Installa un agente in locale

NetApp Console setup and administration

NetApp
January 27, 2026

Sommario

Installa un agente in locale

Installare manualmente un agente Console in locale

Installa un agente Console in locale, quindi accedi e configuralo per farlo funzionare con la tua organizzazione Console.

Se sei un utente VMWare, puoi utilizzare un OVA per installare un agente Console nel tuo VCenter."Scopri di più sull'installazione di un agente in un VCenter."

Prima di procedere all'installazione, è necessario assicurarsi che l'host (VM o host Linux) soddisfi i requisiti e che l'agente della console abbia accesso in uscita a Internet e alle reti di destinazione. Se intendi utilizzare i servizi dati NetApp o le opzioni di archiviazione cloud come Cloud Volumes ONTAP, dovrai creare credenziali nel tuo provider cloud da aggiungere alla Console, in modo che l'agente della Console possa eseguire azioni nel cloud per tuo conto.

Prepararsi all'installazione dell'agente Console

Prima di installare un agente Console, è necessario assicurarsi di disporre di un computer host che soddisfi i requisiti di installazione. Sarà inoltre necessario collaborare con l'amministratore di rete per garantire che l'agente della console abbia accesso in uscita agli endpoint richiesti e alle connessioni alle reti di destinazione.

Requisiti dell'host dell'agente della console di revisione

Eseguire l'agente Console su un host x86 che soddisfi i requisiti di sistema operativo, RAM e porta. Prima di installare l'agente Console, assicurati che il tuo host soddisfi questi requisiti.

L'agente della console riserva l'intervallo UID e GID da 19000 a 19200. Questo intervallo è fisso e non può essere modificato. Se un software di terze parti sul tuo host utilizza UID o GID compresi in questo intervallo, l'installazione dell'agente non andrà a buon fine. NetApp consiglia di utilizzare un host privo di software di terze parti per evitare conflitti.

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.

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

Configurare l'accesso alla rete per l'agente della console

Configurare l'accesso alla rete per garantire che l'agente della console possa gestire le risorse. Richiede connessioni alle reti di destinazione e accesso Internet in uscita a endpoint specifici.

Connessioni alle reti di destinazione

L'agente Console richiede una connessione di rete alla posizione in cui si prevede di creare e gestire i sistemi. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema di archiviazione nel tuo ambiente locale.

Accesso a Internet in uscita

La posizione di rete in cui si distribuisce l'agente Console deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

Endpoint contattati dai computer quando si utilizza la NetApp Console basata sul Web

I computer che accedono alla Console da un browser Web devono avere la possibilità di contattare più endpoint. Sarà necessario utilizzare la Console per configurare l'agente della Console e per l'utilizzo quotidiano della Console.

"Preparare la rete per la console NetApp" .

Endpoint contattati dall'agente della console

L'agente della console necessita di accesso a Internet in uscita per contattare i seguenti endpoint per gestire risorse e processi all'interno dell'ambiente cloud pubblico per le operazioni quotidiane.

Gli endpoint elencati di seguito sono tutti voci CNAME.

Un agente Console installato in sede non può gestire le risorse in Google Cloud. Se vuoi gestire le risorse di Google Cloud, devi installare un agente in Google Cloud.

AWS

Quando l'agente Console è installato in locale, necessita dell'accesso di rete ai seguenti endpoint AWS per gestire i sistemi NetApp (ad esempio Cloud Volumes ONTAP) distribuiti in AWS.

Endpoint contattati dall'agente della console

L'agente della console necessita di accesso a Internet in uscita per contattare i seguenti endpoint per gestire risorse e processi all'interno dell'ambiente cloud pubblico per le operazioni quotidiane.

Gli endpoint elencati di seguito sono tutti voci CNAME.

Punti finali	Scopo
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)	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 .
\ 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.

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://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.

Azzurro

Quando l'agente Console è installato in locale, necessita dell'accesso di rete ai seguenti endpoint di Azure per gestire i sistemi NetApp (ad esempio Cloud Volumes ONTAP) distribuiti in Azure.

Punti finali	Scopo
\ 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.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Per gestire le risorse nelle regioni di Azure Cina.

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.

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"

Crea autorizzazioni cloud per l'agente della console per AWS o Azure

Se si desidera utilizzare i servizi dati NetApp in AWS o Azure con un agente Console locale, è necessario configurare le autorizzazioni nel provider cloud e quindi aggiungere le credenziali all'agente Console dopo averlo installato.

Per gestire tutte le risorse presenti in Google Cloud, è necessario installare l'agente Console.

AWS

Quando l'agente Console è installato in locale, è necessario fornire alla Console le autorizzazioni AWS aggiungendo le chiavi di accesso per un utente IAM che dispone delle autorizzazioni richieste.

È necessario utilizzare questo metodo di autenticazione se l'agente Console è installato in locale. Non è possibile utilizzare un ruolo IAM.

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.

Risultato

Ora dovresti avere le chiavi di accesso per un utente IAM che dispone delle autorizzazioni richieste. Dopo aver installato l'agente Console, associare queste credenziali all'agente Console dalla Console.

Azzurro

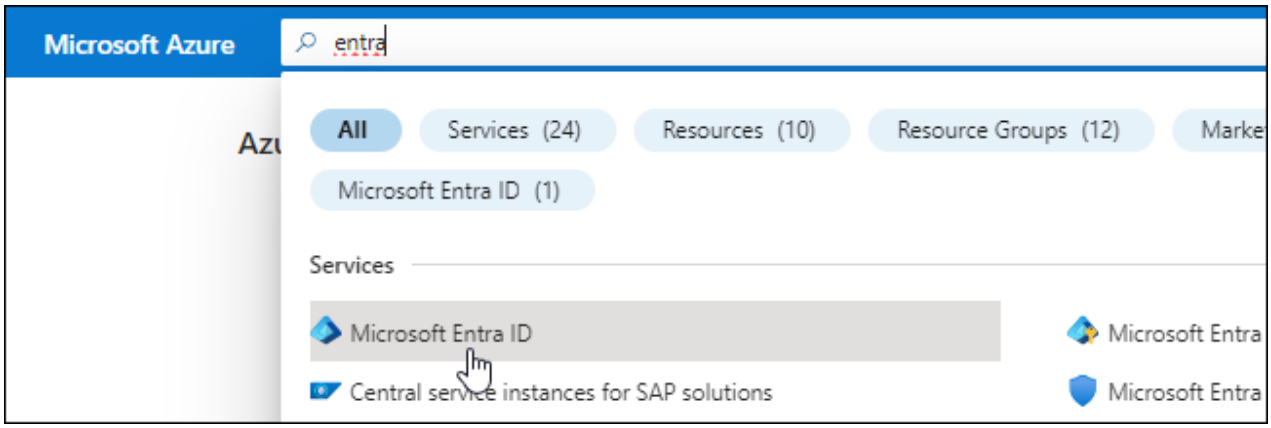
Quando l'agente Console è installato in locale, è necessario fornire all'agente Console le autorizzazioni di Azure impostando un'entità servizio in Microsoft Entra ID e ottenendo le credenziali di Azure necessarie all'agente Console.

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 .

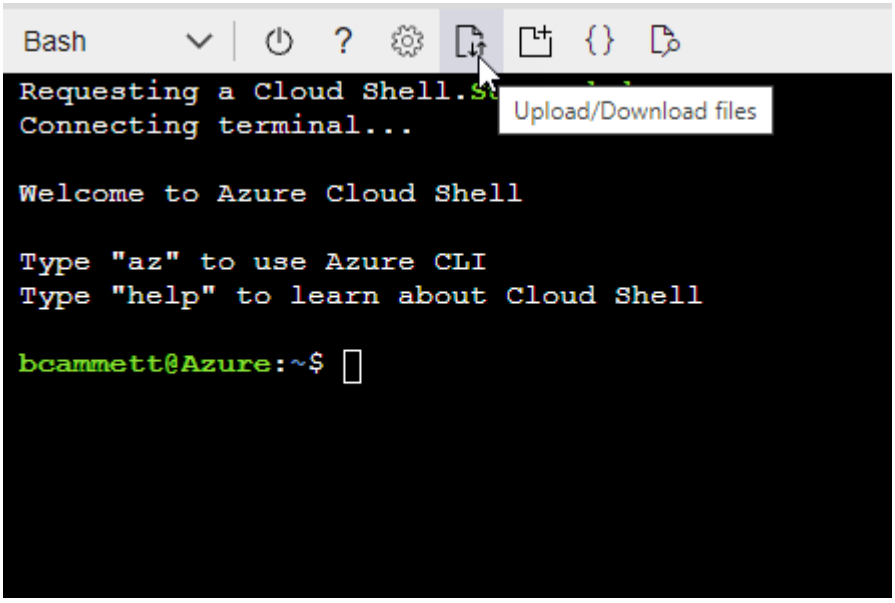
      Esempio

      ```
      "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:

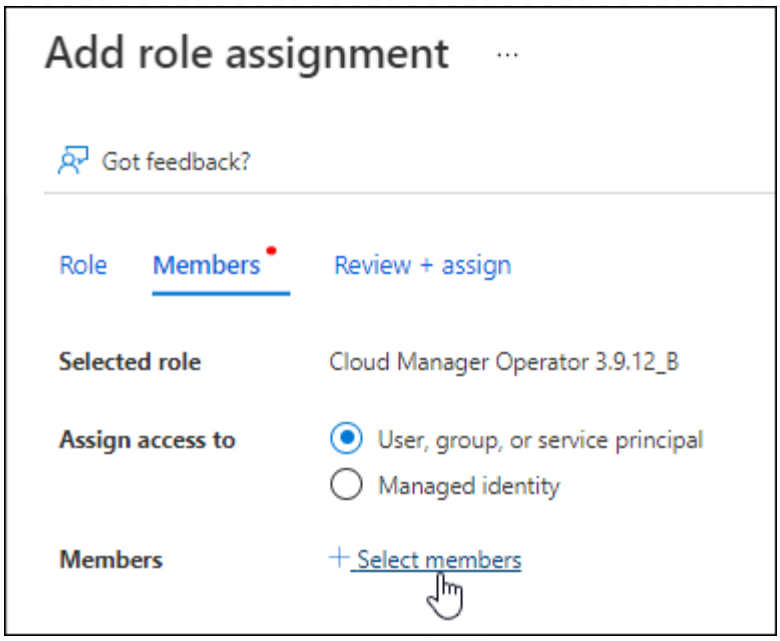
```
az role definition create --role-definition agent_Policy.json
```

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

2. Assegnare l'applicazione al ruolo:

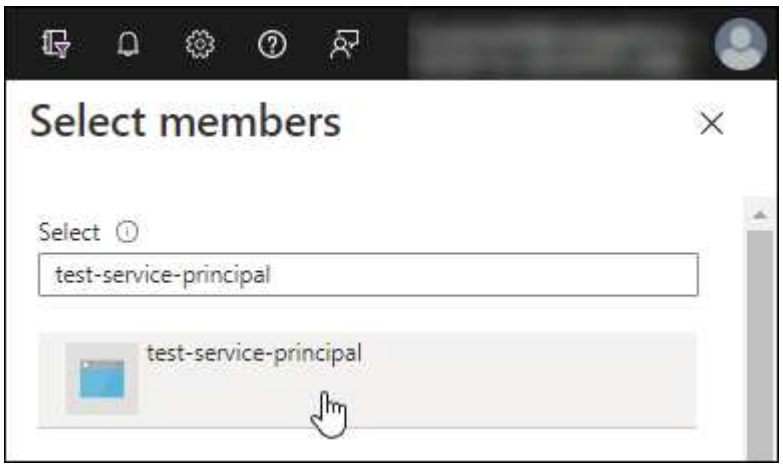
   a. Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
   b. Seleziona l'abbonamento.
   c. Selezionare **Controllo accessi (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.
   e. Nella scheda **Membri**, 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**.

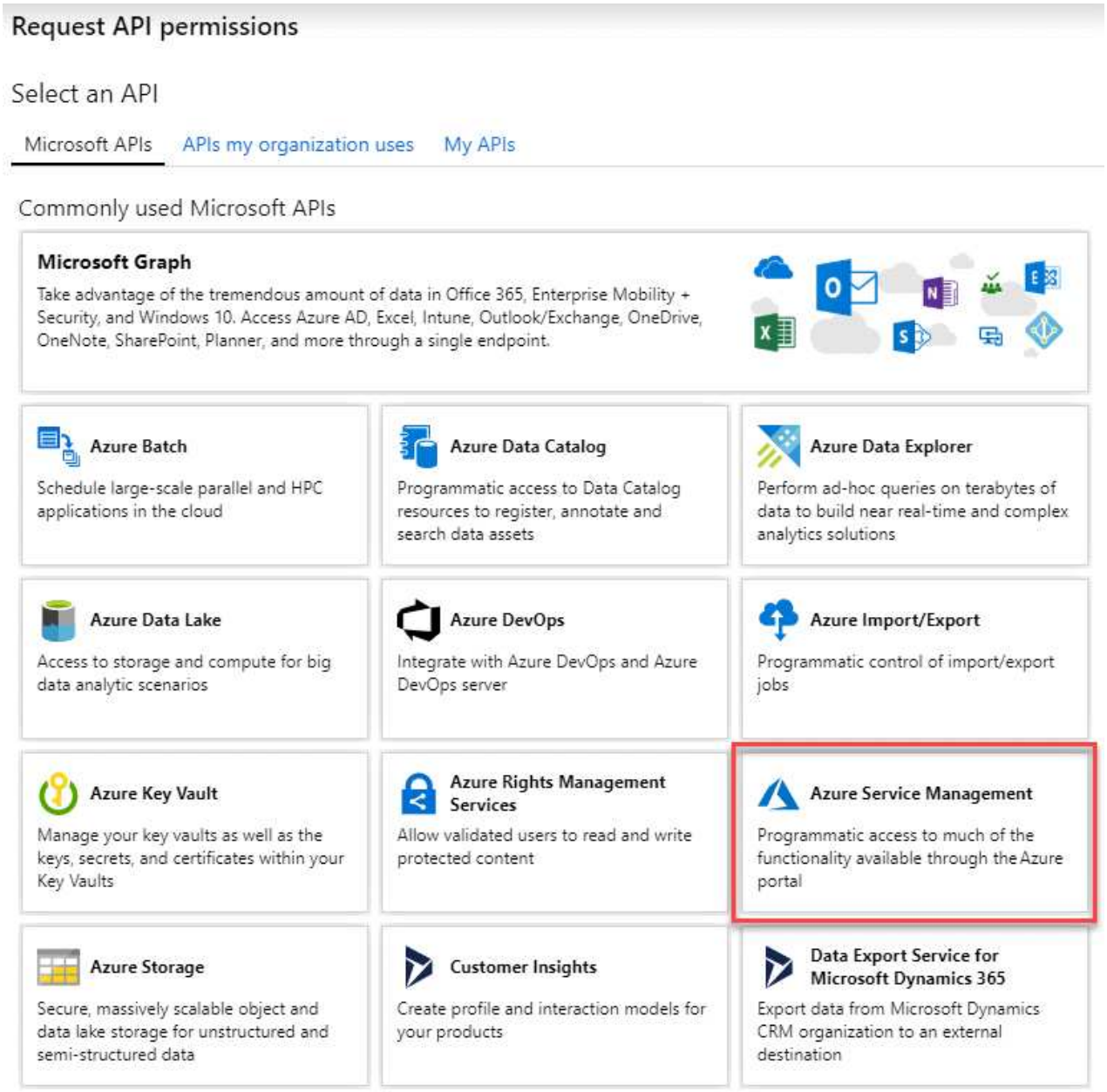
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

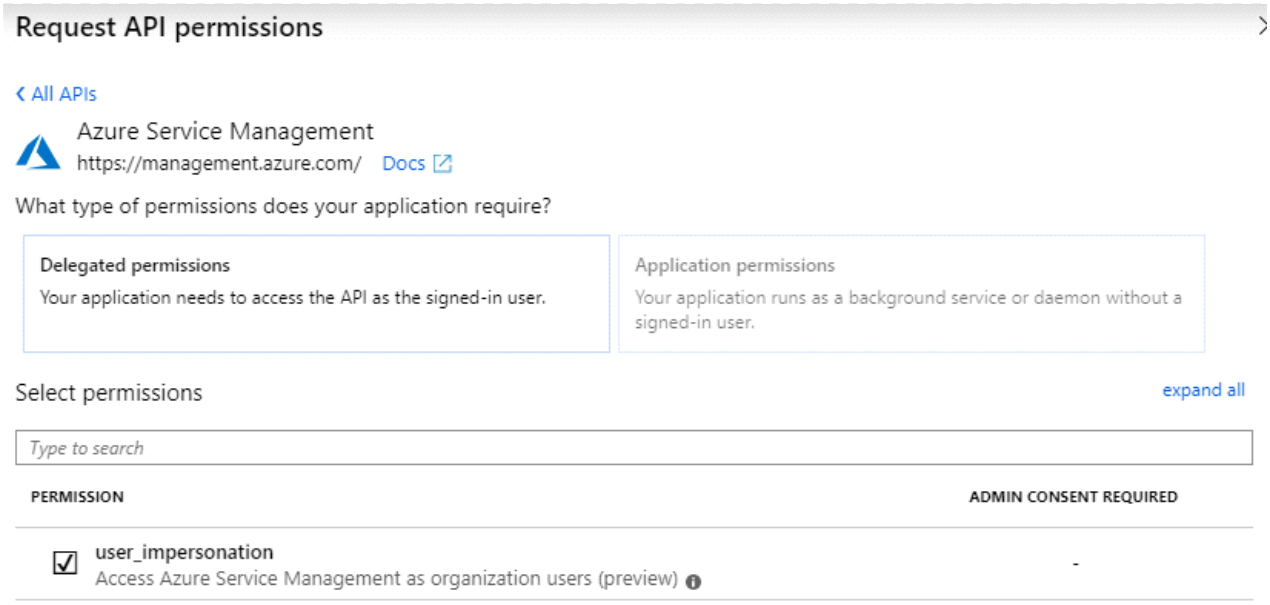
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

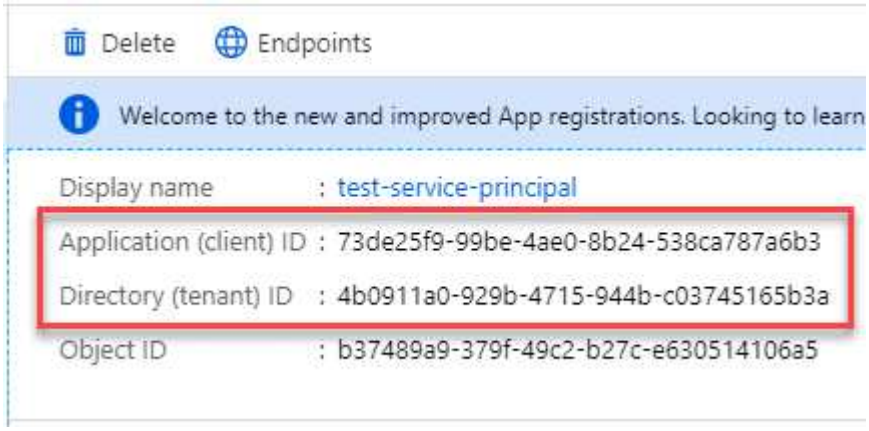


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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

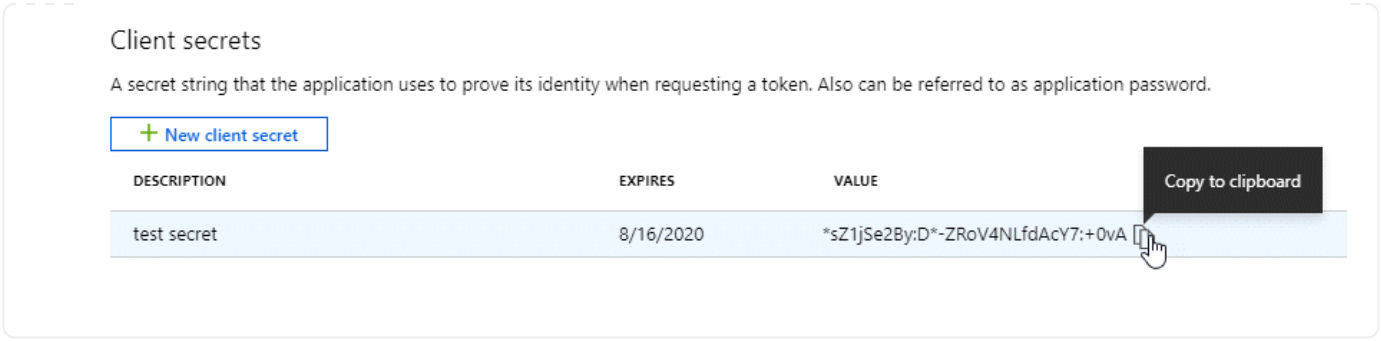
1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)**.



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.



Installare manualmente un agente Console

Quando si installa manualmente un agente Console, è necessario preparare l'ambiente della macchina in modo che soddisfi i requisiti. Avrai bisogno di un computer Linux e dovrai installare Podman o Docker, a seconda del tuo sistema operativo Linux.

Installa 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
```

Installare manualmente l'agente Console

Scarica e installa il software dell'agente Console su un host Linux esistente in locale.

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" .

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.

Cosa succederà adesso?

Sarà necessario registrare l'agente Console nella NetApp Console.

Registrare l'agente della console con NetApp Console

Accedi alla Console e associa l'agente della Console alla tua organizzazione. La modalità di accesso dipende dalla modalità in cui si utilizza la Console. Se si utilizza la Console in modalità standard, è possibile effettuare l'accesso tramite il sito Web SaaS. Se si utilizza la Console in modalità limitata, è necessario effettuare l'accesso localmente dall'host dell'agente della Console.

Passi

1. Aprire un browser Web e immettere l'URL dell'host dell'agente della console:

   L'URL dell'host della console può essere un localhost, un indirizzo IP privato o un indirizzo IP pubblico, a seconda della configurazione dell'host. Ad esempio, se l'agente della console si trova nel cloud pubblico senza un indirizzo IP pubblico, è necessario immettere un indirizzo IP privato da un host che ha una connessione all'host dell'agente della console.

2. Registrati o accedi.
3. Dopo aver effettuato l'accesso, configura la Console:
   a. Specificare l'organizzazione della console da associare all'agente della console.
   b. Inserisci un nome per il sistema.
   c. In **Stai utilizzando un ambiente protetto?** mantieni disattivata la modalità con restrizioni.

      La modalità limitata non è supportata quando l'agente Console è installato in locale.

   d. Seleziona **Iniziamo**.

Fornire le credenziali del provider cloud alla NetApp Console

Dopo aver installato e configurato l'agente Console, aggiungi le tue credenziali cloud in modo che l'agente Console disponga delle autorizzazioni necessarie per eseguire azioni in AWS o Azure.

AWS

Prima di iniziare

Se hai appena creato queste credenziali AWS, potrebbero volerci alcuni minuti prima che siano disponibili. Attendi qualche minuto prima di aggiungere le credenziali alla Console.

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**.

Ora puoi andare al "NetApp Console" per iniziare a utilizzare l'agente Console.

Azzurro

Prima di iniziare

Se hai appena creato queste credenziali di Azure, potrebbero volerci alcuni minuti prima che siano disponibili. Attendi qualche minuto prima di aggiungere le credenziali all'agente della console.

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

L'agente della console ora dispone delle autorizzazioni necessarie per eseguire azioni in Azure per tuo conto. Ora puoi andare al "NetApp Console" per iniziare a utilizzare l'agente Console.

Installa un agente Console in locale utilizzando VCenter

Se sei un utente VMWare, puoi utilizzare un OVA per installare un agente Console nel tuo VCenter. Il download dell'OVA o l'URL sono disponibili tramite la NetApp Console.

Quando si installa un agente Console con gli strumenti VCenter, è possibile utilizzare la console Web della VM per eseguire attività di manutenzione."Scopri di più sulla console VM per l'agente."

Prepararsi all'installazione dell'agente Console

Prima dell'installazione, assicurati che l'host della VM soddisfi i requisiti e che l'agente della console possa accedere a Internet e alle reti di destinazione. Per utilizzare i servizi dati NetApp o Cloud Volumes ONTAP, creare le credenziali del provider cloud affinché l'agente della console esegua azioni per tuo conto.

Requisiti dell'host dell'agente della console di revisione

Prima di installare l'agente Console, assicurarsi che il computer host soddisfi i requisiti di installazione.

- CPU: 8 core o 8 vCPU
- RAM: 32 GB
- Spazio su disco: 165 GB (con provisioning spesso)
- vSphere 7.0 o versione successiva
- Host ESXi 7.03 o superiore

Installare l'agente in un ambiente vCenter anziché direttamente su un host ESXi.

Configurare l'accesso alla rete per l'agente della console

Collaborare con l'amministratore di rete per garantire che l'agente della console abbia accesso in uscita agli endpoint richiesti e alle connessioni alle reti di destinazione.

Connessioni alle reti di destinazione

L'agente Console richiede una connessione di rete alla posizione in cui si prevede di creare e gestire i sistemi. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema di archiviazione nel tuo ambiente locale.

Accesso a Internet in uscita

La posizione di rete in cui si distribuisce l'agente Console deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

Endpoint contattati dai computer quando si utilizza la NetApp Console basata sul Web

I computer che accedono alla Console da un browser Web devono avere la possibilità di contattare più endpoint. Sarà necessario utilizzare la Console per configurare l'agente della Console e per l'utilizzo quotidiano della Console.

"Preparare la rete per la console NetApp" .

Endpoint contattati dall'agente della console

L'agente della console necessita di accesso a Internet in uscita per contattare i seguenti endpoint per gestire risorse e processi all'interno dell'ambiente cloud pubblico per le operazioni quotidiane.

Gli endpoint elencati di seguito sono tutti voci CNAME.

Non è possibile gestire le risorse in Google Cloud con un agente Console installato in sede. Per gestire le risorse di Google Cloud, installa un agente in Google Cloud.

AWS

Quando l'agente Console è installato in locale, necessita dell'accesso di rete ai seguenti endpoint AWS per gestire i sistemi NetApp (ad esempio Cloud Volumes ONTAP) distribuiti in AWS.

Endpoint contattati dall'agente della console

L'agente della console necessita di accesso a Internet in uscita per contattare i seguenti endpoint per gestire risorse e processi all'interno dell'ambiente cloud pubblico per le operazioni quotidiane.

Gli endpoint elencati di seguito sono tutti voci CNAME.

Punti finali	Scopo
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)	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 .
\ 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.

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://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.

Azzurro

Quando l'agente Console è installato in locale, necessita dell'accesso di rete ai seguenti endpoint di Azure per gestire i sistemi NetApp (ad esempio Cloud Volumes ONTAP) distribuiti in Azure.

Punti finali	Scopo
\ 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.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Per gestire le risorse nelle regioni di Azure Cina.

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.

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"

Crea autorizzazioni cloud per l'agente della console per AWS o Azure

Se si desidera utilizzare i servizi dati NetApp in AWS o Azure con un agente Console locale, è necessario configurare le autorizzazioni nel provider cloud in modo da poter aggiungere le credenziali all'agente Console dopo averlo installato.

Non è possibile gestire le risorse in Google Cloud con un agente Console installato in sede. Se vuoi gestire le risorse di Google Cloud, devi installare un agente in Google Cloud.

AWS

Per gli agenti della console in locale, fornire le autorizzazioni AWS aggiungendo le chiavi di accesso utente IAM.

Utilizzare le chiavi di accesso utente IAM per gli agenti della console locale; i ruoli IAM non sono supportati per gli agenti della console locale.

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.

Risultato

Ora dovresti disporre delle chiavi di accesso utente IAM con le autorizzazioni richieste. Dopo aver installato l'agente Console, associa queste credenziali all'agente Console dalla Console.

Azzurro

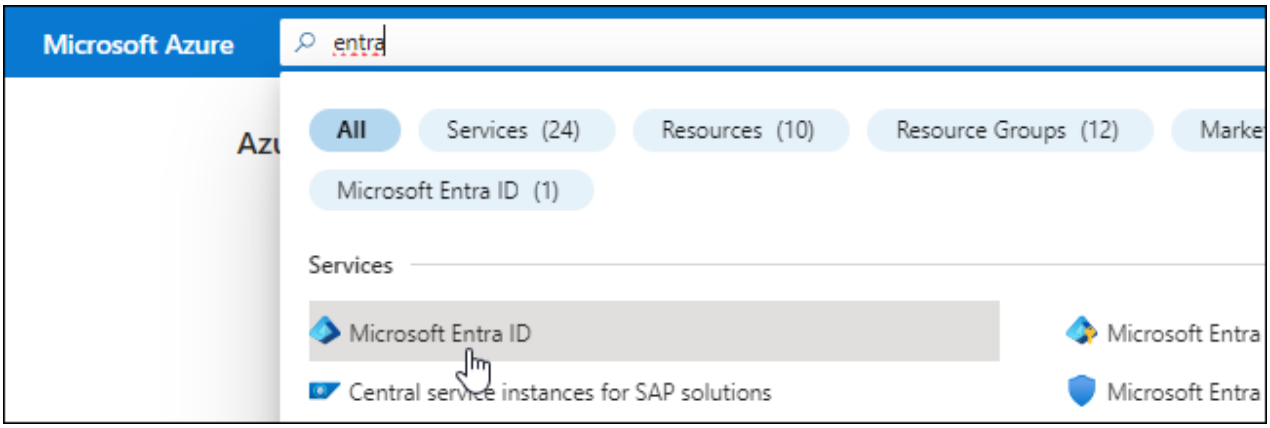
Quando l'agente Console è installato in locale, è necessario concedere all'agente Console le autorizzazioni di Azure impostando un'entità servizio in Microsoft Entra ID e ottenendo le credenziali di Azure necessarie all'agente Console.

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 .

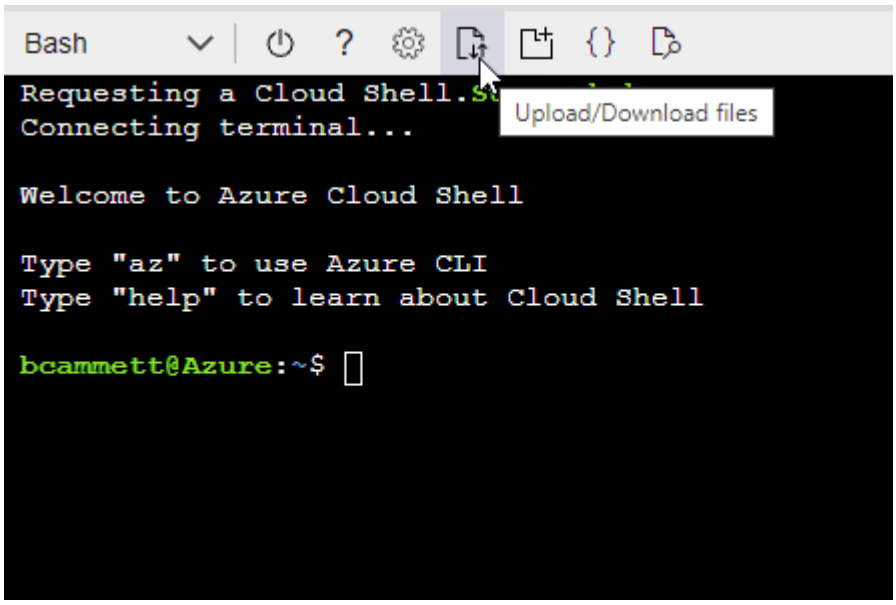
      Esempio

      ```
      "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:

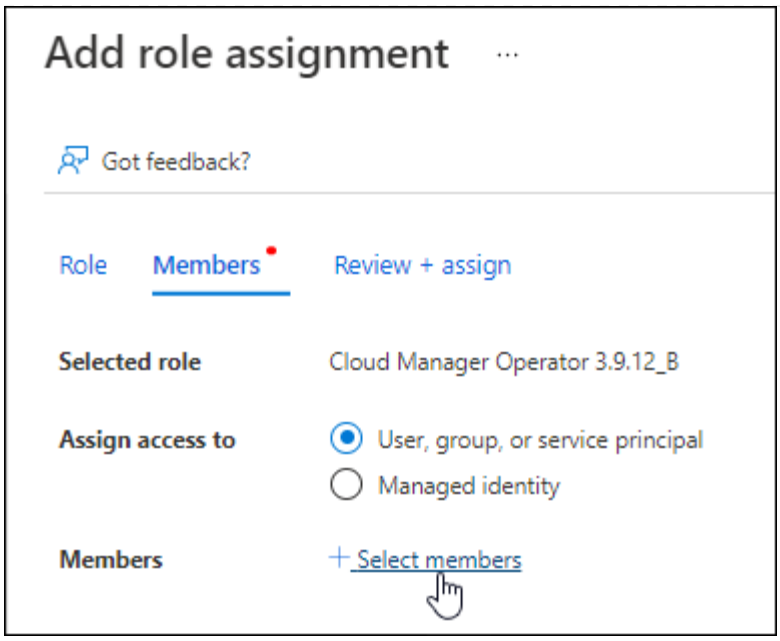
```
az role definition create --role-definition agent_Policy.json
```

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

2. Assegnare l'applicazione al ruolo:

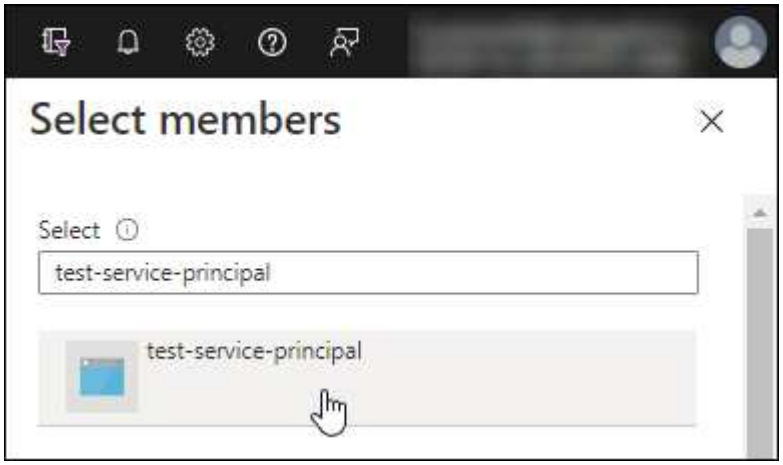
   a. Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
   b. Seleziona l'abbonamento.
   c. Selezionare **Controllo accessi (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.
   e. Nella scheda **Membri**, 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**.

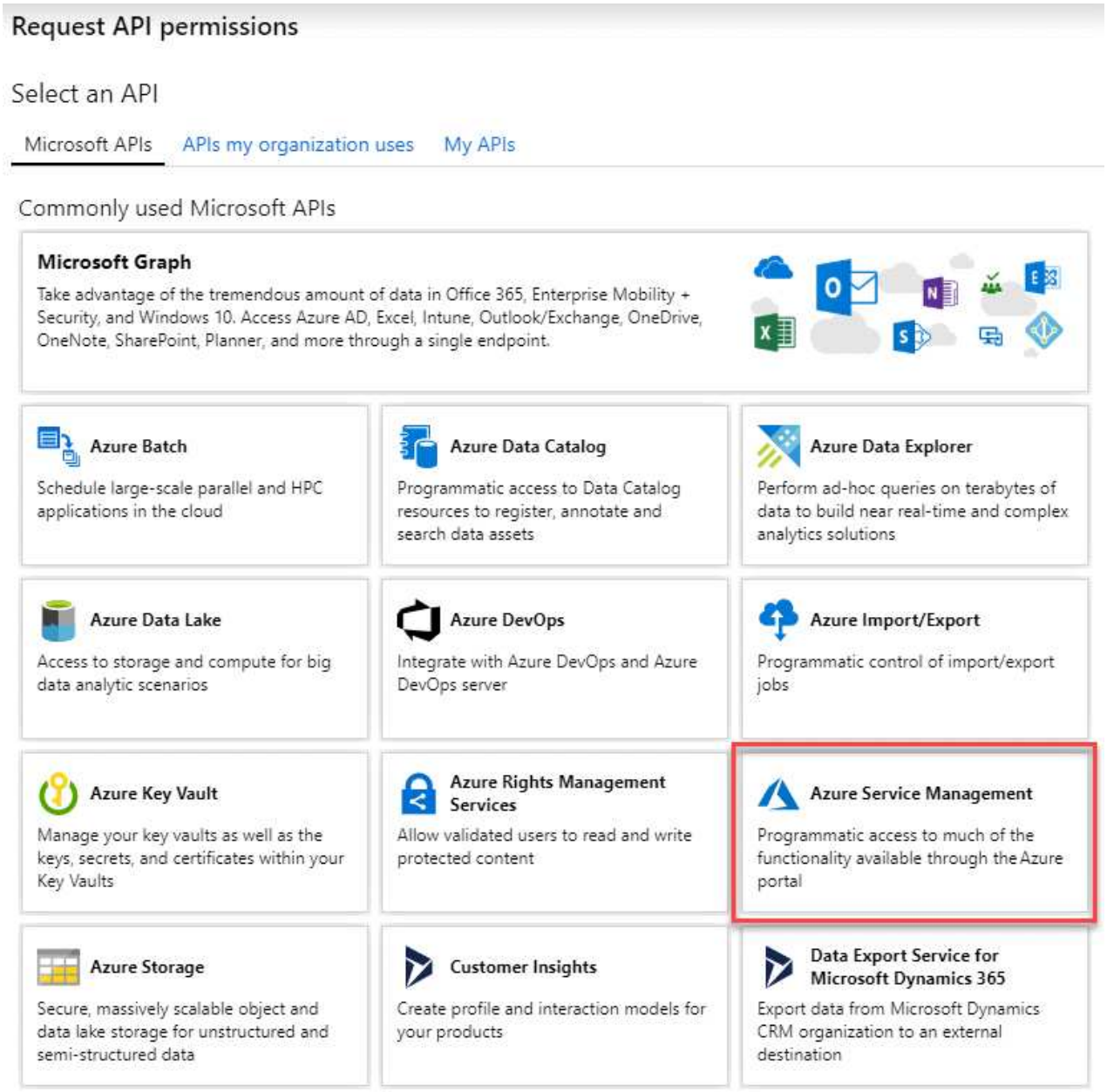
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

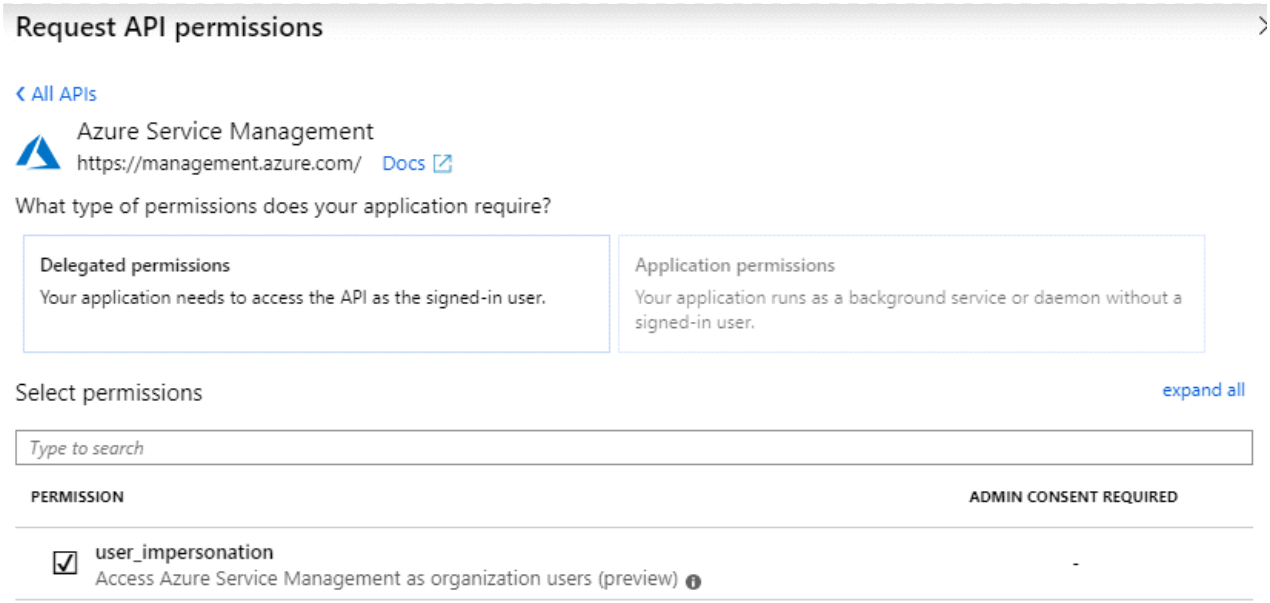
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

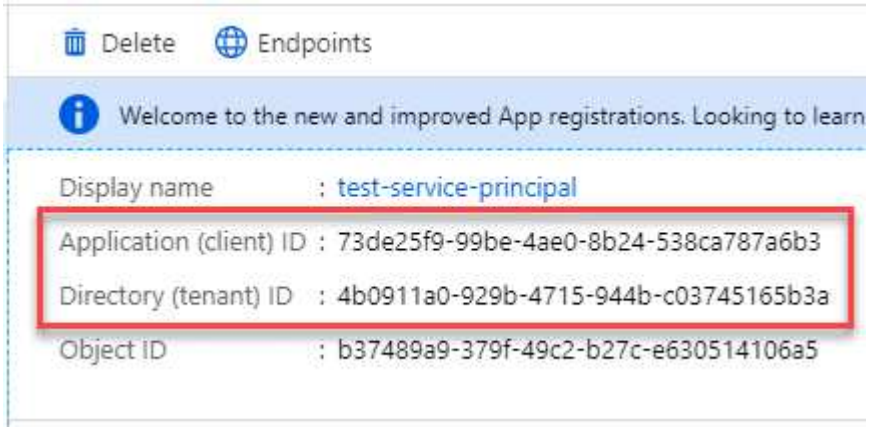


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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

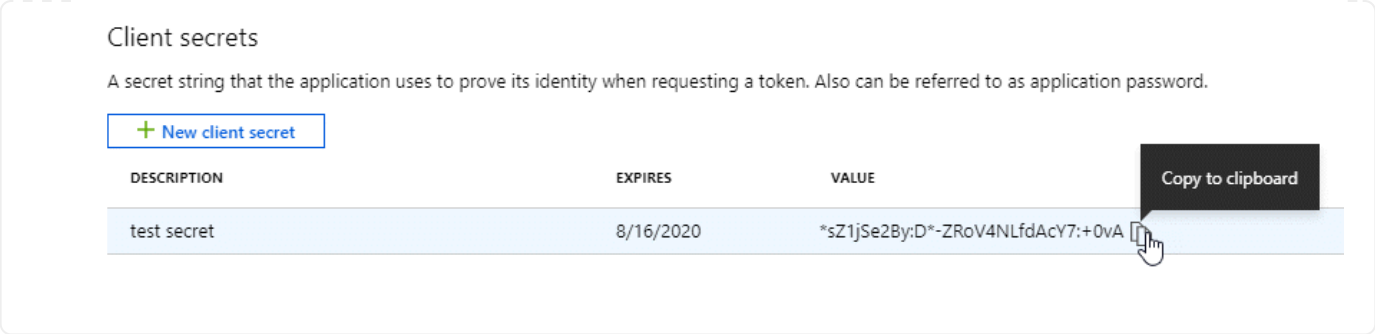
1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)**.



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.



Installa un agente Console nel tuo ambiente VCenter

NetApp supporta l'installazione dell'agente Console nel tuo ambiente VCenter. Il file OVA include un'immagine VM preconfigurata che puoi distribuire nel tuo ambiente VMware. È possibile scaricare un file o distribuire un URL direttamente dalla NetApp Console. Include il software dell'agente Console e un certificato autofirmato.

Scarica l'OVA o copia l'URL

Scarica l'OVA o copia l'URL dell'OVA direttamente dalla NetApp Console.

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona **Distribuisci agente > In locale**.
3. Seleziona **Con OVA**.
4. Scegli se scaricare l'OVA o copiare l'URL da utilizzare in VCenter.

Distribuisci l'agente nel tuo VCenter

Accedi al tuo ambiente VCenter per distribuire l'agente.

Passi

1. Carica il certificato autofirmato tra i tuoi certificati attendibili se il tuo ambiente lo richiede. Dopo l'installazione, sostituire questo certificato."Scopri come sostituire il certificato autofirmato."
2. Distribuire l'OVA dalla libreria dei contenuti o dal sistema locale.

Dal sistema locale	Dalla libreria dei contenuti
a. Fare clic con il pulsante destro del mouse e selezionare **Distribuisci modello OVF…**. b. Scegliere il file OVA dall'URL o andare alla sua posizione, quindi selezionare **Avanti**.	a. Vai alla tua libreria di contenuti e seleziona l'OVA dell'agente Console. b. Seleziona **Azioni** > **Nuova VM da questo modello**

3. Completare la procedura guidata Distribuisci modello OVF per distribuire l'agente della console.
4. Selezionare un nome e una cartella per la VM, quindi selezionare **Avanti**.
5. Selezionare una risorsa di elaborazione, quindi selezionare **Avanti**.
6. Esaminare i dettagli del modello, quindi selezionare **Avanti**.
7. Accettare il contratto di licenza, quindi selezionare **Avanti**.
8. Scegli il tipo di configurazione proxy che desideri utilizzare: proxy esplicito, proxy trasparente o nessun proxy.

9. Selezionare il datastore in cui si desidera distribuire la VM, quindi selezionare **Avanti**. Assicurati che soddisfi i requisiti dell'host.
10. Selezionare la rete a cui si desidera connettere la VM, quindi selezionare **Avanti**. Assicurarsi che la rete sia IPv4 e che disponga di accesso Internet in uscita verso gli endpoint richiesti.
11. nella finestra **Personalizza modello**, compila i seguenti campi:
    - **Informazioni proxy**
      - Se hai selezionato un proxy esplicito, inserisci il nome host o l'indirizzo IP del server proxy e il numero di porta, nonché il nome utente e la password.
      - Se hai selezionato un proxy trasparente, carica il relativo certificato.
    - **Configurazione della macchina virtuale**
      - **Salta controllo configurazione**: questa casella di controllo è deselezionata per impostazione predefinita, il che significa che l'agente esegue un controllo della configurazione per convalidare l'accesso alla rete.
        - NetApp consiglia di lasciare questa casella deselezionata in modo che l'installazione includa un controllo della configurazione dell'agente. Il controllo della configurazione verifica che l'agente abbia accesso alla rete agli endpoint richiesti. Se la distribuzione non riesce a causa di problemi di connettività, è possibile accedere al report di convalida e ai registri dall'host dell'agente. In alcuni casi, se sei sicuro che l'agente abbia accesso alla rete, puoi scegliere di saltare il controllo. Ad esempio, se stai ancora utilizzando il"punti finali precedenti" utilizzato per gli aggiornamenti degli agenti, la convalida fallisce con un errore. Per evitare ciò, selezionare la casella di controllo per installare senza controllo di convalida. "Scopri come aggiornare l'elenco degli endpoint" .
      - **Password di manutenzione**: Imposta la password per `maint` utente che consente l'accesso alla console di manutenzione dell'agente.
      - **Server NTP**: specificare uno o più server NTP per la sincronizzazione dell'ora.
      - **Nome host**: imposta il nome host per questa VM. Non deve includere il dominio di ricerca. Ad esempio, un FQDN di console10.searchdomain.company.com dovrebbe essere inserito come console10.
      - **DNS primario**: specifica il server DNS primario da utilizzare per la risoluzione dei nomi.
      - **DNS secondario**: specifica il server DNS secondario da utilizzare per la risoluzione dei nomi.
      - Domini di ricerca: specifica il nome del dominio di ricerca da utilizzare durante la risoluzione del nome host. Ad esempio, se il nome di dominio completo è console10.searchdomain.company.com, immettere searchdomain.company.com.
      - **Indirizzo IPv4**: l'indirizzo IP mappato sul nome host.
      - **Maschera di sottorete IPv4**: la maschera di sottorete per l'indirizzo IPv4.
      - **Indirizzo gateway IPv4**: l'indirizzo gateway per l'indirizzo IPv4.
12. Selezionare **Avanti**.
13. Rivedi i dettagli nella finestra **Pronto per il completamento**, seleziona **Fine**.

    La barra delle applicazioni di vSphere mostra l'avanzamento della distribuzione dell'agente della console.
14. Accendere la macchina virtuale.

> Se la distribuzione non riesce, è possibile accedere al report di convalida e ai registri dall'host dell'agente."Scopri come risolvere i problemi di installazione."

Registrare l’agente della console con NetApp Console

Accedi alla Console e associa l’agente della Console alla tua organizzazione. La modalità di accesso dipende dalla modalità in cui si utilizza la Console. Se si utilizza la Console in modalità standard, è possibile effettuare l’accesso tramite il sito Web SaaS. Se si utilizza la Console in modalità riservata o privata, è necessario effettuare l’accesso localmente dall’host dell’agente della Console.

Passi

1. Aprire un browser Web e immettere l’URL dell’host dell’agente della console:

   L’URL dell’host della console può essere un localhost, un indirizzo IP privato o un indirizzo IP pubblico, a seconda della configurazione dell’host. Ad esempio, se l’agente della console si trova nel cloud pubblico senza un indirizzo IP pubblico, è necessario immettere un indirizzo IP privato da un host che ha una connessione all’host dell’agente della console.

2. Registrati o accedi.
3. Dopo aver effettuato l’accesso, configura la Console:
   a. Specificare l’organizzazione della console da associare all’agente della console.
   b. Inserisci un nome per il sistema.
   c. In **Stai utilizzando un ambiente protetto?** mantieni disattivata la modalità con restrizioni.

      La modalità limitata non è supportata quando l’agente Console è installato in locale.

   d. Seleziona **Iniziamo**.

Aggiungere le credenziali del provider cloud alla console

Dopo aver installato e configurato l’agente Console, aggiungi le tue credenziali cloud in modo che l’agente Console disponga delle autorizzazioni necessarie per eseguire azioni in AWS o Azure.

AWS

Prima di iniziare

Se hai appena creato queste credenziali AWS, potrebbero volerci alcuni minuti prima che siano disponibili. Attendi qualche minuto prima di aggiungere le credenziali alla Console.

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**.

Ora puoi andare al "NetApp Console" per iniziare a utilizzare l'agente Console.

Azzurro

Prima di iniziare

Se hai appena creato queste credenziali di Azure, potrebbero volerci alcuni minuti prima che siano disponibili. Attendi qualche minuto prima di aggiungere le credenziali all'agente della console.

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

L'agente della console ora dispone delle autorizzazioni necessarie per eseguire azioni in Azure per tuo conto. Ora puoi andare al "NetApp Console" per iniziare a utilizzare l'agente Console.

Porte per l'agente della console locale

L'agente Console utilizza porte *in entrata* quando installato manualmente su un host Linux locale. Fare riferimento a queste porte per scopi di pianificazione.

Queste regole in entrata si applicano a tutte le modalità di distribuzione NetApp Console .

Protocollo	Porta	Scopo
HTTP	80	• Fornisce l’accesso HTTP dai browser Web client all’interfaccia utente locale • Utilizzato durante il processo di aggiornamento Cloud Volumes ONTAP
HTTPS	443	Fornisce l’accesso HTTPS dai browser Web client all’interfaccia utente locale

Informazioni sul copyright

Informazioni sul marchio commerciale