Inizia con la modalità limitata

NetApp Console setup and administration

NetApp
December 12, 2025

Sommario

Inizia con la 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" .

"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.

"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.

"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 .

Sistema operativo	Versioni del sistema operativo supportate	Versioni dell'agente supportate	Strumento contenitore richiesto	SELinux
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 .
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

Sistema operativo	Versioni del sistema operativo supportate	Versioni dell'agente supportate	Strumento contenitore richiesto	SELinux
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.

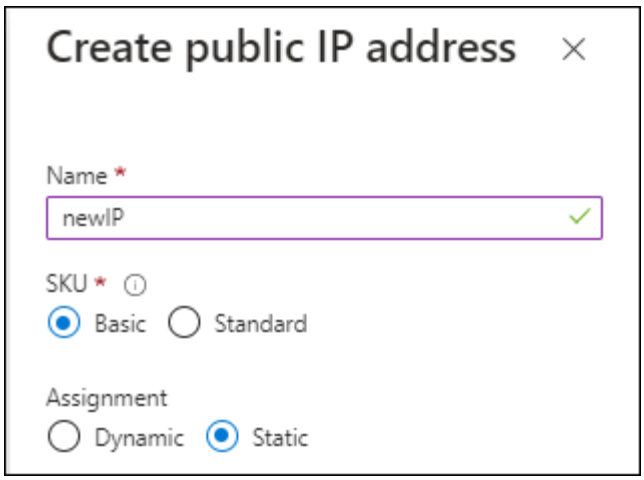
Punti finali	Scopo
Ambienti AWS	Servizi AWS (amazonaws.com): • Formazione delle nuvole • Elastic Compute Cloud (EC2) • Gestione dell'identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • Servizio di archiviazione semplice (S3)

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.

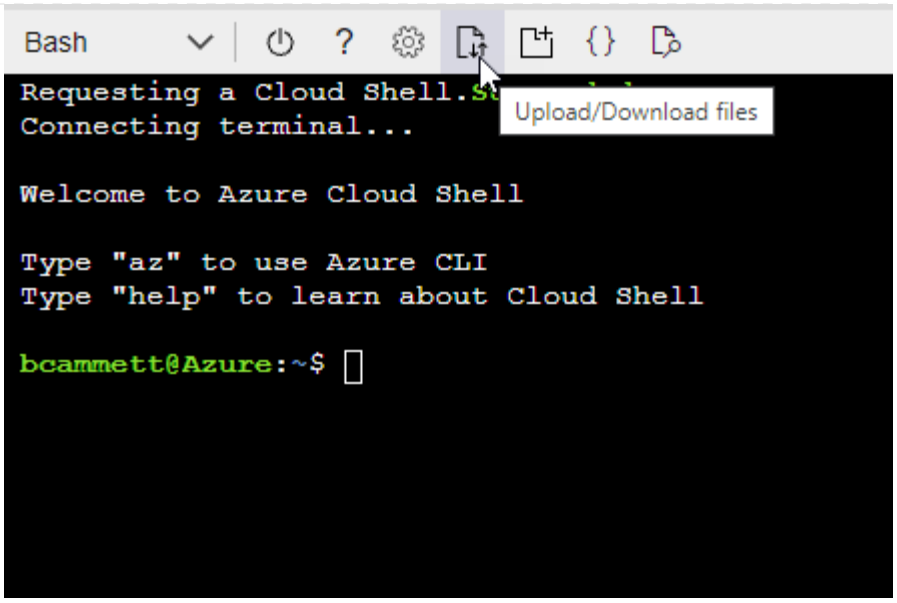
   Esempio

   ```
   "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

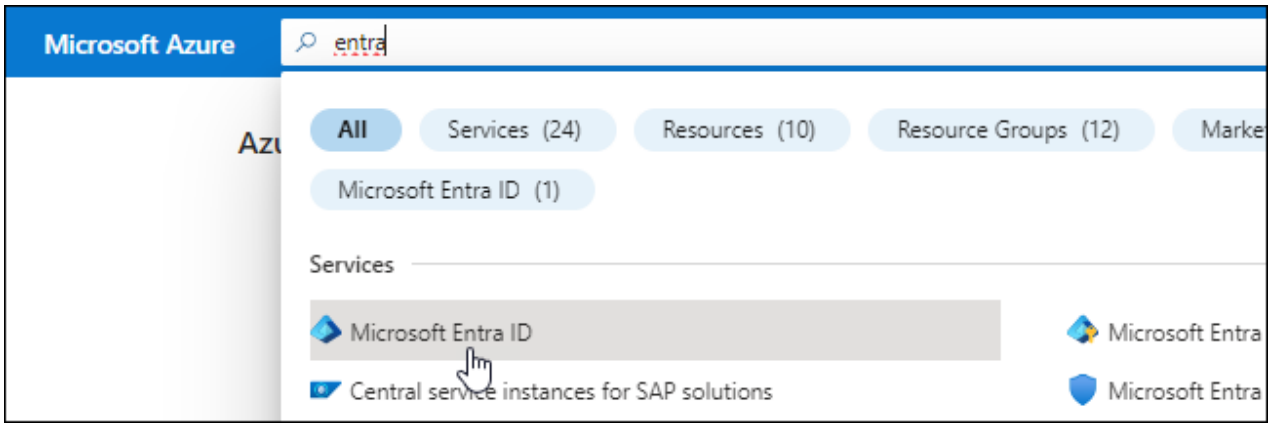
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie alla console. Dopo aver installato l'agente Console, è necessario fornire queste credenziali alla Console.

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 .

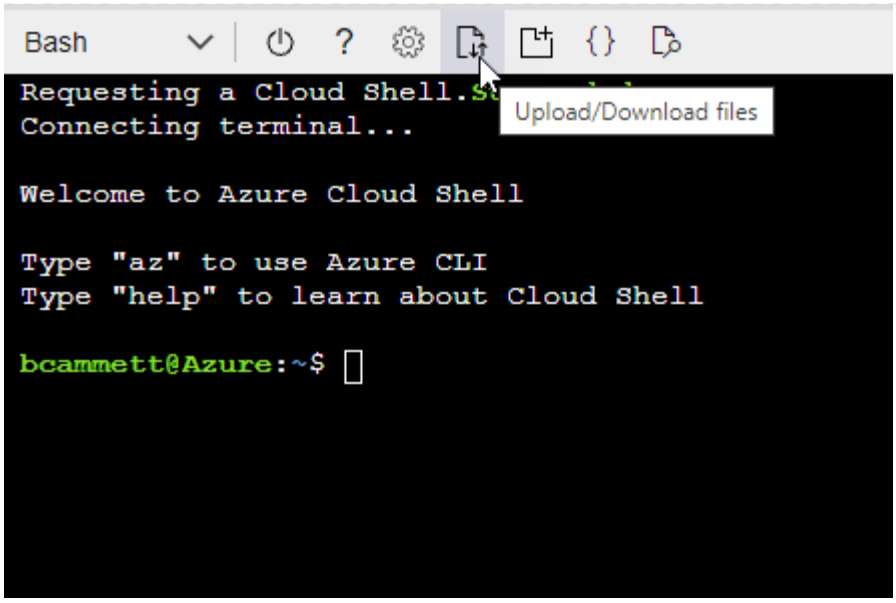
      Esempio

      ```
      "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**.

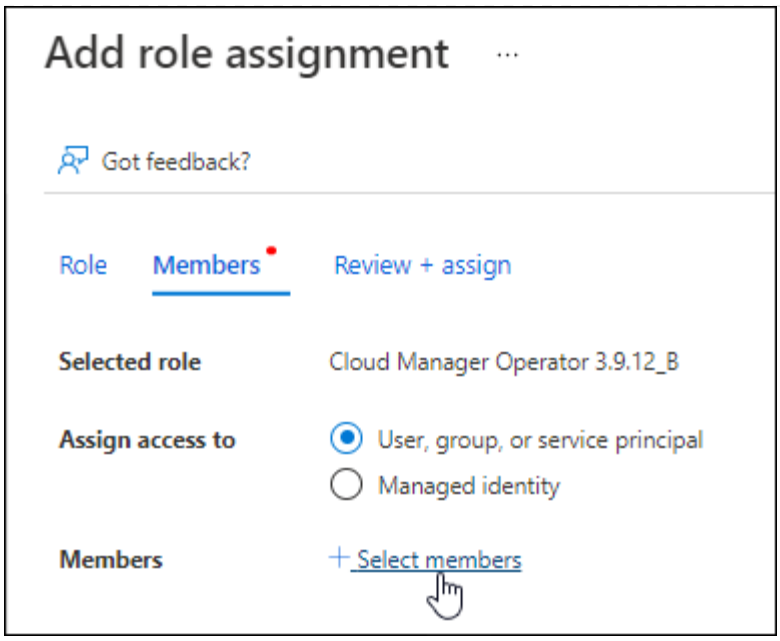
   b. Seleziona l'abbonamento.

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

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

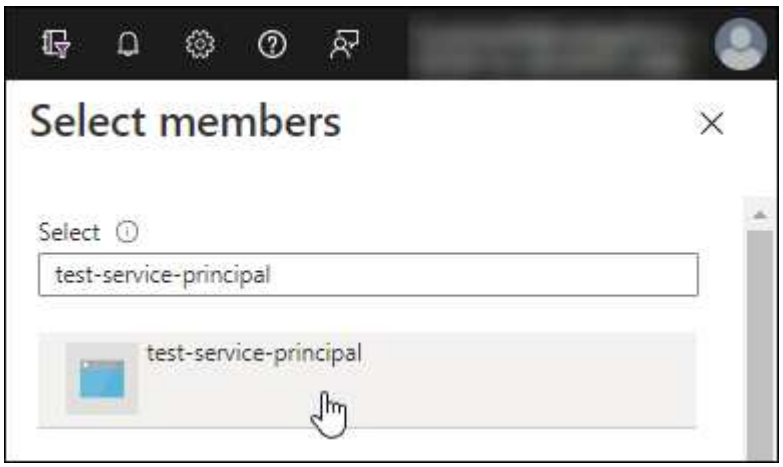
   e. Nella scheda **Membri**, completa i seguenti passaggi:

      - 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**.

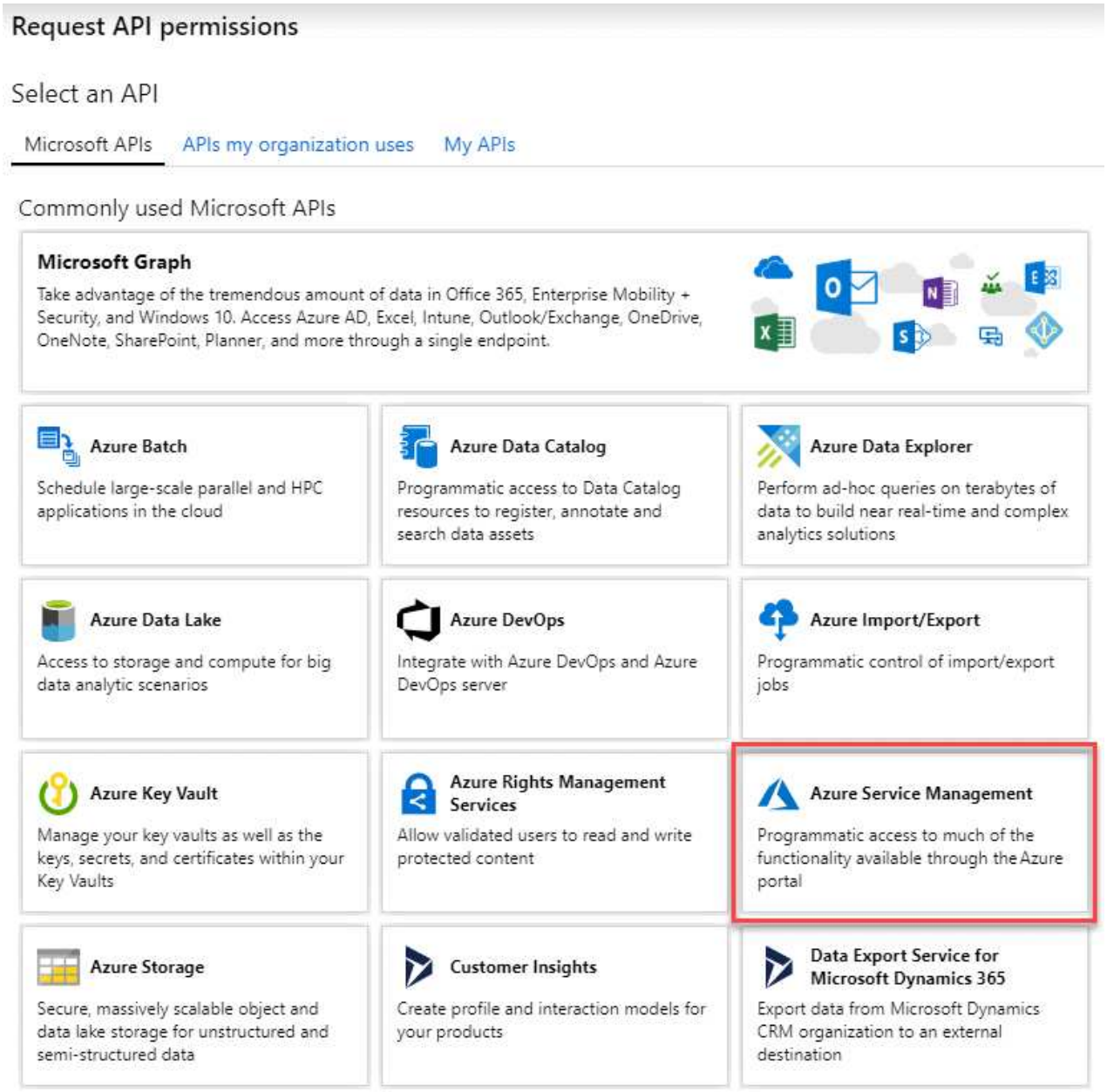
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

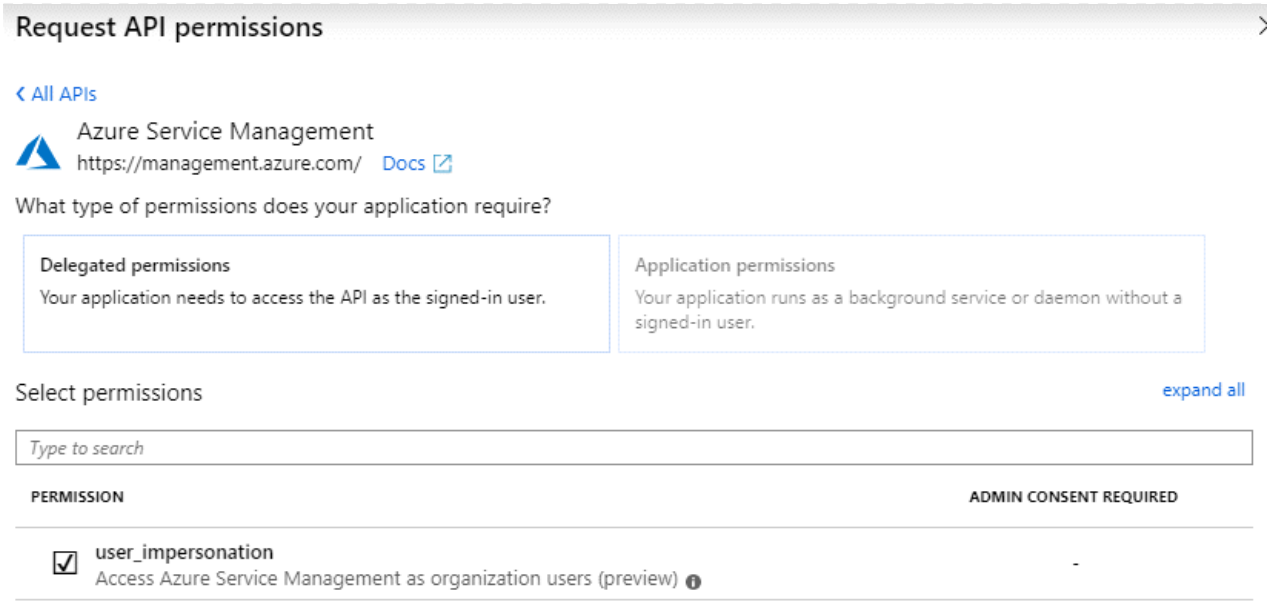
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

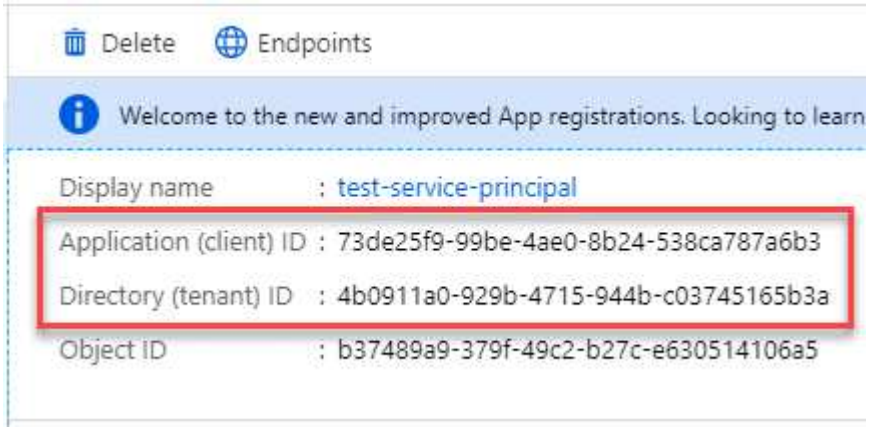


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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.

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"

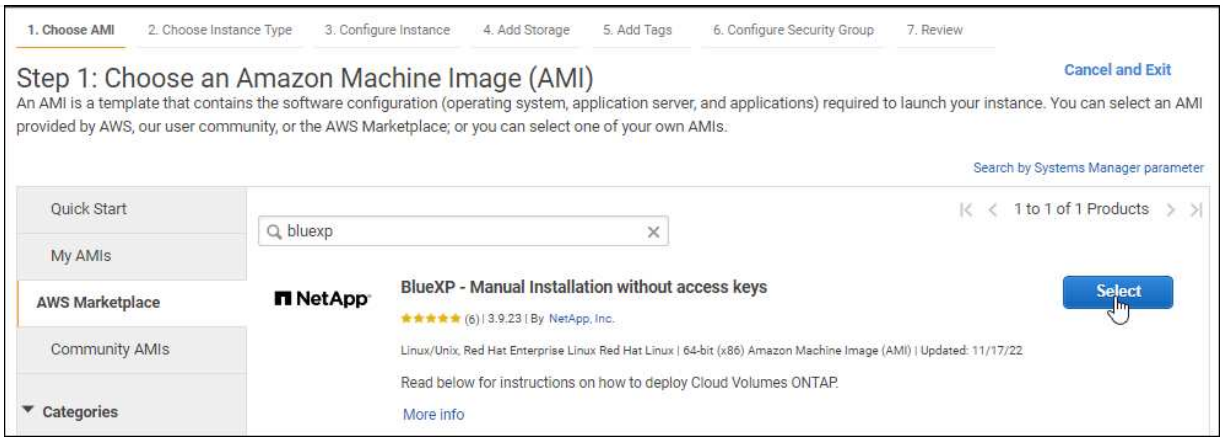
- Un ruolo IAM con una policy associata che include le autorizzazioni richieste per l'agente della console.

  "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.



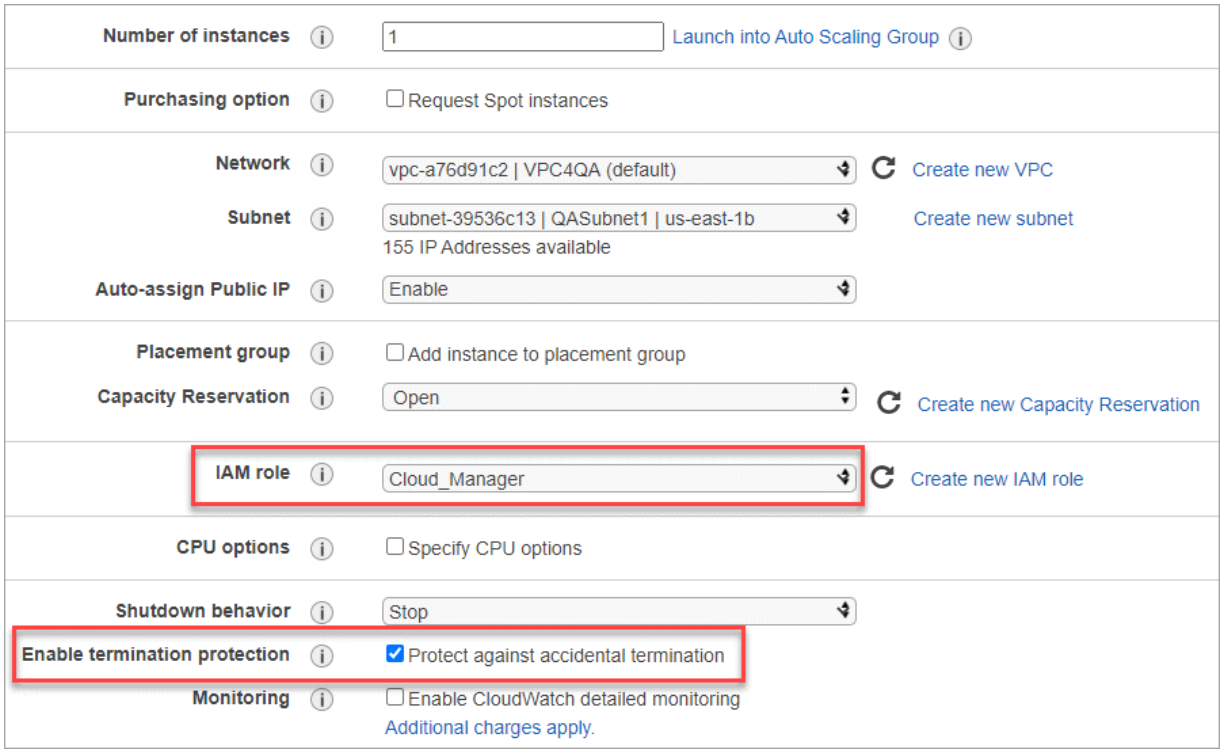
d. Selezionare **Continua**.

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.

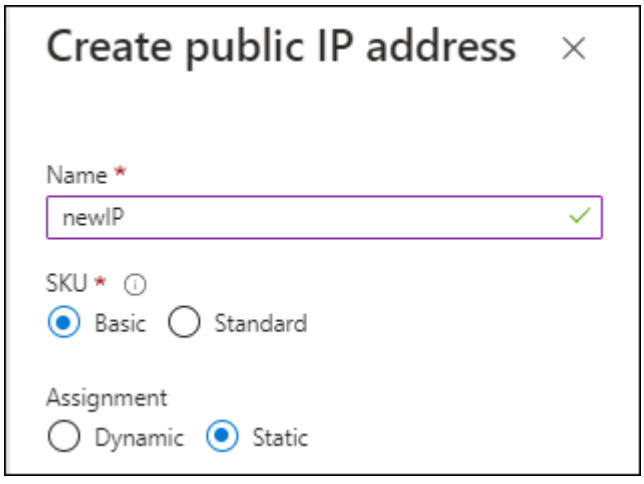
  "Scopri come configurare le autorizzazioni di Azure"

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

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>
```

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

   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 server proxy HTTP o HTTPS utilizzando uno dei seguenti formati:

   - http://indirizzo:porta
   - http://nome-utente:password@indirizzo:porta

- http://nome-dominio%92nome-utente:password@indirizzo:porta
- https://indirizzo:porta
- https://nome-utente:password@indirizzo:porta
- https://nome-dominio%92nome-utente:password@indirizzo:porta

  Notare 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 \ come mostrato sopra.
  - L'agente Console non supporta nomi utente o password che includono il carattere @.
  - Se la password include uno qualsiasi dei seguenti caratteri speciali, è necessario anteporre una barra rovesciata a tale carattere speciale: & o !

    Per esempio:

http://bxpproxyuser:netapp1\!@indirizzo:3128

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

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

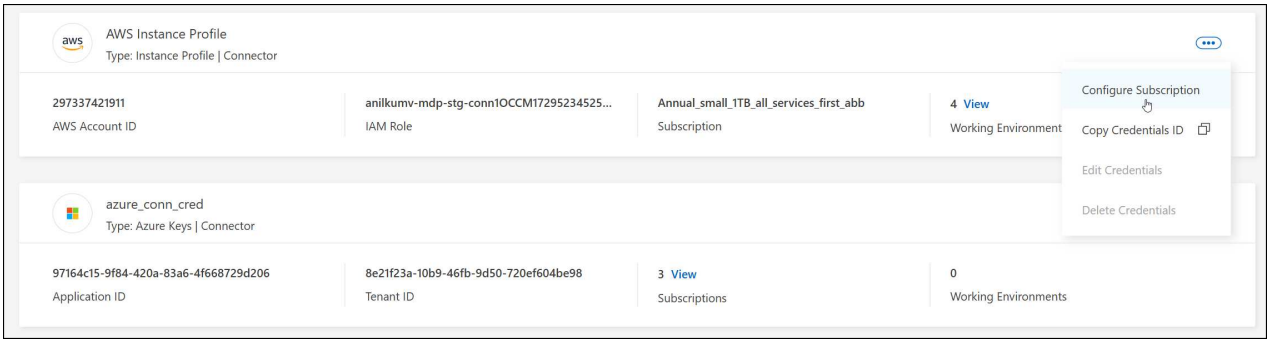
Per potersi iscrivere ai servizi dati, è necessario aver già distribuito un agente Console. È necessario associare un abbonamento al marketplace alle credenziali cloud connesse a un agente della console.

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.

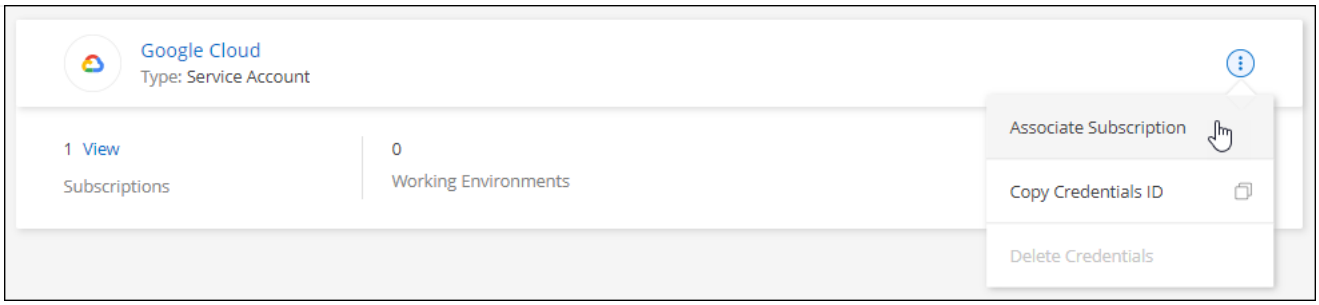
   Per tutte le altre organizzazioni o account, sarà necessario associare manualmente l'abbonamento ripetendo questi passaggi.

      ◦ Seleziona **Salva**.

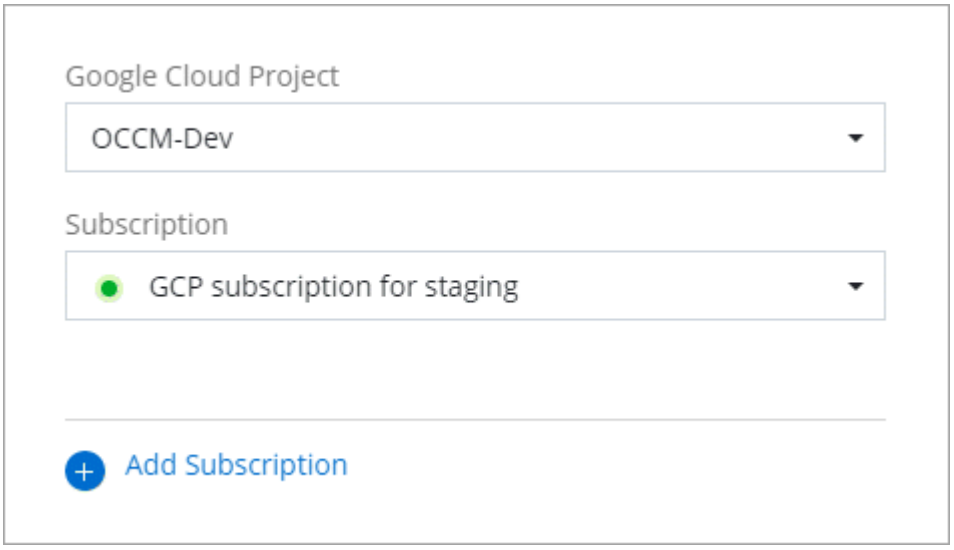
Google Cloud

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**.



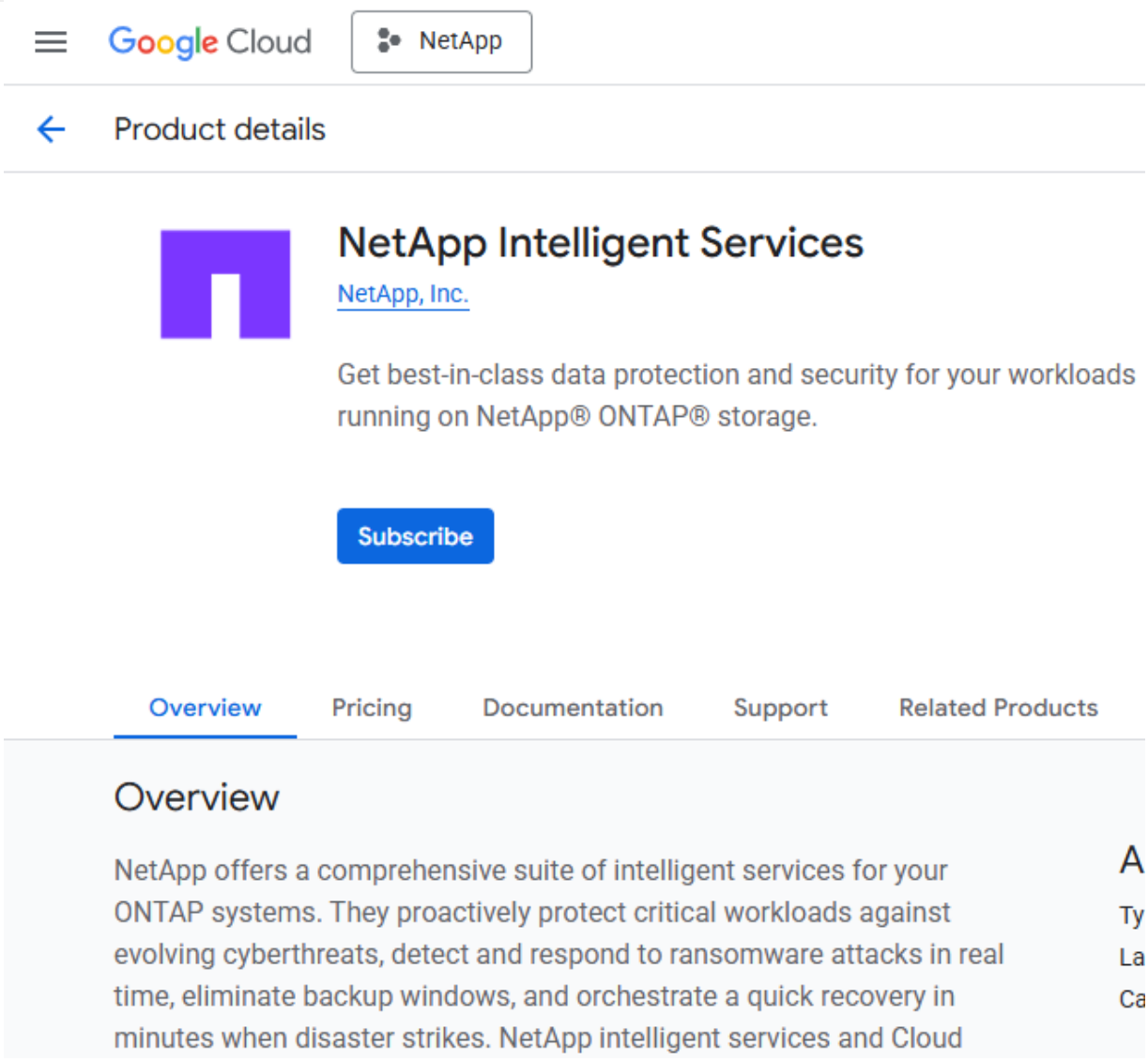
1. Per configurare un abbonamento esistente con le credenziali selezionate, seleziona un progetto Google Cloud e un abbonamento dall'elenco a discesa, quindi seleziona **Configura**.



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.

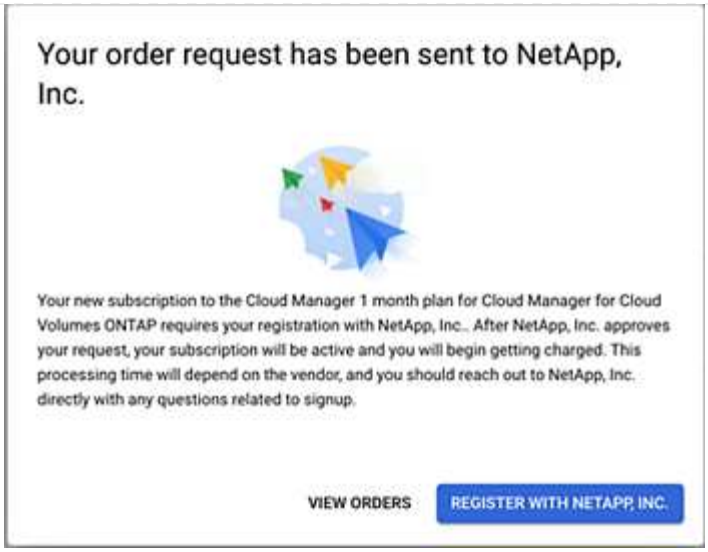


b. Seleziona **Iscriviti**.
c. Seleziona l'account di fatturazione appropriato e accetta i termini e le condizioni.
d. Seleziona **Iscriviti**.

   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.

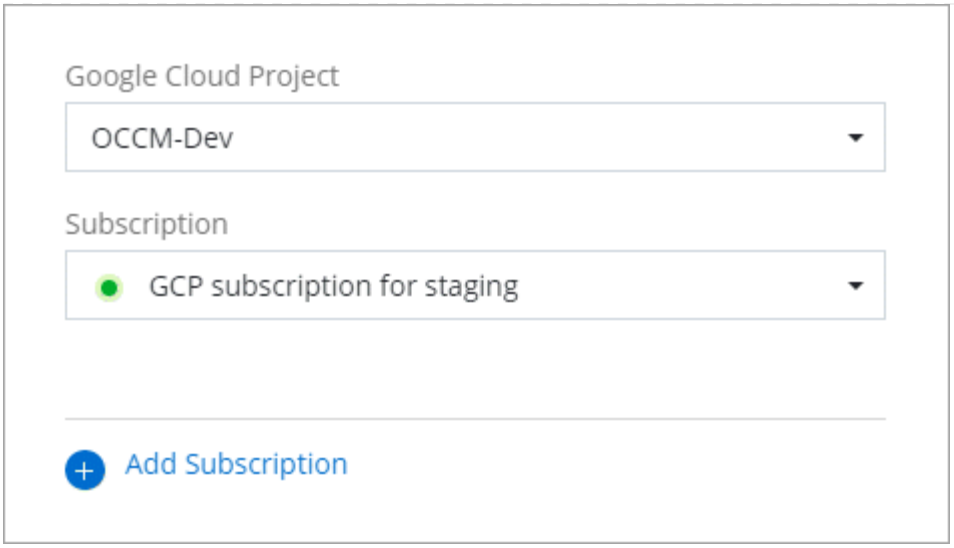
- Seleziona l'organizzazione della Console a cui desideri associare questo abbonamento.
- Nel campo **Sostituisci abbonamento esistente**, scegli se desideri sostituire automaticamente l'abbonamento esistente per un'organizzazione con questo nuovo abbonamento.

  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"

Informazioni sul copyright

Informazioni sul marchio commerciale