad altri componenti essenziali per le operazioni quotidiane.

- "Endpoint che un agente contatta in AWS"
- "Endpoint contattati da un agente in Azure"
- "Endpoint che un agente contatta in Google Cloud"

Posizione supportata per un agente

Nella modalità standard, un agente è supportato nel cloud o presso la tua sede.

Installazione dell'agente della console

È possibile installare un agente utilizzando uno dei seguenti metodi:

- Dalla console
- Da AWS o Azure Marketplace
- Da Google Cloud SDK
- Utilizzando manualmente un programma di installazione su un host Linux nel tuo data center o cloud
- Utilizzare l'OVA fornito nel proprio ambiente VCenter.

Aggiornamenti dell'agente della console

NetApp aggiorna automaticamente il tuo agente ogni mese.

Accesso all'interfaccia utente

L'interfaccia utente è accessibile dalla console basata sul Web fornita tramite il livello SaaS.

Punto finale dell'API

Le chiamate API vengono effettuate al seguente endpoint: \ https://api.bluexp.netapp.com

Autenticazione

Autenticazione con accessi auth0 o NetApp Support Site (NSS). È disponibile la federazione delle identità.

Servizi dati supportati

Sono supportati tutti i servizi dati NetApp . "Scopri di più sui servizi dati NetApp" .

Opzioni di licenza supportate

Gli abbonamenti Marketplace e BYOL sono supportati con la modalità standard; tuttavia, le opzioni di licenza supportate dipendono dal servizio dati NetApp utilizzato. Consultare la documentazione di ciascun servizio per saperne di più sulle opzioni di licenza disponibili.

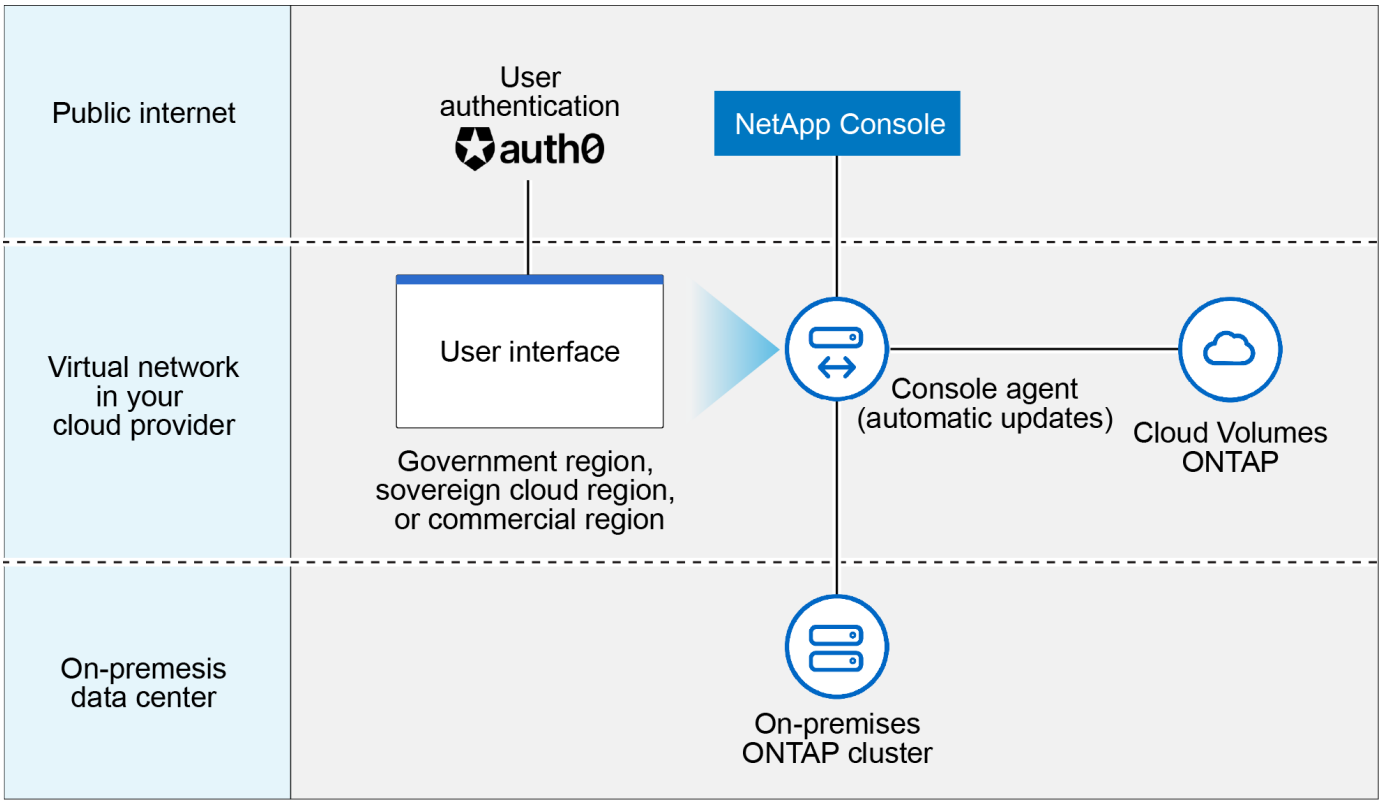
Come iniziare con la modalità standard

Vai al "NetApp Console" e iscriviti.

"Scopri come iniziare con la modalità standard" .

Modalità limitata

L'immagine seguente è un esempio di distribuzione in modalità limitata.



La console funziona come segue in modalità limitata:

Comunicazione in uscita

Un agente necessita di connettività in uscita al livello SaaS della console per servizi dati, aggiornamenti software, autenticazione e trasmissione di metadati.

Il livello SaaS della console non avvia la comunicazione con un agente. Gli agenti avviano tutte le comunicazioni con il livello SaaS della console, estraendo o inviando dati in base alle necessità.

È inoltre richiesta una connessione alle risorse del provider cloud all'interno della regione.

Posizione supportata per un agente

In modalità limitata, un agente è supportato nel cloud: in una regione governativa, sovrana o commerciale.

Installazione dell'agente della console

Puoi effettuare l'installazione da AWS o Azure Marketplace oppure manualmente sul tuo host Linux oppure tramite un OVA scaricabile nel tuo ambiente VCenter.

Aggiornamenti dell'agente della console

NetApp aggiorna automaticamente il software dell'agente con aggiornamenti mensili.

Accesso all'interfaccia utente

L'interfaccia utente è accessibile da una macchina virtuale agente distribuita nella tua regione cloud.

Punto finale dell'API

Le chiamate API vengono effettuate alla macchina virtuale dell'agente.

Autenticazione

L'autenticazione viene fornita tramite auth0. È disponibile anche la federazione delle identità.

Gestione dell’archiviazione e servizi dati supportati

I seguenti servizi di archiviazione e dati con modalità limitata:

Servizi supportati	Note
Azure NetApp Files	Supporto completo
Backup e ripristino	Supportato nelle regioni governative e commerciali con modalità limitata. Non supportato nelle regioni sovrane con modalità limitata. In modalità limitata, NetApp Backup and Recovery supporta solo il backup e il ripristino dei dati del volume ONTAP . "Visualizza l’elenco delle destinazioni di backup supportate per i dati ONTAP" Il backup e il ripristino dei dati delle applicazioni e dei dati delle macchine virtuali non sono supportati.
NetApp Data Classification	Supportato nelle regioni governative con modalità limitata. Non supportato nelle regioni commerciali o nelle regioni sovrane con modalità limitata.
Cloud Volumes ONTAP	Supporto completo
Licenses and subscriptions	È possibile accedere alle informazioni sulla licenza e sull’abbonamento con le opzioni di licenza supportate elencate di seguito per la modalità con restrizioni.
Cluster ONTAP on-premise	Sono supportate sia la rilevazione con un agente Console sia la rilevazione senza un agente Console (rilevazione diretta). Quando si rileva un cluster locale senza un agente Console, la visualizzazione avanzata (System Manager) non è supportata.
Replicazione	Supportato nelle regioni governative con modalità limitata. Non supportato nelle regioni commerciali o nelle regioni sovrane con modalità limitata.

Opzioni di licenza supportate

Con la modalità limitata sono supportate le seguenti opzioni di licenza:

- Abbonamenti Marketplace (contratti orari e annuali)

  Notare quanto segue:

  - Per Cloud Volumes ONTAP, è supportata solo la licenza basata sulla capacità.
  - In Azure, i contratti annuali non sono supportati con le aree governative.
- BYOL

  Per Cloud Volumes ONTAP, con BYOL sono supportate sia le licenze basate sulla capacità che quelle basate sui nodi.

Come iniziare con la modalità limitata

Quando si crea l’organizzazione NetApp Console , è necessario abilitare la modalità limitata.

Se non hai ancora un'organizzazione, ti verrà chiesto di crearne una e di abilitare la modalità con restrizioni quando accedi alla Console per la prima volta da un agente della Console installato manualmente o creato dal marketplace del tuo provider cloud.

Non è possibile modificare l'impostazione della modalità limitata dopo aver creato l'organizzazione.

"Scopri come iniziare con la modalità limitata" .

Confronto tra servizi e funzionalità

La tabella seguente può aiutarti a identificare rapidamente quali servizi e funzionalità sono supportati dalla modalità con restrizioni.

Tieni presente che alcuni servizi potrebbero essere supportati con limitazioni. Per maggiori dettagli su come questi servizi sono supportati con la modalità limitata, fare riferimento alle sezioni precedenti.

Area di prodotto	Servizio o funzionalità dati NetApp	Modalità limitata
Archiviazione Questa parte della tabella elenca il supporto per la gestione dei sistemi di archiviazione dalla Console. Non indica le destinazioni di backup supportate per NetApp Backup and Recovery.	Amazon FSx per ONTAP	NO
	Amazon S3	NO
	Blob azzurro	NO
	Azure NetApp Files	SÌ
	Cloud Volumes ONTAP	SÌ
	Google Cloud NetApp Volumes	NO
	Google Cloud Storage	NO
	Cluster ONTAP on-premise	SÌ
	Serie E	NO
	StorageGRID	NO

Area di prodotto	Servizio o funzionalità dati NetApp	Modalità limitata
Servizi dati	Backup e ripristino NetApp	SÌhttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity["Visualizza l’elenco delle destinazioni di backup supportate per i dati del volume ONTAP"^]
	NetApp Data Classification	SÌ
	NetApp Copy and Sync	NO
	NetApp Disaster Recovery	NO
	NetApp Ransomware Resilience	NO
	NetApp Replication	SÌ
	NetApp Cloud Tiering	NO
	Memorizzazione nella cache del volume NetApp	NO
	Fabbrica di carichi di lavoro NetApp	NO
Caratteristiche	Avvisi	NO
	Digital Advisor	NO
	Gestione delle licenze e degli abbonamenti	SÌ
	Gestione dell’identità e degli accessi	SÌ
	Credenziali	SÌ
	Federazione	SÌ
	Pianificazione del ciclo di vita	NO
	Autenticazione multifattoriale	SÌ
	Conti NSS	SÌ
	Notifiche	SÌ
	Ricerca	SÌ
	Aggiornamenti software	NO
	Sostenibilità	NO
	Revisione contabile	SÌ

Gestisci le credenziali NSS associate alla NetApp Console

Associa un account NetApp Support Site alla tua organizzazione Console per abilitare flussi di lavoro chiave per la gestione dello storage. Queste credenziali NSS sono associate all’intera organizzazione.

La console supporta anche l'associazione di un account NSS per account utente. "Scopri come gestire le credenziali a livello utente" .

Panoramica

Per abilitare le seguenti attività è necessario associare le credenziali del sito di supporto NetApp al numero di serie specifico dell'account della console:

- Distribuzione di Cloud Volumes ONTAP quando si utilizza la propria licenza (BYOL)

  È necessario fornire il proprio account NSS affinché la Console possa caricare la chiave di licenza e abilitare l'abbonamento per il periodo acquistato. Ciò include aggiornamenti automatici per i rinnovi dei termini.

- Registrazione dei sistemi Cloud Volumes ONTAP a consumo

  Per attivare il supporto per il tuo sistema e accedere alle risorse di supporto tecnico NetApp è necessario fornire il tuo account NSS.

- Aggiornamento del software Cloud Volumes ONTAP all'ultima versione

Queste credenziali sono associate al numero di serie specifico del tuo account Console. Gli utenti possono accedere a queste credenziali da **Supporto > Gestione NSS**.

Aggiungi un account NSS

È possibile aggiungere e gestire gli account del sito di supporto NetApp da utilizzare con la Console dalla Dashboard di supporto all'interno della Console.

Una volta aggiunto l'account NSS, la Console utilizza queste informazioni per operazioni quali download di licenze, verifica di aggiornamenti software e future registrazioni di supporto.

È possibile associare più account NSS alla propria organizzazione; tuttavia, non è possibile avere account cliente e account partner all'interno della stessa organizzazione.

NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e le licenze.

Passi

1. In **Amministrazione > Supporto**.
2. Selezionare **Gestione NSS**.
3. Seleziona **Aggiungi account NSS**.
4. Selezionare **Continua** per essere reindirizzati alla pagina di accesso di Microsoft.
5. Nella pagina di accesso, inserisci l'indirizzo email e la password registrati sul sito di supporto NetApp .

   Dopo aver effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

   Si tratta di un ID generato dal sistema che corrisponde al tuo indirizzo email. Nella pagina **Gestione NSS**, puoi visualizzare la tua email da ••• menu.

   - Se hai bisogno di aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Aggiorna credenziali** in ••• menu.

Utilizzando questa opzione ti verrà richiesto di effettuare nuovamente l'accesso. Si noti che il token per questi account scade dopo 90 giorni. Verrà pubblicata una notifica per avvisarti di ciò.

Cosa succederà ora?

Gli utenti possono ora selezionare l'account quando creano nuovi sistemi Cloud Volumes ONTAP e quando registrano sistemi Cloud Volumes ONTAP esistenti.

- "Avvio di Cloud Volumes ONTAP in AWS"
- "Avvio di Cloud Volumes ONTAP in Azure"
- "Avvio di Cloud Volumes ONTAP in Google Cloud"
- "Registrazione dei sistemi pay-as-you-go"

Aggiorna le credenziali NSS

Per motivi di sicurezza, è necessario aggiornare le credenziali NSS ogni 90 giorni. Se le tue credenziali NSS sono scadute, verrai avvisato nel centro notifiche della Console. "Scopri di più sul Centro notifiche" .

Le credenziali scadute possono compromettere quanto segue, ma non sono limitate a:

- Aggiornamenti della licenza, il che significa che non potrai sfruttare la capacità appena acquistata.
- Possibilità di inviare e monitorare i casi di supporto.

Inoltre, puoi aggiornare le credenziali NSS associate alla tua organizzazione se desideri modificare l'account NSS associato alla tua organizzazione. Ad esempio, se la persona associata al tuo account NSS ha lasciato la tua azienda.

Passi

1. In **Amministrazione > Supporto**.
2. Selezionare **Gestione NSS**.
3. Per l'account NSS che desideri aggiornare, seleziona ••• e quindi seleziona **Aggiorna credenziali**.
4. Quando richiesto, seleziona **Continua** per essere reindirizzato alla pagina di accesso di Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione correlati al supporto e alle licenze.

5. Nella pagina di accesso, inserisci l'indirizzo email e la password registrati sul sito di supporto NetApp .

Collega un sistema a un account NSS diverso

Se la tua organizzazione dispone di più account NetApp Support Site, puoi modificare l'account associato a un sistema Cloud Volumes ONTAP .

Per prima cosa devi aver associato l'account alla Console.

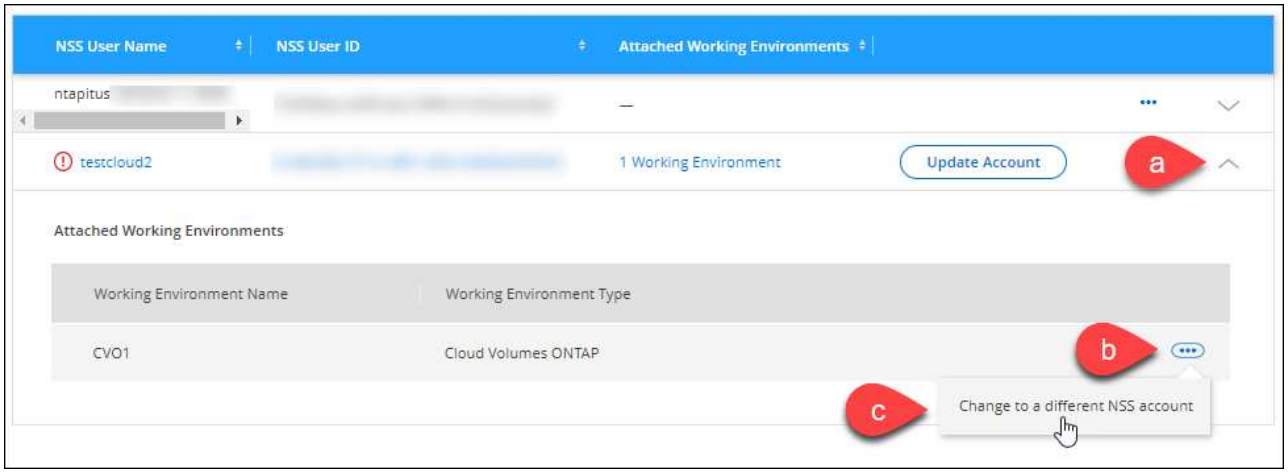
Passi

1. In **Amministrazione > Supporto**.
2. Selezionare **Gestione NSS**.
3. Per modificare l'account NSS, completa i seguenti passaggi:
   a. Espandere la riga relativa all'account del sito di supporto NetApp a cui il sistema è attualmente

associato.

b. Per il sistema per il quale si desidera modificare l'associazione, selezionare ...

c. Seleziona **Cambia in un altro account NSS**.



d. Seleziona l'account e poi seleziona **Salva**.

Visualizza l'indirizzo email di un account NSS

Per motivi di sicurezza, l'indirizzo email associato a un account NSS non viene visualizzato per impostazione predefinita. È possibile visualizzare l'indirizzo e-mail e il nome utente associato a un account NSS.

Quando si accede alla pagina Gestione NSS, la Console genera un token per ogni account nella tabella. Tale token include informazioni sull'indirizzo email associato. Il token viene rimosso quando si esce dalla pagina. Le informazioni non vengono mai memorizzate nella cache, il che contribuisce a proteggere la tua privacy.

Passi

1. In **Amministrazione > Supporto**.
2. Selezionare **Gestione NSS**.
3. Per l'account NSS che desideri aggiornare, seleziona ... e quindi seleziona **Visualizza indirizzo email**. Puoi usare il pulsante Copia per copiare l'indirizzo email.

Rimuovere un account NSS

Elimina tutti gli account NSS che non desideri più utilizzare con la Console.

Non è possibile eliminare un account attualmente associato a un sistema Cloud Volumes ONTAP . Per prima cosa devicollegare tali sistemi a un account NSS diverso .

Passi

1. In **Amministrazione > Supporto**.
2. Selezionare **Gestione NSS**.
3. Per l'account NSS che desideri eliminare, seleziona ... e quindi seleziona **Elimina**.
4. Selezionare **Elimina** per confermare.

Scopri di più sugli agenti NetApp Console

Puoi utilizzare un agente Console per connettere NetApp Console alla tua infrastruttura e orchestrare in modo sicuro le soluzioni di storage su AWS, Azure, Google Cloud o ambienti on-premise, nonché utilizzare servizi di protezione dei dati.

Un agente Console consente di:

- Orchestra le attività di gestione dello storage dalla NetApp Console, come il provisioning Cloud Volumes ONTAP, la configurazione dei volumi di storage, l'utilizzo della classificazione dei dati e altro ancora.
- Autenticazione tramite i ruoli IAM del tuo provider cloud per l'integrazione della fatturazione degli abbonamenti
- Utilizzare servizi dati avanzati (NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience e NetApp Cloud Tiering)
- Utilizzare la Console in modalità limitata.

Se non hai bisogno di un'orchestrazione avanzata o di una protezione dei dati, puoi gestire centralmente i cluster ONTAP on-premise e i servizi di archiviazione cloud-native senza dover distribuire un agente. Sono disponibili anche strumenti di monitoraggio e mobilità dei dati.

Nella tabella seguente vengono mostrate le funzionalità e i servizi che è possibile utilizzare con e senza un agente Console.

	Disponibile con agente	**Disponibile senza agente**
Sistemi di archiviazione supportati:		
Amazon FSx per ONTAP	Sì (funzionalità di scoperta e gestione)	Sì (solo scoperta)
Archiviazione Amazon S3	SÌ	NO
Archiviazione BLOB di Azure	SÌ	SÌ
Azure NetApp Files	SÌ	SÌ
Cloud Volumes ONTAP	SÌ	NO
Sistemi della serie E	SÌ	NO
Google Cloud NetApp Volumes	SÌ	SÌ
Bucket di archiviazione di Google Cloud	SÌ	NO
Sistemi StorageGRID	SÌ	NO
Cluster ONTAP on-premise (gestione e individuazione avanzate)	Sì (gestione avanzata e scoperta)	No (solo scoperta di base)

	Disponibile con agente	Disponibile senza agente
Servizi di gestione dello storage disponibili:		
Avvisi	SÌ	NO
Hub di automazione	SÌ	SÌ
Digital Advisor (Active IQ)	SÌ	NO
Gestione delle licenze e degli abbonamenti	SÌ	NO
Efficienza economica	SÌ	NO
Metriche della dashboard della home page	Sì[2]	NO
Pianificazione del ciclo di vita	SÌ	No[1]
Sostenibilità	SÌ	NO
Aggiornamenti software	SÌ	SÌ
Carichi di lavoro NetApp	SÌ	SÌ
Servizi dati disponibili:		
NetApp Backup and Recovery	SÌ	NO
Classificazione dei dati	SÌ	NO
NetApp Cloud Tiering	SÌ	NO
NetApp Copy and Sync	SÌ	NO
NetApp Disaster Recovery	SÌ	NO
NetApp Ransomware Resilience	SÌ	NO
NetApp Volume Caching	SÌ	NO

[1] È possibile visualizzare la pianificazione del ciclo di vita senza un agente della console, ma è necessario un agente della console per avviare le azioni.

[2] Per ottenere metriche precise nella home page sono necessari agenti della console opportunamente dimensionati e configurati.

Gli agenti della console devono essere operativi in ogni momento

Gli agenti della console sono una parte fondamentale della NetApp Console. È tua responsabilità (in quanto cliente) assicurarti che gli agenti competenti siano sempre attivi, operativi e raggiungibili. La console è in grado di gestire brevi interruzioni dell'agente, ma è necessario risolvere rapidamente i guasti dell'infrastruttura.

La presente documentazione è regolata dall'EULA. L'utilizzo del prodotto al di fuori della documentazione potrebbe influire sulla sua funzionalità e sui diritti EULA.

Posizioni supportate

È possibile installare gli agenti nelle seguenti posizioni:

- Servizi Web Amazon
- Microsoft Azure

  Distribuisci un agente Console in Azure nella stessa area geografica dei sistemi Cloud Volumes ONTAP che gestisce. In alternativa, distribuiscilo nel "Coppia di regioni di Azure" . Ciò garantisce che venga utilizzata una connessione Azure Private Link tra Cloud Volumes ONTAP e i relativi account di archiviazione associati. "Scopri come Cloud Volumes ONTAP utilizza un collegamento privato di Azure"

- Google Cloud

  Per utilizzare la Console e i servizi dati con Google Cloud, distribuisci il tuo agente in Google Cloud.

- Presso la vostra sede

Comunicazione con i provider cloud

L'agente utilizza TLS 1.3 per tutte le comunicazioni con AWS, Azure e Google Cloud.

Modalità limitata

Per utilizzare la Console in modalità limitata, è necessario installare un agente Console e accedere all'interfaccia Console in esecuzione localmente sull'agente Console.

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

Come installare un agente Console

È possibile installare un agente Console direttamente dalla Console, dal marketplace del proprio provider cloud oppure installando manualmente il software sul proprio host Linux o nel proprio ambiente VCenter.

- "Scopri di più sulle modalità di distribuzione NetApp Console"
- "Inizia a usare NetApp Console in modalità standard"
- "Inizia a usare NetApp Console in modalità limitata"

Autorizzazioni del provider cloud

Sono necessarie autorizzazioni specifiche per creare l'agente Console direttamente dalla NetApp Console e un altro set di autorizzazioni per l'agente Console stesso. Se si crea l'agente Console in AWS o Azure direttamente dalla Console, la Console crea l'agente Console con le autorizzazioni necessarie.

Quando si utilizza la Console in modalità standard, il modo in cui si forniscono le autorizzazioni dipende da

come si intende creare l'agente della Console.

Per informazioni su come impostare le autorizzazioni, fare riferimento a quanto segue:

- Modalità standard
  - "Opzioni di installazione dell'agente in AWS"
  - "Opzioni di installazione dell'agente in Azure"
  - "Opzioni di installazione dell'agente in Google Cloud"
  - "Impostare le autorizzazioni cloud per le distribuzioni on-premise"
- "Imposta le autorizzazioni per la modalità limitata"

Per visualizzare le autorizzazioni esatte di cui l'agente della console ha bisogno per le operazioni quotidiane, fare riferimento alle seguenti pagine:

- "Scopri come l'agente della console utilizza le autorizzazioni AWS"
- "Scopri come l'agente Console utilizza le autorizzazioni di Azure"
- "Scopri come l'agente della console utilizza le autorizzazioni di Google Cloud"

È tua responsabilità aggiornare i criteri dell'agente della console man mano che vengono aggiunte nuove autorizzazioni nelle versioni successive. Le note di rilascio elencano le nuove autorizzazioni.

Aggiornamenti degli agenti

NetApp aggiorna mensilmente il software dell'agente per aggiungere funzionalità e migliorare la stabilità. Alcune funzionalità della console, come Cloud Volumes ONTAP e la gestione dei cluster ONTAP in locale, dipendono dalla versione e dalle impostazioni dell'agente della console.

Quando installi l'agente nel cloud, l'agente della console si aggiorna automaticamente se ha accesso a Internet.

Manutenzione del sistema operativo e della VM

La manutenzione del sistema operativo sull'host dell'agente della console è responsabilità del cliente. Ad esempio, il cliente dovrebbe applicare gli aggiornamenti di sicurezza al sistema operativo sull'host dell'agente Console seguendo le procedure standard della propria azienda per la distribuzione del sistema operativo.

Tieni presente che non è necessario che tu (cliente) interrompa alcun servizio sull'host Console gent quando applichi aggiornamenti di sicurezza minori.

Se tu (il cliente) hai bisogno di arrestare e poi riavviare la VM dell'agente della console, dovresti farlo dalla console del tuo provider cloud o utilizzando le procedure standard per la gestione in locale.

L'agente della console deve essere operativo in ogni momento .

Sistemi e agenti multipli

Un agente può gestire più sistemi e supportare i servizi dati nella Console. È possibile utilizzare un singolo agente per gestire più sistemi in base alle dimensioni della distribuzione e ai servizi dati utilizzati.

Per distribuzioni su larga scala, collabora con il tuo rappresentante NetApp per dimensionare il tuo ambiente. In caso di problemi, contattare l'assistenza NetApp .

Ecco alcuni esempi di distribuzioni di agenti:

- Hai un ambiente multicloud (ad esempio, AWS e Azure) e preferisci avere un agente in AWS e un altro in Azure. Ognuno gestisce i sistemi Cloud Volumes ONTAP in esecuzione in tali ambienti.
- Un fornitore di servizi potrebbe utilizzare un'organizzazione Console per fornire servizi ai propri clienti e un'altra organizzazione per fornire il ripristino di emergenza per una delle proprie unità aziendali. Ogni organizzazione ha bisogno del proprio agente.

Scopri di più sulla gestione dell'identità e degli accessi NetApp Console

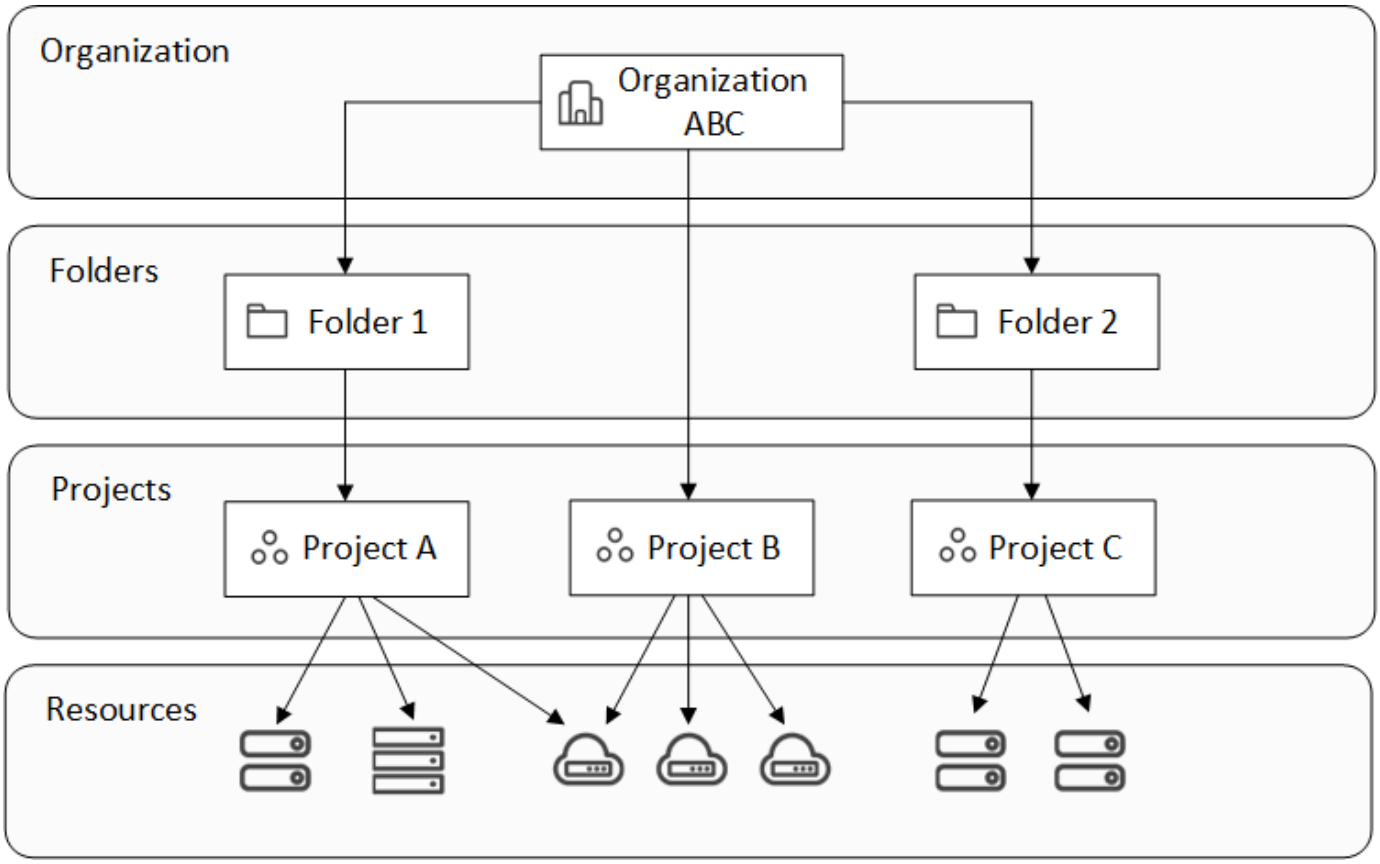
Utilizza la gestione delle identità e degli accessi (IAM) di NetApp Console per organizzare le tue risorse NetApp e controllare l'accesso in base alla struttura aziendale, in base a sede, reparto o progetto.

Le risorse sono organizzate gerarchicamente: l'organizzazione è in alto, seguita dalle cartelle (che possono contenere altre cartelle o progetti) e infine dai progetti, che contengono sistemi di archiviazione, carichi di lavoro e agenti.

Assegnare autorizzazioni di controllo degli accessi basate sui ruoli (RBAC) ai membri a livello di organizzazione, cartella o progetto per garantire che gli utenti abbiano l'accesso appropriato alle risorse.

Per gestire IAM nella NetApp Console, è necessario disporre dei ruoli di *Super admin*, *Organization admin* o *Folder or project admin*.

L'immagine seguente illustra questa gerarchia a livello di base.



]

Componenti di gestione dell'identità e dell'accesso

All'interno di NetApp Console, puoi organizzare le tue risorse di storage utilizzando tre componenti principali: componenti organizzativi, componenti delle risorse e componenti di accesso utente.

Progetti e cartelle all'interno della tua organizzazione

All'interno della struttura IAM, si lavora con tre componenti organizzative: organizzazioni, progetti e cartelle. È possibile concedere l'accesso agli utenti assegnando loro ruoli a uno qualsiasi di questi livelli.

Organizzazione

Un'*organizzazione* è il livello più alto del sistema Console IAM e in genere rappresenta la tua azienda. La tua organizzazione è composta da cartelle, progetti, membri, ruoli e risorse. Gli agenti sono associati a progetti specifici nell'organizzazione.

Progetti

Un *progetto* viene utilizzato per fornire l'accesso a una risorsa di archiviazione. È necessario assegnare le risorse al progetto prima che chiunque possa accedervi. È possibile assegnare più risorse a un singolo progetto e avere anche più progetti. Si assegnano quindi agli utenti le autorizzazioni per il progetto, in modo da consentire loro di accedere alle risorse in esso contenute.

Ad esempio, è possibile associare un sistema ONTAP locale a un singolo progetto o a tutti i progetti della propria organizzazione, a seconda delle esigenze.

"Scopri come aggiungere progetti alla tua organizzazione."

Cartelle

Raggruppa i progetti correlati in *cartelle* per organizzarli in base a posizione, sede o unità aziendale. Non è possibile associare le risorse direttamente alle cartelle, ma assegnando a un utente un ruolo a livello di cartella gli si dà accesso a tutti i progetti in quella cartella.

"Scopri come aggiungere cartelle alla tua organizzazione."

Risorse

Le *Risorse* includono sistemi di archiviazione, abbonamenti Keystone e agenti Console.

+ È necessario associare una risorsa a un progetto prima che chiunque possa accedervi.

+

Ad esempio, potresti associare un sistema Cloud Volumes ONTAP a un progetto o a tutti i progetti della tua organizzazione. Il modo in cui associare una risorsa dipende dalle esigenze della tua organizzazione.

+

"Scopri come associare le risorse ai progetti."

Sistemi di archiviazione e abbonamenti Keystone

I sistemi di storage sono le risorse principali gestite in NetApp Console. NetApp Console supporta la gestione di sistemi di archiviazione sia on-premise che cloud. È necessario aggiungere un sistema di archiviazione a un progetto prima che chiunque possa accedervi.

I sistemi di archiviazione vengono associati automaticamente al progetto in cui vengono aggiunti, ma è possibile associarli anche ad altri progetti o cartelle dalla pagina **Risorse**.

Gli abbonamenti Keystone sono anche risorse che è possibile associare ai progetti per concedere agli utenti l'accesso all'abbonamento in NetApp Console.

Agenti della console

Gli amministratori dell'organizzazione creano agenti Console per gestire i sistemi di storage e abilitare i servizi dati NetApp . Inizialmente gli agenti sono vincolati al progetto in cui vengono creati, ma gli amministratori possono aggiungerli ad altri progetti o cartelle dalla pagina Agenti.

L'associazione di un agente a un progetto consente la gestione delle risorse in quel progetto, mentre l'associazione di un agente a una cartella consente agli amministratori della cartella o del progetto di decidere quali progetti devono utilizzare l'agente. Per fornire capacità di gestione, gli agenti devono essere collegati a progetti specifici.

"Scopri come associare gli agenti ai progetti."

Membri e ruoli

Membri

I membri della tua organizzazione sono account utente o account di servizio. Un account di servizio viene solitamente utilizzato da un'applicazione per completare attività specifiche senza l'intervento umano.

Dopo che i membri si sono registrati a NetApp Console, è necessario aggiungerli alla propria organizzazione. Una volta aggiunti, è possibile assegnare loro dei ruoli per fornire l'accesso alle risorse. È possibile aggiungere manualmente gli account di servizio dalla Console oppure automatizzarne la creazione e la gestione tramite l'API IAM NetApp Console .

"Scopri come aggiungere membri alla tua organizzazione."

Ruoli di accesso

La Console fornisce ruoli di accesso che puoi assegnare ai membri della tua organizzazione.

Quando associ un membro a un ruolo, puoi concedere quel ruolo per l'intera organizzazione, per una cartella specifica o per un progetto specifico. Il ruolo selezionato conferisce a un membro le autorizzazioni per le risorse nella parte selezionata della gerarchia.

NetApp Console fornisce ruoli granulari che aderiscono ai principi del "privilegio minimo", il che significa che i ruoli di accesso sono progettati per dare agli utenti accesso solo a ciò di cui hanno bisogno

Ciò significa che agli utenti potrebbero essere assegnati più ruoli man mano che i loro compiti aumentano.

"Scopri di più sui ruoli di accesso" .

Esempi di strategia IAM

Strategia per piccole organizzazioni

Per le organizzazioni con meno di 50 utenti e una gestione centralizzata dell'archiviazione, si può prendere in considerazione un approccio semplificato che utilizzi i ruoli di Super amministratore e Super visualizzatore.

Esempio: ABC Corporation (team di 5 persone)

- **Struttura:** Unica organizzazione con 3 progetti (Produzione, Sviluppo, Backup)
- **Ruoli:**

- 2 membri senior: ruolo di **Super amministratore** per accesso amministrativo completo
- 3 membri del team: ruolo di **Super viewer** per il monitoraggio senza diritti di modifica

- **Strategia dell'agente:** Singolo agente associato a tutti i progetti per l'accesso alle risorse condivise
- **Vantaggi:** Amministrazione semplificata, ridotta complessità dei ruoli, adatto a team che necessitano di un ampio accesso

Strategia aziendale multiregionale

Per le grandi organizzazioni con attività regionali e team specializzati, è opportuno implementare un approccio gerarchico con cartelle che rappresentano i confini geografici o delle unità aziendali.

Esempio: XYZ Corporation (multinazionale)

- **Struttura:** Organizzazione > Cartelle regionali (Nord America, Europa, Asia-Pacifico) > Cartelle di progetto per regione
- **Ruoli della piattaforma:**
  - 1 **Amministratore dell'organizzazione**: supervisione globale e gestione delle policy
  - 3 **Amministratori di cartelle o progetti**: Controllo regionale (uno per regione)
  - 1 **Amministratore della federazione**: Integrazione del provider di identità aziendale
- **Ruoli di archiviazione per regione:**
  - 9 **Amministratore di storage**: Scopri e gestisci i sistemi di storage nelle regioni assegnate
  - 2 **Visualizzatore di archiviazione**: monitora le risorse di archiviazione nelle diverse regioni
  - 1 **Specialista in integrità del sistema**: Gestisci l'integrità dell'archiviazione senza modifiche al sistema
- **Ruoli del servizio dati:**
  - **Amministratore di backup e ripristino**: per progetto in base alle responsabilità di backup
  - **Amministratore di Ransomware Resilience**: monitoraggio del team di sicurezza nei vari progetti
- **Strategia dell'agente:** Agenti regionali associati a progetti geografici appropriati
- **Vantaggi:** Maggiore sicurezza attraverso la separazione dei ruoli, l'autonomia regionale e la conformità alle normative locali

Strategia di specializzazione dipartimentale

Per le organizzazioni con team specializzati che necessitano di un accesso specifico al servizio dati, utilizzare assegnazioni di ruoli mirate in base alle responsabilità funzionali.

Esempio: TechCorp (azienda tecnologica di medie dimensioni)

- **Struttura:** Organizzazione > Cartelle dipartimentali (IT, Sicurezza, Sviluppo) > Risorse specifiche del progetto
- **Ruoli specializzati:**
  - Team di sicurezza: ruoli di **amministratore di Ransomware Resilience** e **visualizzatore di classificazione**
  - Team di backup: **Super amministratore di backup e ripristino** per operazioni di backup complete
  - Team di sviluppo: **Amministratore di archiviazione** per la gestione dell'ambiente di test

    - Team di conformità: **Analista di supporto operativo** per il monitoraggio e la gestione dei casi di supporto
- **Strategia dell'agente:** Agenti collegati a progetti dipartimentali in base alla proprietà delle risorse
- **Vantaggi:** Controllo degli accessi personalizzato, maggiore efficienza operativa e chiara responsabilità per attività specializzate

Passaggi successivi con IAM nella NetApp Console

- "Introduzione a IAM nella NetApp Console"
- "Monitorare o verificare l'attività IAM"
- "Scopri di più sull'API per NetApp Console IAM"

Inizia con NetApp Console (Saas)

Flusso di lavoro introduttivo (SaaS)

Per iniziare a utilizzare NetApp Console (SaaS), prepara la rete per la Console, registrati e crea un account e utilizza l'assistente della Console per impostare le funzionalità iniziali.

Si accede a una console basata sul Web ospitata come prodotto Software-as-a-service (SaaS) di NetApp. Puoi utilizzare la Console per gestire il tuo ambiente di archiviazione cloud ibrido e utilizzare i servizi dati NetApp .

1 **"Preparare la rete per l'utilizzo della console NetApp"**

Assicurarsi che i computer che accedono alla console NetApp abbiano accesso di rete agli endpoint richiesti.

"Scopri come preparare la rete per la console NetApp ."

2 **"Registrati e crea un'organizzazione"**

Vai al "Console NetApp" e iscriviti. Se ti viene chiesto di creare un'organizzazione e ritieni che ne esista già una per la tua azienda, chiudi la finestra di dialogo e informa l'amministratore dell'organizzazione. Se al momento non esiste un amministratore dell'organizzazione per la tua azienda, puoi rivendicare questo ruolo. "Scopri come contattare un amministratore dell'organizzazione."

A questo punto hai effettuato l'accesso e puoi utilizzare l'assistente NetApp per iniziare a configurare la Console. Per iniziare, associa il tuo account di supporto NetApp e un agente della console per abilitare la funzionalità completa.

Se si sceglie di non utilizzare l'assistente NetApp o di installare un agente Console, è possibile iniziare a gestire l'archiviazione e utilizzare servizi come Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files e altri ancora. "Scopri cosa puoi fare senza un agente Console".

3 **Associa il tuo account NetApp Support Site (NSS)**

Associando il tuo account NetApp Support Site (NSS) alla Console potrai gestire le tue licenze e i tuoi abbonamenti più facilmente, nonché accedere alle risorse di supporto direttamente dalla Console.

4 Creare un agente Console

Le funzionalità avanzate di gestione dello storage e alcuni servizi dati NetApp richiedono l'installazione di un agente Console. L'agente Console consente alla Console di gestire risorse e processi all'interno del tuo ambiente cloud ibrido.

Puoi creare un agente Console nel tuo cloud o nella tua rete locale.

- "Scopri di più su quando sono richiesti gli agenti della console e come funzionano"
- "Scopri come creare un agente Console in AWS"
- "Scopri come creare un agente Console in Azure"
- "Scopri come creare un agente Console in Google Cloud"
- "Scopri come creare un agente Console in locale"

5 Aggiungere un sistema di archiviazione alla Console

All'interno della NetApp Console puoi aggiungere o scoprire sistemi di storage per gestire il tuo ambiente di storage cloud ibrido. Utilizza l'assistente NetApp per aggiungere il tuo primo sistema di storage.

> Se installi un agente Console in AWS, Microsoft Azure o Google Cloud, la Console rileva automaticamente informazioni sui bucket Amazon S3, Azure Blob Storage o Google Cloud Storage nella posizione in cui è installato l'agente. Questi sistemi vengono aggiunti automaticamente alla pagina **Sistemi**.

- "Scopri come scoprire un sistema ONTAP"
- "Scopri come scoprire un sistema StorageGRID"
- "Scopri come scoprire un sistema E-Series"

6 "Iscriviti a NetApp Intelligent Services (facoltativo)"

Iscriviti a NetApp Intelligent Services tramite il tuo provider cloud per una fatturazione oraria (PAYGO) o annuale. Un abbonamento include NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience, NetApp Disaster Recovery e NetApp Data Classification.

Preparare l'accesso alla rete per NetApp Console

NetApp Console, l'agente NetApp Console e i servizi dati NetApp richiedono l'accesso a Internet in uscita e la possibilità di contattare gli endpoint necessari.

Sarà necessario configurare l'accesso alla rete per quanto segue:

- Computer che accedono alla NetApp Console come software come servizio (SaaS)
- Agenti console installabili in locale o nel cloud. Agenti della console.

Con la versione 4.0.0, NetApp ha ridotto gli endpoint di rete richiesti per la Console e gli agenti della Console, migliorando la sicurezza e semplificando la distribuzione. È importante sottolineare che tutte le distribuzioni precedenti alla versione 4.0.0 continuano a essere pienamente supportate. Sebbene gli endpoint precedenti rimangano disponibili per gli agenti esistenti, NetApp consiglia vivamente di aggiornare le regole del firewall agli endpoint correnti dopo aver confermato il corretto aggiornamento degli agenti."Scopri come aggiornare l'elenco degli endpoint."

Endpoint contattati da NetApp Console e dagli agenti della console

Ogni agente distribuito e ogni computer che accede alla NetApp Console devono disporre di connessioni agli endpoint elencati di seguito.

Gli agenti della console distribuiti nel tuo provider cloud necessitano di accedere agli endpoint rispettivi di quel provider cloud.

Punti finali	Scopo
\ https://mysupport.netapp.com	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ https://signin.b2c.netapp.com	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ https://support.netapp.com	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Per ottenere immagini per gli aggiornamenti dell'agente della console. • Quando si distribuisce un nuovo agente, il controllo di convalida verifica la connettività agli endpoint correnti. Se usi"punti finali precedenti" , il controllo di convalida fallisce. Per evitare questo errore, saltare il controllo di convalida. Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. "Scopri come aggiornare l'elenco degli endpoint" . • Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.

Gli endpoint del provider cloud hanno contattato l'agente della console

Gli agenti della console devono avere accesso ad endpoint aggiuntivi se sono distribuiti nel tuo provider cloud.

Configurare l'accesso all'endpoint di rete del provider cloud prima di installare l'agente Console.

- "Configurare l'accesso alla rete AWS per un agente della console"
- "Configurare l'accesso alla rete di Azure per un agente della console"
- "Configurare l'accesso alla rete Google Cloud per un agente della console"

Endpoint dei servizi dati contattati dall'agente della console

Alcuni servizi dati NetApp e Cloud Volumes ONTAP richiedono che l'agente disponga di un accesso Internet in uscita aggiuntivo.

Endpoint per Cloud Volumes ONTAP

- "Endpoint per Cloud Volumes ONTAP in AWS"
- "Endpoint per Cloud Volumes ONTAP in Azure"
- "Endpoint per Cloud Volumes ONTAP in Google Cloud"

Endpoint per carichi di lavoro

L'agente della console deve essere in grado di accedere al seguente endpoint per NetApp Workloads.

Punti finali	Scopo
\ https://api.workloads.netapp.com	La console basata sul Web contatta questo endpoint per interagire con le API di Workload Factory per gestire e utilizzare i carichi di lavoro basati su FSx for ONTAP.

Registrati o accedi alla NetApp Console

Per utilizzare la Console, registrati o accedi con le credenziali del sito di supporto NetApp oppure crea un account di accesso NetApp Console . Se sei il primo della tua azienda a registrarti, puoi creare una nuova organizzazione come amministratore. Se la tua azienda ha già un'organizzazione, registrati o accedi con le credenziali del sito di supporto NetApp o con l'accesso Single Sign-On (SSO) aziendale.

Registrati a NetApp Console come amministratore iniziale dell'organizzazione

Se la tua azienda non dispone di un'organizzazione NetApp Console , registrati per crearne una. Il primo utente diventa l'amministratore dell'organizzazione e gestisce gli account utente e le autorizzazioni. È possibile aggiornare i ruoli e aggiungere altri amministratori in un secondo momento.

Passi

1. Apri un browser web e vai su "NetApp Console"
2. Se disponi di un account NetApp Support Site, inserisci l'indirizzo e-mail associato al tuo account direttamente nella pagina **Accedi**.

La Console ti registra come parte di questo accesso iniziale con le tue credenziali del sito di supporto NetApp .

3. Se vuoi registrarti creando un login alla Console, seleziona **Registrati**.
   a. Nella pagina **Iscriviti**, inserisci le informazioni richieste e seleziona **Avanti**.

      Nel modulo di registrazione sono ammessi solo caratteri inglesi.

   b. Controlla la tua casella di posta per trovare un'e-mail da NetApp che include le istruzioni per verificare il tuo indirizzo e-mail.

      Verifica il tuo indirizzo email per completare la registrazione.

4. Dopo aver effettuato l'accesso, leggere e accettare il Contratto di licenza con l'utente finale.
5. Nella pagina **Benvenuto**, crea un'organizzazione.
6. Seleziona **Iniziamo**.

+ In qualità di utente alle prime armi e amministratore dell'organizzazione, puoi seguire una procedura guidata per aggiungere risorse di archiviazione, creare un agente della console e altro ancora. "Scopri come utilizzare l'Assistente Console."

Prossimi passi

In qualità di amministratore, dopo aver completato i passaggi inclusi in Console Assistant, dovresti pianificare la tua strategia di identità e accesso, aggiungere utenti alla tua organizzazione e assegnare ruoli. "Scopri di più sulla gestione dell'identità e degli accessi per NetApp Console"

Registrati o accedi alla NetApp Console quando esiste già un'organizzazione

Se la tua azienda ha già un'organizzazione NetApp Console , registrati o accedi per accedervi. Il metodo di registrazione o di accesso varia a seconda che la tua azienda utilizzi la federazione delle identità o disponga delle credenziali del sito di supporto NetApp . In caso contrario, creare un accesso NetApp Console .

Passi

1. Apri un browser web e vai su "NetApp Console"
2. Se disponi di un account NetApp Support Site o se la tua azienda ha configurato l'accesso singolo (SSO), inserisci l'indirizzo e-mail associato o le credenziali SSO nella pagina **Accedi**. Segui le istruzioni per completare l'accesso.

   In entrambi i casi, l'iscrizione alla Console avviene tramite questo accesso iniziale.

3. Se vuoi registrarti creando un login alla Console, seleziona **Registrati**.
   a. Nella pagina **Iscriviti**, inserisci le informazioni richieste e seleziona **Avanti**.

      Nel modulo di registrazione sono ammessi solo caratteri inglesi.

   b. Controlla la tua casella di posta per trovare un'e-mail da NetApp che include le istruzioni per verificare il tuo indirizzo e-mail.

      Verifica il tuo indirizzo email per completare la registrazione.

4. Dopo aver effettuato l'accesso, leggere e accettare il Contratto di licenza con l'utente finale.

5. Se il sistema ti chiede di creare un'organizzazione, chiudi la finestra di dialogo e contatta un amministratore della Console affinché possa aggiungerti all'organizzazione della Console e concederti l'accesso. "Scopri come contattare un amministratore dell'organizzazione."

Prossimi passi

Dopo aver ottenuto l'accesso alla tua organizzazione, puoi iniziare a gestire l'archiviazione e a utilizzare i servizi dati che ti sono stati assegnati.

Inizia a utilizzare l'assistente NetApp Console

Se sei un utente alle prime armi di NetApp Console (SaaS) con il ruolo di amministratore dell'organizzazione, puoi utilizzare l'assistente della console per ricevere assistenza durante il processo di configurazione iniziale. L'assistente ti aiuta ad aggiungere un account NetApp Support Site (NSS), un agente della console, un cluster e una licenza o un abbonamento, semplificando l'avvio della gestione dei tuoi dati.

Ruoli richiesti per accedere all'assistente della console

L'assistente della console è disponibile solo per gli utenti con ruolo di amministratore dell'organizzazione.

Per impostazione predefinita, la NetApp Console visualizza l'assistente della console nella home page per gli utenti che accedono per la prima volta e che dispongono del ruolo di amministratore dell'organizzazione. Rimane disponibile finché non si completano le attività obbligatorie di creazione di un agente Console e di aggiunta di un sistema.

Utilizzare l'assistente per completare queste attività, che forniscono la configurazione minima per l'ambiente NetApp Console :

- Aggiungi un account NetApp Support Site (NSS).

  "Scopri come aggiungere un account NSS".

- Connettiti al tuo spazio di archiviazione distribuendo un agente Console.

  "Scopri come installare un agente Console in locale."

- Gestire un sistema di archiviazione aggiungendo o scoprendo un cluster
- Aggiungi un abbonamento al marketplace o una licenza PAYGO.

  "Scopri come aggiungere licenze e abbonamenti".

- Esaminare le informazioni sui servizi dati.

Introduzione a NetApp Console (modalità limitata)

Flusso di lavoro introduttivo (modalità limitata)

Inizia a utilizzare la NetApp Console in modalità limitata preparando l'ambiente e distribuendo l'agente della console.

La modalità limitata è in genere utilizzata da enti governativi statali e locali e da aziende regolamentate, comprese le distribuzioni nelle regioni AWS GovCloud e Azure Government. Prima di iniziare, assicurati di

aver compreso"Agenti della console" E"modalità di distribuzione" .

1 "Prepararsi per la distribuzione"

1. Preparare un host Linux dedicato che soddisfi i requisiti di CPU, RAM, spazio su disco, strumento di orchestrazione dei container e altro ancora.
2. Impostare una rete che fornisca l'accesso alle reti di destinazione, l'accesso a Internet in uscita per le installazioni manuali e l'accesso a Internet in uscita per l'accesso quotidiano.
3. Imposta le autorizzazioni nel tuo provider cloud in modo da poterle associare all'istanza dell'agente Console dopo averla distribuita.

2 "Distribuisci l'agente della console"

1. Installa l'agente Console dal marketplace del tuo provider cloud oppure installa manualmente il software sul tuo host Linux.
2. Per configurare la NetApp Console , apri un browser Web e inserisci l'indirizzo IP dell'host Linux.
3. Fornire all'agente della console le autorizzazioni precedentemente impostate.

3 "Iscriviti a NetApp Intelligent Services (facoltativo)"

Facoltativo: abbonati a NetApp Intelligent Services dal marketplace del tuo provider cloud per pagare i servizi dati a una tariffa oraria (PAYGO) o tramite un contratto annuale. I NetApp Intelligent Services includono NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience e NetApp Disaster Recovery. NetApp Data Classification è incluso nel tuo abbonamento senza costi aggiuntivi.

Prepararsi per la distribuzione in modalità limitata

Preparare l'ambiente prima di distribuire NetApp Console in modalità limitata. È necessario esaminare i requisiti dell'host, preparare la rete, impostare le autorizzazioni e altro ancora.

Passaggio 1: comprendere come funziona la modalità con restrizioni

Prima di iniziare, è necessario comprendere il funzionamento della NetApp Console in modalità limitata.

Utilizzare l'interfaccia basata su browser disponibile localmente dall'agente NetApp Console installato. Non è possibile accedere alla NetApp Console dalla console basata sul Web fornita tramite il livello SaaS.

Inoltre, non tutte le funzionalità della Console e i servizi dati NetApp sono disponibili.

"Scopri come funziona la modalità con restrizioni" .

Passaggio 2: rivedere le opzioni di installazione

In modalità limitata, è possibile installare l'agente Console solo nel cloud. Sono disponibili le seguenti opzioni di installazione:

- Dal Marketplace AWS

- Da Azure Marketplace
- Installazione manuale dell'agente Console sul tuo host Linux in esecuzione su AWS, Azure o Google Cloud

Passaggio 3: rivedere i requisiti dell'host

Per eseguire l'agente Console, un host deve soddisfare requisiti specifici di sistema operativo, RAM e porta.

Quando si distribuisce l'agente Console da AWS o Azure Marketplace, l'immagine include i componenti software e del sistema operativo richiesti. Devi semplicemente scegliere un tipo di istanza che soddisfi i requisiti di CPU e RAM.

Host dedicato

L'agente Console richiede un host dedicato. È supportata qualsiasi architettura che soddisfi i seguenti requisiti dimensionali:

- CPU: 8 core o 8 vCPU
- RAM: 32 GB
- Spazio su disco: si consigliano 165 GB per l'host, con i seguenti requisiti di partizione:
  - `/opt`: Devono essere disponibili 120 GiB di spazio

    L'agente utilizza `/opt` per installare il `/opt/application/netapp` directory e il suo contenuto.

  - `/var`: Devono essere disponibili 40 GiB di spazio

    L'agente della console richiede questo spazio in `/var` perché Podman o Docker sono progettati per creare i contenitori all'interno di questa directory. Nello specifico, creeranno contenitori nel `/var/lib/containers/storage` elenco e `/var/lib/docker` per Docker. I montaggi esterni o i collegamenti simbolici non funzionano per questo spazio.

Tipo di istanza AWS EC2

Un tipo di istanza che soddisfa i requisiti di CPU e RAM. NetApp consiglia t3.2xlarge.

Dimensioni della VM di Azure

Un tipo di istanza che soddisfa i requisiti di CPU e RAM. NetApp consiglia Standard_D8s_v3.

Tipo di macchina Google Cloud

Un tipo di istanza che soddisfa i requisiti di CPU e RAM. NetApp consiglia n2-standard-8.

L'agente Console è supportato in Google Cloud su un'istanza VM con un sistema operativo che supporta "Funzionalità della VM schermata"

Ipervisore

È richiesto un hypervisor bare metal o hosted certificato per eseguire un sistema operativo supportato.

Requisiti del sistema operativo e del contenitore

L'agente Console è supportato con i seguenti sistemi operativi quando si utilizza la Console in modalità standard o in modalità limitata. Prima di installare l'agente è necessario uno strumento di orchestrazione dei container.

Sistema operativo	Versioni del sistema operativo supportate	Versioni dell'agente supportate	Strumento contenitore richiesto	SELinux
Red Hat Enterprise Linux		9,6 • Solo versioni in lingua inglese. • L'host deve essere registrato presso Red Hat Subscription Management. Se non è registrato, l'host non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione dell'agente.	4.0.0 o versione successiva con la console in modalità standard o modalità limitata	Podman versione 5.4.0 con podman-compose 1.5.0. Visualizza i requisiti di configurazione di Podman .
Supportato in modalità di applicazione o modalità permissiva		da 9,1 a 9,4 • Solo versioni in lingua inglese. • L'host deve essere registrato presso Red Hat Subscription Management. Se non è registrato, l'host non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione dell'agente.	3.9.50 o versione successiva con la Console in modalità standard o modalità limitata	Podman versione 4.9.4 con podman-compose 1.5.0. Visualizza i requisiti di configurazione di Podman .

Sistema operativo	Versioni del sistema operativo supportate	Versioni dell'agente supportate	Strumento contenitore richiesto	SELinux
Supportato in modalità di applicazione o modalità permissiva		da 8,6 a 8,10 • Solo versioni in lingua inglese. • L'host deve essere registrato presso Red Hat Subscription Management. Se non è registrato, l'host non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione dell'agente.	3.9.50 o versione successiva con la Console in modalità standard o modalità limitata	Podman versione 4.6.1 o 4.9.4 con podman-compose 1.0.6. Visualizza i requisiti di configurazione di Podman .
Supportato in modalità di applicazione o modalità permissiva	Ubuntu		24,04 LTS	3.9.45 o versione successiva con la NetApp Console in modalità standard o in modalità limitata
Docker Engine dalla versione 23.06 alla 28.0.0.	Non supportato		22,04 LTS	3.9.50 o successivo

Passaggio 4: installare Podman o Docker Engine

Per installare manualmente l'agente Console, preparare l'host installando Podman o Docker Engine.

A seconda del sistema operativo in uso, prima di installare l'agente è necessario utilizzare Podman o Docker Engine.

- Podman è richiesto per Red Hat Enterprise Linux 8 e 9.

  Visualizza le versioni di Podman supportate .

- Docker Engine è richiesto per Ubuntu.

  Visualizza le versioni supportate di Docker Engine .

Esempio 1. Passi

Podman

Per installare e configurare Podman, segui questi passaggi:

- Abilita e avvia il servizio podman.socket
- Installa python3
- Installa il pacchetto podman-compose versione 1.0.6
- Aggiungere podman-compose alla variabile d'ambiente PATH
- Se si utilizza Red Hat Enterprise Linux, verificare che la versione di Podman utilizzi Netavark Aardvark DNS anziché CNI

Dopo aver installato l'agente, regolare la porta aardvark-dns (predefinita: 53) per evitare conflitti di porta DNS. Seguire le istruzioni per configurare la porta.

Passi

1. Rimuovere il pacchetto podman-docker se è installato sull'host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installa Podman.

   È possibile ottenere Podman dai repository ufficiali di Red Hat Enterprise Linux.

   a. Per Red Hat Enterprise Linux 9,6:

   ```
   sudo dnf install podman-5:<version>
   ```

   Dove <versione> è la versione supportata di Podman che stai installando. Visualizza le versioni di Podman supportate .

   b. Per Red Hat Enterprise Linux dalla versione 9.1 alla 9.4:

   ```
   sudo dnf install podman-4:<version>
   ```

   Dove <versione> è la versione supportata di Podman che stai installando. Visualizza le versioni di Podman supportate .

   c. Per Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-4:<version>
   ```

   Dove <versione> è la versione supportata di Podman che stai installando. Visualizza le versioni di Podman supportate .

3. Abilitare e avviare il servizio podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Installa python3.

```
sudo dnf install python3
```

5. Installa il pacchetto repository EPEL se non è già disponibile sul tuo sistema.

   Questo passaggio è necessario perché podman-compose è disponibile nel repository Extra Packages for Enterprise Linux (EPEL).

6. Se si utilizza Red Hat Enterprise 9:

   a. Installare il pacchetto del repository EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. Installa il pacchetto podman-compose 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Se si utilizza Red Hat Enterprise Linux 8:

   a. Installare il pacchetto del repository EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. Installa il pacchetto podman-compose 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```

   > Utilizzando il `dnf install` il comando soddisfa il requisito per aggiungere podman-compose alla variabile d'ambiente PATH. Il comando di installazione aggiunge podman-compose a /usr/bin, che è già incluso nel `secure_path` opzione sull'host.

   c. Se si utilizza Red Hat Enterprise Linux 8, verificare che la versione di Podman utilizzi NetAvark con Aardvark DNS anziché CNI.

i. Controlla se il tuo networkBackend è impostato su CNI eseguendo il seguente comando:

```
podman info | grep networkBackend
```

ii. Se networkBackend è impostato su `CNI` , dovrai cambiarlo in `netavark` .

iii. Installare `netavark` E `aardvark-dns` utilizzando il seguente comando:

```
dnf install aardvark-dns netavark
```

iv. Apri il `/etc/containers/containers.conf` file e modificare l'opzione network_backend per utilizzare "netavark" invece di "cni".

Se `/etc/containers/containers.conf` non esiste, apportare le modifiche alla configurazione `/usr/share/containers/containers.conf` .

v. Riavvia Podman.

```
systemctl restart podman
```

vi. Verificare che networkBackend sia ora modificato in "netavark" utilizzando il seguente comando:

```
podman info | grep networkBackend
```

Motore Docker

Per installare Docker Engine, seguire la documentazione di Docker.

Passi

1. "Visualizza le istruzioni di installazione da Docker"

   Segui i passaggi per installare una versione supportata di Docker Engine. Non installare la versione più recente, poiché non è supportata dalla Console.

2. Verificare che Docker sia abilitato e in esecuzione.

```
sudo systemctl enable docker && sudo systemctl start docker
```

Passaggio 5: preparare l'accesso alla rete

Configura l'accesso alla rete in modo che l'agente della console possa gestire le risorse nel tuo cloud pubblico. Oltre a disporre di una rete virtuale e di una subnet per l'agente della console, è necessario assicurarsi che siano soddisfatti i seguenti requisiti.

Connessioni alle reti di destinazione

Assicurarsi che l'agente della console disponga di una connessione di rete alle posizioni di archiviazione. Ad esempio, la VPC o la VNet in cui si prevede di distribuire Cloud Volumes ONTAP oppure il data center in cui risiedono i cluster ONTAP locali.

Preparare la rete per l'accesso degli utenti alla NetApp Console

In modalità limitata, gli utenti accedono alla Console dalla VM dell'agente Console. L'agente della console contatta alcuni endpoint per completare le attività di gestione dei dati. Questi endpoint vengono contattati dal computer di un utente quando vengono completate azioni specifiche dalla Console.

Gli agenti della console precedenti alla versione 4.0.0 necessitano di endpoint aggiuntivi. Se hai eseguito l'aggiornamento alla versione 4.0.0 o successiva, puoi rimuovere i vecchi endpoint dall'elenco consentito."Scopri di più sull'accesso alla rete richiesto per le versioni precedenti alla 4.0.0."

+

Punti finali	Scopo
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ https://cdn.auth0.com \ https://services.cloud.netapp.com	Il browser Web si connette a questi endpoint per l'autenticazione centralizzata degli utenti tramite la NetApp Console.

Accesso a Internet in uscita per le operazioni quotidiane

La posizione di rete dell'agente della console deve disporre di accesso a Internet in uscita. Deve essere in grado di raggiungere i servizi SaaS della NetApp Console e gli endpoint all'interno del rispettivo ambiente cloud pubblico.

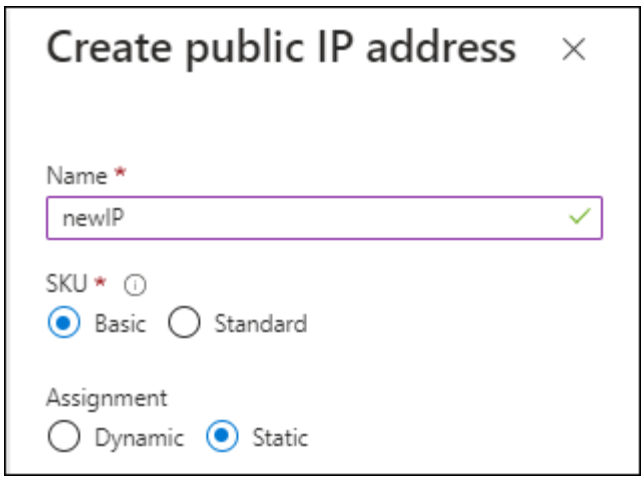
Punti finali	Scopo
Ambienti AWS	Servizi AWS (amazonaws.com): • Formazione delle nuvole • Elastic Compute Cloud (EC2) • Gestione dell'identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • Servizio di archiviazione semplice (S3)

Punti finali	Scopo
Per gestire le risorse AWS. L'endpoint dipende dalla tua regione AWS. "Per i dettagli, fare riferimento alla documentazione AWS"	Amazon FsX per NetApp ONTAP: • api.workloads.netapp.com
La console basata sul Web contatta questo endpoint per interagire con le API di Workload Factory per gestire e utilizzare i carichi di lavoro basati su FSx per ONTAP .	**Ambienti Azure**
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Per gestire le risorse nelle aree pubbliche di Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Per gestire le risorse nelle aree di Azure Government.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Per gestire le risorse nelle regioni di Azure Cina.
Ambienti Google Cloud	\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects
Per gestire le risorse in Google Cloud.	• Endpoint NetApp Console *
\ https://mysupport.netapp.com	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ https://signin.b2c.netapp.com	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.

Punti finali	Scopo
\ https://support.netapp.com	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Per ottenere immagini per gli aggiornamenti dell'agente della console. • Quando si distribuisce un nuovo agente, il controllo di convalida verifica la connettività agli endpoint correnti. Se usi"punti finali precedenti" , il controllo di convalida fallisce. Per evitare questo errore, saltare il controllo di convalida. Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. "Scopri come aggiornare l'elenco degli endpoint" . • Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.

Indirizzo IP pubblico in Azure

Se si desidera utilizzare un indirizzo IP pubblico con la macchina virtuale dell'agente Console in Azure, l'indirizzo IP deve utilizzare uno SKU di base per garantire che la Console utilizzi questo indirizzo IP pubblico.



Se invece si utilizza un indirizzo IP SKU standard, la Console utilizza l'indirizzo IP *privato* dell'agente della Console, anziché l'IP pubblico. Se il computer che stai utilizzando per accedere alla Console non ha accesso a quell'indirizzo IP privato, le azioni dalla Console non riusciranno.

"Documentazione di Azure: SKU IP pubblico"

Server proxy

NetApp supporta sia configurazioni proxy esplicite che trasparenti. Se si utilizza un proxy trasparente, è necessario fornire solo il certificato per il server proxy. Se si utilizza un proxy esplicito, saranno necessari anche l'indirizzo IP e le credenziali.

- indirizzo IP
- Credenziali
- Certificato HTTPS

porti

Non c'è traffico in entrata verso l'agente della console, a meno che non venga avviato dall'utente o utilizzato come proxy per inviare messaggi AutoSupport da Cloud Volumes ONTAP al supporto NetApp .

- HTTP (80) e HTTPS (443) forniscono l'accesso all'interfaccia utente locale, che utilizzerai in rare circostanze.
- SSH (22) è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.
- Le connessioni in ingresso sulla porta 3128 sono necessarie se si distribuiscono sistemi Cloud Volumes ONTAP in una subnet in cui non è disponibile una connessione Internet in uscita.

  Se i sistemi Cloud Volumes ONTAP non dispongono di una connessione Internet in uscita per inviare messaggi AutoSupport , la Console configura automaticamente tali sistemi per utilizzare un server proxy incluso nell'agente della Console. L'unico requisito è assicurarsi che il gruppo di sicurezza dell'agente Console consenta connessioni in entrata sulla porta 3128. Sarà necessario aprire questa porta dopo aver distribuito l'agente Console.

Abilita NTP

Se si prevede di utilizzare NetApp Data Classification per analizzare le origini dati aziendali, è necessario abilitare un servizio Network Time Protocol (NTP) sia sull'agente della console sia sul sistema NetApp Data Classification, in modo che l'ora sia sincronizzata tra i sistemi. "Scopri di più sulla classificazione dei dati NetApp"

Se intendi creare un agente Console dal marketplace del tuo provider cloud, implementa questo requisito di rete dopo aver creato l'agente Console.

Passaggio 6: preparare le autorizzazioni cloud

L'agente Console richiede le autorizzazioni del provider cloud per distribuire Cloud Volumes ONTAP in una rete virtuale e per utilizzare i servizi dati NetApp . È necessario impostare le autorizzazioni nel provider cloud e quindi associare tali autorizzazioni all'agente Console.

Per visualizzare i passaggi richiesti, seleziona l'opzione di autenticazione da utilizzare per il tuo provider cloud.

Ruolo AWS IAM

Utilizzare un ruolo IAM per fornire autorizzazioni all'agente della console.

Se stai creando l'agente della console da AWS Marketplace, ti verrà chiesto di selezionare quel ruolo IAM quando avvii l'istanza EC2.

Se si installa manualmente l'agente Console sul proprio host Linux, associare il ruolo all'istanza EC2.

Passi

1. Accedi alla console AWS e vai al servizio IAM.
2. Crea una policy:
   a. Selezionare **Criteri > Crea criterio**.
   b. Seleziona **JSON** e copia e incolla il contenuto del"Criterio IAM per l'agente della console" .
   c. Completare i passaggi rimanenti per creare la policy.
3. Crea un ruolo IAM:
   a. Selezionare **Ruoli > Crea ruolo**.
   b. Selezionare **Servizio AWS > EC2**.
   c. Aggiungi autorizzazioni allegando la policy appena creata.
   d. Completa i passaggi rimanenti per creare il ruolo.

Risultato

Ora disponi di un ruolo IAM per l'istanza EC2 dell'agente Console.

Chiave di accesso AWS

Imposta le autorizzazioni e una chiave di accesso per un utente IAM. Dopo aver installato l'agente della Console e configurato la Console, sarà necessario fornire alla Console la chiave di accesso AWS.

Passi

1. Accedi alla console AWS e vai al servizio IAM.
2. Crea una policy:
   a. Selezionare **Criteri > Crea criterio**.
   b. Seleziona **JSON** e copia e incolla il contenuto del"Criterio IAM per l'agente della console" .
   c. Completare i passaggi rimanenti per creare la policy.

      A seconda dei servizi dati NetApp che intendi utilizzare, potrebbe essere necessario creare una seconda policy.

   Per le regioni standard, le autorizzazioni sono distribuite su due policy. Sono necessarie due policy a causa del limite massimo di dimensione dei caratteri per le policy gestite in AWS. "Scopri di più sui criteri IAM per l'agente della console" .
3. Associare i criteri a un utente IAM.
   - "Documentazione AWS: creazione di ruoli IAM"
   - "Documentazione AWS: aggiunta e rimozione di policy IAM"
4. Assicurarsi che l'utente disponga di una chiave di accesso che è possibile aggiungere alla NetApp

Console dopo aver installato l'agente della console.

Ruolo di Azure

Creare un ruolo personalizzato di Azure con le autorizzazioni richieste. Assegnerai questo ruolo alla VM dell'agente Console.

Tieni presente che puoi creare un ruolo personalizzato di Azure tramite il portale di Azure, Azure PowerShell, Azure CLI o REST API. I passaggi seguenti mostrano come creare il ruolo utilizzando l'interfaccia della riga di comando di Azure. Se preferisci utilizzare un metodo diverso, fai riferimento a "Documentazione di Azure"

Passi

1. Se intendi installare manualmente il software sul tuo host, abilita un'identità gestita assegnata dal sistema sulla macchina virtuale, in modo da poter fornire le autorizzazioni di Azure richieste tramite un ruolo personalizzato.

   "Documentazione di Microsoft Azure: configurare le identità gestite per le risorse di Azure su una macchina virtuale tramite il portale di Azure"

2. Copia il contenuto del"autorizzazioni di ruolo personalizzate per il connettore" e salvarli in un file JSON.
3. Modificare il file JSON aggiungendo gli ID di sottoscrizione di Azure all'ambito assegnabile.

   Dovresti aggiungere l'ID per ogni sottoscrizione di Azure che desideri utilizzare con NetApp Console.

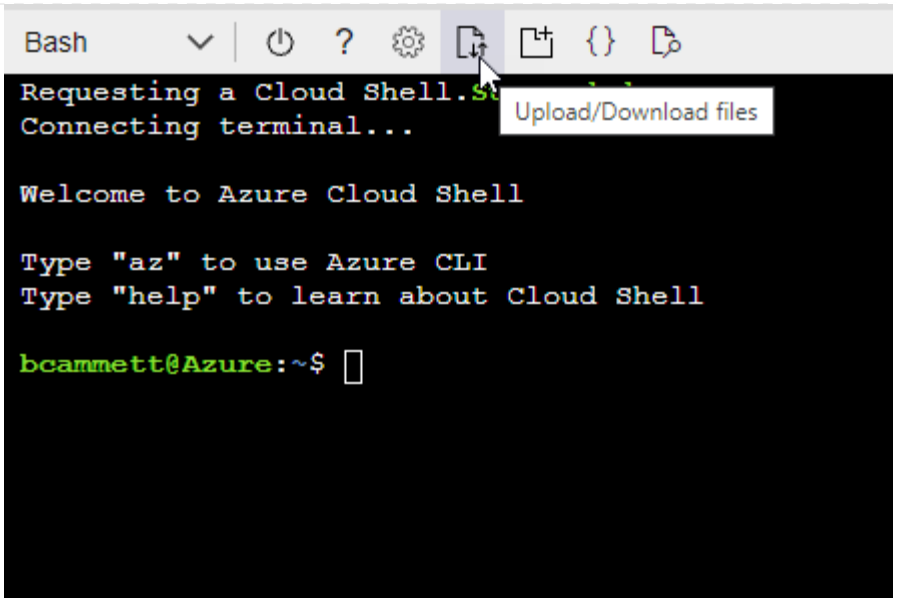
   Esempio

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

4. Utilizzare il file JSON per creare un ruolo personalizzato in Azure.

   I passaggi seguenti descrivono come creare il ruolo utilizzando Bash in Azure Cloud Shell.

   a. Inizio "Azure Cloud Shell" e scegli l'ambiente Bash.
   b. Carica il file JSON.



c. Utilizzare l'interfaccia della riga di comando di Azure per creare il ruolo personalizzato:

```
az role definition create --role-definition agent_Policy.json
```

Entità del servizio di Azure

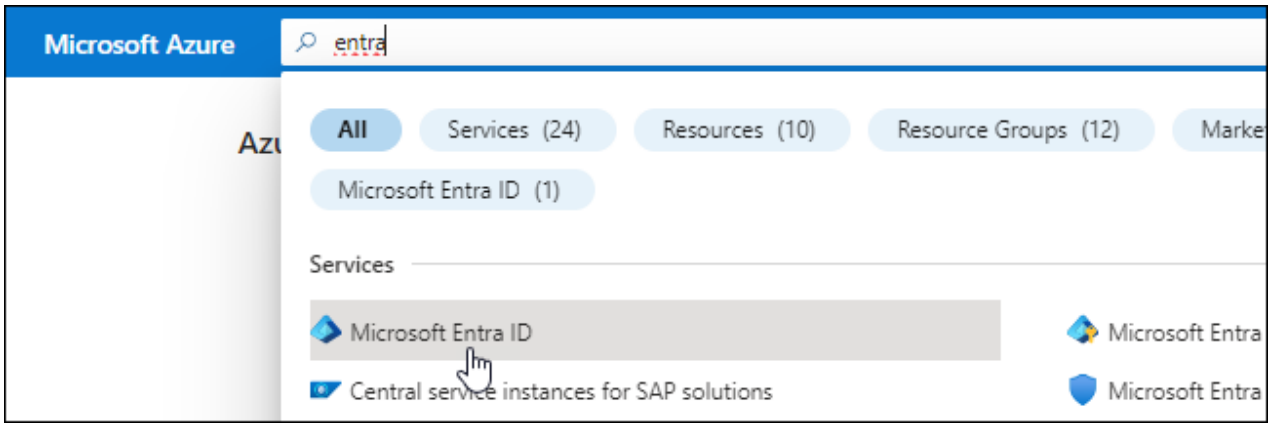
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie alla console. Dopo aver installato l'agente Console, è necessario fornire queste credenziali alla Console.

Creare un'applicazione Microsoft Entra per il controllo degli accessi basato sui ruoli

1. Assicurati di disporre delle autorizzazioni in Azure per creare un'applicazione Active Directory e per assegnare l'applicazione a un ruolo.

   Per i dettagli, fare riferimento a "Documentazione di Microsoft Azure: autorizzazioni richieste"

2. Dal portale di Azure, aprire il servizio **Microsoft Entra ID**.



3. Nel menu, seleziona **Registrazioni app**.
4. Selezionare **Nuova registrazione**.
5. Specificare i dettagli sull'applicazione:

- **Nome**: inserisci un nome per l'applicazione.
- **Tipo di account**: seleziona un tipo di account (qualsiasi funzionerà con la NetApp Console).
- **URI di reindirizzamento**: puoi lasciare vuoto questo campo.

6. Seleziona **Registrati**.

   Hai creato l'applicazione AD e il servizio principale.

Assegnare l'applicazione a un ruolo

1. Crea un ruolo personalizzato:

   Tieni presente che puoi creare un ruolo personalizzato di Azure tramite il portale di Azure, Azure PowerShell, Azure CLI o REST API. I passaggi seguenti mostrano come creare il ruolo utilizzando l'interfaccia della riga di comando di Azure. Se preferisci utilizzare un metodo diverso, fai riferimento a "Documentazione di Azure"

   a. Copia il contenuto del"autorizzazioni di ruolo personalizzate per l'agente della console" e salvarli in un file JSON.

   b. Modificare il file JSON aggiungendo gli ID di sottoscrizione di Azure all'ambito assegnabile.

      È necessario aggiungere l'ID per ogni sottoscrizione di Azure da cui gli utenti creeranno i sistemi Cloud Volumes ONTAP .

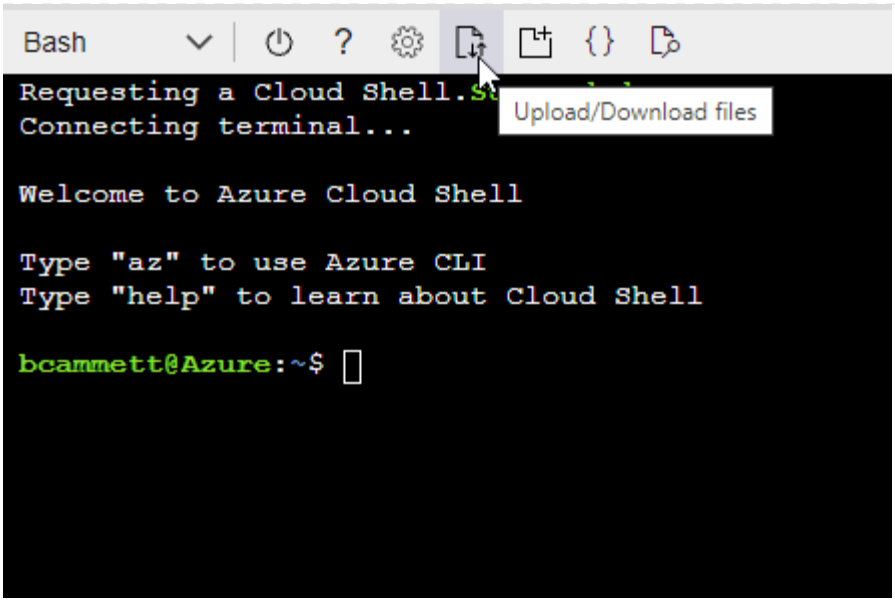
      Esempio

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ]
      ```

   c. Utilizzare il file JSON per creare un ruolo personalizzato in Azure.

      I passaggi seguenti descrivono come creare il ruolo utilizzando Bash in Azure Cloud Shell.

      - Inizio "Azure Cloud Shell" e scegli l'ambiente Bash.
      - Carica il file JSON.



- Utilizzare l'interfaccia della riga di comando di Azure per creare il ruolo personalizzato:

```
az role definition create --role-definition agent_Policy.json
```

Ora dovresti avere un ruolo personalizzato denominato Operatore Console che puoi assegnare alla macchina virtuale dell'agente Console.

2. Assegnare l'applicazione al ruolo:

   a. Dal portale di Azure, aprire il servizio **Sottoscrizioni**.

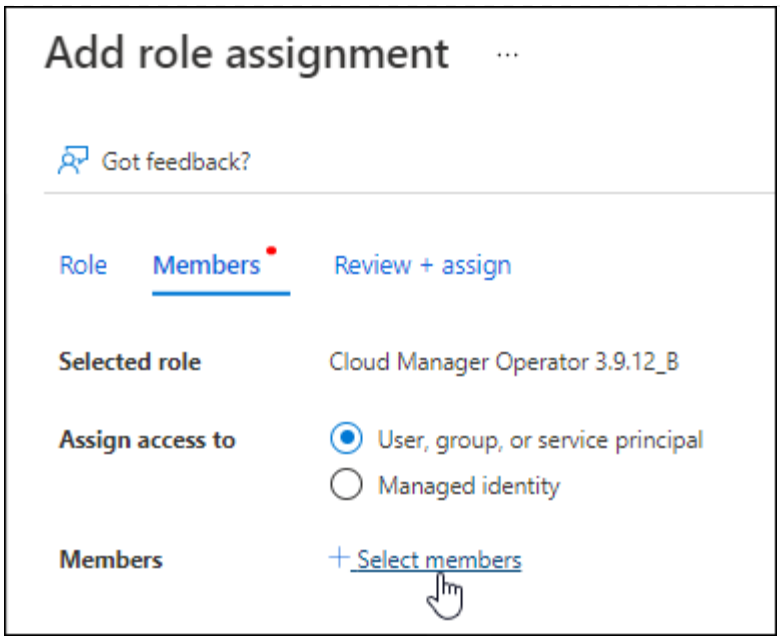
   b. Seleziona l'abbonamento.

   c. Selezionare **Controllo accessi (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.

   d. Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.

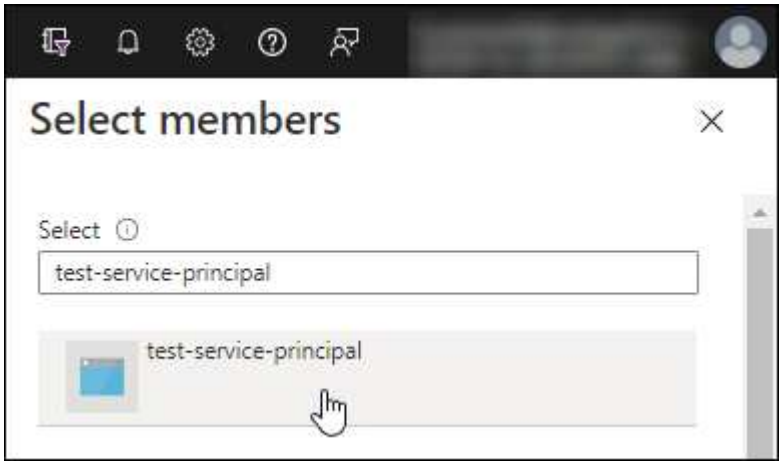
   e. Nella scheda **Membri**, completa i seguenti passaggi:

      - Mantieni selezionato **Utente, gruppo o entità servizio**.
      - Seleziona **Seleziona membri**.



- Cerca il nome dell'applicazione.

  Ecco un esempio:



- Selezionare l'applicazione e fare clic su **Seleziona**.
- Selezionare **Avanti**.

f. Seleziona **Revisiona + assegna**.

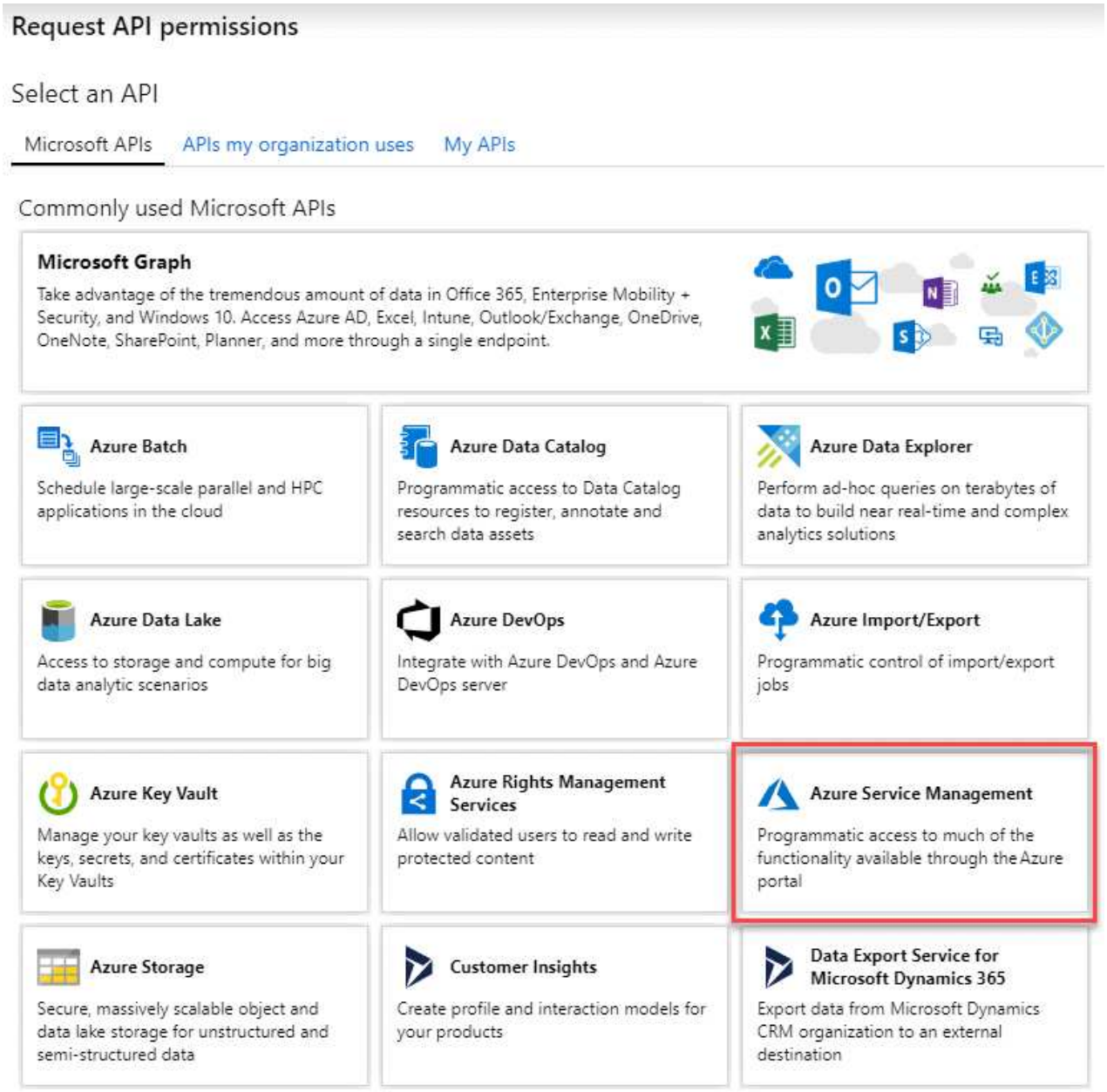
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

Se si desidera distribuire Cloud Volumes ONTAP da più sottoscrizioni di Azure, è necessario associare l'entità servizio a ciascuna di tali sottoscrizioni. Nella NetApp Console, puoi selezionare l'abbonamento che desideri utilizzare durante la distribuzione Cloud Volumes ONTAP.

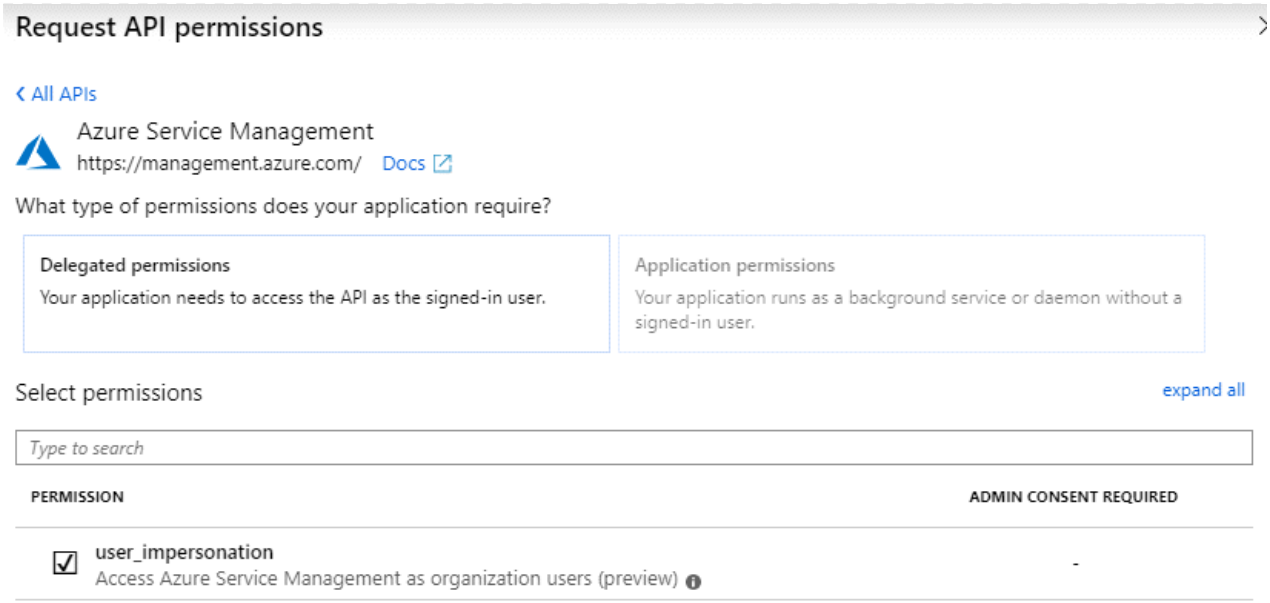
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Selezionare **Autorizzazioni API > Aggiungi un'autorizzazione**.

3. In **API Microsoft**, seleziona **Azure Service Management**.

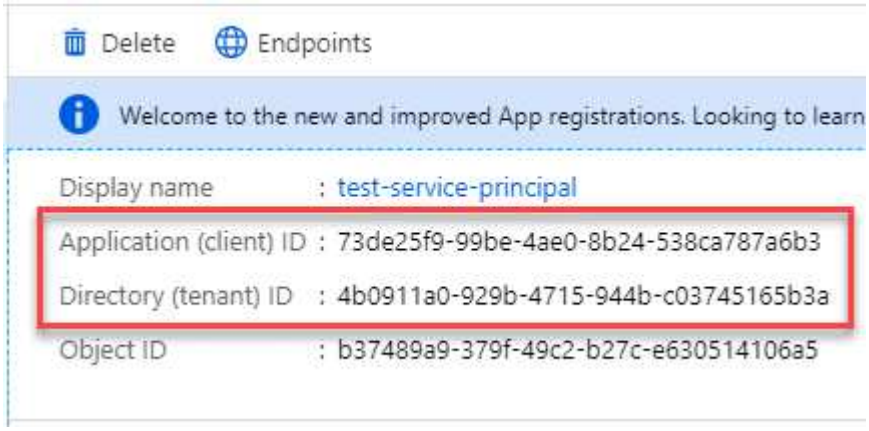


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



Ottieni l'ID dell'applicazione e l'ID della directory per l'applicazione

1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)**.



Quando si aggiunge l'account Azure alla console, è necessario fornire l'ID dell'applicazione (client) e l'ID della directory (tenant) per l'applicazione. La console utilizza gli ID per effettuare l'accesso in modo programmatico.

Crea un segreto client

1. Aprire il servizio **Microsoft Entra ID**.
2. Seleziona **Registrazioni app** e seleziona la tua applicazione.
3. Selezionare **Certificati e segreti > Nuovo segreto client**.
4. Fornire una descrizione del segreto e una durata.
5. Selezionare **Aggiungi**.
6. Copia il valore del segreto client.

Risultato

Il tuo service principal è ora configurato e dovresti aver copiato l'ID dell'applicazione (client), l'ID della directory (tenant) e il valore del segreto client. Quando si aggiunge un account Azure, è necessario immettere queste informazioni nella Console.

Account di servizio Google Cloud

Crea un ruolo e applicalo a un account di servizio che utilizzerai per l'istanza della VM dell'agente Console.

Passi

1. Crea un ruolo personalizzato in Google Cloud:

   a. Creare un file YAML che includa le autorizzazioni definite in"Criterio dell'agente della console per Google Cloud" .

   b. Da Google Cloud, attiva Cloud Shell.

   c. Carica il file YAML che include le autorizzazioni richieste per l'agente della console.

   d. Crea un ruolo personalizzato utilizzando `gcloud iam roles create` comando.

      L'esempio seguente crea un ruolo denominato "agente" a livello di progetto:

```
gcloud iam roles create agent --project=myproject --file=agent.yaml
```

   +
   "Documentazione di Google Cloud: creazione e gestione di ruoli personalizzati"

2. Crea un account di servizio in Google Cloud:

   a. Dal servizio IAM e amministrazione, seleziona **Account di servizio > Crea account di servizio**.

   b. Inserisci i dettagli dell'account di servizio e seleziona **Crea e continua**.

   c. Seleziona il ruolo che hai appena creato.

   d. Completa i passaggi rimanenti per creare il ruolo.

      "Documentazione di Google Cloud: creazione di un account di servizio"

Passaggio 7: abilita le API di Google Cloud

Per distribuire Cloud Volumes ONTAP in Google Cloud sono necessarie diverse API.

Fare un passo

1. "Abilita le seguenti API di Google Cloud nel tuo progetto"
    - API di Cloud Infrastructure Manager
    - API di Cloud Deployment Manager V2
    - API di registrazione cloud
    - API di Cloud Resource Manager
    - API di Compute Engine
    - API di gestione dell'identità e dell'accesso (IAM)
    - API del servizio di gestione delle chiavi cloud (KMS)

      (Obbligatorio solo se si prevede di utilizzare NetApp Backup and Recovery con chiavi di crittografia gestite dal cliente (CMEK))

Distribuisci l'agente della console in modalità limitata

Distribuisci l'agente Console in modalità limitata in modo da poter utilizzare la NetApp Console con connettività in uscita limitata. Per iniziare, installa l'agente Console, configura la Console accedendo all'interfaccia utente in esecuzione sull'agente Console, quindi fornisci le autorizzazioni cloud configurate in precedenza.

Passaggio 1: installare l'agente della console

Installa l'agente Console dal marketplace del tuo provider cloud oppure manualmente su un host Linux.

Prima di installare l'agente Console, è necessario preparare l'ambiente. Puoi eseguire l'installazione da AWS Marketplace, da Azure Marketplace o manualmente sul tuo host Linux in esecuzione su AWS, Azure o Google Cloud.

AWS Commercial Marketplace

Prima di iniziare

Avere quanto segue:

- Una VPC e una subnet che soddisfano i requisiti di rete.

  "Scopri i requisiti di rete"

- Un ruolo IAM con una policy associata che include le autorizzazioni richieste per l'agente della console.

  "Scopri come impostare le autorizzazioni AWS"

- Autorizzazioni per iscriversi e annullare l'iscrizione ad AWS Marketplace per il tuo utente IAM.
- Conoscenza dei requisiti di CPU e RAM per l'agente.

  "Requisiti dell'agente di revisione".

- Una coppia di chiavi per l'istanza EC2.

Passi

1. Vai al "Elenco degli agenti NetApp Console su AWS Marketplace"
2. Nella pagina Marketplace, seleziona **Continua ad abbonarti**.
3. Per abbonarsi al software, selezionare **Accetta i termini**.

   Il processo di iscrizione può richiedere alcuni minuti.

4. Una volta completato il processo di sottoscrizione, seleziona **Continua alla configurazione**.
5. Nella pagina **Configura questo software**, assicurati di aver selezionato la regione corretta, quindi seleziona **Continua per avviare**.
6. Nella pagina **Avvia questo software**, in **Scegli azione**, seleziona **Avvia tramite EC2** e poi seleziona **Avvia**.

   Utilizzare la console EC2 per avviare l'istanza e associare un ruolo IAM. Ciò non è possibile con l'azione **Avvia dal sito Web**.

7. Seguire le istruzioni per configurare e distribuire l'istanza:
   - **Nome e tag**: inserisci un nome e dei tag per l'istanza.
   - **Immagini dell'applicazione e del sistema operativo**: saltare questa sezione. L'AMI dell'agente Console è già selezionata.
   - **Tipo di istanza**: a seconda della disponibilità regionale, scegli un tipo di istanza che soddisfi i requisiti di RAM e CPU (t3.2xlarge è preselezionato e consigliato).
   - **Coppia di chiavi (accesso)**: seleziona la coppia di chiavi che desideri utilizzare per connetterti in modo sicuro all'istanza.
   - **Impostazioni di rete**: modifica le impostazioni di rete secondo necessità:
     - Selezionare la VPC e la subnet desiderate.
     - Specificare se l'istanza deve avere un indirizzo IP pubblico.

        - Specificare le impostazioni del gruppo di sicurezza che abilitano i metodi di connessione richiesti per l'istanza dell'agente Console: SSH, HTTP e HTTPS.

          "Visualizza le regole del gruppo di sicurezza per AWS" .

    - **Configura archiviazione**: mantieni le dimensioni e il tipo di disco predefiniti per il volume root.

      Se si desidera abilitare la crittografia Amazon EBS sul volume root, selezionare **Avanzate**, espandere **Volume 1**, selezionare **Crittografato** e quindi scegliere una chiave KMS.

    - **Dettagli avanzati**: in **Profilo istanza IAM**, seleziona il ruolo IAM che include le autorizzazioni richieste per l'agente della console.
    - **Riepilogo**: rivedere il riepilogo e selezionare **Avvia istanza**.

Risultato

AWS avvia il software con le impostazioni specificate. L'agente Console viene distribuito in circa cinque minuti.

Cosa succederà ora?

Configurare la NetApp Console.

AWS Gov Marketplace

Prima di iniziare

Avere quanto segue:

- Una VPC e una subnet che soddisfano i requisiti di rete.

  "Scopri i requisiti di rete"

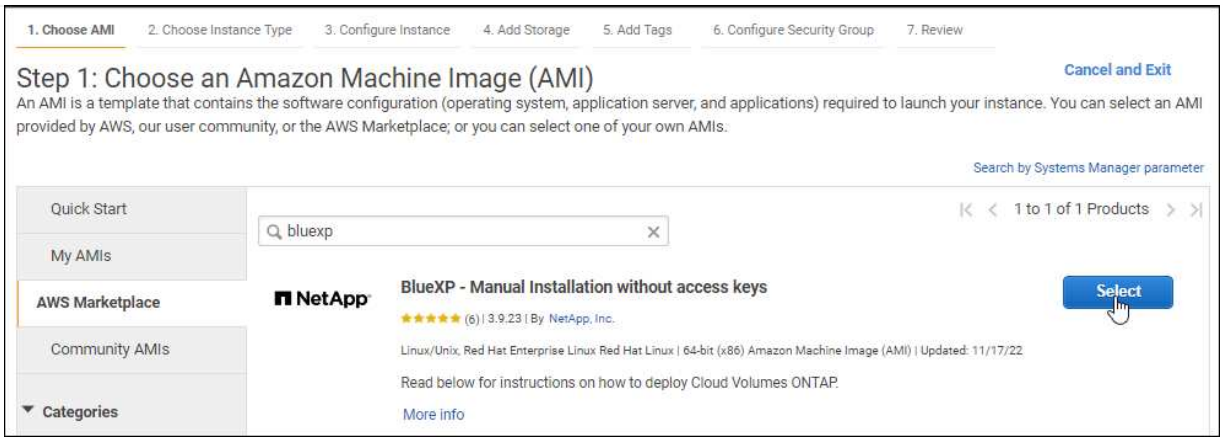
- Un ruolo IAM con una policy associata che include le autorizzazioni richieste per l'agente della console.

  "Scopri come impostare le autorizzazioni AWS"

- Autorizzazioni per iscriversi e annullare l'iscrizione ad AWS Marketplace per il tuo utente IAM.
- Una coppia di chiavi per l'istanza EC2.

Passi

1. Vai all'offerta dell'agente NetApp Console in AWS Marketplace.
    a. Aprire il servizio EC2 e selezionare **Avvia istanza**.
    b. Seleziona **AWS Marketplace**.
    c. Cerca NetApp Console e seleziona l'offerta.



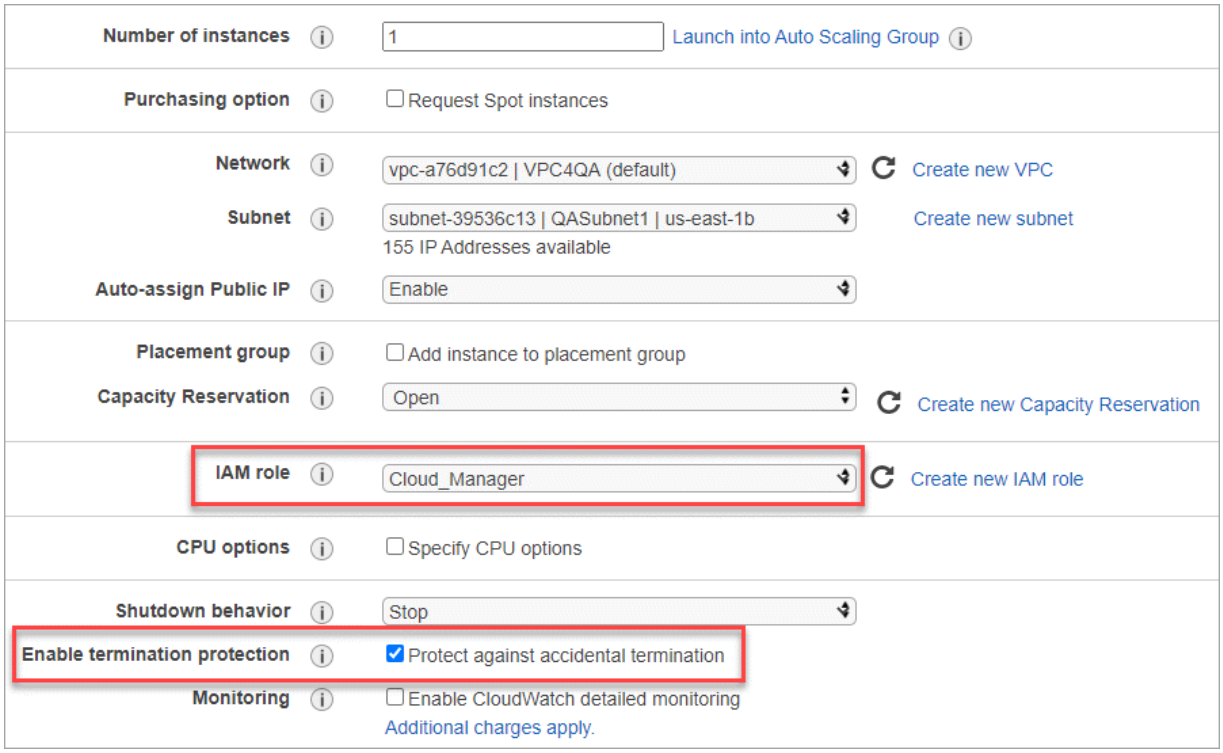
d. Selezionare **Continua**.

2. Segui le istruzioni per configurare e avviare l'istanza:

   - **Scegli un tipo di istanza**: a seconda della disponibilità nella regione, scegli uno dei tipi di istanza supportati (si consiglia t3.2xlarge).

     "Esaminare i requisiti dell'istanza" .

   - **Configura i dettagli dell'istanza**: seleziona una VPC e una subnet, scegli il ruolo IAM creato nel passaggio 1, abilita la protezione dalla terminazione (consigliato) e scegli qualsiasi altra opzione di configurazione che soddisfi i tuoi requisiti.



   - **Aggiungi spazio di archiviazione**: mantieni le opzioni di archiviazione predefinite.
   - **Aggiungi tag**: se lo desideri, inserisci i tag per l'istanza.
   - **Configura gruppo di sicurezza**: specifica i metodi di connessione richiesti per l'istanza dell'agente Console: SSH, HTTP e HTTPS.
   - **Revisione**: rivedi le tue selezioni e seleziona **Avvia**.

Risultato

AWS avvia il software con le impostazioni specificate. L'agente Console viene distribuito in circa cinque minuti.

Cosa succederà ora?

Configurare la console.

Azure Gov Marketplace

Prima di iniziare

Dovresti avere quanto segue:

- Una rete virtuale e una sottorete che soddisfano i requisiti di rete.

  "Scopri i requisiti di rete"

- Un ruolo personalizzato di Azure che include le autorizzazioni richieste per l'agente della console.

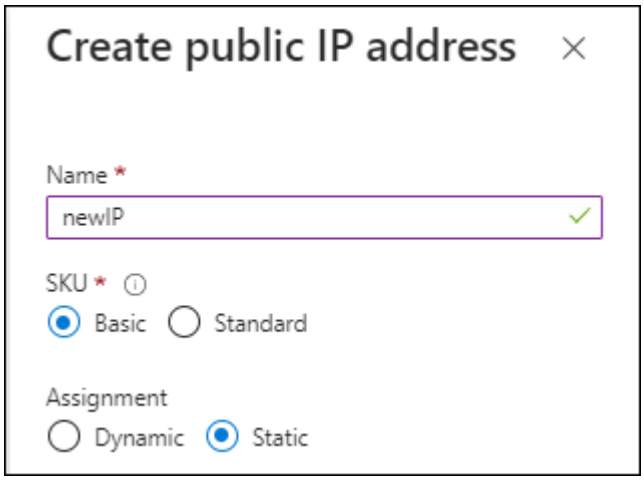
  "Scopri come configurare le autorizzazioni di Azure"

Passi

1. Vai alla pagina della macchina virtuale dell'agente NetApp Console in Azure Marketplace.
   - "Pagina di Azure Marketplace per le regioni commerciali"
   - "Pagina di Azure Marketplace per le regioni di Azure Government"
2. Seleziona **Ottienilo ora** e poi seleziona **Continua**.
3. Dal portale di Azure, seleziona **Crea** e segui i passaggi per configurare la macchina virtuale.

   Durante la configurazione della VM, tenere presente quanto segue:

   - **Dimensioni VM**: scegli una dimensione VM che soddisfi i requisiti di CPU e RAM. Consigliamo Standard_D8s_v3.
   - **Dischi**: l'agente Console può funzionare in modo ottimale sia con dischi HDD che SSD.
   - **IP pubblico**: per utilizzare un indirizzo IP pubblico con la VM dell'agente Console, selezionare uno SKU di base.

     Se invece si utilizza un indirizzo IP SKU standard, la Console utilizza l'indirizzo IP *privato* dell'agente della Console, anziché l'IP pubblico. Se il computer utilizzato per accedere alla

Console non riesce a raggiungere l'indirizzo IP privato, la Console non funziona.

"Documentazione di Azure: SKU IP pubblico"

- **Gruppo di sicurezza di rete**: l'agente della console richiede connessioni in entrata tramite SSH, HTTP e HTTPS.

  "Visualizza le regole del gruppo di sicurezza per Azure" .

- **Identità**: in **Gestione**, seleziona **Abilita identità gestita assegnata dal sistema**.

  Un'identità gestita consente alla macchina virtuale dell'agente della console di identificarsi con l'ID Microsoft Entra senza credenziali. "Scopri di più sulle identità gestite per le risorse di Azure" .

4. Nella pagina **Revisiona + crea**, rivedi le tue selezioni e seleziona **Crea** per avviare la distribuzione.

Risultato

Azure distribuisce la macchina virtuale con le impostazioni specificate. La macchina virtuale e il software dell'agente della console dovrebbero essere in esecuzione entro circa cinque minuti.

Cosa succederà ora?

Configurare la NetApp Console.

Installazione manuale (obbligatoria per Google Cloud)

Puoi installare manualmente l'agente Console sul tuo host Linux in esecuzione su AWS, Azure o Google Cloud.

Prima di iniziare

Dovresti avere quanto segue:

- Privilegi di root per installare l'agente Console.
- Dettagli su un server proxy, se è necessario un proxy per l'accesso a Internet dall'agente della console.

  Dopo l'installazione è possibile configurare un server proxy, ma per farlo è necessario riavviare l'agente della console.

- Un certificato firmato da una CA, se il server proxy utilizza HTTPS o se il proxy è un proxy di intercettazione.

  Non è possibile impostare un certificato per un server proxy trasparente durante l'installazione manuale dell'agente Console. Se è necessario impostare un certificato per un server proxy trasparente, è necessario utilizzare la Console di manutenzione dopo l'installazione. Scopri di più su"Console di manutenzione dell'agente" .

- È necessario disattivare il controllo della configurazione che verifica la connettività in uscita durante l'installazione. L'installazione manuale fallisce se questo controllo non è disabilitato."Scopri come disattivare i controlli di configurazione per le installazioni manuali."
- A seconda del sistema operativo in uso, prima di installare l'agente Console è necessario utilizzare Podman o Docker Engine.

Informazioni su questo compito

Dopo l'installazione, l'agente Console si aggiorna automaticamente se è disponibile una nuova versione.

Passi

1. Se le variabili di sistema *http_proxy* o *https_proxy* sono impostate sull'host, rimuoverle:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Se non si rimuovono queste variabili di sistema, l'installazione fallirà.

2. Scaricare il software dell'agente Console e copiarlo sull'host Linux. È possibile scaricarlo dalla NetApp Console o dal sito di supporto NetApp .
   - NetApp Console: vai su **Agenti > Gestione > Distribuisci agente > On-prem > Installazione manuale**.

     Scegli di scaricare i file di installazione dell'agente o un URL ai file.

   - Sito di supporto NetApp (necessario se non si ha già accesso alla console) "Sito di supporto NetApp" ,
3. Assegnare le autorizzazioni per eseguire lo script.

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

   Dove <versione> è la versione dell'agente Console scaricato.

4. Se si esegue l'installazione in un ambiente Government Cloud, disattivare i controlli di configurazione."Scopri come disattivare i controlli di configurazione per le installazioni manuali."
5. Eseguire lo script di installazione.

   ```
   ./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
   server> --cacert <path and file name of a CA-signed certificate>
   ```

   Sarà necessario aggiungere le informazioni sul proxy se la rete richiede un proxy per l'accesso a Internet. È possibile aggiungere un proxy esplicito durante l'installazione. I parametri `--proxy` e `--cacert` sono facoltativi e non verrà richiesto di aggiungerli. Se si dispone di un proxy server esplicito, sarà necessario immettere i parametri come mostrato.

   Se vuoi configurare un proxy trasparente, puoi farlo dopo l'installazione. "Scopri di più sulla console di manutenzione dell'agente"

+

Ecco un esempio di configurazione di un server proxy esplicito con un certificato firmato da una CA:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

+
`--proxy` configura l'agente Console per utilizzare un proxy server utilizzando uno dei seguenti formati:

+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-name:password@address:port * https://address:port * https://user-name:password@address:port * https://domain-name%92user-name:password@address:port

+ Nota quanto segue:

+ **L'utente può essere un utente locale o un utente di dominio.** Per un utente di dominio, è necessario utilizzare il codice ASCII per una \ come mostrato sopra. **L'agente Console non supporta nomi utente o password che includono il carattere @.** Se la password include uno dei seguenti caratteri speciali, è necessario eseguire l'escape di quel carattere speciale anteponendo una barra rovesciata: & o !

+ Ad esempio:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Se hai utilizzato Podman, dovrai modificare la porta aardvark-dns.
   a. Eseguire l'SSH sulla macchina virtuale dell'agente Console.
   b. Aprire il file podman */usr/share/containers/containers.conf* e modificare la porta scelta per il servizio DNS Aardvark. Ad esempio, cambialo in 54.

      ```
      vi /usr/share/containers/containers.conf
      ```

      Per esempio:

      ```
      # Port to use for dns forwarding daemon with netavark in rootful
      bridge
      # mode and dns enabled.
      # Using an alternate port might be useful if other DNS services
      should
      # run on the machine.
      #
      dns_bind_port = 54
      ```

   a. Riavviare la macchina virtuale dell'agente Console.

Risultato

L'agente Console è ora installato. Al termine dell'installazione, il servizio agente della console (occm) viene riavviato due volte se è stato specificato un server proxy.

Cosa succederà ora?

Configurare la NetApp Console.

Passaggio 2: configurare NetApp Console

Quando si accede alla console per la prima volta, viene richiesto di scegliere un'organizzazione per l'agente della console e di abilitare la modalità con restrizioni.

Prima di iniziare

La persona che configura l'agente della Console deve accedere alla Console utilizzando un account di accesso che non appartenga già a un'organizzazione della Console.

Se il tuo login è associato a un'altra organizzazione, dovrai registrarti con un nuovo login. Altrimenti, non vedrai l'opzione per abilitare la modalità limitata nella schermata di configurazione.

Passi

1. Aprire un browser Web da un host che dispone di una connessione all'istanza dell'agente Console e immettere il seguente URL dell'agente Console installato.
2. Registrati o accedi alla NetApp Console.
3. Dopo aver effettuato l'accesso, configura la Console:

    a. Immettere un nome per l'agente della console.

    b. Immettere un nome per una nuova organizzazione della Console.

    c. Seleziona **Stai lavorando in un ambiente protetto?**

    d. Seleziona **Abilita la modalità con restrizioni su questo account**.

    Tieni presente che non puoi modificare questa impostazione dopo aver creato l'account. Non potrai abilitare la modalità con restrizioni in un secondo momento, né potrai disabilitarla in un secondo momento.

    Se hai distribuito l'agente Console in una regione governativa, la casella di controllo è già abilitata e non può essere modificata. Questo perché la modalità limitata è l'unica supportata nelle regioni governative.

    a. Seleziona **Iniziamo**.

Risultato

L'agente Console è ora installato e configurato con la tua organizzazione Console. Tutti gli utenti devono accedere alla Console utilizzando l'indirizzo IP dell'istanza dell'agente della Console.

Cosa succederà ora?

Fornisci alla Console le autorizzazioni precedentemente impostate.

Passaggio 3: fornire le autorizzazioni all'agente della console

Se hai installato l'agente Console da Azure Marketplace o manualmente, devi concedere le autorizzazioni impostate in precedenza.

Questi passaggi non si applicano se hai distribuito l'agente della console da AWS Marketplace perché hai scelto il ruolo IAM richiesto durante la distribuzione.

"Scopri come preparare le autorizzazioni cloud" .

Ruolo AWS IAM

Collega il ruolo IAM creato in precedenza all'istanza EC2 in cui hai installato l'agente Console.

Questi passaggi sono validi solo se hai installato manualmente l'agente Console in AWS. Per le distribuzioni di AWS Marketplace, hai già associato l'istanza dell'agente della console a un ruolo IAM che include le autorizzazioni richieste.

Passi

1. Vai alla console Amazon EC2.
2. Selezionare **Istanze**.
3. Selezionare l'istanza dell'agente Console.
4. Selezionare **Azioni > Sicurezza > Modifica ruolo IAM**.
5. Selezionare il ruolo IAM e selezionare **Aggiorna ruolo IAM**.

Chiave di accesso AWS

Fornire alla NetApp Console la chiave di accesso AWS per un utente IAM che dispone delle autorizzazioni richieste.

Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Selezionare **Credenziali dell'organizzazione**.
3. Selezionare **Aggiungi credenziali** e seguire i passaggi della procedura guidata.
   a. **Posizione delle credenziali**: seleziona *Amazon Web Services > Agente.
   b. **Definisci credenziali**: inserisci una chiave di accesso AWS e una chiave segreta.
   c. **Abbonamento Marketplace**: associa un abbonamento Marketplace a queste credenziali abbonandoti ora o selezionando un abbonamento esistente.
   d. **Revisione**: conferma i dettagli sulle nuove credenziali e seleziona **Aggiungi**.

Ruolo di Azure

Accedere al portale di Azure e assegnare il ruolo personalizzato di Azure alla macchina virtuale dell'agente della console per una o più sottoscrizioni.

Passi

1. Dal portale di Azure, apri il servizio **Sottoscrizioni** e seleziona la tua sottoscrizione.

   È importante assegnare il ruolo dal servizio **Abbonamenti** perché questo specifica l'ambito dell'assegnazione del ruolo a livello di abbonamento. L'*ambito* definisce l'insieme di risorse a cui si applica l'accesso. Se si specifica un ambito a un livello diverso (ad esempio, a livello di macchina virtuale), la possibilità di completare azioni dall'interno della NetApp Console ne risentirà.

   "Documentazione di Microsoft Azure: comprendere l'ambito di Azure RBAC"

2. Selezionare **Controllo accessi (IAM)** > **Aggiungi** > **Aggiungi assegnazione ruolo**.
3. Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.

   Console Operator è il nome predefinito fornito nel criterio. Se hai scelto un nome diverso per il ruolo, seleziona quel nome.

4. Nella scheda **Membri**, completa i seguenti passaggi:
    a. Assegna l'accesso a un'**identità gestita**.
    b. Selezionare **Seleziona membri**, selezionare l'abbonamento in cui è stata creata la macchina virtuale dell'agente Console, in **Identità gestita**, scegliere **Macchina virtuale**, quindi selezionare la macchina virtuale dell'agente Console.
    c. Seleziona **Seleziona**.
    d. Selezionare **Avanti**.
    e. Seleziona **Revisiona + assegna**.
    f. Se si desidera gestire risorse in sottoscrizioni Azure aggiuntive, passare a tale sottoscrizione e ripetere questi passaggi.

Entità del servizio di Azure

Fornire alla NetApp Console le credenziali per l'entità servizio di Azure configurata in precedenza.

Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Selezionare **Aggiungi credenziali** e seguire i passaggi della procedura guidata.
    a. **Posizione delle credenziali**: selezionare **Microsoft Azure > Agente**.
    b. **Definisci credenziali**: immetti le informazioni sull'entità servizio Microsoft Entra che concede le autorizzazioni richieste:
        - ID applicazione (client)
        - ID directory (tenant)
        - Segreto del cliente
    c. **Abbonamento Marketplace**: associa un abbonamento Marketplace a queste credenziali abbonandoti ora o selezionando un abbonamento esistente.
    d. **Revisione**: conferma i dettagli sulle nuove credenziali e seleziona **Aggiungi**.

Risultato

la NetApp Console ora dispone delle autorizzazioni necessarie per eseguire azioni in Azure per tuo conto.

Account di servizio Google Cloud

Associare l'account di servizio alla VM dell'agente Console.

Passi

1. Vai al portale di Google Cloud e assegna l'account di servizio all'istanza VM dell'agente Console.

    "Documentazione di Google Cloud: modifica dell'account di servizio e degli ambiti di accesso per un'istanza"

2. Se si desidera gestire le risorse in altri progetti, concedere l'accesso aggiungendo l'account di servizio con il ruolo di agente della console a quel progetto. Sarà necessario ripetere questo passaggio per ogni progetto.

Iscriviti a NetApp Intelligent Services (modalità limitata)

Abbonati a NetApp Intelligent Services dal marketplace del tuo provider cloud per pagare i servizi dati a una tariffa oraria (PAYGO) o tramite un contratto annuale. Se hai acquistato una licenza da NetApp (BYOL), devi anche abbonarti all'offerta del marketplace. L'addebito avviene sempre per primo sulla tua licenza, ma ti verrà addebitata la tariffa oraria se superi la capacità consentita o se scade il termine della licenza.

Un abbonamento al marketplace consente di addebitare i seguenti servizi dati con modalità limitata:

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification è abilitato tramite l'abbonamento, ma l'utilizzo della classificazione è gratuito.

Prima di iniziare

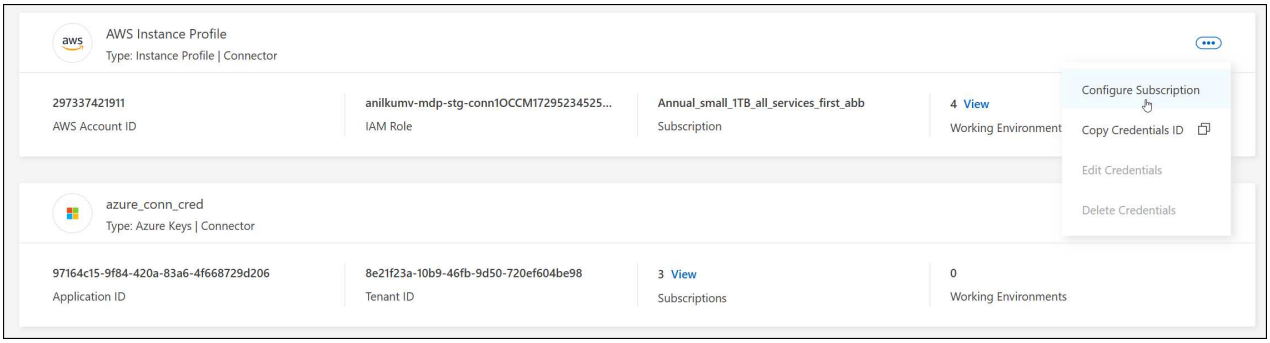
Per potersi iscrivere ai servizi dati, è necessario aver già distribuito un agente Console. È necessario associare un abbonamento al marketplace alle credenziali cloud connesse a un agente della console.

AWS

Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Selezionare **Credenziali dell'organizzazione**.
3. Selezionare il menu azioni per un set di credenziali associate a un agente della console, quindi selezionare **Configura abbonamento**.

   È necessario selezionare le credenziali associate a un agente Console. Non è possibile associare un abbonamento al marketplace alle credenziali associate alla NetApp Console.



4. Per associare le credenziali a un abbonamento esistente, seleziona l'abbonamento dall'elenco a discesa e seleziona **Configura**.
5. Per associare le credenziali a un nuovo abbonamento, seleziona **Aggiungi abbonamento > Continua** e segui i passaggi indicati in AWS Marketplace:

   a. Seleziona **Visualizza opzioni di acquisto**.

   b. Seleziona **Iscriviti**.

   c. Seleziona **Configura il tuo account**.

      Verrai reindirizzato alla NetApp Console.

   d. Dalla pagina **Assegnazione abbonamento**:

      - Seleziona le organizzazioni o gli account della Console a cui desideri associare questo abbonamento.
      - Nel campo **Sostituisci abbonamento esistente**, scegli se desideri sostituire automaticamente l'abbonamento esistente per un'organizzazione o un account con questo nuovo abbonamento.

        La Console sostituisce l'abbonamento esistente per tutte le credenziali nell'organizzazione o nell'account con questo nuovo abbonamento. Se un set di credenziali non è mai stato associato a un abbonamento, questo nuovo abbonamento non sarà associato a tali credenziali.

   Per tutte le altre organizzazioni o account, sarà necessario associare manualmente l'abbonamento ripetendo questi passaggi.

   ◦ Seleziona **Salva**.

Azzurro

Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Selezionare **Credenziali dell'organizzazione**.
3. Selezionare il menu azioni per un set di credenziali associate a un agente della console, quindi selezionare **Configura abbonamento**.

   È necessario selezionare le credenziali associate a un agente Console. Non è possibile associare un abbonamento al marketplace alle credenziali associate alla NetApp Console.

4. Per associare le credenziali a un abbonamento esistente, seleziona l'abbonamento dall'elenco a discesa e seleziona **Configura**.
5. Per associare le credenziali a un nuovo abbonamento, seleziona **Aggiungi abbonamento > Continua** e segui i passaggi in Azure Marketplace:

   a. Se richiesto, accedi al tuo account Azure.
   b. Seleziona **Iscriviti**.
   c. Compila il modulo e seleziona **Iscriviti**.
   d. Una volta completato il processo di sottoscrizione, seleziona **Configura account ora**.

      Verrai reindirizzato alla NetApp Console.

   e. Dalla pagina **Assegnazione abbonamento**:
      - Seleziona le organizzazioni o gli account della Console a cui desideri associare questo abbonamento.
      - Nel campo **Sostituisci abbonamento esistente**, scegli se desideri sostituire automaticamente l'abbonamento esistente per un'organizzazione o un account con questo nuovo abbonamento.

        La Console sostituisce l'abbonamento esistente per tutte le credenziali nell'organizzazione o nell'account con questo nuovo abbonamento. Se un set di credenziali non è mai stato associato a un abbonamento, questo nuovo abbonamento non sarà associato a tali credenziali.

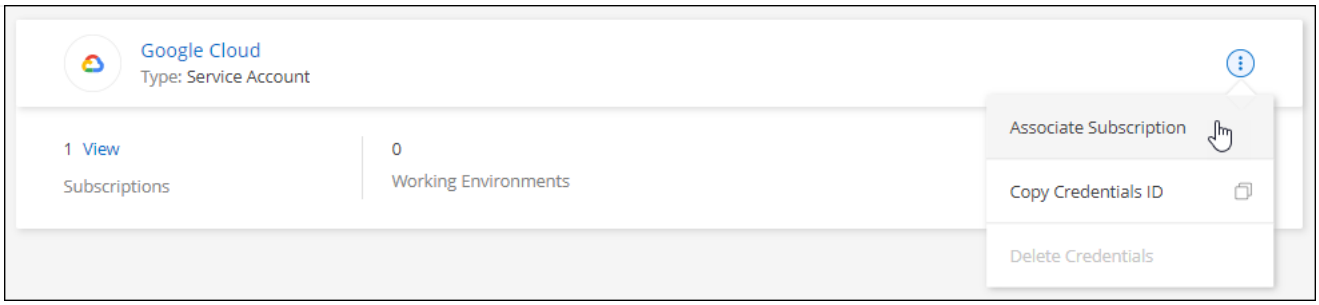
   Per tutte le altre organizzazioni o account, sarà necessario associare manualmente l'abbonamento ripetendo questi passaggi.

      ◦ Seleziona **Salva**.

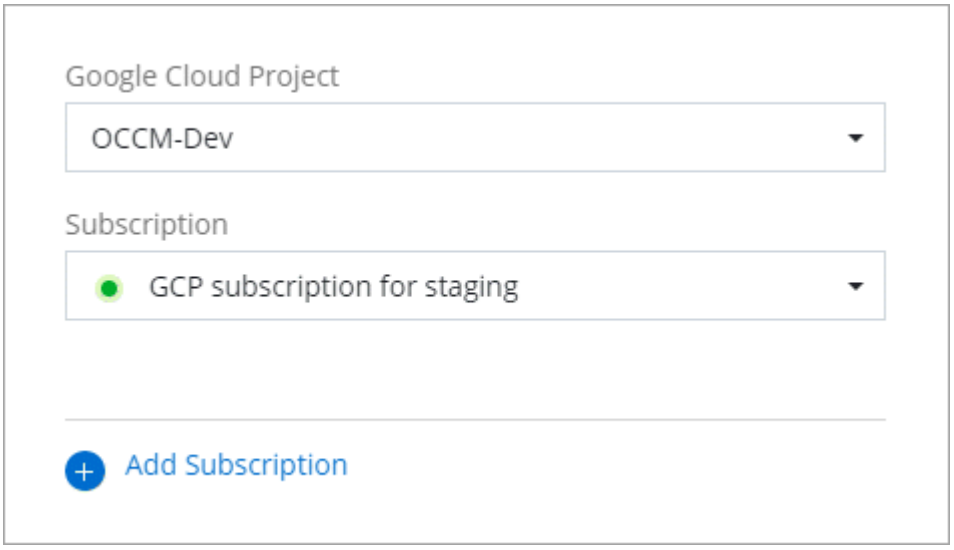
Google Cloud

Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Selezionare **Credenziali dell'organizzazione**.
3. Selezionare il menu azioni per un set di credenziali associate a un agente della console, quindi selezionare **Configura abbonamento**.



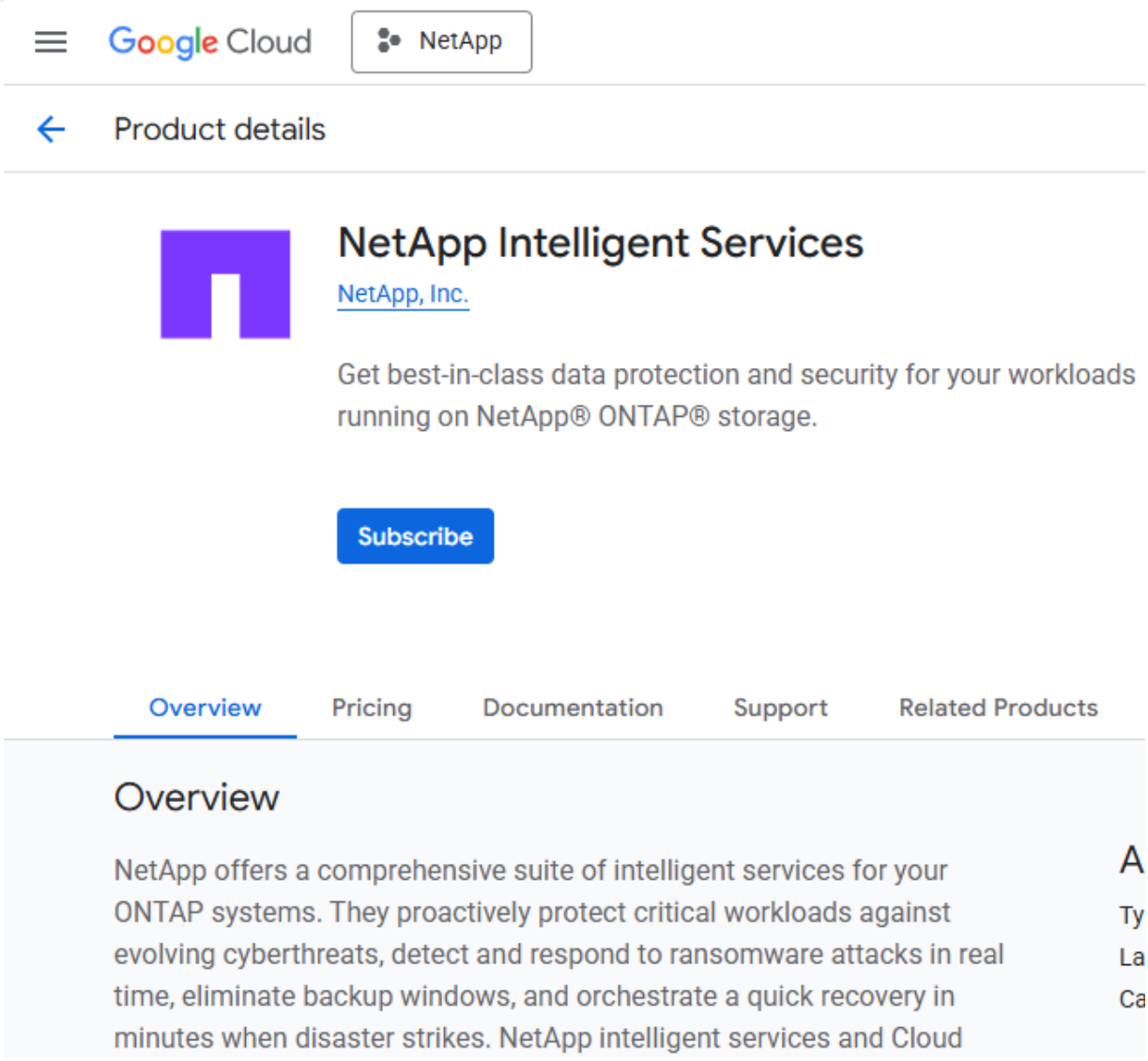
1. Per configurare un abbonamento esistente con le credenziali selezionate, seleziona un progetto Google Cloud e un abbonamento dall'elenco a discesa, quindi seleziona **Configura**.



2. Se non hai ancora un abbonamento, seleziona **Aggiungi abbonamento > Continua** e segui i passaggi indicati in Google Cloud Marketplace.

Prima di completare i passaggi seguenti, assicurati di disporre sia dei privilegi di amministratore della fatturazione nel tuo account Google Cloud sia di un accesso alla NetApp Console .

a. Dopo essere stato reindirizzato al "Pagina NetApp Intelligent Services su Google Cloud Marketplace" , assicurati che nel menu di navigazione in alto sia selezionato il progetto corretto.

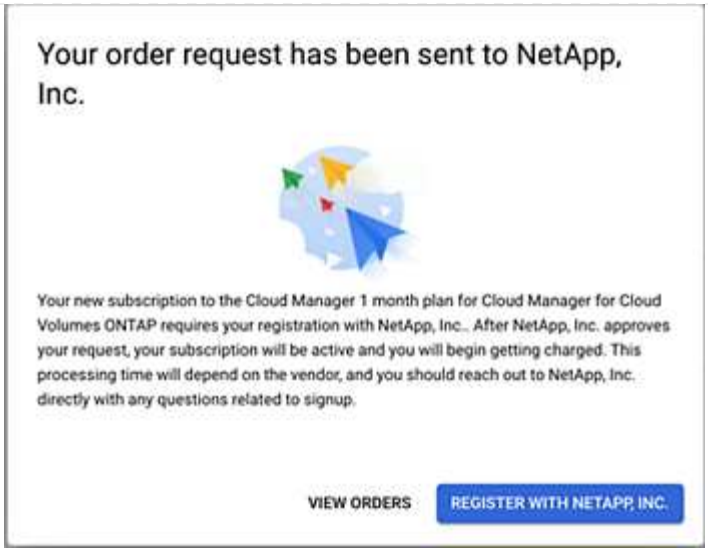


b. Seleziona **Iscriviti**.
c. Seleziona l'account di fatturazione appropriato e accetta i termini e le condizioni.
d. Seleziona **Iscriviti**.

   Questo passaggio invia la richiesta di trasferimento a NetApp.

e. Nella finestra di dialogo pop-up, seleziona **Registrati con NetApp, Inc.**

   Questo passaggio deve essere completato per collegare l'abbonamento a Google Cloud all'organizzazione o all'account della Console. Il processo di collegamento di un abbonamento non sarà completato finché non verrai reindirizzato da questa pagina e non accederai alla Console.



f. Completa i passaggi nella pagina **Assegnazione abbonamento**:

> Se qualcuno della tua organizzazione ha già un abbonamento al marketplace dal tuo account di fatturazione, verrai reindirizzato a "la pagina Cloud Volumes ONTAP nella NetApp Console" Invece. Se ciò non è previsto, contatta il team di vendita NetApp . Google consente un solo abbonamento per account di fatturazione Google.

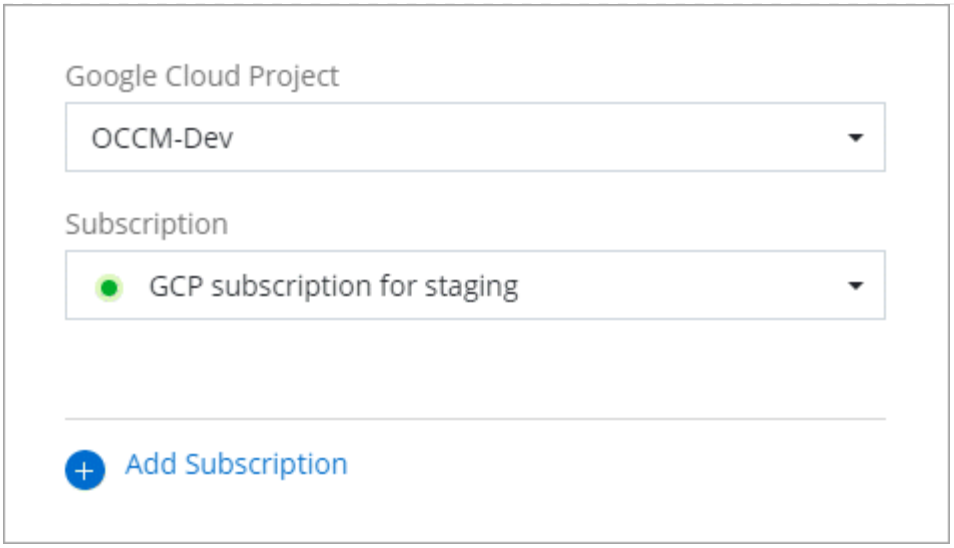
- Seleziona l'organizzazione della Console a cui desideri associare questo abbonamento.
- Nel campo **Sostituisci abbonamento esistente**, scegli se desideri sostituire automaticamente l'abbonamento esistente per un'organizzazione con questo nuovo abbonamento.

  La Console sostituisce l'abbonamento esistente per tutte le credenziali nell'organizzazione con questo nuovo abbonamento. Se un set di credenziali non è mai stato associato a un abbonamento, questo nuovo abbonamento non sarà associato a tali credenziali.

Per tutte le altre organizzazioni o account, sarà necessario associare manualmente l'abbonamento ripetendo questi passaggi.

- Seleziona **Salva**.

3. Una volta completato questo processo, torna alla pagina Credenziali nella Console e seleziona questo nuovo abbonamento.



Informazioni correlate

- "Gestisci le licenze basate sulla capacità BYOL per Cloud Volumes ONTAP"
- "Gestire le licenze BYOL per i servizi dati"
- "Gestisci le credenziali e gli abbonamenti AWS"
- "Gestisci le credenziali e gli abbonamenti di Azure"
- "Gestisci le credenziali e gli abbonamenti di Google Cloud"

Cosa puoi fare dopo (modalità limitata)

Dopo aver iniziato a utilizzare NetApp Console in modalità limitata, puoi iniziare a utilizzare i servizi supportati da tale modalità.

Per assistenza, fare riferimento alla documentazione di questi servizi:

- "Documentazione Azure NetApp Files"
- "Documenti di backup e ripristino"
- "Documenti di classificazione"
- "Documentazione Cloud Volumes ONTAP"
- "Documenti del portafoglio digitale"
- "Documentazione del cluster ONTAP locale"
- "Documenti di replicazione"

Informazioni correlate

"Modalità di distribuzione NetApp Console"

Inizia con la modalità privata

Flusso di lavoro introduttivo (modalità privata BlueXP)

La modalità privata BlueXP (interfaccia BlueXP legacy) viene in genere utilizzata con ambienti locali privi di connessione Internet e con regioni cloud sicure, tra cui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. NetApp continua a supportare questi ambienti con l'interfaccia legacy BlueXP .

"Documentazione PDF per la modalità privata BlueXP"

Funzionalità e servizi dati supportati con la modalità privata

La tabella seguente può aiutarti a identificare rapidamente quali servizi e funzionalità BlueXP sono supportati in modalità privata.

Tieni presente che alcuni servizi potrebbero essere supportati con limitazioni.

Area di prodotto	Servizio o funzionalità BlueXP	Modalità privata
Ambienti di lavoro Questa parte della tabella elenca il supporto per la gestione dell'ambiente di lavoro dalla tela BlueXP . Non indica le destinazioni di backup supportate per il BlueXP backup and recovery.	Amazon FSx per ONTAP	NO
	Amazon S3	NO
	Blob azzurro	NO
	Azure NetApp Files	NO
	Cloud Volumes ONTAP	SÌ
	Google Cloud NetApp Volumes	NO
	Google Cloud Storage	NO
	Cluster ONTAP on-premise	SÌ
	Serie E	NO
	StorageGRID	NO

Area di prodotto	Servizio o funzionalità BlueXP	Modalità privata
Servizi	Avvisi	NO
	Backup e ripristino	SÌhttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity["Visualizza l'elenco delle destinazioni di backup supportate per i dati del volume ONTAP"^]
	Classificazione	SÌ
	Copia e sincronizza	NO
	Consulente digitale	NO
	Portafoglio digitale	SÌ
	Ripristino dopo un disastro	NO
	Efficienza economica	NO
	Resilienza al ransomware	NO
	Replicazione	SÌ
	Aggiornamenti software	NO
	Sostenibilità	NO
	Livelli	NO
	Memorizzazione nella cache del volume	NO
	Fabbrica del carico di lavoro	NO
Caratteristiche	Gestione dell'identità e degli accessi	SÌ
	Credenziali	SÌ
	Federazione	NO
	Autenticazione multifattoriale	NO
	Conti NSS	NO
	Notifiche	NO
	Ricerca	NO
	Cronologia	SÌ

Informazioni sul copyright

Informazioni sul marchio commerciale