Amministrare e monitorare

NetApp Console setup and administration

NetApp
February 11, 2026

Sommario

Amministrare e monitorare

Associare gli account di supporto NetApp

Gestisci le credenziali NSS associate alla NetApp Console

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

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

Panoramica

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

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

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

- Registrazione dei sistemi Cloud Volumes ONTAP a consumo

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

- Aggiornamento del software Cloud Volumes ONTAP all'ultima versione

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

Aggiungi un account NSS

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

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

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

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

Passi

1. In **Amministrazione > Supporto**.
2. Selezionare **Gestione NSS**.

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

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

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

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

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

Cosa succederà ora?

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

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

Aggiorna le credenziali NSS

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

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

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

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

Passi

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

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

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

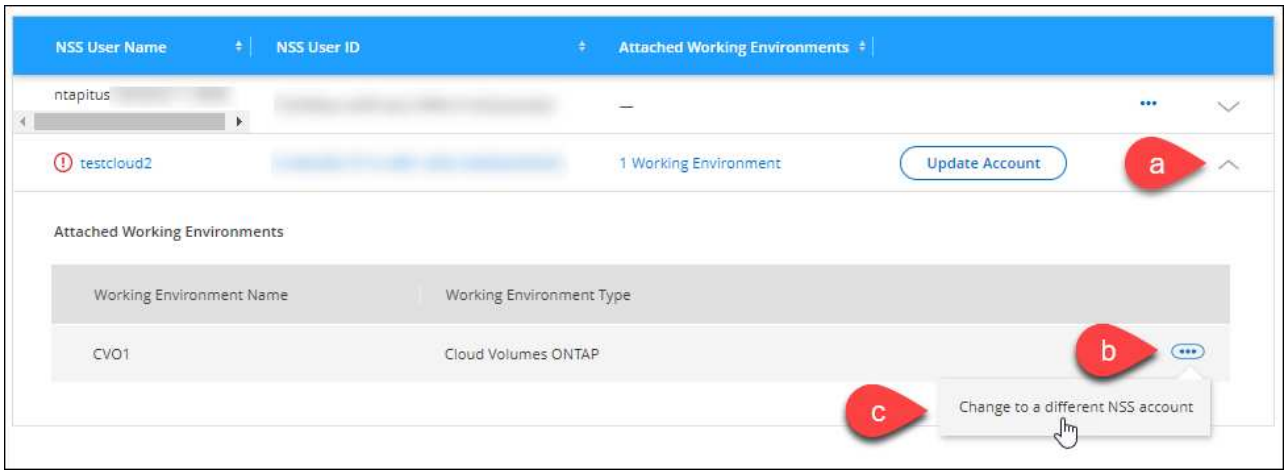
Collega un sistema a un account NSS diverso

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

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

Passi

1. In **Amministrazione > Supporto**.
2. Selezionare **Gestione NSS**.
3. Per modificare l'account NSS, completa i seguenti passaggi:
   a. Espandere la riga relativa all'account del sito di supporto NetApp a cui il sistema è attualmente associato.
   b. Per il sistema per il quale si desidera modificare l'associazione, selezionare •••
   c. Seleziona **Cambia in un altro account NSS**.



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

Visualizza l'indirizzo email di un account NSS

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

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

Passi

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

Rimuovere un account NSS

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

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

Passi

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

Gestisci le credenziali associate al tuo accesso NetApp Console

A seconda delle azioni eseguite nella Console, potresti aver associato le credenziali ONTAP e le credenziali del sito di supporto NetApp (NSS) al tuo accesso utente. Dopo averle associate, potrai visualizzare e gestire tali credenziali. Ad esempio, se modifichi la password per queste credenziali, dovrai aggiornare la password nella Console.

Credenziali ONTAP

Gli utenti necessitano delle credenziali di amministratore ONTAP per individuare i cluster ONTAP nella Console. Tuttavia, l'accesso a ONTAP System Manager dipende dall'utilizzo o meno di un agente Console.

Senza un agente Console

Agli utenti viene richiesto di immettere le proprie credenziali ONTAP per accedere a ONTAP System Manager per il cluster. Gli utenti possono scegliere di salvare queste credenziali nella Console, il che significa che non verrà loro richiesto di immetterle ogni volta. Le credenziali utente sono visibili solo all'utente interessato e possono essere gestite dalla pagina Credenziali utente.

Con un agente Console

Per impostazione predefinita, agli utenti non viene richiesto di immettere le proprie credenziali ONTAP per accedere a ONTAP System Manager. Tuttavia, un amministratore della Console (con il ruolo di amministratore dell'organizzazione) può configurare la Console in modo che richieda agli utenti di immettere le proprie credenziali ONTAP . Quando questa impostazione è abilitata, gli utenti devono immettere ogni volta le proprie credenziali ONTAP .

"Saperne di più."

Credenziali NSS

Le credenziali NSS associate all'accesso alla NetApp Console consentono la registrazione del supporto, la gestione dei casi e l'accesso a Digital Advisor.

- Quando accedi a **Supporto > Risorse** e ti registri per ricevere supporto, ti verrà chiesto di associare le credenziali NSS al tuo login.

  In questo modo la tua organizzazione o il tuo account vengono registrati per il supporto e viene attivato il diritto al supporto. Solo un utente nella tua organizzazione deve associare un account NetApp Support Site al proprio login per registrarsi al supporto e attivare il diritto al supporto. Una volta completata questa operazione, la pagina **Risorse** mostrerà che il tuo account è registrato per l'assistenza.

"Scopri come registrarti per ricevere supporto"

- Quando accedi a **Amministrazione > Supporto > Gestione casi**, ti verrà chiesto di immettere le tue credenziali NSS, se non l'hai già fatto. Questa pagina ti consente di creare e gestire i casi di supporto associati al tuo account NSS e alla tua azienda.
- Quando accedi a Digital Advisor nella Console, ti verrà chiesto di effettuare l'accesso a Digital Advisor inserendo le tue credenziali NSS.

Tieni presente quanto segue in merito all'account NSS associato al tuo accesso:

- L'account è gestito a livello utente, il che significa che non è visibile agli altri utenti che effettuano l'accesso.
- Per ogni utente può essere associato un solo account NSS al Digital Advisor e alla gestione dei casi di supporto.
- Se stai provando ad associare un account NetApp Support Site a un sistema Cloud Volumes ONTAP , puoi scegliere solo tra gli account NSS aggiunti all'organizzazione di cui sei membro.

  Le credenziali a livello di account NSS sono diverse dall'account NSS associato al tuo accesso. Le credenziali a livello di account NSS consentono di distribuire Cloud Volumes ONTAP con BYOL, registrare sistemi PAYGO e aggiornare il relativo software.

  "Scopri di più sull'utilizzo delle credenziali NSS con la tua organizzazione o account NetApp Console" .

Gestisci le tue credenziali utente

Gestisci le tue credenziali utente aggiornando il nome utente e la password oppure eliminando le credenziali.

Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Selezionare **Credenziali utente**.
3. Se non disponi ancora di credenziali utente, puoi selezionare **Aggiungi credenziali NSS** per aggiungere il tuo account NetApp Support Site.
4. Gestisci le credenziali esistenti scegliendo le seguenti opzioni dal menu Azioni:
   - **Aggiorna credenziali**: aggiorna il nome utente e la password dell'account.
   - **Elimina credenziali**: rimuovi l'account NSS associato al tuo accesso alla Console.

Agenti della console

Scopri di più sugli agenti NetApp Console

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

Un agente Console consente di:

- Orchestra le attività di gestione dello storage dalla NetApp Console, come il provisioning Cloud Volumes ONTAP, la configurazione dei volumi di storage, l'utilizzo della classificazione dei dati e altro ancora.
- Autenticazione tramite i ruoli IAM del tuo provider cloud per l'integrazione della fatturazione degli

abbonamenti

- Utilizzare servizi dati avanzati (NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience e NetApp Cloud Tiering)
- Utilizzare la Console in modalità limitata.

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

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

	Disponibile con agente	**Disponibile senza agente**
Sistemi di archiviazione supportati:		
Amazon FSx per ONTAP	Sì (funzionalità di scoperta e gestione)	Sì (solo scoperta)
Archiviazione Amazon S3	SÌ	NO
Archiviazione BLOB di Azure	SÌ	SÌ
Azure NetApp Files	SÌ	SÌ
Cloud Volumes ONTAP	SÌ	NO
Sistemi della serie E	SÌ	NO
Google Cloud NetApp Volumes	SÌ	SÌ
Bucket di archiviazione di Google Cloud	SÌ	NO
Sistemi StorageGRID	SÌ	NO
Cluster ONTAP on-premise (gestione e individuazione avanzate)	Sì (gestione avanzata e scoperta)	No (solo scoperta di base)
Servizi di gestione dello storage disponibili:		
Avvisi	SÌ	NO
Hub di automazione	SÌ	SÌ
Digital Advisor (Active IQ)	SÌ	NO
Gestione delle licenze e degli abbonamenti	SÌ	NO

	Disponibile con agente	Disponibile senza agente
Efficienza economica	SÌ	NO
Metriche della dashboard della home page	Sì[2]	NO
Pianificazione del ciclo di vita	SÌ	No[1]
Sostenibilità	SÌ	NO
Aggiornamenti software	SÌ	SÌ
Carichi di lavoro NetApp	SÌ	SÌ
Servizi dati disponibili:		
NetApp Backup and Recovery	SÌ	NO
Classificazione dei dati	SÌ	NO
NetApp Cloud Tiering	SÌ	NO
NetApp Copy and Sync	SÌ	NO
NetApp Disaster Recovery	SÌ	NO
NetApp Ransomware Resilience	SÌ	NO
NetApp Volume Caching	SÌ	NO

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

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

Gli agenti della console devono essere operativi in ogni momento

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

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

Posizioni supportate

È possibile installare gli agenti nelle seguenti posizioni:

- Servizi Web Amazon
- Microsoft Azure

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

- Google Cloud

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

- Presso la vostra sede

Comunicazione con i provider cloud

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

Modalità limitata

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

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

Come installare un agente Console

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

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

Autorizzazioni del provider cloud

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

Quando si utilizza la Console in modalità standard, il modo in cui si forniscono le autorizzazioni dipende da come si intende creare l'agente della Console.

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

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

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

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

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

Aggiornamenti degli agenti

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

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

Manutenzione del sistema operativo e della VM

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

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

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

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

Sistemi e agenti multipli

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

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

Ecco alcuni esempi di distribuzioni di agenti:

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

Distribuisci un agente della console

AWS

Opzioni di installazione dell'agente console in AWS

Esistono diversi modi per creare un agente Console in AWS. Il metodo più comune è quello diretto dalla NetApp Console .

Sono disponibili le seguenti opzioni di installazione:

- "Crea l'agente Console direttamente dalla Console"(questa è l'opzione standard)

  Questa azione avvia un'istanza EC2 che esegue Linux e il software dell'agente Console in una VPC di tua scelta.

- "Creare un agente della console da AWS Marketplace"

  Questa azione avvia anche un'istanza EC2 che esegue Linux e il software dell'agente della console, ma la distribuzione viene avviata direttamente da AWS Marketplace anziché dalla console.

- "Scarica e installa manualmente il software sul tuo host Linux"

L'opzione di installazione scelta influisce sul modo in cui ci si prepara all'installazione. Ciò include il modo in cui fornisci alla Console le autorizzazioni necessarie per autenticare e gestire le risorse in AWS.

Crea un agente Console in AWS dalla NetApp Console

È possibile creare un agente Console in AWS direttamente dalla NetApp Console. Prima di creare un agente Console in AWS dalla Console, è necessario configurare la rete e preparare le autorizzazioni AWS.

Prima di iniziare

- Dovresti avere un"comprensione degli agenti della console" .
- Dovresti rivedere"Limitazioni dell'agente della console" .

Passaggio 1: configurare la rete per la distribuzione di un agente della console in AWS

Assicurarsi che il percorso di rete in cui si prevede di installare l'agente Console supporti i seguenti requisiti. Questi requisiti consentono all'agente della console di gestire risorse e processi nel cloud ibrido.

VPC e sottorete

Quando si crea l'agente Console, è necessario specificare la VPC e la subnet in cui deve risiedere.

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 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.
\ 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.

Punti finali	Scopo
\ 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.

Endpoint contattati dalla console NetApp

Utilizzando la NetApp Console basata sul Web fornita tramite il livello SaaS, questa contatta diversi endpoint per completare le attività di gestione dei dati. Sono inclusi gli endpoint contattati per distribuire l'agente della Console dalla Console.

"Visualizza l'elenco degli endpoint contattati dalla console NetApp" .

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"

Sarà necessario implementare questo requisito di rete dopo aver creato l'agente Console.

Passaggio 2: impostare le autorizzazioni AWS per l'agente della console

La console deve autenticarsi con AWS prima di poter distribuire l'agente della console nella VPC. Puoi scegliere uno di questi metodi di autenticazione:

- Consentire alla Console di assumere un ruolo IAM che disponga delle autorizzazioni richieste
- Fornire una chiave di accesso AWS e una chiave segreta per un utente IAM che dispone delle autorizzazioni richieste

In entrambe le opzioni, il primo passo è creare un criterio IAM. Questa policy contiene solo le autorizzazioni necessarie per avviare l'agente della console in AWS dalla console.

Se necessario, è possibile limitare la policy IAM utilizzando l'IAM `Condition` elemento. "Documentazione AWS: Elemento Condizione"

Passi

1. Vai alla console AWS IAM.
2. Selezionare **Criteri > Crea criterio**.
3. Selezionare **JSON**.
4. Copia e incolla la seguente policy:

   Questa policy contiene solo le autorizzazioni necessarie per avviare l'agente della console in AWS dalla console. Quando la Console crea l'agente della Console, applica un nuovo set di autorizzazioni all'agente della Console che consente all'agente della Console di gestire le risorse AWS. "Visualizza le autorizzazioni richieste per l'agente della console stesso".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
```

```
            "kms:ListAliases",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/OCCMInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
  ]
}
```

5. Selezionare **Avanti** e aggiungere tag, se necessario.
6. Selezionare **Avanti** e immettere un nome e una descrizione.
7. Selezionare **Crea policy**.
8. È possibile associare il criterio a un ruolo IAM che la Console può assumere oppure a un utente IAM in modo da poter fornire alla Console le chiavi di accesso:
   - (Opzione 1) Impostare un ruolo IAM che la Console può assumere:
     i. Vai alla console AWS IAM nell'account di destinazione.
     ii. In Gestione accessi, seleziona **Ruoli > Crea ruolo** e segui i passaggi per creare il ruolo.
     iii. In **Tipo di entità attendibile**, seleziona **Account AWS**.
     iv. Seleziona **Un altro account AWS** e inserisci l'ID dell'account SaaS della console: 952013314444
     v. Seleziona la policy creata nella sezione precedente.
     vi. Dopo aver creato il ruolo, copia l'ARN del ruolo in modo da poterlo incollare nella Console quando crei l'agente della Console.
   - (Opzione 2) Impostare le autorizzazioni per un utente IAM in modo da poter fornire alla Console le chiavi di accesso:
     i. Dalla console AWS IAM, seleziona **Utenti** e poi seleziona il nome utente.
     ii. Seleziona **Aggiungi autorizzazioni > Allega direttamente i criteri esistenti**.
     iii. Seleziona la policy che hai creato.
     iv. Selezionare **Avanti** e quindi **Aggiungi autorizzazioni**.
     v. Assicurati di disporre della chiave di accesso e della chiave segreta per l'utente IAM.

Risultato

Ora dovresti avere un ruolo IAM con le autorizzazioni richieste o un utente IAM con le autorizzazioni richieste. Quando si crea l'agente Console dalla Console, è possibile fornire informazioni sul ruolo o sulle chiavi di accesso.

Passaggio 3: creare l'agente della console

Creare l'agente Console direttamente dalla console basata sul Web.

Informazioni su questo compito

- La creazione dell'agente Console dalla Console distribuisce un'istanza EC2 in AWS utilizzando una configurazione predefinita. Non passare a un'istanza EC2 più piccola con meno CPU o meno RAM dopo aver creato l'agente Console. "Scopri la configurazione predefinita per l'agente Console" .
- Quando la Console crea l'agente Console, crea anche un ruolo IAM e un profilo per l'agente. Questo ruolo include autorizzazioni che consentono all'agente della console di gestire le risorse AWS. Assicurarsi che il ruolo venga aggiornato man mano che nelle versioni future verranno aggiunte nuove autorizzazioni. "Scopri di più sulla policy IAM per l'agente della console".

Prima di iniziare

Dovresti avere quanto segue:

- Un metodo di autenticazione AWS: un ruolo IAM o chiavi di accesso per un utente IAM con le autorizzazioni richieste.
- Una VPC e una subnet che soddisfano i requisiti di rete.
- Una coppia di chiavi per l'istanza EC2.
- Dettagli su un server proxy, se è necessario un proxy per l'accesso a Internet dall'agente della console.
- Impostare"requisiti di rete" .
- Impostare"Autorizzazioni AWS" .

Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona **Distribuisci agente > AWS**
3. Per creare l'agente Console, seguire i passaggi della procedura guidata:
4. Nella pagina **Introduzione** viene fornita una panoramica del processo
5. Nella pagina **Credenziali AWS**, specifica la tua regione AWS e poi scegli un metodo di autenticazione, che può essere un ruolo IAM che la Console può assumere oppure una chiave di accesso AWS e una chiave segreta.

   Se si sceglie **Assumi ruolo**, è possibile creare il primo set di credenziali dalla procedura guidata di distribuzione dell'agente della console. Ogni ulteriore set di credenziali deve essere creato dalla pagina Credenziali. Saranno quindi disponibili tramite la procedura guidata in un elenco a discesa. "Scopri come aggiungere credenziali aggiuntive" .

6. Nella pagina **Dettagli**, fornire i dettagli sull'agente della console.
   - Inserisci un nome.
   - Aggiungi tag personalizzati (metadati).
   - Scegli se desideri che la Console crei un nuovo ruolo con le autorizzazioni richieste oppure se desideri

selezionare un ruolo esistente che hai impostato con"i permessi richiesti" .

- Scegliere se si desidera crittografare i dischi EBS dell'agente Console. È possibile utilizzare la chiave di crittografia predefinita oppure una chiave personalizzata.

7. Nella pagina **Rete**, specificare una VPC, una subnet e una coppia di chiavi per l'agente, scegliere se abilitare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.

   Assicurati di disporre della coppia di chiavi corretta per accedere alla macchina virtuale dell'agente Console. Senza una coppia di chiavi non è possibile accedervi.

8. Nella pagina **Gruppo di sicurezza**, scegliere se creare un nuovo gruppo di sicurezza o se selezionarne uno esistente che consenta le regole in entrata e in uscita richieste.

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

9. Rivedi le tue selezioni per verificare che la configurazione sia corretta.

   a. La casella di controllo **Convalida configurazione agente** è selezionata per impostazione predefinita affinché la Console convalidi i requisiti di connettività di rete durante la distribuzione. Se la Console non riesce a distribuire l'agente, fornisce un report per aiutarti a risolvere il problema. Se la distribuzione riesce, non viene fornito alcun report.

   Se stai ancora utilizzando il"punti finali precedenti" utilizzato per gli aggiornamenti degli agenti, la convalida fallisce con un errore. Per evitare ciò, deselezionare la casella di controllo per saltare il controllo di convalida.

10. Selezionare **Aggiungi**.

    La console distribuisce l'agente in circa 10 minuti. Rimani sulla pagina fino al completamento del processo.

Risultato

Una volta completato il processo, l'agente della Console sarà disponibile per l'uso dalla Console.

Se la distribuzione non riesce, puoi scaricare un report e i registri dalla Console per aiutarti a risolvere i problemi."Scopri come risolvere i problemi di installazione."

Se disponi di bucket Amazon S3 nello stesso account AWS in cui hai creato l'agente della console, vedrai apparire automaticamente un ambiente di lavoro Amazon S3 nella pagina **Sistemi**. "Scopri come gestire i bucket S3 dalla NetApp Console"

Creare un agente della console da AWS Marketplace

È possibile creare un agente Console in AWS direttamente da AWS Marketplace. Per creare un agente Console da AWS Marketplace, è necessario configurare la rete, preparare le autorizzazioni AWS, esaminare i requisiti dell'istanza e quindi creare l'agente Console.

Prima di iniziare

- Dovresti avere un"comprensione degli agenti della console" .
- Dovresti rivedere"Limitazioni dell'agente della console" .

Passaggio 1: configurare la rete

Assicurarsi che il percorso di rete per l'agente della console soddisfi i seguenti requisiti per gestire le risorse del cloud ibrido.

VPC e sottorete

Quando si crea l'agente Console, è necessario specificare la VPC e la subnet in cui deve risiedere.

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 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.

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.

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"

Implementare questo accesso alla rete dopo aver creato l'agente Console.

Passaggio 2: impostare le autorizzazioni AWS

Per preparare la distribuzione di un marketplace, crea policy IAM in AWS e associale a un ruolo IAM. Quando si crea l'agente della console da AWS Marketplace, viene richiesto di selezionare il 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.

      Potrebbe essere necessario creare una seconda policy basata sui servizi dati NetApp che si intende utilizzare. 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. 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 che puoi associare all'istanza EC2 durante la distribuzione da AWS Marketplace.

Passaggio 3: rivedere i requisiti dell'istanza

Quando si crea l'agente Console, è necessario scegliere un tipo di istanza EC2 che soddisfi i seguenti requisiti.

processore
8 core o 8 vCPU

Memoria RAM
32 GB

Tipo di istanza AWS EC2
Un tipo di istanza che soddisfa i requisiti di CPU e RAM. NetApp consiglia t3.2xlarge.

Passaggio 4: creare l'agente della console

Crea l'agente della console direttamente da AWS Marketplace.

Informazioni su questo compito

La creazione dell'agente Console da AWS Marketplace distribuisce un'istanza EC2 in AWS utilizzando una configurazione predefinita. "Scopri la configurazione predefinita per l'agente Console" .

Prima di iniziare

Dovresti avere quanto segue:

- Una VPC e una subnet che soddisfano i requisiti di rete.
- Un ruolo IAM con una policy associata che include le autorizzazioni richieste per l'agente della console.
- Autorizzazioni per iscriversi e annullare l'iscrizione ad AWS Marketplace per il tuo utente IAM.
- Una conoscenza dei requisiti di CPU e RAM per l'istanza.
- 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**.

  AWS avvia l'agente della console con le impostazioni specificate e l'agente della console viene eseguito in circa dieci minuti.

> Se l'installazione non riesce, è possibile visualizzare i registri e un report per risolvere il problema."Scopri come risolvere i problemi di installazione."

8. Aprire un browser Web da un host che dispone di una connessione alla macchina virtuale dell'agente Console e all'URL dell'agente Console.
9. Dopo aver effettuato l'accesso, configura l'agente 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.

      Per utilizzare la Console in modalità standard, disattivare la modalità limitata. Dovresti abilitare la modalità limitata solo se disponi di un ambiente sicuro e desideri disconnettere questo account dai servizi backend della Console. Se è così,"segui i passaggi per iniziare a usare NetApp Console in modalità limitata" .
   d. Seleziona **Iniziamo**.

Risultato

L'agente Console è ora installato e configurato con la tua organizzazione Console.

Apri un browser web e vai su "NetApp Console" per iniziare a utilizzare l'agente Console con la Console.

Se disponi di bucket Amazon S3 nello stesso account AWS in cui hai creato l'agente della console, vedrai

apparire automaticamente un ambiente di lavoro Amazon S3 nella pagina **Sistemi**. "Scopri come gestire i bucket S3 dalla NetApp Console"

Installa manualmente l'agente Console in AWS

È possibile installare manualmente un agente Console su un host Linux in esecuzione su AWS. Per installare manualmente l'agente Console sul tuo host Linux, devi esaminare i requisiti dell'host, configurare la rete, preparare le autorizzazioni AWS, installare l'agente Console e quindi fornire le autorizzazioni preparate.

Prima di iniziare

- Dovresti avere un"comprensione degli agenti della console" .
- Dovresti rivedere"Limitazioni dell'agente della console" .

Passaggio 1: rivedere i requisiti dell'host

Assicurarsi che l'host che esegue il software dell'agente Console soddisfi i requisiti relativi al sistema operativo, alla RAM e alle porte.

> 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.

Tipo di istanza AWS EC2

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

Ipervisore

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

Requisiti del sistema operativo e del contenitore

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

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

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

coppia di chiavi

Quando si crea l'agente Console, è necessario selezionare una coppia di chiavi EC2 da utilizzare con l'istanza.

Limite di hop di risposta PUT quando si utilizza IMDSv2

Se IMDSv2 è abilitato (impostazione predefinita per le nuove istanze EC2), impostare il limite di hop della risposta PUT su 3. In caso contrario, il sistema visualizza un errore di inizializzazione dell'interfaccia utente durante la configurazione dell'agente.

- "Richiedere l'uso di IMDSv2 sulle istanze Amazon EC2"
- "Documentazione AWS: modifica del limite di hop della risposta PUT"

Passaggio 2: installare 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 3: configurazione della rete

Assicurati che il percorso di rete supporti i seguenti requisiti affinché l'agente della console possa gestire le risorse nel tuo cloud ibrido.

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.

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.

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.

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"

Passaggio 4: impostare le autorizzazioni AWS per la console

Fornire le autorizzazioni AWS alla NetApp Console utilizzando una di queste opzioni:

- Opzione 1: creare policy IAM e associarle a un ruolo IAM che è possibile associare all'istanza EC2.
- Opzione 2: fornire alla Console la chiave di accesso AWS per un utente IAM che dispone delle autorizzazioni richieste.

Seguire i passaggi per preparare le autorizzazioni per la Console.

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. 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 che puoi associare all'istanza EC2 dopo aver installato l'agente Console.

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.

Risultato

Ora hai un utente IAM che ha le autorizzazioni richieste e una chiave di accesso che puoi fornire alla

Console.

Passaggio 5: installare l'agente della console

Dopo aver completato i prerequisiti, installa manualmente il software sul tuo host Linux.

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.

2. Attendi il completamento dell'installazione.

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

   Se l'installazione non riesce, puoi visualizzare il report e i registri di installazione per aiutarti a risolvere i problemi."Scopri come risolvere i problemi di installazione."

1. Aprire un browser Web da un host che dispone di una connessione alla macchina virtuale dell'agente Console e immettere il seguente URL:

   https://ipaddress

2. Dopo aver effettuato l'accesso, configura l'agente Console:

   a. Specificare l'organizzazione da associare all'agente Console.

   b. Inserisci un nome per il sistema.

   c. In **Stai utilizzando un ambiente protetto?** mantieni disattivata la modalità con restrizioni.

      È consigliabile disattivare la modalità limitata perché questi passaggi descrivono come utilizzare la Console in modalità standard. Dovresti abilitare la modalità limitata solo se disponi di un ambiente sicuro e desideri disconnettere questo account dai servizi backend. Se è così,"segui i passaggi per iniziare a utilizzare la NetApp Console in modalità limitata" .

   d. Seleziona **Iniziamo**.

Se disponi di bucket Amazon S3 nello stesso account AWS in cui hai creato l'agente della console, vedrai automaticamente un sistema di archiviazione Amazon S3 apparire nella pagina **Sistemi**. "Scopri come gestire i bucket S3 da NetApp ConsoleP"

Passaggio 6: fornire le autorizzazioni alla NetApp Console

Dopo aver installato l'agente Console, fornisci le autorizzazioni AWS configurate in modo che l'agente Console possa gestire i tuoi dati e l'infrastruttura di storage in AWS.

Ruolo IAM

Collega il ruolo IAM creato all'istanza EC2 dell'agente Console.

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**.

Vai al "NetApp Console" per iniziare a utilizzare l'agente Console.

Chiave di accesso AWS

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

Passi

1. Assicurarsi che nella Console sia attualmente selezionato l'agente Console corretto.
2. Selezionare **Amministrazione > Credenziali**.
3. Selezionare **Credenziali dell'organizzazione**.
4. 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**.

Vai al "NetApp Console" per iniziare a utilizzare l'agente Console.

Azzurro

Opzioni di installazione dell'agente console in Azure

Esistono diversi modi per creare un agente Console in Azure. Il metodo più comune è quello diretto dalla NetApp Console .

Sono disponibili le seguenti opzioni di installazione:

- "Crea un agente Console direttamente dalla NetApp Console"(questa è l'opzione standard)

  Questa azione avvia una macchina virtuale che esegue Linux e il software dell'agente Console in una rete virtuale di tua scelta.

- "Creare un agente console da Azure Marketplace"

  Questa azione avvia anche una macchina virtuale che esegue Linux e il software dell'agente della console, ma la distribuzione viene avviata direttamente da Azure Marketplace anziché dalla console.

- "Scarica e installa manualmente il software sul tuo host Linux"

L'opzione di installazione scelta influisce sul modo in cui ci si prepara all'installazione. Ciò include il modo in cui si forniscono all'agente della console le autorizzazioni necessarie per autenticare e gestire le risorse in Azure.

Creare un agente console in Azure dalla NetApp Console

Per creare un agente Console in Azure dalla NetApp Console, è necessario configurare la rete, preparare le autorizzazioni di Azure e quindi creare l'agente Console.

Prima di iniziare

- Dovresti avere un"comprensione degli agenti della console" .
- Dovresti rivedere"Limitazioni dell'agente della console" .

Passaggio 1: configurare la rete

Assicurarsi che il percorso di rete in cui si prevede di installare l'agente Console supporti i seguenti requisiti. Questi requisiti consentono all'agente Console di gestire le risorse cloud ibride.

Regione azzurra

Se si utilizza Cloud Volumes ONTAP, l'agente della console deve essere distribuito nella stessa regione di Azure dei sistemi Cloud Volumes ONTAP che gestisce oppure nella "Coppia di regioni di Azure" per i sistemi Cloud Volumes ONTAP . Questo requisito garantisce che venga utilizzata una connessione Azure Private Link tra Cloud Volumes ONTAP e i relativi account di archiviazione associati.

"Scopri come Cloud Volumes ONTAP utilizza un collegamento privato di Azure"

VNet e subnet

Quando si crea l'agente Console, è necessario specificare la rete virtuale e la subnet in cui deve risiedere.

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 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
\ 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.

Punti finali	Scopo
\ 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.
\ 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.

Punti finali	Scopo
\ 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.

Endpoint contattati dalla console NetApp

Utilizzando la NetApp Console basata sul Web fornita tramite il livello SaaS, questa contatta diversi endpoint per completare le attività di gestione dei dati. Sono inclusi gli endpoint contattati per distribuire l'agente della Console dalla Console.

"Visualizza l'elenco degli endpoint contattati dalla console NetApp" .

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"

Dopo aver creato l'agente Console, è necessario implementare questo requisito di rete.

Passaggio 2: creare un criterio di distribuzione dell'agente della console (ruolo personalizzato)

È necessario creare un ruolo personalizzato che disponga delle autorizzazioni per distribuire l'agente Console in Azure.

Crea un ruolo personalizzato di Azure che puoi assegnare al tuo account Azure o a un'entità servizio Microsoft Entra. La console esegue l'autenticazione con Azure e utilizza queste autorizzazioni per creare l'agente della console per tuo conto.

La console distribuisce la macchina virtuale dell'agente console in Azure, abilita un "identità gestita assegnata dal sistema" , crea il ruolo richiesto e lo assegna alla VM. "Esaminare come la Console utilizza le autorizzazioni" .

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. Copiare le autorizzazioni richieste per un nuovo ruolo personalizzato in Azure e salvarle in un file JSON.

   Questo ruolo personalizzato contiene solo le autorizzazioni necessarie per avviare la macchina virtuale dell'agente della console in Azure dalla console. Non utilizzare questa politica per altre situazioni. Quando la Console crea l'agente Console, applica un nuovo set di autorizzazioni alla VM dell'agente Console che consente all'agente Console di gestire le risorse di Azure.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
```

```
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
```

```
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Azure SetupAsService",
  "IsCustom": "true"
}
```

2. Modifica il JSON aggiungendo l'ID della tua sottoscrizione Azure all'ambito assegnabile.

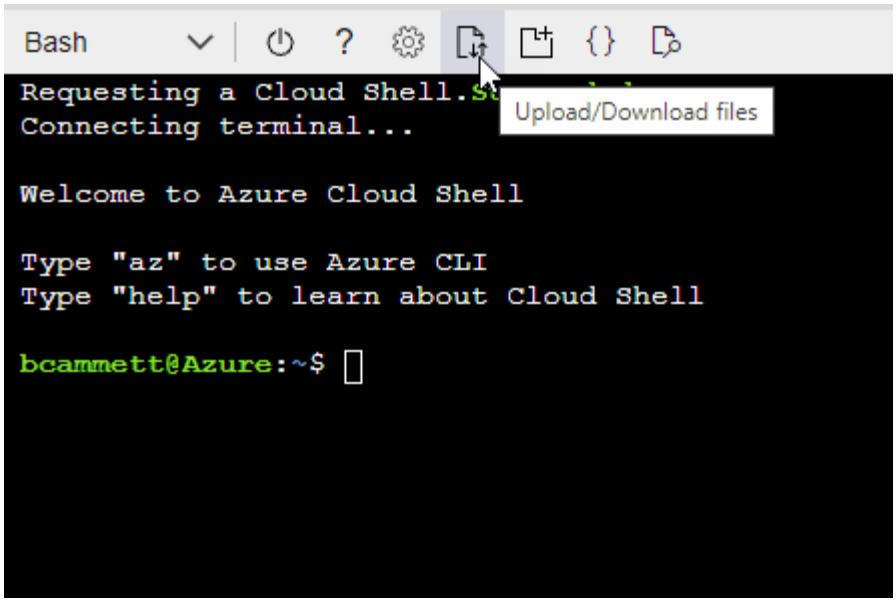
   Esempio

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]
```

3. 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. Immettere il seguente comando dell'interfaccia della riga di comando di Azure:

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

Ora hai un ruolo personalizzato denominato *Azure SetupAsService*. Puoi applicare questo ruolo personalizzato al tuo account utente o a un'entità servizio.

Passaggio 3: imposta l'autenticazione

Quando si crea l'agente della console dalla console, è necessario fornire un accesso che consenta alla console di autenticarsi con Azure e distribuire la macchina virtuale. Hai due opzioni:

1. Quando richiesto, Sign in con il tuo account Azure. Questo account deve disporre di autorizzazioni Azure specifiche. Questa è l'opzione predefinita.
2. Fornire dettagli su un'entità servizio Microsoft Entra. Anche questo servizio principale richiede autorizzazioni specifiche.

Seguire i passaggi per preparare uno di questi metodi di autenticazione da utilizzare con la Console.

Account Azure

Assegnare il ruolo personalizzato all'utente che distribuirà l'agente della Console dalla Console.

Passi

1. Nel portale di Azure, aprire il servizio **Sottoscrizioni** e selezionare la sottoscrizione dell'utente.
2. Fare clic su **Controllo accessi (IAM)**.
3. Fare clic su **Aggiungi** > **Aggiungi assegnazione ruolo** e quindi aggiungere le autorizzazioni:
   a. Selezionare il ruolo **Azure SetupAsService** e fare clic su **Avanti**.

      Azure SetupAsService è il nome predefinito fornito nei criteri di distribuzione dell'agente della console per Azure. Se hai scelto un nome diverso per il ruolo, seleziona quel nome.

   b. Mantieni selezionato **Utente, gruppo o entità servizio**.
   c. Fai clic su **Seleziona membri**, scegli il tuo account utente e fai clic su **Seleziona**.
   d. Fare clic su **Avanti**.
   e. Fare clic su **Revisiona + assegna**.

Principale del servizio

Invece di accedere con il tuo account Azure, puoi fornire alla Console le credenziali di un'entità servizio di Azure che dispone delle autorizzazioni necessarie.

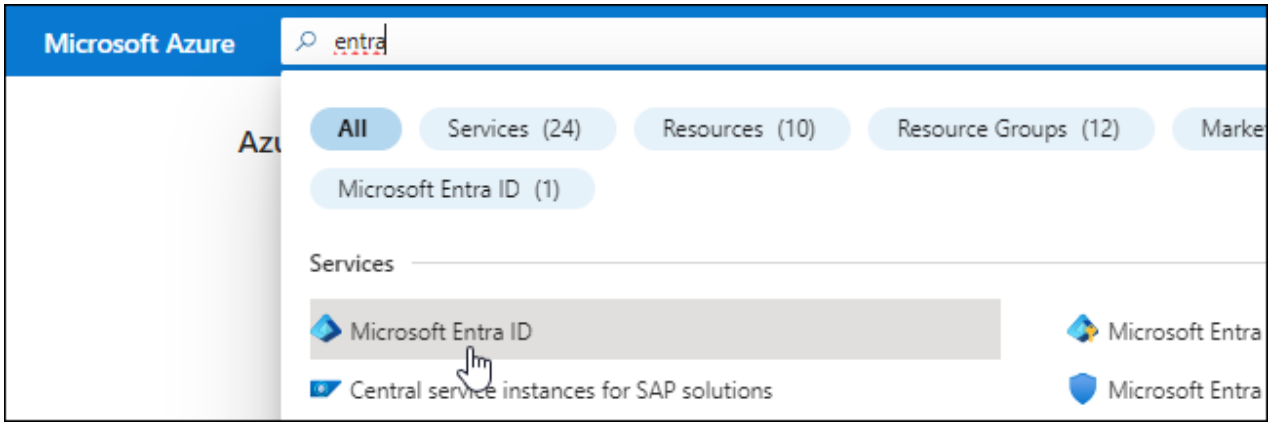
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie alla console.

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**.

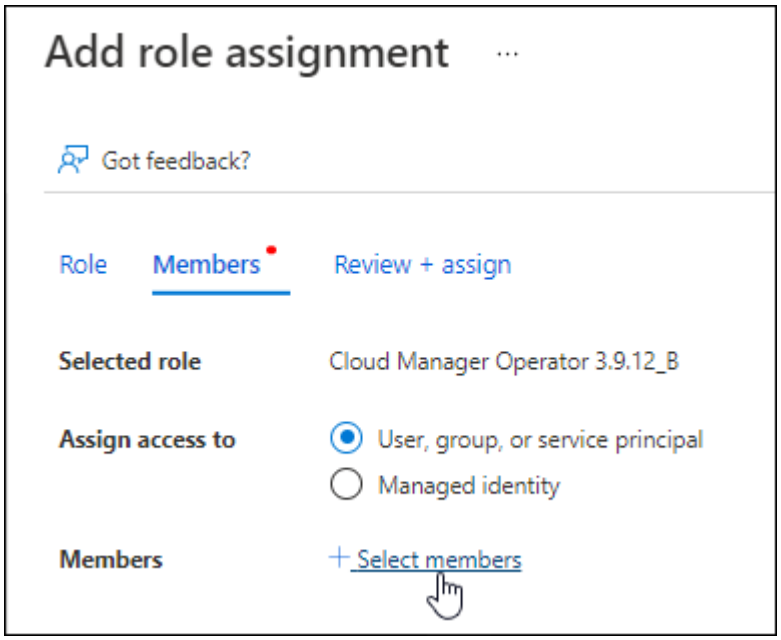
   Hai creato l'applicazione AD e il servizio principale.

Assegna il ruolo personalizzato all'applicazione

1. Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
2. Seleziona l'abbonamento.
3. Fare clic su **Controllo accessi (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
4. Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e fai clic su **Avanti**.
5. Nella scheda **Membri**, completa i seguenti passaggi:

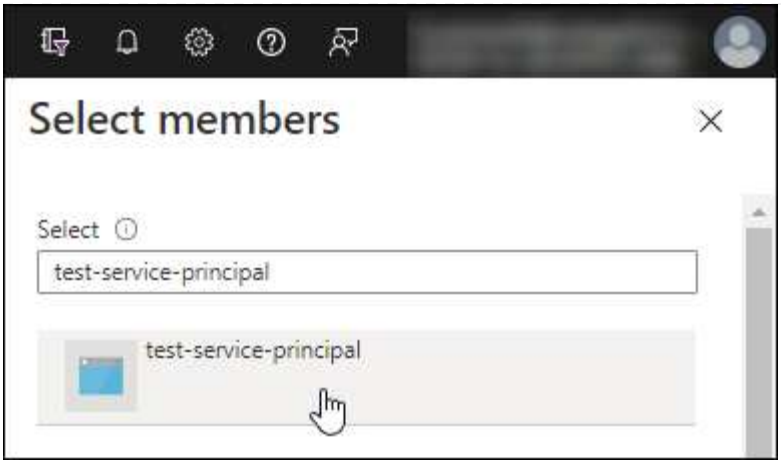
   a. Mantieni selezionato **Utente, gruppo o entità servizio**.

   b. Fare clic su **Seleziona membri**.



   c. Cerca il nome dell'applicazione.

   Ecco un esempio:



a. Selezionare l'applicazione e fare clic su **Seleziona**.
b. Fare clic su **Avanti**.

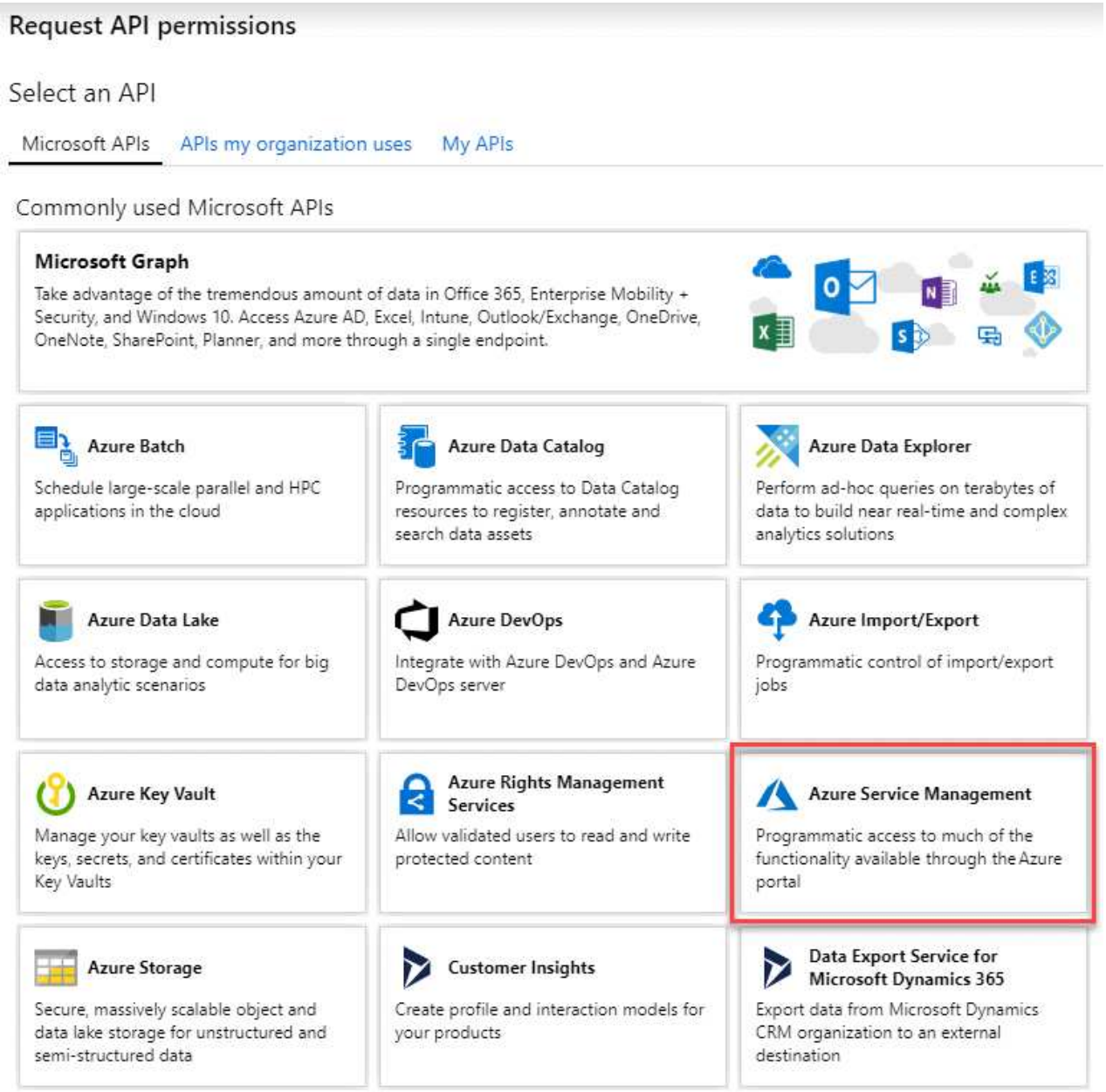
6. Fare clic su **Revisiona + assegna**.

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

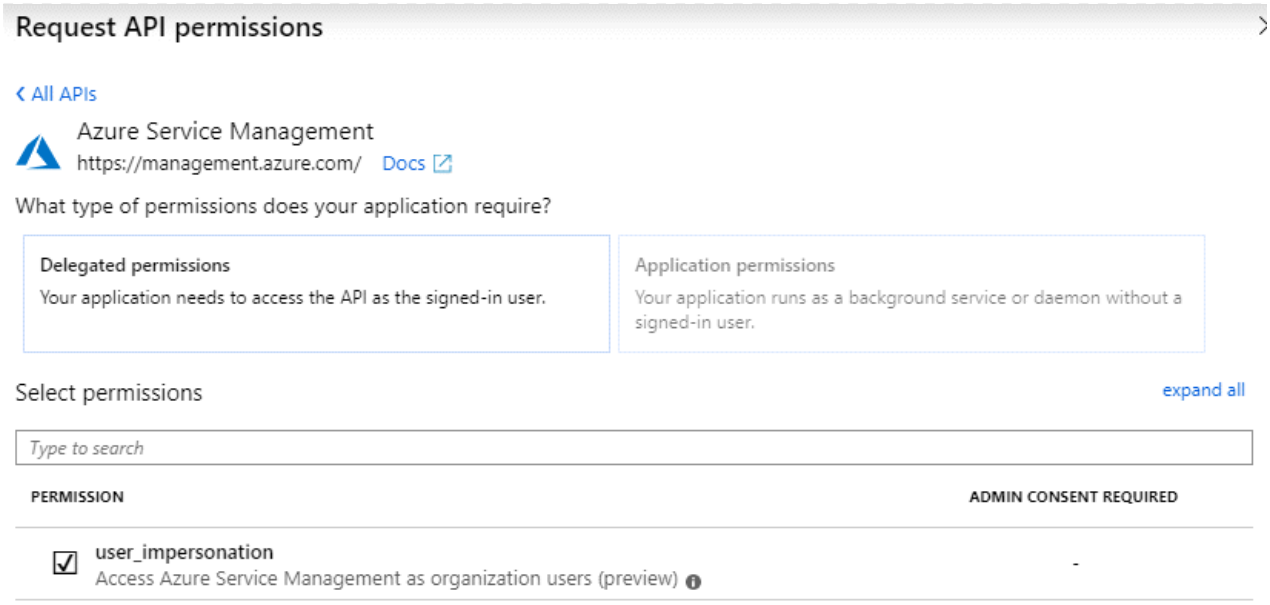
   Se si desidera gestire risorse in più sottoscrizioni di Azure, è necessario associare l'entità servizio a ciascuna di tali sottoscrizioni. Ad esempio, la Console consente di selezionare l'abbonamento che si desidera utilizzare durante la distribuzione Cloud Volumes ONTAP.

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**.

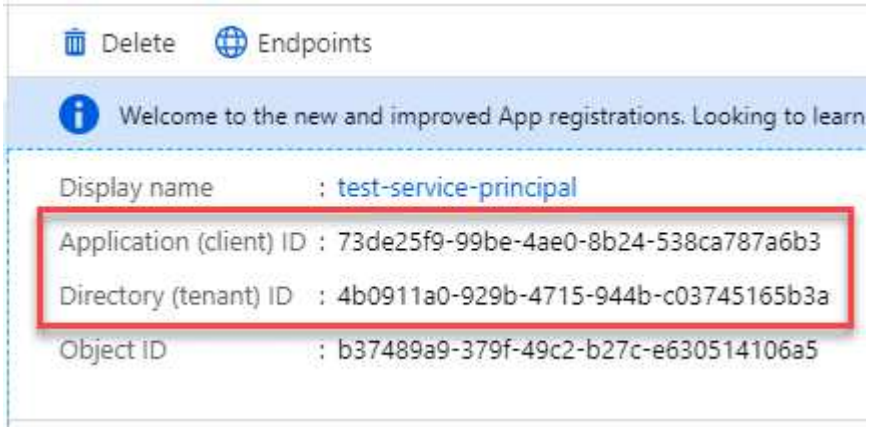


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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. È necessario immettere queste informazioni nella Console quando si crea l'agente della Console.

Passaggio 4: creare l'agente della console

Creare l'agente Console direttamente dalla NetApp Console.

Informazioni su questo compito

- La creazione dell'agente Console dalla Console distribuisce una macchina virtuale in Azure utilizzando una configurazione predefinita. Non passare a un'istanza VM più piccola con meno CPU o meno RAM dopo aver creato l'agente Console. "Scopri la configurazione predefinita per l'agente Console" .
- Quando la Console distribuisce l'agente Console, crea un ruolo personalizzato e lo assegna alla VM dell'agente Console. Questo ruolo include autorizzazioni che consentono all'agente della console di gestire le risorse di Azure. È necessario assicurarsi che il ruolo venga mantenuto aggiornato man mano che vengono aggiunte nuove autorizzazioni nelle versioni successive. "Scopri di più sul ruolo personalizzato per l'agente della console" .

Prima di iniziare

Dovresti avere quanto segue:

- Un abbonamento Azure.
- Una rete virtuale e una subnet nella regione Azure di tua scelta.
- Dettagli su un server proxy, se la tua organizzazione necessita di un proxy per tutto il traffico Internet in uscita:
  - indirizzo IP
  - Credenziali
  - Certificato HTTPS
- Una chiave pubblica SSH, se si desidera utilizzare tale metodo di autenticazione per la macchina virtuale dell'agente Console. L'altra opzione per il metodo di autenticazione è quella di utilizzare una password.

  "Scopri come connetterti a una VM Linux in Azure"

- Se non si desidera che la Console crei automaticamente un ruolo di Azure per l'agente della Console, sarà necessario crearne uno proprio"utilizzando la politica in questa pagina" .

  Queste autorizzazioni sono riservate all'agente Console stesso. Si tratta di un set di autorizzazioni diverso da quello configurato in precedenza per distribuire la VM dell'agente Console.

Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona **Distribuisci agente > Azure**
3. Nella pagina **Revisione**, rivedere i requisiti per la distribuzione di un agente. Tali requisiti sono descritti dettagliatamente anche sopra in questa pagina.
4. Nella pagina **Autenticazione macchina virtuale**, seleziona l'opzione di autenticazione che corrisponde alla configurazione delle autorizzazioni di Azure:

   - Seleziona **Accedi** per accedere al tuo account Microsoft, che dovrebbe disporre delle autorizzazioni necessarie.

     Il modulo è di proprietà e ospitato da Microsoft. Le tue credenziali non vengono fornite a NetApp.

     Se hai già effettuato l'accesso a un account Azure, la console utilizzerà automaticamente tale account. Se hai più account, potrebbe essere necessario prima disconnetterti per assicurarti di utilizzare l'account corretto.

   - Selezionare **Principio servizio Active Directory** per immettere le informazioni sul principio servizio Microsoft Entra che concede le autorizzazioni richieste:
     - ID applicazione (client)
     - ID directory (tenant)
     - Segreto del cliente

   Scopri come ottenere questi valori per un'entità di servizio .

5. Nella pagina **Autenticazione macchina virtuale**, scegli una sottoscrizione di Azure, una posizione, un nuovo gruppo di risorse o un gruppo di risorse esistente, quindi scegli un metodo di autenticazione per la macchina virtuale dell'agente della console che stai creando.

   Il metodo di autenticazione per la macchina virtuale può essere una password o una chiave pubblica SSH.

   "Scopri come connetterti a una VM Linux in Azure"

6. Nella pagina **Dettagli**, inserisci un nome per l'agente, specifica i tag e scegli se desideri che la Console crei un nuovo ruolo con le autorizzazioni richieste o se desideri selezionare un ruolo esistente che hai impostato con"i permessi richiesti" .

   Tieni presente che puoi scegliere gli abbonamenti Azure associati a questo ruolo. Ogni sottoscrizione scelta fornisce all'agente della console le autorizzazioni per gestire le risorse in tale sottoscrizione (ad esempio, Cloud Volumes ONTAP).

7. Nella pagina **Rete**, seleziona una rete virtuale e una subnet, se abilitare un indirizzo IP pubblico e, facoltativamente, specifica una configurazione proxy.

   - Nella pagina **Gruppo di sicurezza**, scegliere se creare un nuovo gruppo di sicurezza o se selezionarne uno esistente che consenta le regole in entrata e in uscita richieste.

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

8. Rivedi le tue selezioni per verificare che la configurazione sia corretta.

   a. La casella di controllo **Convalida configurazione agente** è selezionata per impostazione predefinita affinché la Console convalidi i requisiti di connettività di rete durante la distribuzione. Se la Console non

riesce a distribuire l'agente, fornisce un report per aiutarti a risolvere il problema. Se la distribuzione riesce, non viene fornito alcun report.

Se stai ancora utilizzando il"punti finali precedenti" utilizzato per gli aggiornamenti degli agenti, la convalida fallisce con un errore. Per evitare ciò, deselezionare la casella di controllo per saltare il controllo di convalida.

9. Selezionare **Aggiungi**.

La Console prepara l'agente in circa 10 minuti. Rimani sulla pagina fino al completamento del processo.

Risultato

Una volta completato il processo, l'agente della Console sarà disponibile per l'uso dalla Console.

Se la distribuzione non riesce, puoi scaricare un report e i registri dalla Console per aiutarti a risolvere i problemi."Scopri come risolvere i problemi di installazione."

Se si dispone di Azure Blob Storage nello stesso account Azure in cui è stato creato l'agente Console, Azure Blob Storage verrà visualizzato automaticamente nella pagina **Sistemi**. "Scopri come gestire l'archiviazione BLOB di Azure dalla NetApp Console"

Creare un agente console da Azure Marketplace

È possibile creare un agente Console in Azure direttamente da Azure Marketplace. Per creare un agente Console da Azure Marketplace, è necessario configurare la rete, preparare le autorizzazioni di Azure, esaminare i requisiti dell'istanza e quindi creare l'agente Console.

Prima di iniziare

- Dovresti avere un"comprensione degli agenti della console" .
- Revisione"Limitazioni dell'agente della console" .

Passaggio 1: configurare la rete

Assicurati che il percorso di rete in cui intendi installare l'agente Console supporti i seguenti requisiti. Questi requisiti consentono all'agente Console di gestire le risorse nel tuo cloud ibrido.

Regione azzurra

Se si utilizza Cloud Volumes ONTAP, l'agente della console deve essere distribuito nella stessa regione di Azure dei sistemi Cloud Volumes ONTAP che gestisce oppure nella "Coppia di regioni di Azure" per i sistemi Cloud Volumes ONTAP . Questo requisito garantisce che venga utilizzata una connessione Azure Private Link tra Cloud Volumes ONTAP e i relativi account di archiviazione associati.

"Scopri come Cloud Volumes ONTAP utilizza un collegamento privato di Azure"

VNet e subnet

Quando si crea l'agente Console, è necessario specificare la rete virtuale e la subnet in cui deve risiedere.

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 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
\ 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.
\ 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.

Punti finali	Scopo
\ 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"

Implementare i requisiti di rete dopo aver creato l'agente Console.

Passaggio 2: rivedere i requisiti della VM

Quando si crea l'agente Console, scegliere un tipo di macchina virtuale che soddisfi i seguenti requisiti.

processore

8 core o 8 vCPU

Memoria RAM

32 GB

Dimensioni della VM di Azure

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

Passaggio 3: impostare le autorizzazioni

È possibile concedere le autorizzazioni nei seguenti modi:

- Opzione 1: assegnare un ruolo personalizzato alla macchina virtuale di Azure utilizzando un'identità gestita assegnata dal sistema.
- Opzione 2: fornire alla console le credenziali per un'entità servizio di Azure che disponga delle autorizzazioni richieste.

Per impostare le autorizzazioni per la Console, seguire questi passaggi.

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"

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.

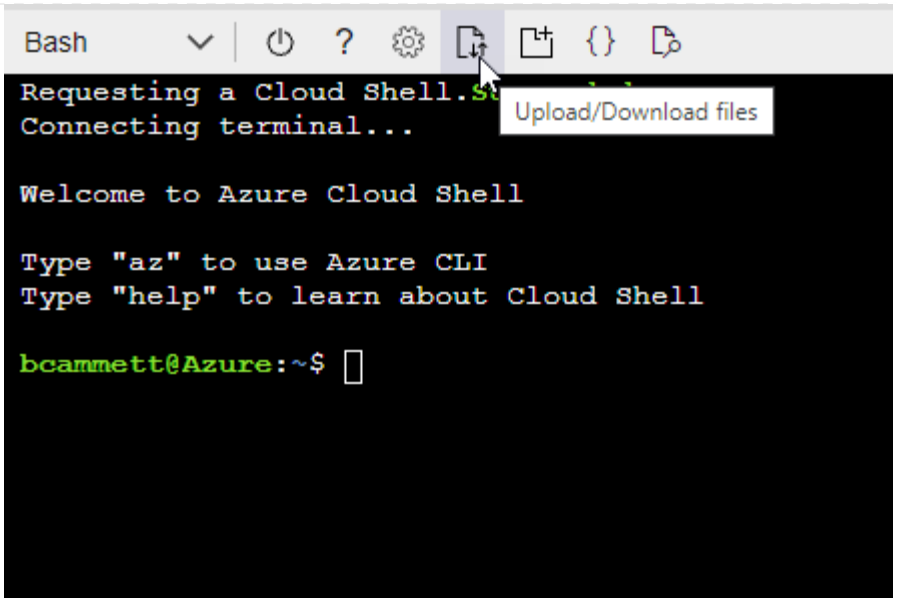
   Esempio

   ```
   "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
```

Principale del servizio

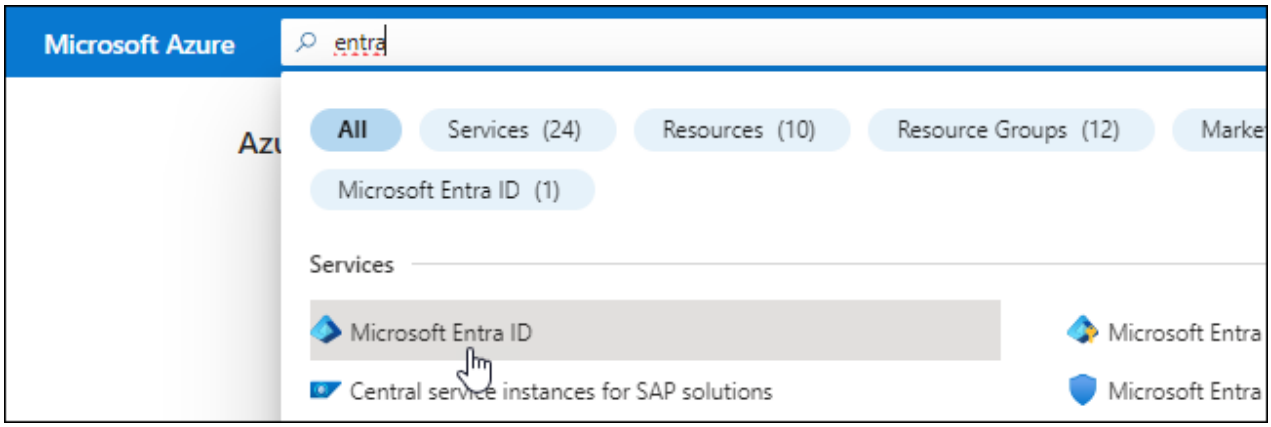
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie alla console.

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 .

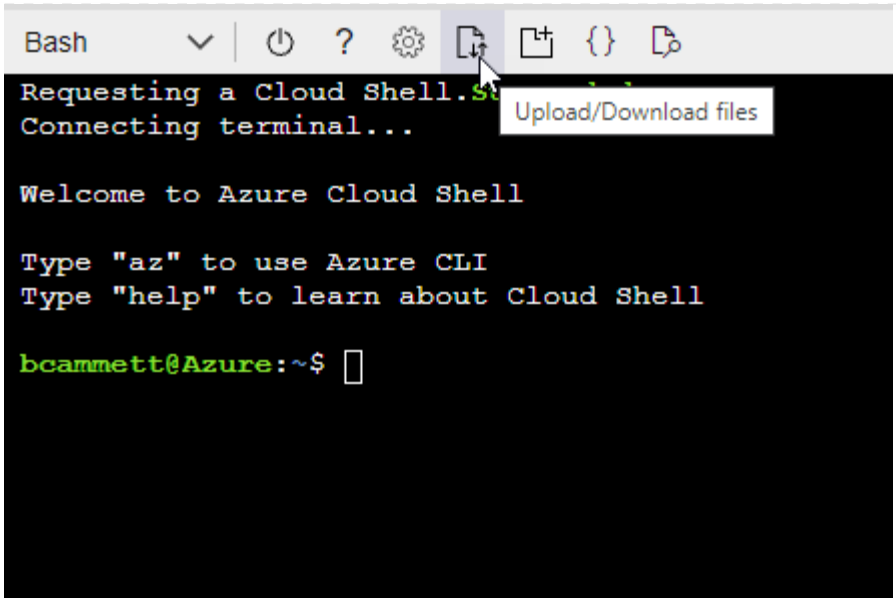
      Esempio

      ```
      "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**.

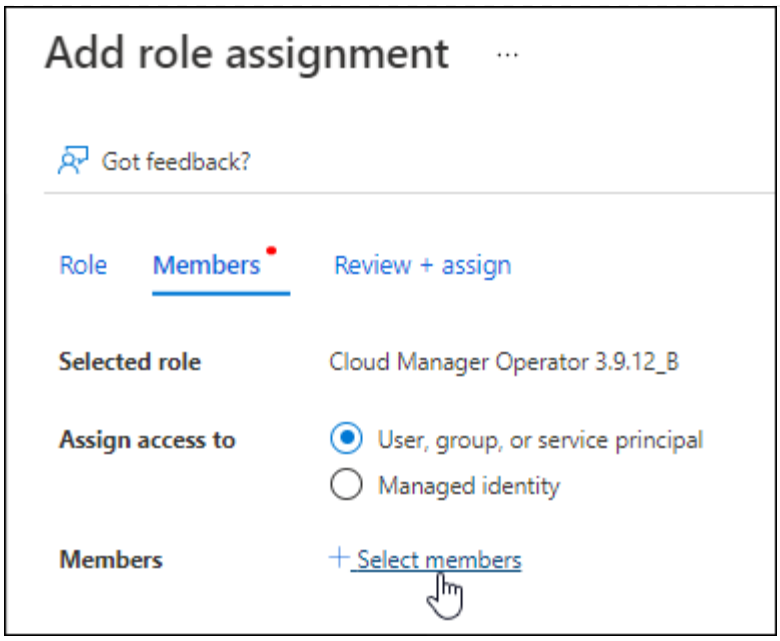
   b. Seleziona l'abbonamento.

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

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

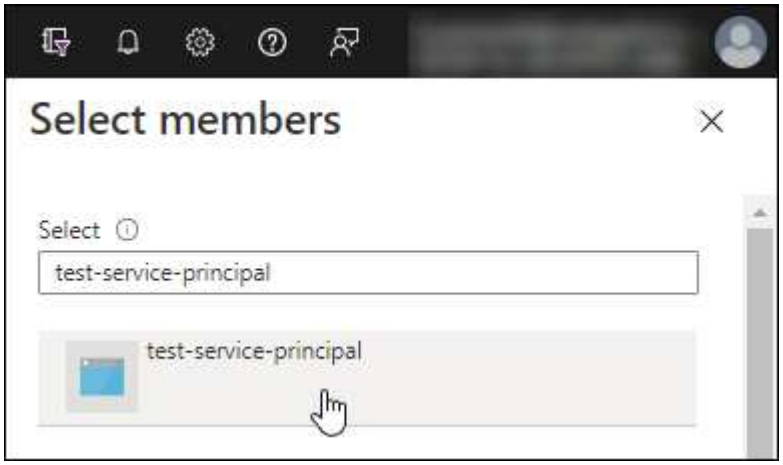
   e. Nella scheda **Membri**, completa i seguenti passaggi:

      - 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**.

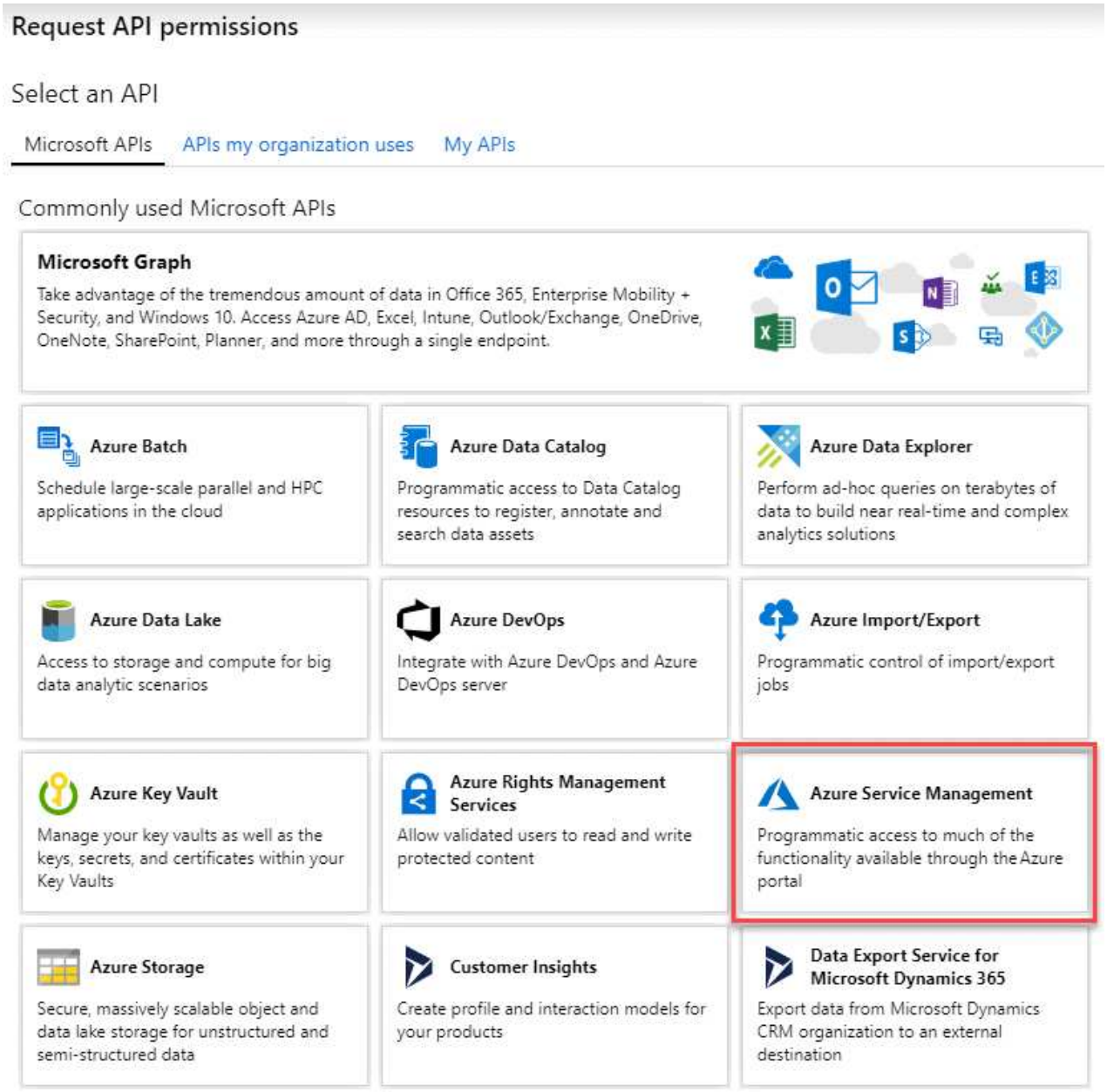
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

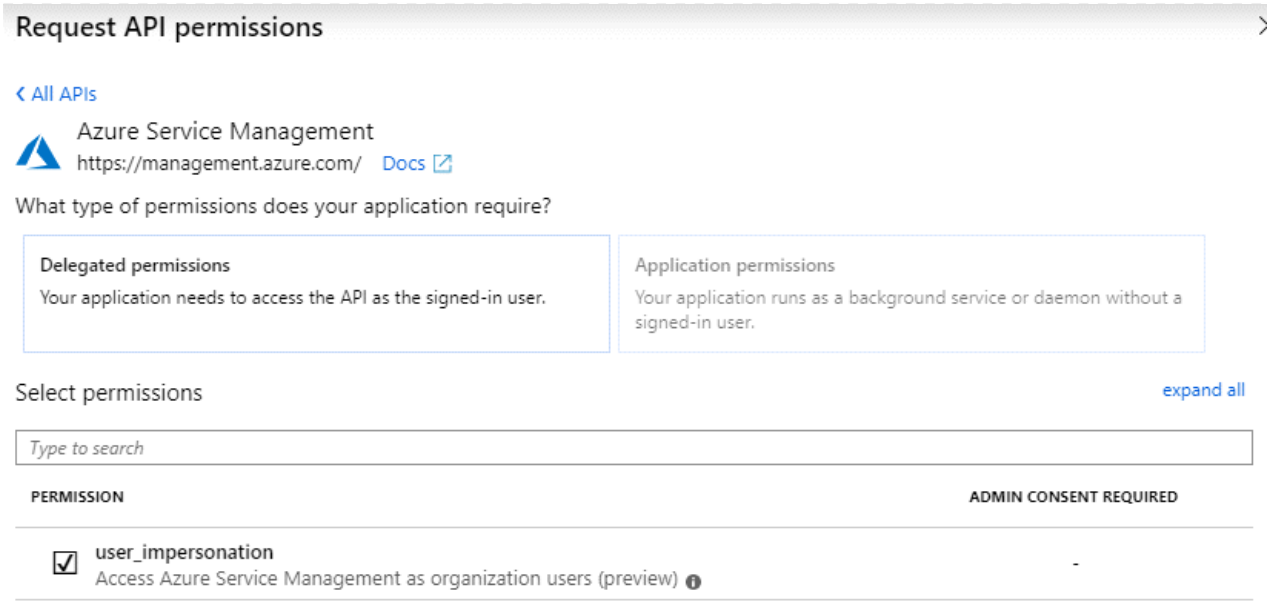
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

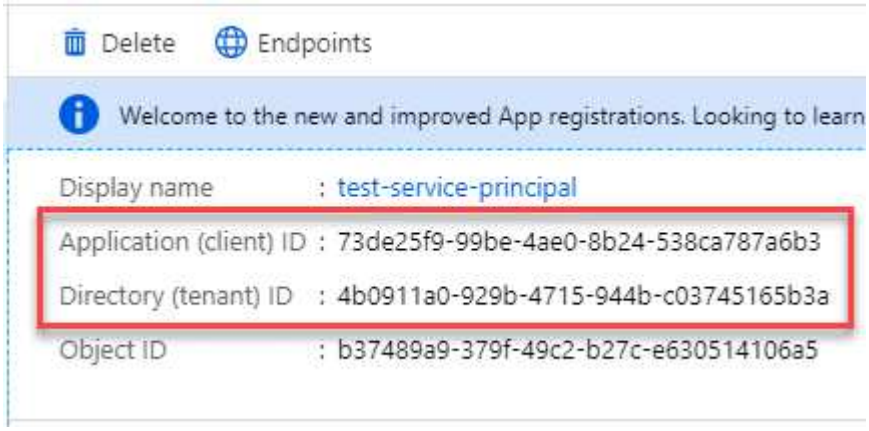


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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

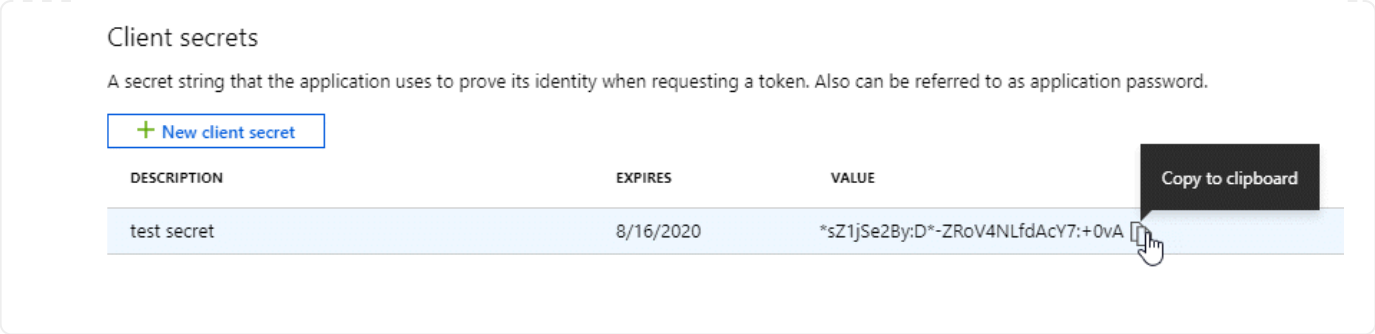
1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)**.



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.



Passaggio 4: creare l'agente della console

Avviare l'agente Console direttamente da Azure Marketplace.

Informazioni su questo compito

La creazione dell'agente Console da Azure Marketplace imposta una macchina virtuale con una configurazione predefinita. "Scopri la configurazione predefinita per l'agente Console" .

Prima di iniziare

Dovresti avere quanto segue:

- Un abbonamento Azure.
- Una rete virtuale e una subnet nella regione Azure di tua scelta.
- Dettagli su un server proxy, se la tua organizzazione necessita di un proxy per tutto il traffico Internet in uscita:
  - indirizzo IP
  - Credenziali
  - Certificato HTTPS
- Una chiave pubblica SSH, se si desidera utilizzare tale metodo di autenticazione per la macchina virtuale dell'agente Console. L'altra opzione per il metodo di autenticazione è quella di utilizzare una password.

  "Scopri come connetterti a una VM Linux in Azure"

- Se non si desidera che la Console crei automaticamente un ruolo di Azure per l'agente della Console, sarà necessario crearne uno proprio"utilizzando la politica in questa pagina" .

  Queste autorizzazioni sono per l'istanza dell'agente Console stessa. Si tratta di un set di autorizzazioni diverso da quello configurato in precedenza per distribuire la VM dell'agente Console.

Passi

1. Vai alla pagina della macchina virtuale dell'agente NetApp Console in Azure Marketplace.

   "Pagina di Azure Marketplace per le regioni commerciali"

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.
- **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**.

  Questa impostazione è importante perché un'identità gestita consente alla macchina virtuale dell'agente della console di identificarsi con l'ID Microsoft Entra senza fornire alcuna credenziale. "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.

   Azure distribuisce la macchina virtuale con le impostazioni specificate. Entro circa dieci minuti dovresti vedere la macchina virtuale e il software dell'agente della console in esecuzione.

   Se l'installazione non riesce, è possibile visualizzare i registri e un report per risolvere il problema."Scopri come risolvere i problemi di installazione."

5. Aprire un browser Web da un host che dispone di una connessione alla macchina virtuale dell'agente Console e immettere il seguente URL:

   https://ipaddress

6. Dopo aver effettuato l'accesso, configura l'agente 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.

      Per utilizzare la Console in modalità standard, disattivare la modalità limitata. Dovresti abilitare la modalità limitata solo se disponi di un ambiente sicuro e desideri disconnettere questo account dai servizi backend della Console. Se è così,"segui i passaggi per iniziare a usare la Console in modalità limitata" .

   d. Seleziona **Iniziamo**.

Risultato

Ora hai installato l'agente Console e lo hai configurato con la tua organizzazione Console.

Se si dispone di un archivio BLOB di Azure nella stessa sottoscrizione di Azure in cui è stato creato l'agente della console, nella pagina **Sistemi** verrà visualizzato automaticamente un sistema di archiviazione BLOB di Azure. "Scopri come gestire l'archiviazione BLOB di Azure dalla console"

Passaggio 5: fornire le autorizzazioni all'agente della console

Ora che hai creato l'agente Console, devi fornirgli le autorizzazioni impostate in precedenza. La concessione delle autorizzazioni consente all'agente della console di gestire i dati e l'infrastruttura di archiviazione in Azure.

Ruolo personalizzato

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.

Cosa succederà ora?

Vai al "NetApp Console" per iniziare a utilizzare l'agente Console.

Principale del servizio

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 console ora dispone delle autorizzazioni necessarie per eseguire azioni in Azure per tuo conto.

Installare manualmente l'agente Console in Azure

Per installare manualmente l'agente Console sul tuo host Linux, devi esaminare i requisiti dell'host, configurare la rete, preparare le autorizzazioni di Azure, installare l'agente Console e quindi fornire le autorizzazioni preparate.

Prima di iniziare

- Dovresti avere un"comprensione degli agenti della console" .
- Dovresti rivedere"Limitazioni dell'agente della console" .

Passaggio 1: rivedere i requisiti dell'host

Il software dell'agente Console deve essere eseguito su un host che soddisfi specifici requisiti del sistema operativo, requisiti di RAM, requisiti di porta e così via.

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.

Dimensioni della VM di Azure

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

Ipervisore

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

Requisiti del sistema operativo e del contenitore

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

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

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

Passaggio 2: installare 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 2. 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 3: configurazione della rete

Assicurarsi che il percorso di rete in cui si prevede di installare l'agente Console supporti i seguenti requisiti. Soddisfacendo questi requisiti, l'agente della console può gestire risorse e processi all'interno del tuo ambiente cloud ibrido.

Regione azzurra

Se si utilizza Cloud Volumes ONTAP, l'agente della console deve essere distribuito nella stessa regione di Azure dei sistemi Cloud Volumes ONTAP che gestisce oppure nella "Coppia di regioni di Azure" per i sistemi Cloud Volumes ONTAP . Questo requisito garantisce che venga utilizzata una connessione Azure Private Link tra Cloud Volumes ONTAP e i relativi account di archiviazione associati.

"Scopri come Cloud Volumes ONTAP utilizza un collegamento privato di Azure"

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.

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.
\ 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.

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"

Passaggio 4: impostare le autorizzazioni di distribuzione dell'agente della console

È necessario fornire le autorizzazioni di Azure all'agente della console utilizzando una delle seguenti opzioni:

- Opzione 1: assegnare un ruolo personalizzato alla macchina virtuale di Azure utilizzando un'identità gestita assegnata dal sistema.
- Opzione 2: fornire all'agente della console le credenziali per un'entità servizio di Azure che disponga delle autorizzazioni richieste.

Seguire i passaggi per preparare le autorizzazioni per l'agente Console.

Crea un ruolo personalizzato per la distribuzione dell'agente della 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.

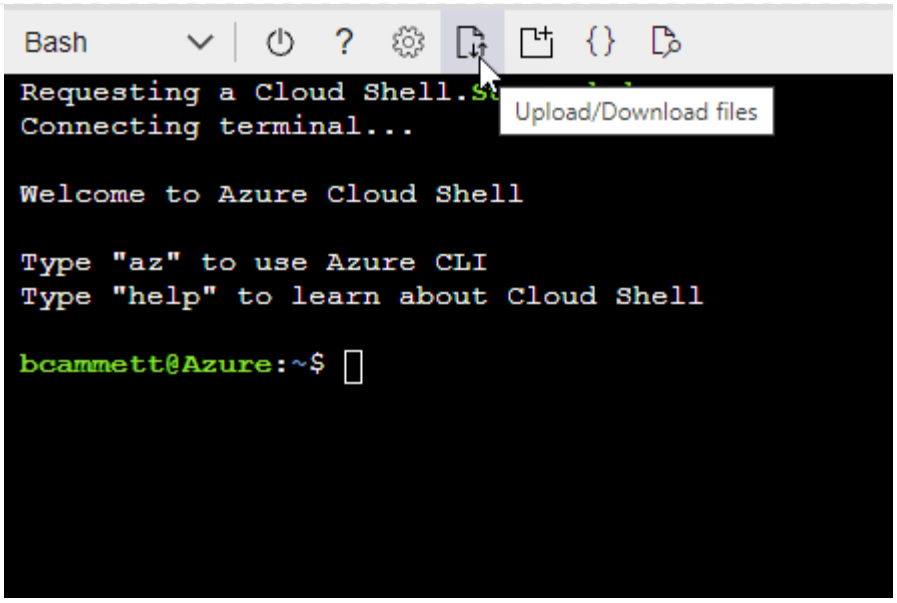
   Esempio

   ```
   "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
```

Principale del servizio

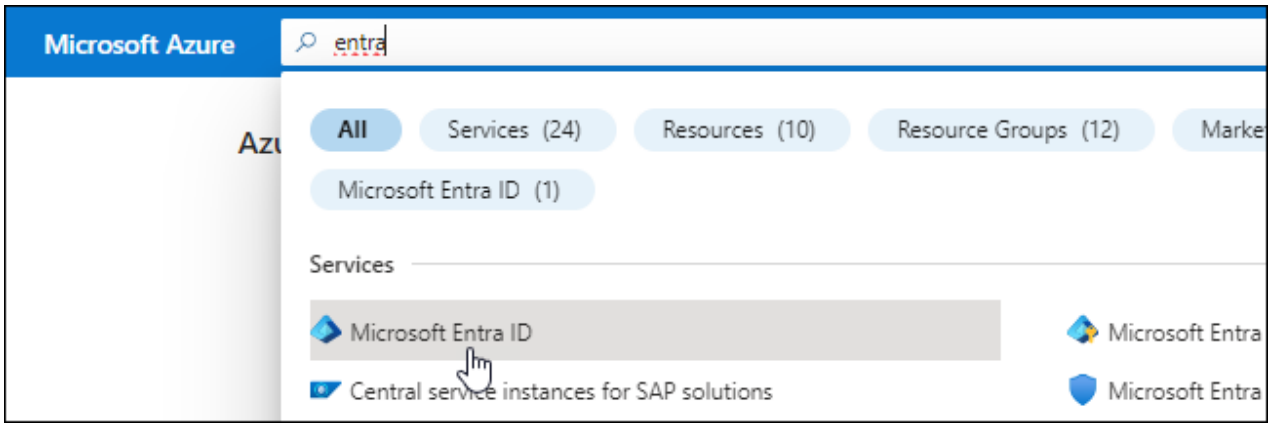
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie all'agente della console.

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 .

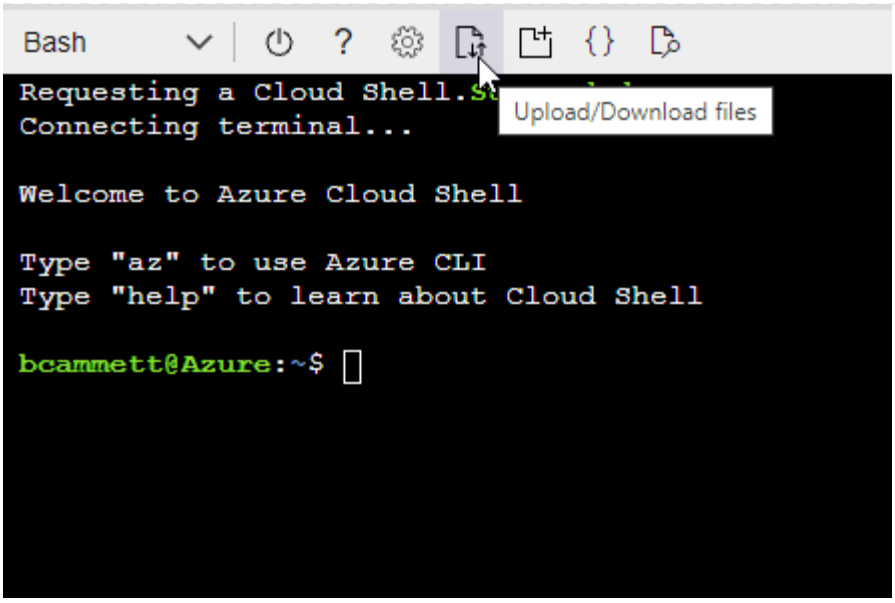
      Esempio

      ```
      "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**.

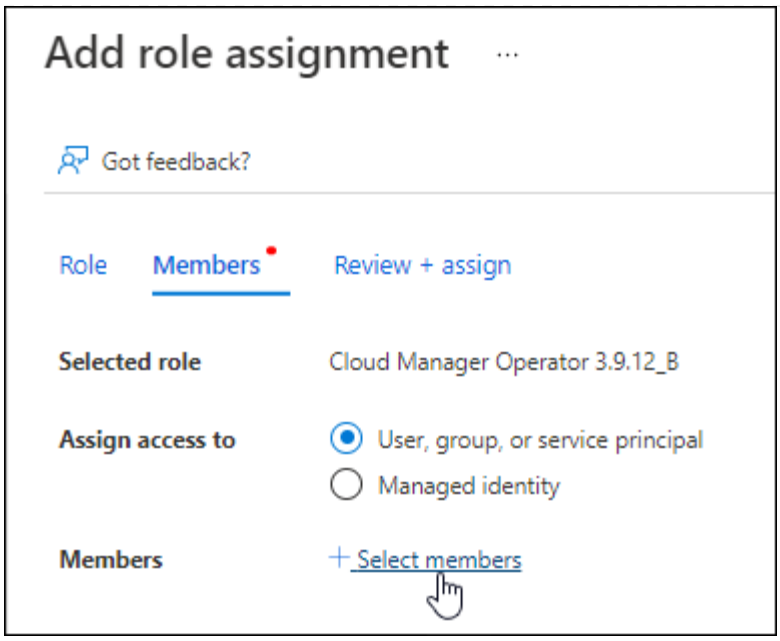
   b. Seleziona l'abbonamento.

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

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

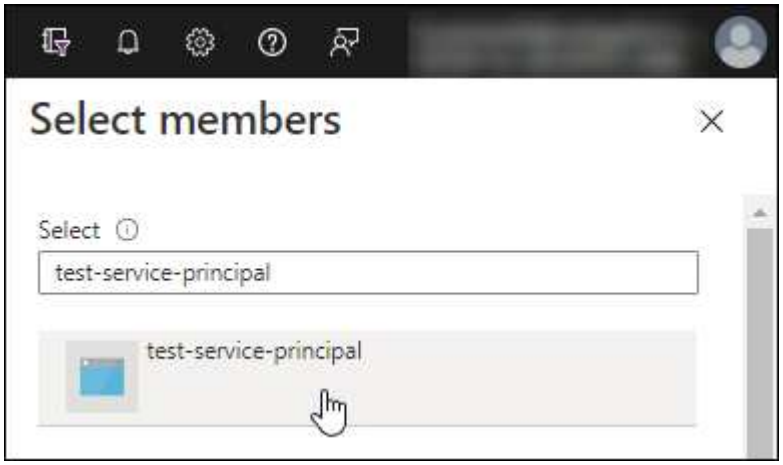
   e. Nella scheda **Membri**, completa i seguenti passaggi:

      - 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**.

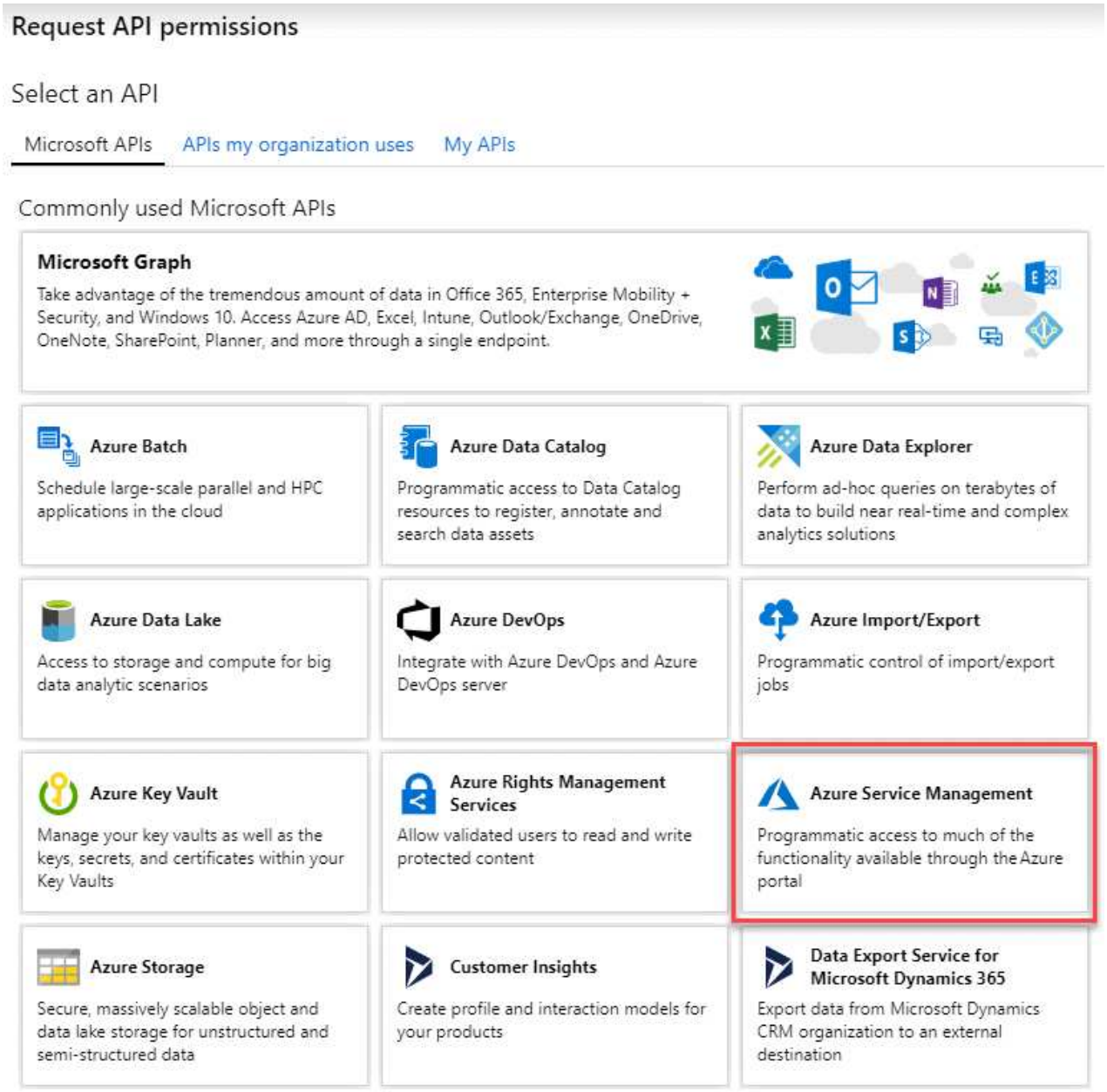
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

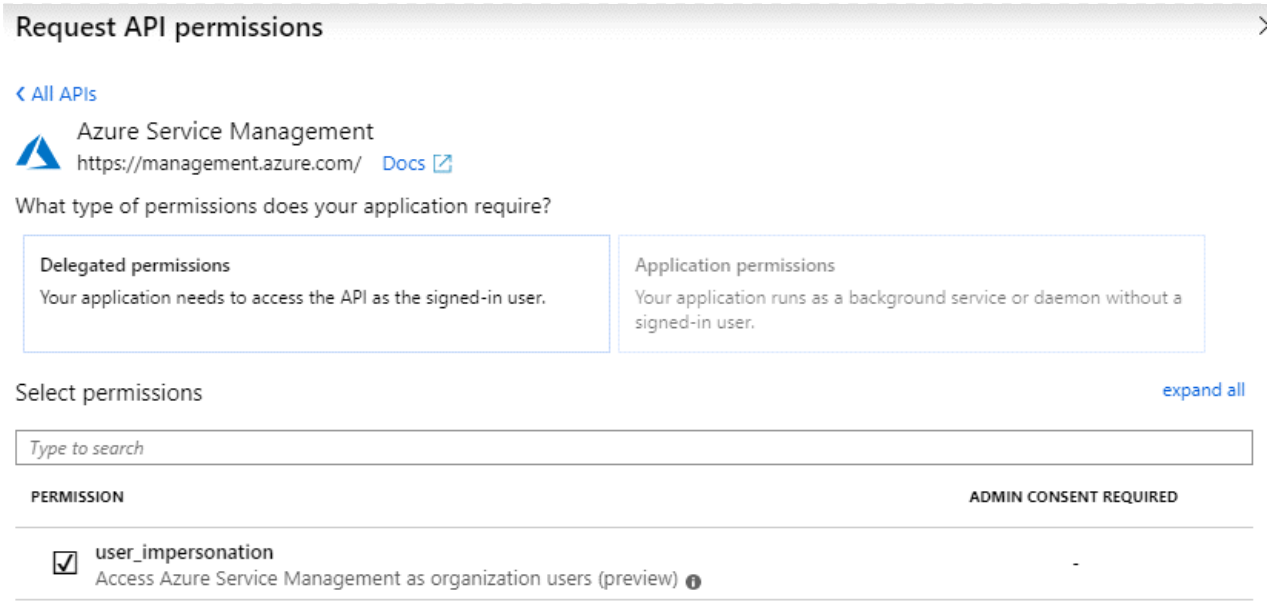
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

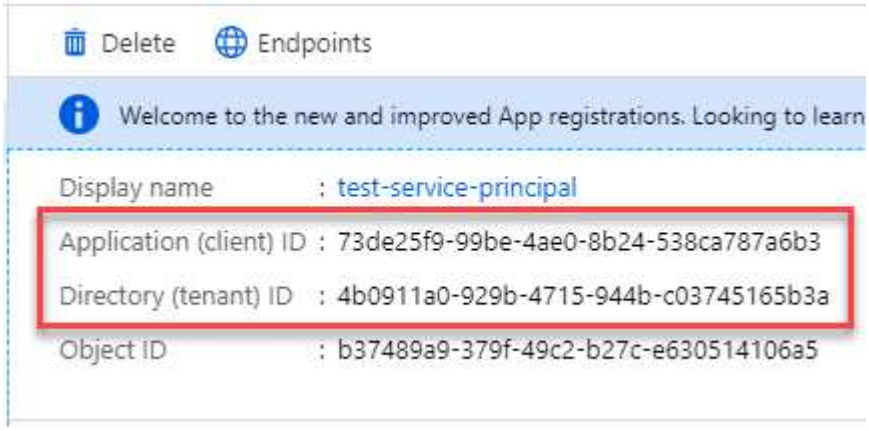


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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.

Passaggio 5: installare l'agente della console

Una volta completati i prerequisiti, puoi installare manualmente il software sul tuo host Linux.

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" .

- Un'identità gestita abilitata sulla macchina virtuale in Azure, 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"

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.
2. Attendi il completamento dell'installazione.

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

   Se l'installazione non riesce, puoi visualizzare il report e i registri di installazione per aiutarti a risolvere i problemi."Scopri come risolvere i problemi di installazione."

1. Aprire un browser Web da un host che dispone di una connessione alla macchina virtuale dell'agente Console e immettere il seguente URL:

   https://ipaddress

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

      È consigliabile disattivare la modalità limitata perché questi passaggi descrivono come utilizzare la

Console in modalità standard. Dovresti abilitare la modalità limitata solo se disponi di un ambiente sicuro e desideri disconnettere questo account dai servizi backend. Se è così,"segui i passaggi per iniziare a utilizzare la NetApp Console in modalità limitata" .

d. Seleziona **Iniziamo**.

Se si dispone di un archivio BLOB di Azure nella stessa sottoscrizione di Azure in cui è stato creato l'agente della console, nella pagina **Sistemi** verrà visualizzato automaticamente un sistema di archiviazione BLOB di Azure. "Scopri come gestire l'archiviazione BLOB di Azure dalla NetApp Console"

Passaggio 6: fornire le autorizzazioni alla NetApp Console

Ora che hai installato l'agente Console, devi fornirgli le autorizzazioni di Azure configurate in precedenza. L'assegnazione delle autorizzazioni consente alla Console di gestire i dati e l'infrastruttura di archiviazione in Azure.

Ruolo personalizzato

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.

Cosa succederà ora?

Vai al "NetApp Console" per iniziare a utilizzare l'agente Console.

Principale del servizio

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.

Google Cloud

Opzioni di installazione dell'agente della console in Google Cloud

Esistono diversi modi per creare un agente Console in Google Cloud. Il metodo più comune è quello diretto dalla NetApp Console .

Sono disponibili le seguenti opzioni di installazione:

- "Crea l'agente Console direttamente dalla Console"(questa è l'opzione standard)

  Questa azione avvia un'istanza VM che esegue Linux e il software dell'agente Console in una VPC di tua scelta.

- "Crea l'agente della console utilizzando Google Platform"

  Questa azione avvia anche un'istanza VM che esegue Linux e il software dell'agente Console, ma la distribuzione viene avviata direttamente da Google Cloud, anziché dalla Console.

- "Scarica e installa manualmente il software sul tuo host Linux"

L'opzione di installazione scelta influisce sul modo in cui ci si prepara all'installazione. Ciò include il modo in cui fornisci alla Console le autorizzazioni necessarie per autenticare e gestire le risorse in Google Cloud.

Crea un agente Console in Google Cloud da NetApp Console

È possibile creare un agente Console in Google Cloud dalla Console. È necessario configurare la rete, preparare le autorizzazioni di Google Cloud, abilitare le API di Google Cloud e quindi creare l'agente della console.

Prima di iniziare

- Dovresti avere un"comprensione degli agenti della console" .
- Dovresti rivedere"Limitazioni dell'agente della console" .

Passaggio 1: configurare la rete

Configurare la rete per garantire che l'agente della console possa gestire le risorse, con connessioni alle reti di destinazione e accesso a Internet in uscita.

VPC e sottorete

Quando si crea l'agente Console, è necessario specificare la VPC e la subnet in cui deve risiedere.

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 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
\ 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.
\ 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.

Punti finali	Scopo
\ 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.

Endpoint contattati dalla console NetApp

Utilizzando la NetApp Console basata sul Web fornita tramite il livello SaaS, questa contatta diversi endpoint per completare le attività di gestione dei dati. Sono inclusi gli endpoint contattati per distribuire l'agente della Console dalla Console.

"Visualizza l'elenco degli endpoint contattati dalla console NetApp" .

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"

Implementare questo requisito di rete dopo aver creato l'agente Console.

Passaggio 2: impostare le autorizzazioni per creare l'agente della console

Prima di poter distribuire un agente Console dalla Console, è necessario impostare le autorizzazioni per l'utente di Google Platform che distribuisce la VM dell'agente Console.

Passi

1. Crea un ruolo personalizzato in Google Platform:

   a. Crea un file YAML che includa le seguenti autorizzazioni:

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
```

```
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
```

```
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Da Google Cloud, attiva Cloud Shell.

c. Carica il file YAML che include le autorizzazioni richieste.

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

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

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

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

2. Assegna questo ruolo personalizzato all'utente che distribuirà l'agente della Console dalla Console o tramite gcloud.

"Documenti di Google Cloud: Concedi un singolo ruolo"

Passaggio 3: creare un account di servizio Google Cloud da utilizzare con l'agente

È necessario un account di servizio Google Cloud per fornire all'agente della Console le autorizzazioni di cui la Console ha bisogno per gestire le risorse in Google Cloud. Quando si crea l'agente Console, è necessario associare questo account di servizio alla VM dell'agente Console.

È tua responsabilità aggiornare il ruolo personalizzato man mano che vengono aggiunte nuove autorizzazioni nelle versioni successive. Se saranno necessarie nuove autorizzazioni, queste saranno elencate nelle note di rilascio.

Passi

1. Crea un ruolo personalizzato in Google Cloud:

a. Crea un file YAML che includa il contenuto del"autorizzazioni dell'account di servizio per l'agente della console" .

b. Da Google Cloud, attiva Cloud Shell.

c. Carica il file YAML che include le autorizzazioni richieste.

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 connector --project=myproject --file=agent.yaml
```

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

2. Crea un account di servizio in Google Cloud e assegna il ruolo all'account di servizio:

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"

3. Se si prevede di distribuire i sistemi Cloud Volumes ONTAP in progetti diversi da quello in cui risiede l'agente della console, sarà necessario fornire all'account di servizio dell'agente della console l'accesso a tali progetti.

Ad esempio, supponiamo che l'agente Console si trovi nel progetto 1 e che si desideri creare sistemi Cloud Volumes ONTAP nel progetto 2. Sarà necessario concedere l'accesso all'account di servizio nel progetto 2.

a. Dal servizio IAM e amministrazione, seleziona il progetto Google Cloud in cui desideri creare i sistemi Cloud Volumes ONTAP .

b. Nella pagina **IAM**, seleziona **Concedi accesso** e fornisci i dettagli richiesti.

- Inserisci l'email dell'account di servizio dell'agente della console.
- Selezionare il ruolo personalizzato dell'agente della console.
- Seleziona **Salva**.

Per maggiori dettagli, fare riferimento a "Documentazione di Google Cloud"

Passaggio 4: impostare le autorizzazioni VPC condivise

Se si utilizza una VPC condivisa per distribuire risorse in un progetto di servizio, sarà necessario preparare le autorizzazioni.

Questa tabella è di riferimento e il tuo ambiente dovrebbe riflettere la tabella delle autorizzazioni una volta completata la configurazione IAM.

Visualizza le autorizzazioni VPC condivise

Identità	Creatore	Ospitato in	Autorizzazioni del progetto di servizio	Autorizzazioni del progetto host	Scopo
Account Google per distribuire l'agente	Costume	Progetto di servizio	"Politica di distribuzione degli agenti"	compute.networkUser	Distribuzione dell'agente nel progetto di servizio
account di servizio agente	Costume	Progetto di servizio	"Politica dell'account del servizio agente"	compute.networkUser deploymentmanager.editor	Distribuzione e manutenzione di Cloud Volumes ONTAP e dei servizi nel progetto di servizio
Account di servizio Cloud Volumes ONTAP	Costume	Progetto di servizio	membro storage.admin: account di servizio NetApp Console come serviceAccount.user	N / A	(Facoltativo) Per NetApp Cloud Tiering e NetApp Backup and Recovery
Agente di servizio delle API di Google	Google Cloud	Progetto di servizio	(Predefinito) Editor	compute.networkUser	Interagisce con le API di Google Cloud per conto della distribuzione. Consente alla Console di utilizzare la rete condivisa.
Account di servizio predefinito di Google Compute Engine	Google Cloud	Progetto di servizio	(Predefinito) Editor	compute.networkUser	Distribuisce istanze di Google Cloud e infrastrutture di elaborazione per conto della distribuzione. Consente alla Console di utilizzare la rete condivisa.

Note:

1. deploymentmanager.editor è necessario nel progetto host solo se non si passano regole del firewall alla distribuzione e si sceglie di lasciare che la Console le crei per conto proprio. Se non è specificata alcuna regola, la NetApp Console crea una distribuzione nel progetto host che contiene la regola del firewall VPC0.
2. firewall.create e firewall.delete sono necessari solo se non si passano regole del firewall alla distribuzione e si sceglie di lasciare che la Console le crei per conto proprio. Queste autorizzazioni si trovano nel file .yaml dell'account Console. Se si distribuisce una coppia HA utilizzando una VPC condivisa, queste autorizzazioni verranno utilizzate per creare le regole del firewall per VPC1, 2 e 3. Per tutte le altre distribuzioni, queste autorizzazioni verranno utilizzate anche per creare regole per VPC0.
3. Per Cloud Tiering, l'account del servizio di tiering deve avere il ruolo serviceAccount.user sull'account

del servizio, non solo a livello di progetto. Attualmente, se si assegna serviceAccount.user a livello di progetto, le autorizzazioni non vengono visualizzate quando si esegue una query sull'account di servizio con getIAMPolicy.

Passaggio 5: abilita le API di Google Cloud

È necessario abilitare diverse API di Google Cloud prima di distribuire l'agente Console e Cloud Volumes ONTAP.

Fare un passo

1. Abilita le seguenti API di Google Cloud nel tuo progetto:
   - API di Cloud Deployment Manager V2
   - API di Cloud Infrastructure Manager
   - API di registrazione cloud
   - API di Cloud Resource Manager
   - API di Compute Engine
   - API di gestione dell'identità e dell'accesso (IAM)
   - Cloud Key Management Service (KMS) API (obbligatoria solo se si prevede di utilizzare NetApp Backup and Recovery con chiavi di crittografia gestite dal cliente (CMEK))
   - Cloud Quotas API (necessaria per le distribuzioni Cloud Volumes ONTAP tramite Infrastructure Manager)

"Documentazione di Google Cloud: abilitazione delle API"

Passaggio 6: creare l'agente della console

Crea un agente Console direttamente dalla Console.

La creazione dell'agente Console distribuisce un'istanza di macchina virtuale in Google Cloud utilizzando una configurazione predefinita. Non passare a un'istanza VM più piccola con meno CPU o meno RAM dopo aver creato l'agente Console. "Scopri la configurazione predefinita per l'agente Console" .

Quando distribuisci un agente in Google Cloud, l'agente crea un bucket in cui archiviare i file di distribuzione.

Prima di iniziare

Dovresti avere quanto segue:

- Le autorizzazioni Google Cloud richieste per creare l'agente Console e un account di servizio per la VM dell'agente Console.
- Una VPC e una subnet che soddisfano i requisiti di rete.
- Dettagli su un server proxy, se è necessario un proxy per l'accesso a Internet dall'agente della console.

Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona **Distribuisci agente > Google Cloud**
3. Nella pagina **Distribuzione di un agente**, rivedi i dettagli su ciò di cui avrai bisogno. Hai due opzioni:

a. Selezionare **Continua** per preparare la distribuzione utilizzando la guida integrata nel prodotto. Ogni passaggio della guida integrata nel prodotto include le informazioni contenute in questa pagina della documentazione.

b. Seleziona **Vai alla distribuzione** se hai già effettuato la preparazione seguendo i passaggi indicati in questa pagina.

4. Per creare l'agente Console, seguire i passaggi della procedura guidata:

   - Se richiesto, accedi al tuo account Google, che dovrebbe disporre delle autorizzazioni necessarie per creare l'istanza della macchina virtuale.

     Il modulo è di proprietà e ospitato da Google. Le tue credenziali non vengono fornite a NetApp.

   - **Dettagli**: immettere un nome per l'istanza della macchina virtuale, specificare i tag, selezionare un progetto e quindi selezionare l'account di servizio che dispone delle autorizzazioni richieste (fare riferimento alla sezione precedente per i dettagli).
   - **Posizione**: specificare una regione, una zona, una VPC e una subnet per l'istanza.
   - **Rete**: scegliere se abilitare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.
   - **Tag di rete**: aggiungere un tag di rete all'istanza dell'agente Console se si utilizza un proxy trasparente. I tag di rete devono iniziare con una lettera minuscola e possono contenere lettere minuscole, numeri e trattini. I tag devono terminare con una lettera minuscola o un numero. Ad esempio, potresti utilizzare il tag "console-agent-proxy".
   - **Criterio firewall**: scegliere se creare un nuovo criterio firewall o se selezionarne uno esistente che consenta le regole in entrata e in uscita richieste.

     "Regole del firewall in Google Cloud"

5. Rivedi le tue selezioni per verificare che la configurazione sia corretta.

   a. La casella di controllo **Convalida configurazione agente** è selezionata per impostazione predefinita affinché la Console convalidi i requisiti di connettività di rete durante la distribuzione. Se la Console non riesce a distribuire l'agente, fornisce un report per aiutarti a risolvere il problema. Se la distribuzione riesce, non viene fornito alcun report.

   Se stai ancora utilizzando il"punti finali precedenti" utilizzato per gli aggiornamenti degli agenti, la convalida fallisce con un errore. Per evitare ciò, deselezionare la casella di controllo per saltare il controllo di convalida.

6. Selezionare **Aggiungi**.

   L'agente sarà pronto in circa 10 minuti; resta sulla pagina fino al completamento del processo.

Risultato

Una volta completato il processo, l'agente Console è disponibile per l'uso.

Se la distribuzione non riesce, puoi scaricare un report e i registri dalla Console per aiutarti a risolvere i problemi."Scopri come risolvere i problemi di installazione."

Se disponi di bucket Google Cloud Storage nello stesso account Google Cloud in cui hai creato l'agente Console, vedrai automaticamente un sistema Google Cloud Storage apparire nella pagina **Sistemi**. "Scopri

come gestire Google Cloud Storage dalla Console"

Crea un agente Console da Google Cloud

Per creare un agente Console in Google Cloud utilizzando Google Cloud, è necessario configurare la rete, preparare le autorizzazioni di Google Cloud, abilitare le API di Google Cloud e quindi creare l'agente Console.

Prima di iniziare

- Dovresti avere un"comprensione degli agenti della console" .
- Dovresti rivedere"Limitazioni dell'agente della console" .

Passaggio 1: configurare la rete

Configurare la rete per consentire all'agente della console di gestire le risorse e connettersi alle reti di destinazione e a Internet.

VPC e sottorete

Quando si crea l'agente Console, è necessario specificare la VPC e la subnet in cui deve risiedere.

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 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
\ 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.
\ https://mysupport.netapp.com	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .

Punti finali	Scopo
\ 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.

Endpoint contattati dalla console NetApp

Utilizzando la NetApp Console basata sul Web fornita tramite il livello SaaS, questa contatta diversi endpoint per completare le attività di gestione dei dati. Sono inclusi gli endpoint contattati per distribuire

l’agente della Console dalla Console.

"Visualizza l’elenco degli endpoint contattati dalla console NetApp" .

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"

Implementare questo requisito di rete dopo aver creato l’agente Console.

Passaggio 2: impostare le autorizzazioni per creare l’agente della console

Imposta le autorizzazioni per l’utente di Google Cloud per distribuire la VM dell’agente della console da Google Cloud.

Passi

1. Crea un ruolo personalizzato in Google Platform:

   a. Crea un file YAML che includa le seguenti autorizzazioni:

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console
agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Da Google Cloud, attiva Cloud Shell.

c. Carica il file YAML che include le autorizzazioni richieste.

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

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

gcloud iam roles create connectorDeployment --project=myproject --file=connector-deployment.yaml

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

2. Assegna questo ruolo personalizzato all'utente che distribuisce l'agente Console da Google Cloud.

   "Documenti di Google Cloud: Concedi un singolo ruolo"

Passaggio 3: impostare le autorizzazioni per le operazioni dell'agente della console

È necessario un account di servizio Google Cloud per fornire all'agente della Console le autorizzazioni di cui la Console ha bisogno per gestire le risorse in Google Cloud. Quando si crea l'agente Console, è necessario associare questo account di servizio alla VM dell'agente Console.

È tua responsabilità aggiornare il ruolo personalizzato man mano che vengono aggiunte nuove autorizzazioni nelle versioni successive. Se saranno necessarie nuove autorizzazioni, queste saranno elencate nelle note di rilascio.

Passi

1. Crea un ruolo personalizzato in Google Cloud:

   a. Crea un file YAML che includa il contenuto del"autorizzazioni dell'account di servizio per l'agente della console" .

   b. Da Google Cloud, attiva Cloud Shell.

   c. Carica il file YAML che include le autorizzazioni richieste.

   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 connector --project=myproject --file=agent.yaml
      ```

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

2. Crea un account di servizio in Google Cloud e assegna il ruolo all'account di servizio:

   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"

3. Se si prevede di distribuire i sistemi Cloud Volumes ONTAP in progetti diversi da quello in cui risiede l'agente della console, sarà necessario fornire all'account di servizio dell'agente della console l'accesso a tali progetti.

   Ad esempio, supponiamo che l'agente Console si trovi nel progetto 1 e che si desideri creare sistemi Cloud Volumes ONTAP nel progetto 2. Sarà necessario concedere l'accesso all'account di servizio nel progetto 2.

   a. Dal servizio IAM e amministrazione, seleziona il progetto Google Cloud in cui desideri creare i sistemi Cloud Volumes ONTAP .

b. Nella pagina **IAM**, seleziona **Concedi accesso** e fornisci i dettagli richiesti.
   - Inserisci l'email dell'account di servizio dell'agente della console.
   - Selezionare il ruolo personalizzato dell'agente della console.
   - Seleziona **Salva**.

Per maggiori dettagli, fare riferimento a "Documentazione di Google Cloud"

Passaggio 4: impostare le autorizzazioni VPC condivise

Se si utilizza una VPC condivisa per distribuire risorse in un progetto di servizio, sarà necessario preparare le autorizzazioni.

Questa tabella è di riferimento e il tuo ambiente dovrebbe riflettere la tabella delle autorizzazioni una volta completata la configurazione IAM.

Visualizza le autorizzazioni VPC condivise

Identità	Creatore	Ospitato in	Autorizzazioni del progetto di servizio	Autorizzazioni del progetto host	Scopo
Account Google per distribuire l'agente	Costume	Progetto di servizio	"Politica di distribuzione degli agenti"	compute.networkUser	Distribuzione dell'agente nel progetto di servizio
account di servizio agente	Costume	Progetto di servizio	"Politica dell'account del servizio agente"	compute.networkUser deploymentmanager.editor	Distribuzione e manutenzione di Cloud Volumes ONTAP e dei servizi nel progetto di servizio
Account di servizio Cloud Volumes ONTAP	Costume	Progetto di servizio	membro storage.admin: account di servizio NetApp Console come serviceAccount.user	N / A	(Facoltativo) Per NetApp Cloud Tiering e NetApp Backup and Recovery
Agente di servizio delle API di Google	Google Cloud	Progetto di servizio	(Predefinito) Editor	compute.networkUser	Interagisce con le API di Google Cloud per conto della distribuzione. Consente alla Console di utilizzare la rete condivisa.
Account di servizio predefinito di Google Compute Engine	Google Cloud	Progetto di servizio	(Predefinito) Editor	compute.networkUser	Distribuisce istanze di Google Cloud e infrastrutture di elaborazione per conto della distribuzione. Consente alla Console di utilizzare la rete condivisa.

Note:

1. deploymentmanager.editor è necessario nel progetto host solo se non si passano regole del firewall alla distribuzione e si sceglie di lasciare che la Console le crei per conto proprio. Se non è specificata alcuna regola, la NetApp Console crea una distribuzione nel progetto host che contiene la regola del firewall VPC0.
2. firewall.create e firewall.delete sono necessari solo se non si passano regole del firewall alla distribuzione e si sceglie di lasciare che la Console le crei per conto proprio. Queste autorizzazioni si trovano nel file .yaml dell'account Console. Se si distribuisce una coppia HA utilizzando una VPC condivisa, queste autorizzazioni verranno utilizzate per creare le regole del firewall per VPC1, 2 e 3. Per tutte le altre distribuzioni, queste autorizzazioni verranno utilizzate anche per creare regole per VPC0.
3. Per Cloud Tiering, l'account del servizio di tiering deve avere il ruolo serviceAccount.user sull'account

del servizio, non solo a livello di progetto. Attualmente, se si assegna serviceAccount.user a livello di progetto, le autorizzazioni non vengono visualizzate quando si esegue una query sull'account di servizio con getIAMPolicy.

Passaggio 5: abilita le API di Google Cloud

Abilitare diverse API di Google Cloud prima di distribuire l'agente Console e Cloud Volumes ONTAP.

Fare un passo

1. Abilita le seguenti API di Google Cloud nel tuo progetto:
   - API di Cloud Deployment Manager V2
   - API di Cloud Infrastructure Manager
   - API di registrazione cloud
   - API di Cloud Resource Manager
   - API di Compute Engine
   - API di gestione dell'identità e dell'accesso (IAM)
   - Cloud Key Management Service (KMS) API (obbligatoria solo se si prevede di utilizzare NetApp Backup and Recovery con chiavi di crittografia gestite dal cliente (CMEK))
   - Cloud Quotas API (necessaria per le distribuzioni Cloud Volumes ONTAP tramite Infrastructure Manager)

"Documentazione di Google Cloud: abilitazione delle API"

Passaggio 6: creare l'agente della console

Crea un agente Console utilizzando Google Cloud.

La creazione dell'agente Console distribuisce un'istanza VM in Google Cloud con la configurazione predefinita. Non passare a un'istanza VM più piccola con meno CPU o meno RAM dopo aver creato l'agente Console. "Scopri la configurazione predefinita per l'agente Console" .

Prima di iniziare

Dovresti avere quanto segue:

- Le autorizzazioni Google Cloud richieste per creare l'agente Console e un account di servizio per la VM dell'agente Console.
- Una VPC e una subnet che soddisfano i requisiti di rete.
- Comprensione dei requisiti delle istanze VM.
  - **CPU**: 8 core o 8 vCPU
  - **RAM**: 32 GB
  - **Tipo di macchina**: Consigliamo n2-standard-8.

    L'agente Console è supportato in Google Cloud su un'istanza VM con un sistema operativo che supporta le funzionalità Shielded VM.

Passi

1. Accedi a Google Cloud SDK utilizzando il metodo che preferisci.

In questo esempio viene utilizzata una shell locale con gcloud SDK installato, ma è possibile utilizzare anche Google Cloud Shell.

Per ulteriori informazioni su Google Cloud SDK, visitare il sito"Pagina della documentazione di Google Cloud SDK" .

2. Verifica di aver effettuato l'accesso come utente che dispone delle autorizzazioni richieste definite nella sezione precedente:

```
gcloud auth list
```

L'output dovrebbe mostrare quanto segue, dove * è l'account utente desiderato con cui effettuare l'accesso:

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install them,
please run:
$ gcloud components update
```

3. Esegui il `gcloud compute instances create` comando:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

nome-istanza
Nome dell'istanza desiderato per l'istanza VM.

progetto

(Facoltativo) Il progetto in cui si desidera distribuire la VM.

account di servizio

L'account di servizio specificato nell'output del passaggio 2.

zona

La zona in cui si desidera distribuire la VM

senza indirizzo

(Facoltativo) Non viene utilizzato alcun indirizzo IP esterno (è necessario un NAT cloud o un proxy per instradare il traffico verso Internet pubblico)

tag di rete

(Facoltativo) Aggiungere il tagging di rete per collegare una regola del firewall utilizzando i tag all'istanza dell'agente della console

percorso di rete

(Facoltativo) Aggiungi il nome della rete in cui distribuire l'agente della console (per una VPC condivisa, è necessario il percorso completo)

percorso di sottorete

(Facoltativo) Aggiungi il nome della subnet in cui distribuire l'agente della console (per una VPC condivisa, è necessario il percorso completo)

percorso-chiave-kms

(Facoltativo) Aggiungere una chiave KMS per crittografare i dischi dell'agente della console (è necessario applicare anche le autorizzazioni IAM)

Per maggiori informazioni su queste bandiere, visita il"Documentazione dell'SDK di Google Cloud Compute" .

L'esecuzione del comando distribuisce l'agente Console. L'istanza dell'agente Console e il software dovrebbero essere in esecuzione entro circa cinque minuti.

4. 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.

5. Dopo aver effettuato l'accesso, configura l'agente Console:
   a. Specificare l'organizzazione della console da associare all'agente della console.

      "Scopri di più sulla gestione dell'identità e degli accessi" .

   b. Inserisci un nome per il sistema.

Risultato

L'agente Console è ora installato e configurato con la tua organizzazione Console.

Apri un browser web e vai su "NetApp Console" per iniziare a utilizzare l'agente Console.

Per installare manualmente l'agente Console sul tuo host Linux, devi esaminare i requisiti dell'host, configurare la rete, preparare le autorizzazioni di Google Cloud, abilitare le API di Google Cloud, installare la Console e quindi fornire le autorizzazioni preparate.

Prima di iniziare

- Dovresti avere un"comprensione degli agenti della console" .
- Dovresti rivedere"Limitazioni dell'agente della console" .

Passaggio 1: rivedere i requisiti dell'host

Il software dell'agente Console deve essere eseguito su un host che soddisfi specifici requisiti del sistema operativo, requisiti di RAM, requisiti di porta e così via.

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.

Tipo di macchina Google Cloud

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

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

Ipervisore

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

Requisiti del sistema operativo e del contenitore

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

container.

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

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

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"

Passaggio 2: installare 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 3. 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 3: configurazione della rete

Configura la tua rete in modo che l'agente della console possa gestire risorse e processi all'interno del tuo ambiente cloud ibrido. Ad esempio, è necessario assicurarsi che le connessioni siano disponibili per le reti di destinazione e che sia disponibile l'accesso a Internet in uscita.

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.

Punti finali	Scopo
\ 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.
\ 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.

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"

Passaggio 4: impostare le autorizzazioni per l'agente della console

È necessario un account di servizio Google Cloud per fornire all'agente della Console le autorizzazioni di cui la Console ha bisogno per gestire le risorse in Google Cloud. Quando si crea l'agente Console, è necessario associare questo account di servizio alla VM dell'agente Console.

È tua responsabilità aggiornare il ruolo personalizzato man mano che vengono aggiunte nuove autorizzazioni nelle versioni successive. Se saranno necessarie nuove autorizzazioni, queste saranno elencate nelle note di rilascio.

Passi

1. Crea un ruolo personalizzato in Google Cloud:

   a. Crea un file YAML che includa il contenuto del"autorizzazioni dell'account di servizio per l'agente della console" .

   b. Da Google Cloud, attiva Cloud Shell.

   c. Carica il file YAML che include le autorizzazioni richieste.

   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 connector --project=myproject --file=agent.yaml
      ```

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

2. Crea un account di servizio in Google Cloud e assegna il ruolo all'account di servizio:

   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"

3. Se si prevede di distribuire i sistemi Cloud Volumes ONTAP in progetti diversi da quello in cui risiede

l’agente della console, sarà necessario fornire all’account di servizio dell’agente della console l’accesso a tali progetti.

Ad esempio, supponiamo che l’agente Console si trovi nel progetto 1 e che si desideri creare sistemi Cloud Volumes ONTAP nel progetto 2. Sarà necessario concedere l’accesso all’account di servizio nel progetto 2.

a. Dal servizio IAM e amministrazione, seleziona il progetto Google Cloud in cui desideri creare i sistemi Cloud Volumes ONTAP .
b. Nella pagina **IAM**, seleziona **Concedi accesso** e fornisci i dettagli richiesti.
    - Inserisci l’email dell’account di servizio dell’agente della console.
    - Selezionare il ruolo personalizzato dell’agente della console.
    - Seleziona **Salva**.

Per maggiori dettagli, fare riferimento a "Documentazione di Google Cloud"

Passaggio 5: impostare le autorizzazioni VPC condivise

Se si utilizza una VPC condivisa per distribuire risorse in un progetto di servizio, sarà necessario preparare le autorizzazioni.

Questa tabella è di riferimento e il tuo ambiente dovrebbe riflettere la tabella delle autorizzazioni una volta completata la configurazione IAM.

Visualizza le autorizzazioni VPC condivise

Identità	Creatore	Ospitato in	Autorizzazioni del progetto di servizio	Autorizzazioni del progetto host	Scopo
Account Google per distribuire l'agente	Costume	Progetto di servizio	"Politica di distribuzione degli agenti"	compute.networkUser	Distribuzione dell'agente nel progetto di servizio
account di servizio agente	Costume	Progetto di servizio	"Politica dell'account del servizio agente"	compute.networkUser deploymentmanager.editor	Distribuzione e manutenzione di Cloud Volumes ONTAP e dei servizi nel progetto di servizio
Account di servizio Cloud Volumes ONTAP	Costume	Progetto di servizio	membro storage.admin: account di servizio NetApp Console come serviceAccount.user	N / A	(Facoltativo) Per NetApp Cloud Tiering e NetApp Backup and Recovery
Agente di servizio delle API di Google	Google Cloud	Progetto di servizio	(Predefinito) Editor	compute.networkUser	Interagisce con le API di Google Cloud per conto della distribuzione. Consente alla Console di utilizzare la rete condivisa.
Account di servizio predefinito di Google Compute Engine	Google Cloud	Progetto di servizio	(Predefinito) Editor	compute.networkUser	Distribuisce istanze di Google Cloud e infrastrutture di elaborazione per conto della distribuzione. Consente alla Console di utilizzare la rete condivisa.

Note:

1. deploymentmanager.editor è necessario nel progetto host solo se non si passano regole del firewall alla distribuzione e si sceglie di lasciare che la Console le crei per conto proprio. Se non è specificata alcuna regola, la NetApp Console crea una distribuzione nel progetto host che contiene la regola del firewall VPC0.
2. firewall.create e firewall.delete sono necessari solo se non si passano regole del firewall alla distribuzione e si sceglie di lasciare che la Console le crei per conto proprio. Queste autorizzazioni si trovano nel file .yaml dell'account Console. Se si distribuisce una coppia HA utilizzando una VPC condivisa, queste autorizzazioni verranno utilizzate per creare le regole del firewall per VPC1, 2 e 3. Per tutte le altre distribuzioni, queste autorizzazioni verranno utilizzate anche per creare regole per VPC0.
3. Per Cloud Tiering, l'account del servizio di tiering deve avere il ruolo serviceAccount.user sull'account

del servizio, non solo a livello di progetto. Attualmente, se si assegna serviceAccount.user a livello di progetto, le autorizzazioni non vengono visualizzate quando si esegue una query sull'account di servizio con getIAMPolicy.

Passaggio 6: abilita le API di Google Cloud

Prima di poter distribuire un agente Console in Google Cloud, è necessario abilitare diverse API di Google Cloud.

Fare un passo

1. Abilita le seguenti API di Google Cloud nel tuo progetto:
    - API di Cloud Deployment Manager V2
    - API di Cloud Infrastructure Manager
    - API di registrazione cloud
    - API di Cloud Resource Manager
    - API di Compute Engine
    - API di gestione dell'identità e dell'accesso (IAM)
    - Cloud Key Management Service (KMS) API (obbligatoria solo se si prevede di utilizzare NetApp Backup and Recovery con chiavi di crittografia gestite dal cliente (CMEK))
    - Cloud Quotas API (necessaria per le distribuzioni Cloud Volumes ONTAP tramite Infrastructure Manager)

"Documentazione di Google Cloud: abilitazione delle API"

Passaggio 7: installare l'agente della console

Una volta completati i prerequisiti, puoi installare manualmente il software sul tuo host Linux.

Quando si distribuisce un agente, il sistema crea anche un bucket Google Cloud per archiviare i file di distribuzione.

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.
2. Attendi il completamento dell'installazione.

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

Se l'installazione non riesce, puoi visualizzare il report e i registri di installazione per aiutarti a risolvere i problemi."Scopri come risolvere i problemi di installazione."

1. Aprire un browser Web da un host che dispone di una connessione alla macchina virtuale dell'agente Console e immettere il seguente URL:

   https://ipaddress

2. Dopo aver effettuato l'accesso, configura l'agente Console:

   a. Specificare l'organizzazione da associare all'agente Console.

   b. Inserisci un nome per il sistema.

   c. In **Stai utilizzando un ambiente protetto?** mantieni disattivata la modalità con restrizioni.

      È consigliabile disattivare la modalità limitata perché questi passaggi descrivono come utilizzare la Console in modalità standard. Dovresti abilitare la modalità limitata solo se disponi di un ambiente sicuro e desideri disconnettere questo account dai servizi backend. Se è così,"segui i passaggi per iniziare a utilizzare la NetApp Console in modalità limitata" .

   d. Seleziona **Iniziamo**.

   Se l'installazione non riesce, è possibile visualizzare i registri e un report per risolvere il problema."Scopri come risolvere i problemi di installazione."

Se disponi di bucket Google Cloud Storage nello stesso account Google Cloud in cui hai creato l'agente Console, vedrai automaticamente un sistema Google Cloud Storage apparire nella pagina **Sistemi**. "Scopri come gestire Google Cloud Storage dalla NetApp Console"

Passaggio 8: fornire le autorizzazioni all'agente della console

È necessario fornire all'agente della console le autorizzazioni Google Cloud configurate in precedenza. Fornendo le autorizzazioni, l'agente della console può gestire i dati e l'infrastruttura di archiviazione in Google Cloud.

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 desideri gestire le risorse in altri progetti Google Cloud, concedi 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.

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

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

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

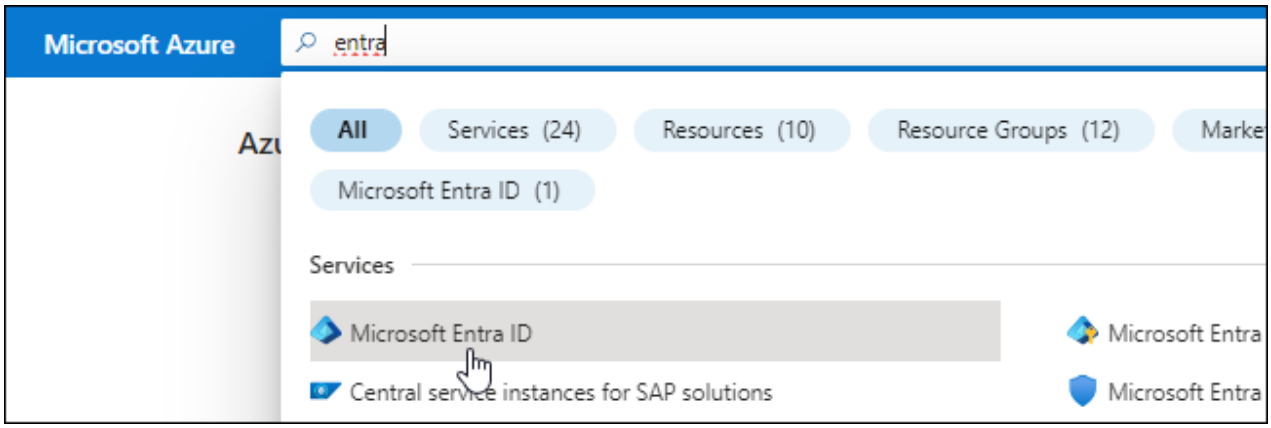
Quando l'agente Console è installato in locale, è necessario fornire all'agente Console le autorizzazioni di Azure impostando un'entità servizio in Microsoft Entra ID e ottenendo le credenziali di Azure necessarie all'agente Console.

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 .

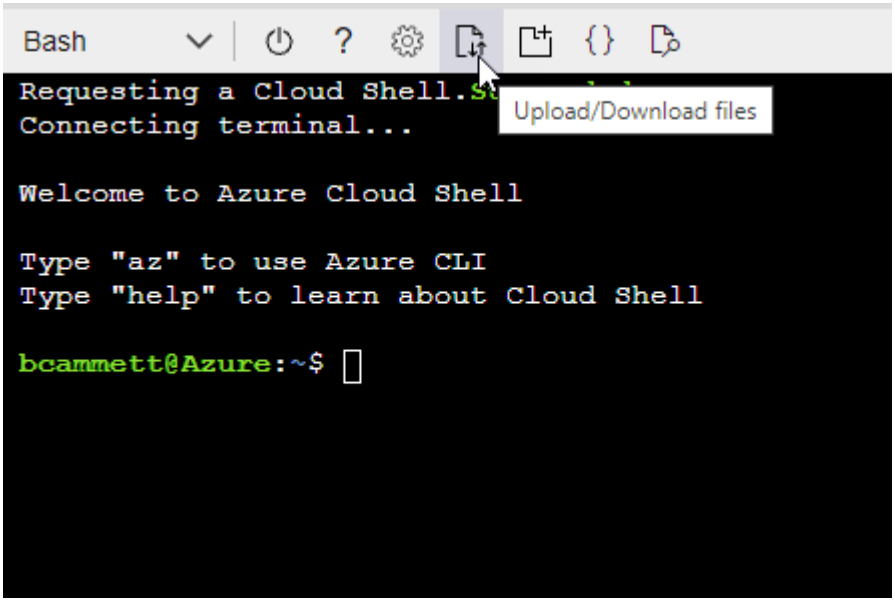
      Esempio

      ```
      "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:

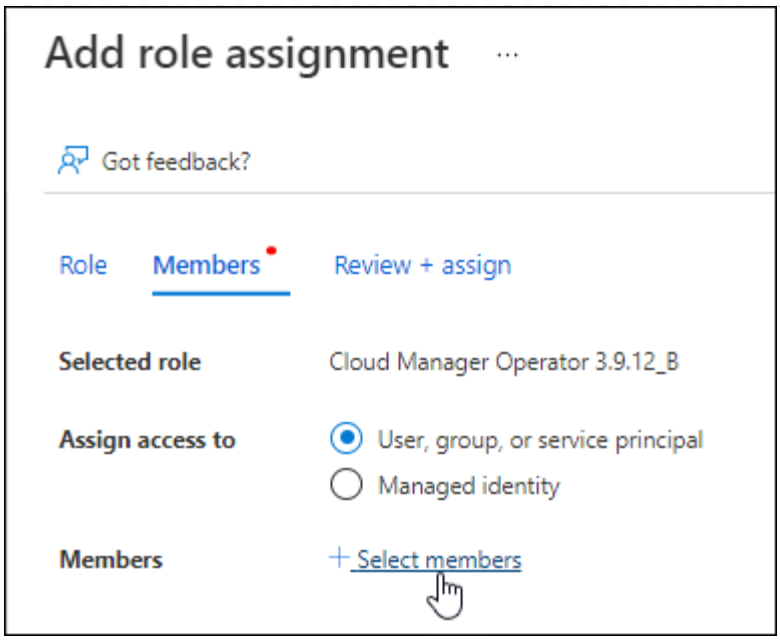
```
az role definition create --role-definition agent_Policy.json
```

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

2. Assegnare l'applicazione al ruolo:

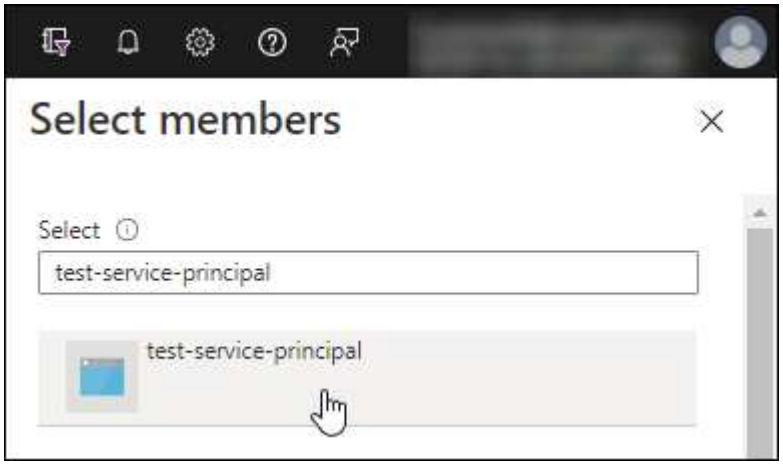
   a. Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
   b. Seleziona l'abbonamento.
   c. Selezionare **Controllo accessi (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.
   e. Nella scheda **Membri**,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

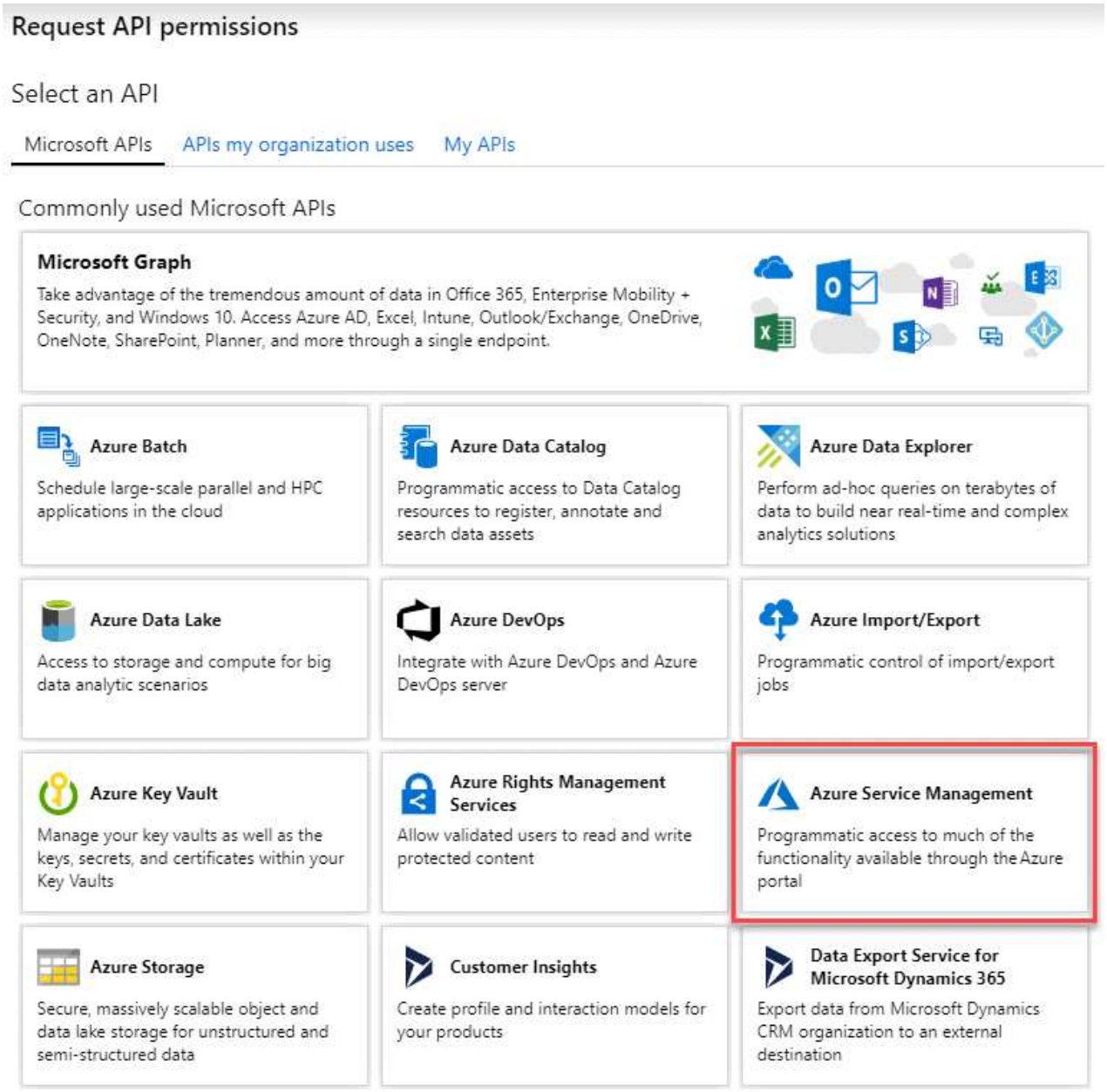
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

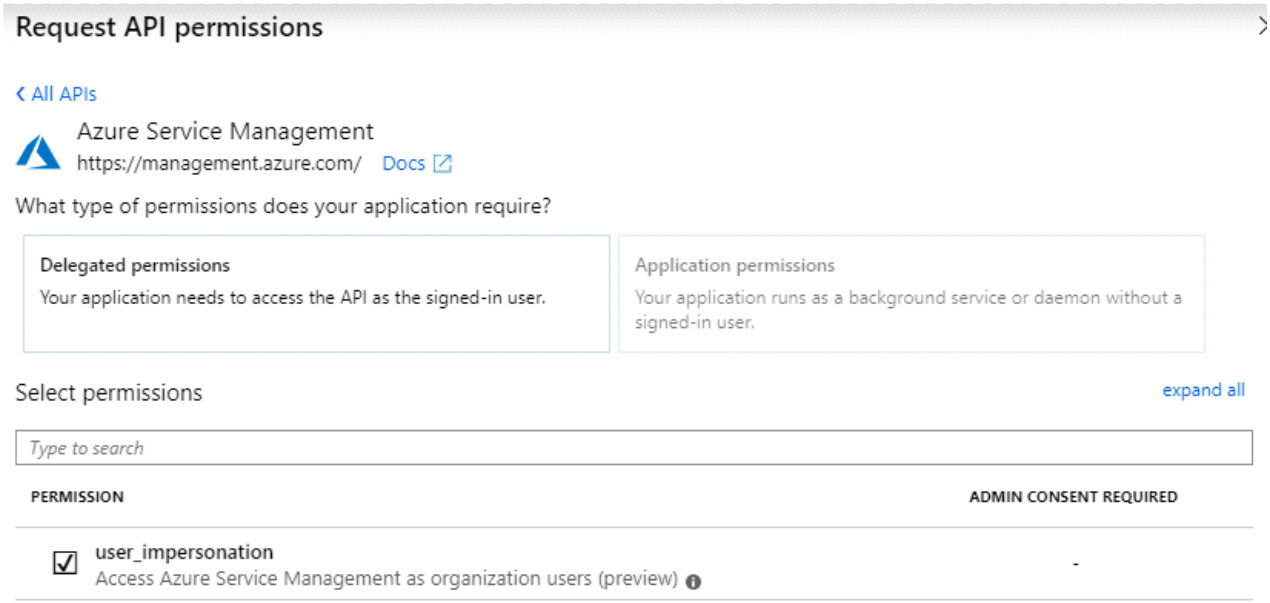
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

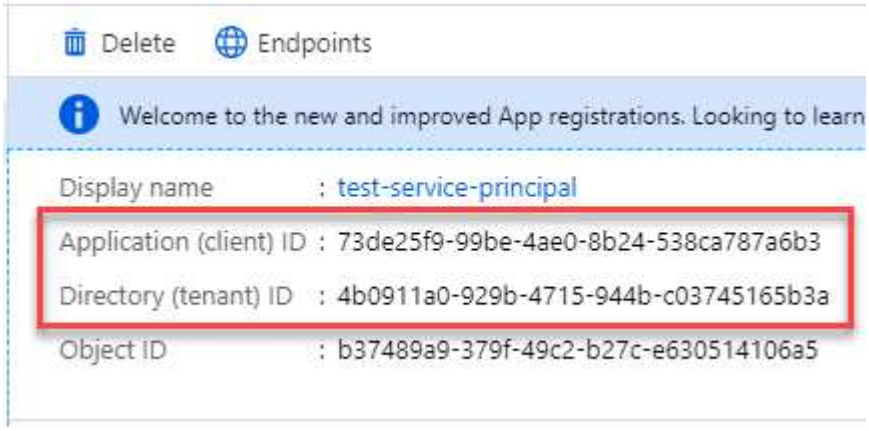


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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

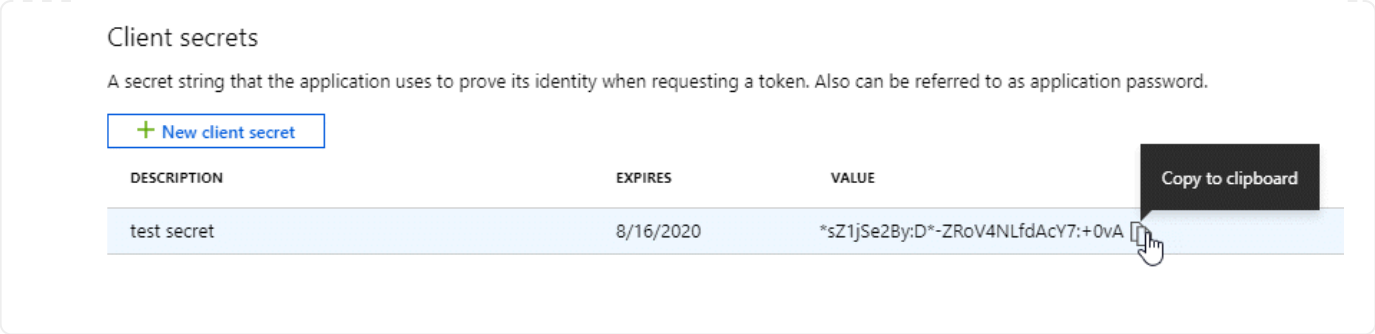
1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)**.



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 4. 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

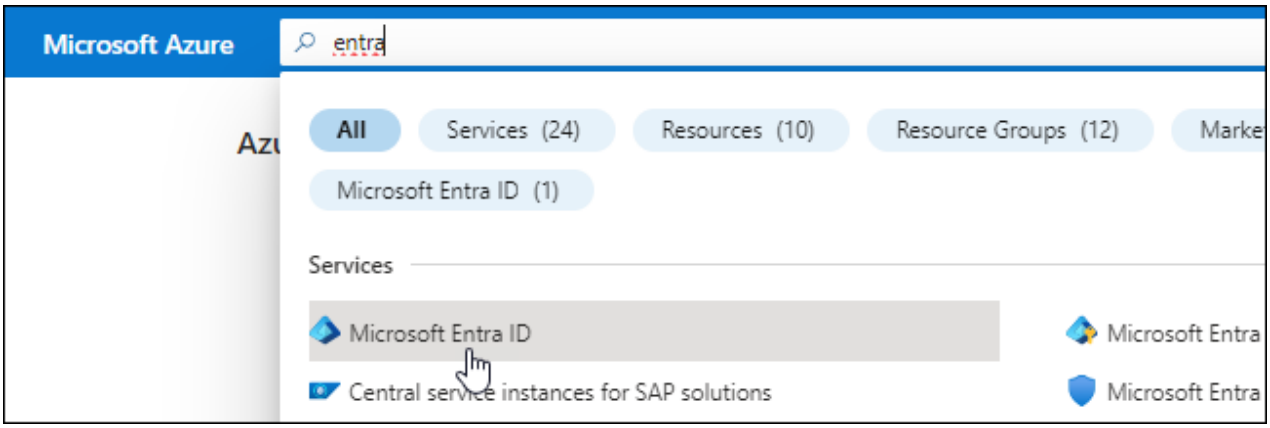
Quando l'agente Console è installato in locale, è necessario concedere all'agente Console le autorizzazioni di Azure impostando un'entità servizio in Microsoft Entra ID e ottenendo le credenziali di Azure necessarie all'agente Console.

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 .

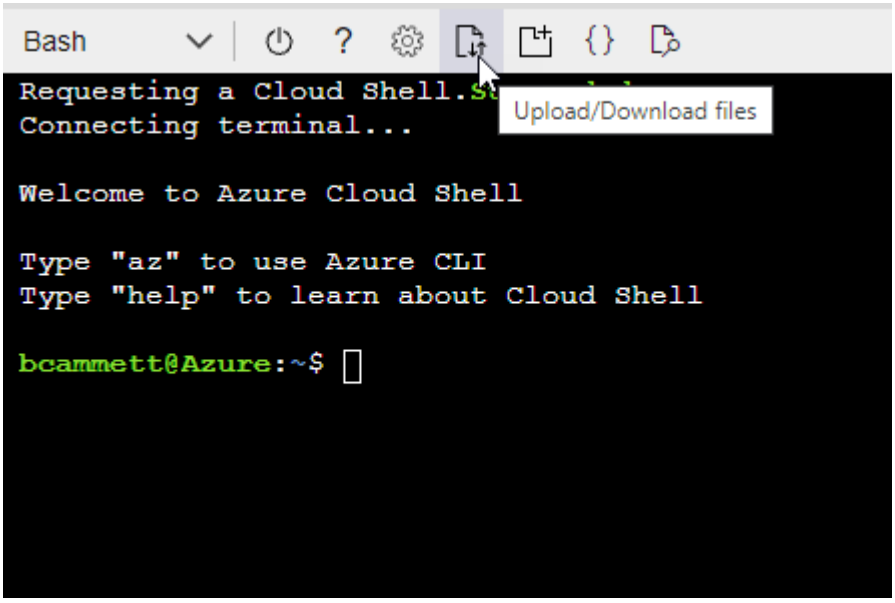
      Esempio

      ```
      "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:

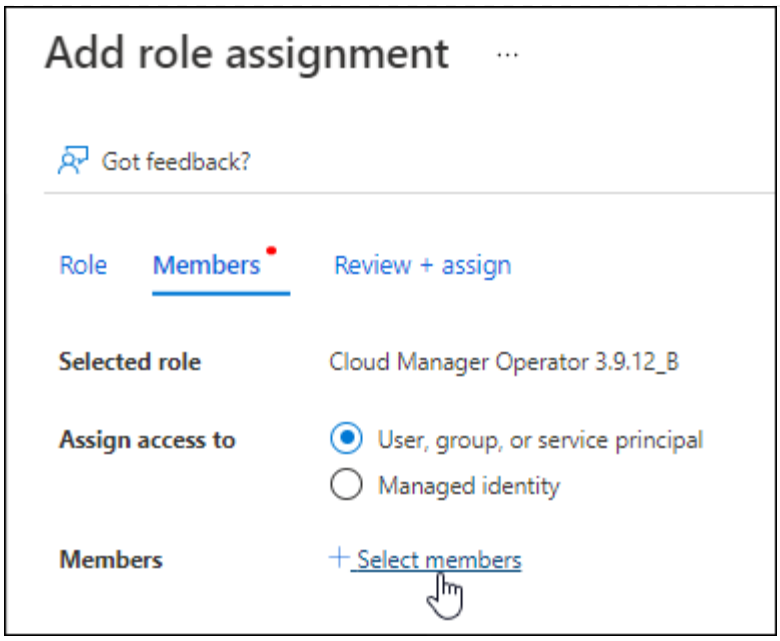
```
az role definition create --role-definition agent_Policy.json
```

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

2. Assegnare l'applicazione al ruolo:

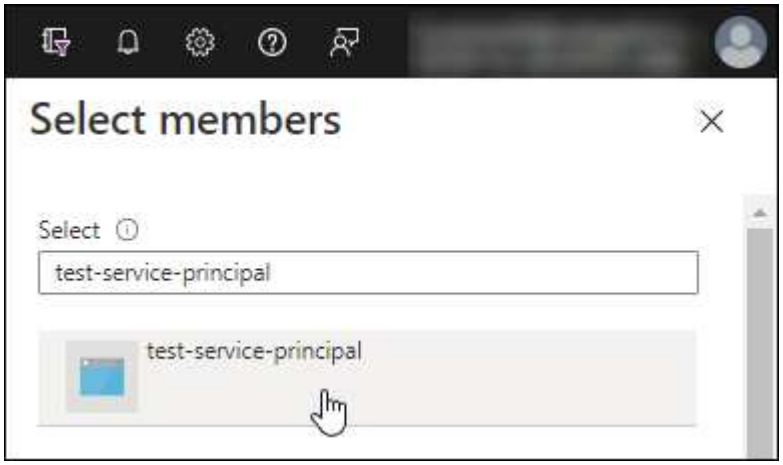
   a. Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
   b. Seleziona l'abbonamento.
   c. Selezionare **Controllo accessi (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.
   e. Nella scheda **Membri**,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

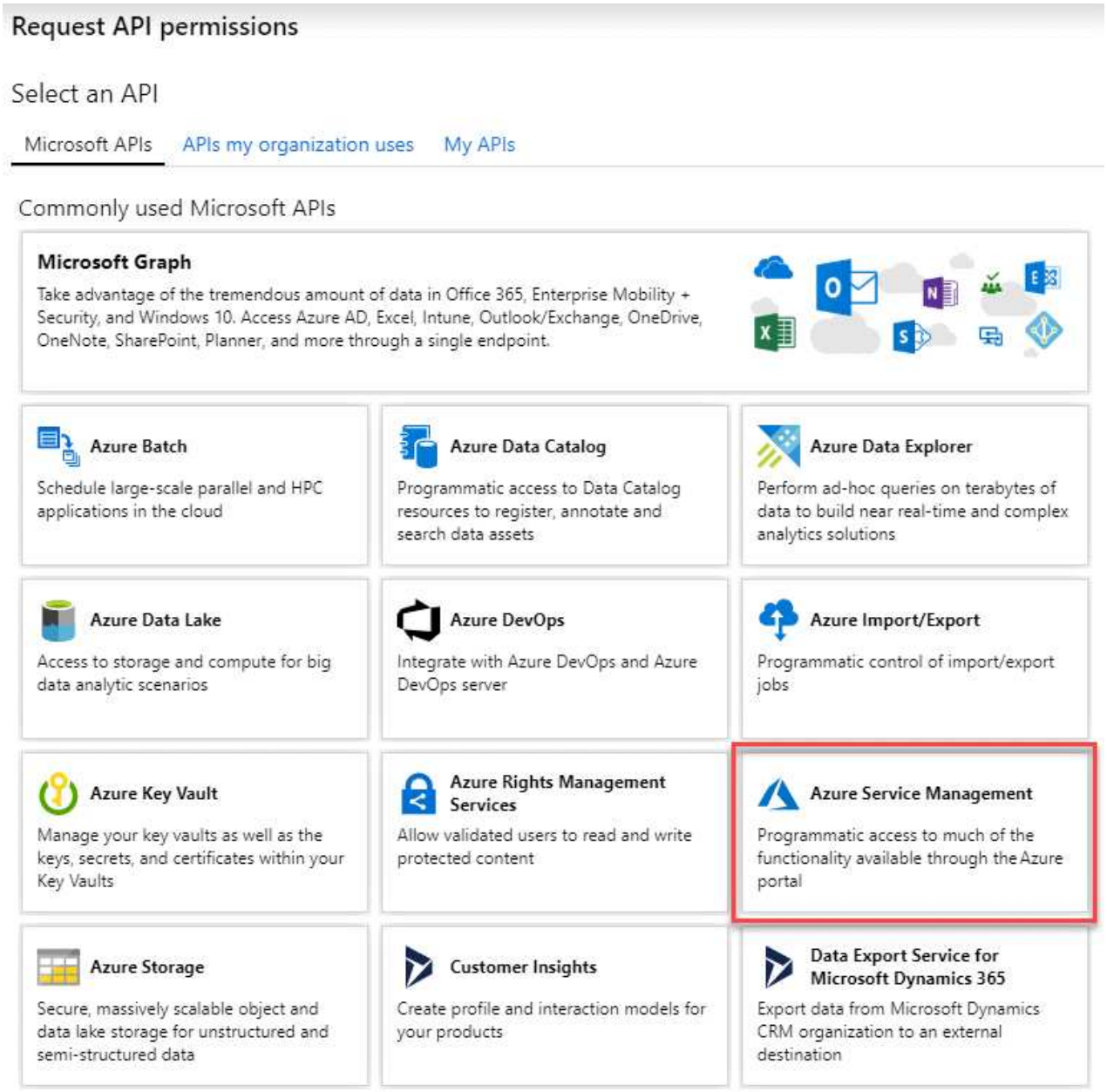
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

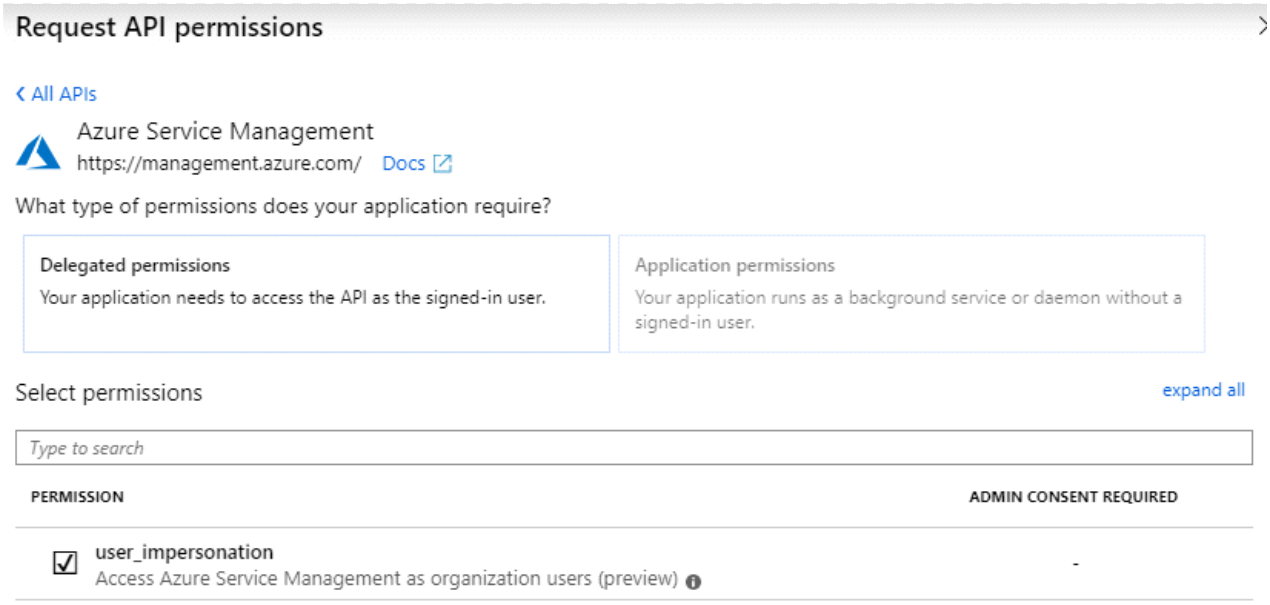
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

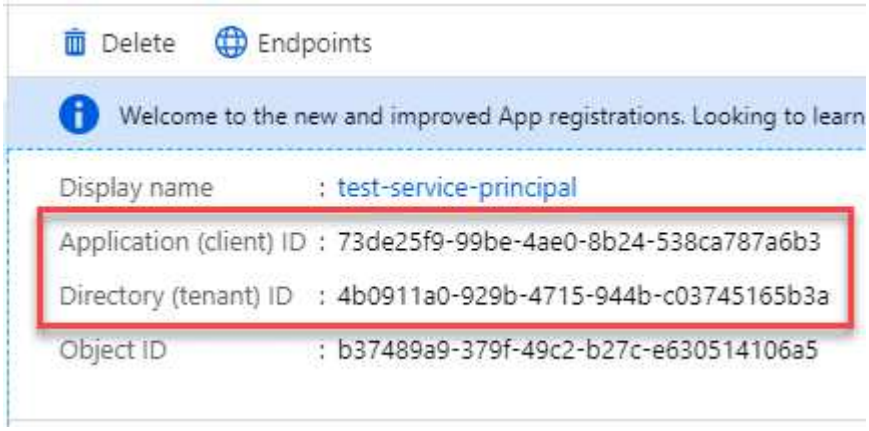


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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

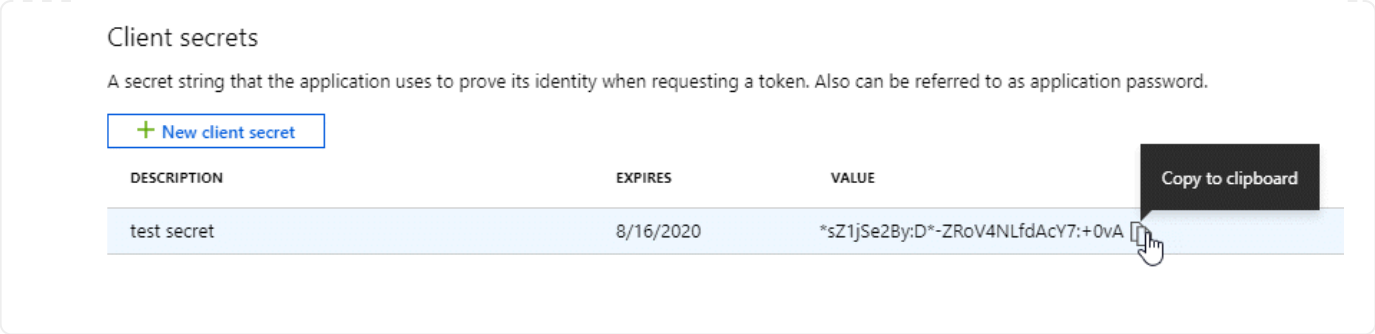
1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)**.



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

Mantieni gli agenti della console

Gestire un host VCenter o ESXi per l'agente della console

Dopo aver distribuito l'agente della console, è possibile apportare modifiche all'host VCenter o ESXi esistente. Ad esempio, è possibile aumentare la CPU o la RAM dell'istanza VM che ospita l'agente Console.

Eseguire queste attività di manutenzione utilizzando la console Web della VM:

- Aumentare la dimensione del disco
- Riavviare l'agente
- Aggiorna percorsi statici
- Aggiorna i domini di ricerca

Limitazioni

L'aggiornamento dell'agente tramite la console non è ancora supportato. Inoltre, è possibile visualizzare solo informazioni sull'indirizzo IP, DNS e gateway.

Accedi alla console di manutenzione della VM

È possibile accedere alla console di manutenzione dal client VSphere.

Passi

1. Apri il client VSphere e accedi al tuo VCenter.
2. Selezionare l'istanza della VM che ospita l'agente della console.
3. Selezionare **Avvia Web Console**.
4. Accedi all'istanza della VM utilizzando il nome utente e la password specificati al momento della creazione dell'istanza della VM. Il nome utente è `maint` e la password è quella specificata quando hai creato l'istanza della VM.

Cambia la password dell'utente principale

Puoi cambiare la password per `maint` utente.

Passi

1. Apri il client VSphere e accedi al tuo VCenter.
2. Selezionare l'istanza della VM che ospita l'agente della console.

3. Selezionare **Avvia Web Console**.
4. Accedi all'istanza della VM utilizzando il nome utente e la password specificati al momento della creazione dell'istanza della VM. Il nome utente è `maint` e la password è quella specificata quando hai creato l'istanza della VM.
5. Entra `1` per visualizzare il `System Configuration` menu.
6. Entra `1` per modificare la password dell'utente addetto alla manutenzione e seguire le istruzioni visualizzate sullo schermo.

Aumentare la CPU o la RAM dell'istanza della VM

È possibile aumentare la CPU o la RAM dell'istanza VM che ospita l'agente Console.

Modifica le impostazioni dell'istanza VM nell'host VCenter o ESXi, quindi utilizza la console di manutenzione per applicare le modifiche.

Passaggi nel client VSphere

1. Apri il client VSphere e accedi al tuo VCenter.
2. Selezionare l'istanza della VM che ospita l'agente della console.
3. Fare clic con il pulsante destro del mouse sull'istanza della VM e selezionare **Modifica impostazioni**.
4. Aumentare lo spazio sul disco rigido utilizzato per /opt o per la partizione /var.
   a. Selezionare **Disco rigido 2** per aumentare lo spazio sul disco rigido utilizzato per /opt.
   b. Selezionare **Disco rigido 3** per aumentare lo spazio sul disco rigido utilizzato per /var.
5. Salva le modifiche.

Passaggi nella console di manutenzione

1. Apri il client VSphere e accedi al tuo VCenter.
2. Selezionare l'istanza della VM che ospita l'agente della console.
3. Selezionare **Avvia Web Console**.
4. Accedi all'istanza della VM utilizzando il nome utente e la password specificati al momento della creazione dell'istanza della VM. Il nome utente è `maint` e la password è quella specificata quando hai creato l'istanza della VM.
5. Entra `1 to view the `System Configuration` menu.
6. Entra `2` e seguire le istruzioni visualizzate sullo schermo. La console esegue la scansione per trovare nuove impostazioni e aumenta le dimensioni delle partizioni.

Visualizza le impostazioni di rete per la VM dell'agente

Visualizzare le impostazioni di rete per la VM dell'agente nel client VSphere per confermare o risolvere i problemi di rete. È possibile visualizzare (non aggiornare) solo le seguenti impostazioni di rete: indirizzo IP e dettagli DNS.

Passi

1. Apri il client VSphere e accedi al tuo VCenter.
2. Selezionare l'istanza della VM che ospita l'agente della console.
3. Selezionare **Avvia Web Console**.

4. Accedi all'istanza della VM utilizzando il nome utente e la password specificati al momento della creazione dell'istanza della VM. Il nome utente è `maint` e la password è quella specificata quando hai creato l'istanza della VM.
5. Entra `2` per visualizzare il `Network Configuration` menu.
6. Immettere un numero compreso tra 1 e 6 per visualizzare le impostazioni di rete corrispondenti.

Aggiornare le route statiche per la VM dell'agente

Aggiungere, aggiornare o rimuovere percorsi statici per la VM dell'agente in base alle esigenze.

Passi

1. Apri il client VSphere e accedi al tuo VCenter.
2. Selezionare l'istanza della VM che ospita l'agente della console.
3. Selezionare **Avvia Web Console**.
4. Accedi all'istanza della VM utilizzando il nome utente e la password specificati al momento della creazione dell'istanza della VM. Il nome utente è `maint` e la password è quella specificata quando hai creato l'istanza della VM.
5. Entra `2` per visualizzare il `Network Configuration` menu.
6. Entra `7` per aggiornare i percorsi statici e seguire le istruzioni visualizzate sullo schermo.
7. Premere Invio.
8. Facoltativamente, apportare ulteriori modifiche.
9. Entra `9` per confermare le modifiche.

Aggiorna le impostazioni di ricerca del dominio per la VM dell'agente

È possibile aggiornare le impostazioni del dominio di ricerca per la VM dell'agente.

Passi

1. Apri il client VSphere e accedi al tuo VCenter.
2. Selezionare l'istanza della VM che ospita l'agente della console.
3. Selezionare **Avvia Web Console**.
4. Accedi all'istanza della VM utilizzando il nome utente e la password specificati al momento della creazione dell'istanza della VM. Il nome utente è `maint` e la password è quella specificata quando hai creato l'istanza della VM.
5. Entra `2` ` per visualizzare il `Network Configuration` menu.
6. Entra `8` per aggiornare le impostazioni di ricerca del dominio e seguire le istruzioni visualizzate sullo schermo.
7. Premere Invio.
8. Facoltativamente, apportare ulteriori modifiche.
9. Entra `9` per confermare le modifiche.

Accedi agli strumenti diagnostici dell'agente

Accedi agli strumenti diagnostici per risolvere i problemi con l'agente Console. L'assistenza NetApp potrebbe

chiederti di farlo durante la risoluzione dei problemi.

Passi

1. Apri il client VSphere e accedi al tuo VCenter.
2. Selezionare l'istanza della VM che ospita l'agente della console.
3. Selezionare **Avvia Web Console**.
4. Accedi all'istanza della VM utilizzando il nome utente e la password specificati al momento della creazione dell'istanza della VM. Il nome utente è `maint` e la password è quella specificata quando hai creato l'istanza della VM.
5. Entra `3` per visualizzare il menu Supporto e diagnostica.
6. Entra `1` per accedere agli strumenti diagnostici e seguire le istruzioni visualizzate sullo schermo. + Ad esempio, è possibile verificare che tutti i servizi dell'agente siano in esecuzione. "Controllare lo stato dell'agente della console" .

Accedi agli strumenti diagnostici dell'agente da remoto

È possibile accedere agli strumenti diagnostici da remoto con uno strumento come Putty. Abilitare l'accesso SSH alla VM dell'agente assegnando una password monouso.

L'accesso SSH consente funzionalità avanzate del terminale come copia e incolla.

Passi

1. Apri il client VSphere e accedi al tuo VCenter.
2. Selezionare l'istanza della VM che ospita l'agente della console.
3. Selezionare **Avvia Web Console**.
4. Accedi all'istanza della VM utilizzando il nome utente e la password specificati al momento della creazione dell'istanza della VM. Il nome utente è `maint` e la password è quella specificata quando hai creato l'istanza della VM.
5. Entra `3` per visualizzare il `Support and Diagnostics` menu.
6. Entra `2` per accedere agli strumenti diagnostici e seguire le istruzioni sullo schermo per configurare una password monouso che scade dopo 24 ore.
7. Utilizzare uno strumento SSH come Putty per connettersi alla VM dell'agente utilizzando il nome utente `diag` e la password monouso che hai configurato.

Installa un certificato firmato da una CA per l'accesso alla console basata sul Web

Quando si utilizza la NetApp Console in modalità limitata, l'interfaccia utente è accessibile dalla macchina virtuale dell'agente della console distribuita nella propria regione cloud o in locale. Per impostazione predefinita, la Console utilizza un certificato SSL autofirmato per fornire un accesso HTTPS sicuro alla console basata sul Web in esecuzione sull'agente della Console.

Se richiesto dalla tua azienda, puoi installare un certificato firmato da un'autorità di certificazione (CA), che garantisce una protezione di sicurezza migliore rispetto a un certificato autofirmato. Dopo aver installato il certificato, la Console utilizza il certificato firmato dalla CA quando gli utenti accedono alla console basata sul Web.

Installa un certificato HTTPS

Installare un certificato firmato da una CA per l'accesso sicuro alla console basata sul Web in esecuzione sull'agente Console.

Informazioni su questo compito

È possibile installare il certificato utilizzando una delle seguenti opzioni:

- Generare una richiesta di firma del certificato (CSR) dalla Console, inviare la richiesta di certificato a una CA, quindi installare il certificato firmato dalla CA sull'agente della Console.

  La coppia di chiavi utilizzata dalla Console per generare la CSR è memorizzata internamente sull'agente della Console. La Console recupera automaticamente la stessa coppia di chiavi (chiave privata) quando si installa il certificato sull'agente Console.

- Installa un certificato firmato da una CA di cui sei già in possesso.

  Con questa opzione, la CSR non viene generata tramite la Console. Il CSR viene generato separatamente e la chiave privata viene archiviata esternamente. Quando installi il certificato, fornisci alla Console la chiave privata.

Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona il menu azioni per un agente Console e seleziona **Configurazione HTTPS**.

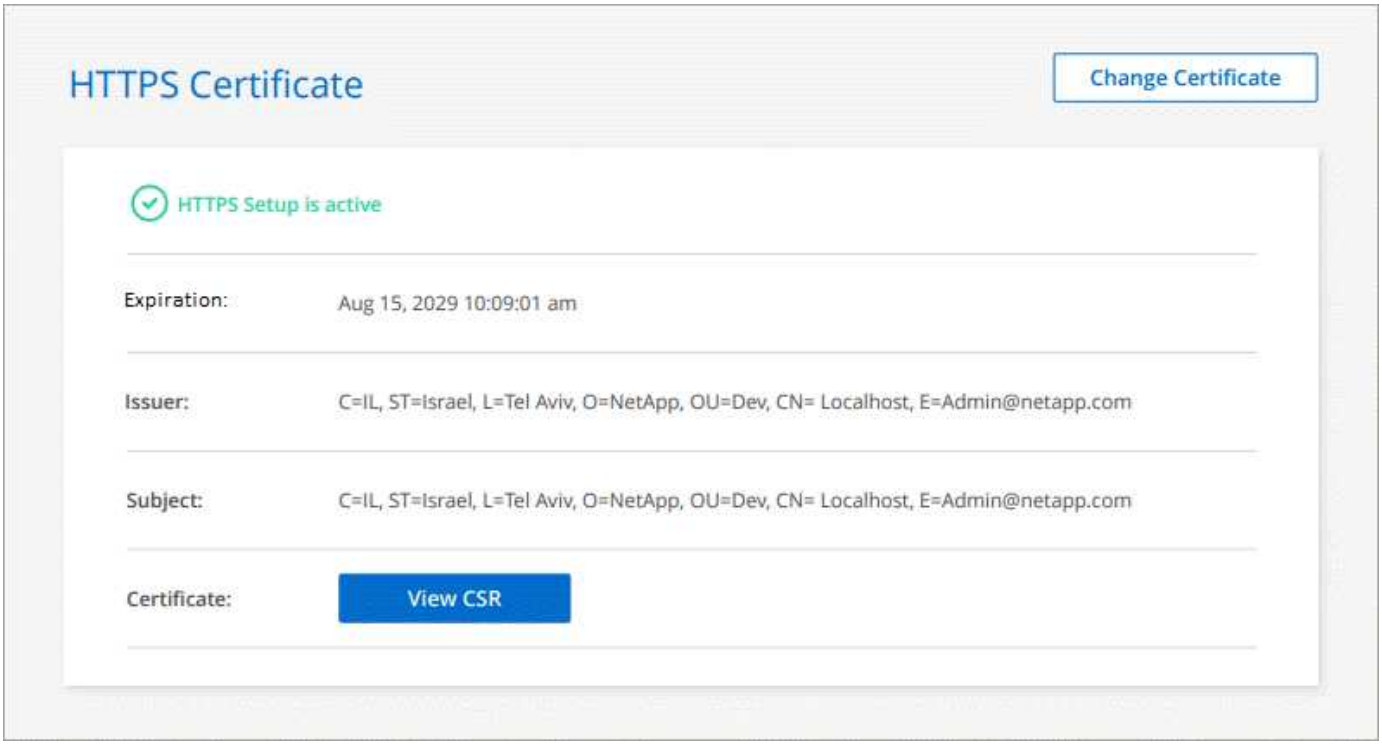
   Per modificarlo, è necessario che l'agente della console sia connesso.

3. Nella pagina Configurazione HTTPS, installa un certificato generando una richiesta di firma del certificato (CSR) o installando il tuo certificato firmato da una CA:

Opzione	Descrizione
Generare una CSR	a. Immettere il nome host o il DNS dell'host dell'agente della console (il suo nome comune), quindi selezionare **Genera CSR**. La console visualizza una richiesta di firma del certificato. b. Utilizzare il CSR per inviare una richiesta di certificato SSL a una CA. Il certificato deve utilizzare il formato X.509 codificato Base-64 Privacy Enhanced Mail (PEM). c. Carica il file del certificato e seleziona **Installa**.
Installa il tuo certificato firmato da CA	a. Selezionare **Installa certificato firmato da CA**. b. Caricare sia il file del certificato che la chiave privata, quindi selezionare **Installa**. Il certificato deve utilizzare il formato X.509 codificato Base-64 Privacy Enhanced Mail (PEM).

Risultato

L'agente Console ora utilizza il certificato firmato dalla CA per fornire un accesso HTTPS sicuro. L'immagine seguente mostra un agente configurato per l'accesso sicuro:



Rinnova il certificato HTTPS della console

Per garantire un accesso sicuro, è necessario rinnovare il certificato HTTPS dell'agente prima della scadenza. Se non si rinnova il certificato prima della scadenza, verrà visualizzato un avviso quando gli utenti accedono alla console Web tramite HTTPS.

Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona il menu azioni per un agente Console e seleziona **Configurazione HTTPS**.

   Vengono visualizzati i dettagli relativi al certificato, inclusa la data di scadenza.

3. Selezionare **Cambia certificato** e seguire i passaggi per generare una CSR o installare il proprio certificato firmato da una CA.

Configurare un agente Console per utilizzare un server proxy

Se le policy aziendali richiedono l'utilizzo di un server proxy per tutte le comunicazioni verso Internet, è necessario configurare gli agenti in modo che utilizzino tale server proxy. Se non hai configurato un agente Console per utilizzare un server proxy durante l'installazione, puoi configurare l'agente Console per utilizzare quel server proxy in qualsiasi momento.

Il server proxy dell'agente consente l'accesso a Internet in uscita senza un IP pubblico o un gateway NAT. Il server proxy fornisce connettività in uscita solo per l'agente Console, non per i sistemi Cloud Volumes ONTAP

.

Se i sistemi Cloud Volumes ONTAP non dispongono di accesso a Internet in uscita, la Console li configura per utilizzare il server proxy dell'agente della Console. È necessario assicurarsi che il gruppo di sicurezza dell'agente Console consenta le connessioni in entrata sulla porta 3128. Aprire questa porta dopo aver distribuito l'agente Console.

Se l'agente della console non dispone di una connessione Internet in uscita, i sistemi Cloud Volumes ONTAP non possono utilizzare il server proxy configurato.

Configurazioni supportate

- I server proxy trasparenti sono supportati per gli agenti che servono i sistemi Cloud Volumes ONTAP . Se si utilizzano i servizi dati NetApp con Cloud Volumes ONTAP, creare un agente dedicato per Cloud Volumes ONTAP in cui è possibile utilizzare un server proxy trasparente.
- I server proxy espliciti sono supportati da tutti gli agenti, compresi quelli che gestiscono i sistemi Cloud Volumes ONTAP e quelli che gestiscono i servizi dati NetApp .
- HTTP e HTTPS.
- Il server proxy può risiedere nel cloud o nella tua rete.

Una volta configurato un proxy, non è possibile modificarne il tipo. Se è necessario modificare il tipo di proxy, è necessario rimuovere l'agente Console e aggiungere un nuovo agente con il nuovo tipo di proxy.

Abilita un proxy esplicito su un agente della console

Quando si configura un agente Console per utilizzare un server proxy, sia l'agente stesso che i sistemi Cloud Volumes ONTAP da esso gestiti (inclusi eventuali mediatori HA) utilizzano tutti il server proxy.

Questa operazione riavvia l'agente Console. Verificare che l'agente della console sia inattivo prima di procedere.

Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona il menu azioni per un agente della console e seleziona **Modifica agente**.

   Per modificarlo, l'agente della console deve essere attivo.

3. Selezionare **Configurazione proxy HTTP**.
4. Selezionare **Proxy esplicito** nel campo Tipo di configurazione.
5. Seleziona **Abilita proxy**.
6. Specificare il server utilizzando la sintassi http://address:port O https://address:port
7. Specificare un nome utente e una password se è richiesta l'autenticazione di base per il server.

   Notare quanto segue:

   - L'utente può essere un utente locale o un utente di dominio.

- Per un utente di dominio, è necessario immettere il codice ASCII per \ come segue: domain-name%92user-name

  Ad esempio: netapp%92proxy

- La Console non supporta password che includono il carattere @.

8. Seleziona **Salva**.

Abilita un proxy trasparente per un agente della console

Solo Cloud Volumes ONTAP supporta l'utilizzo di un proxy trasparente sull'agente della console. Se si utilizzano i servizi dati NetApp oltre a Cloud Volumes ONTAP, è necessario creare un agente separato da utilizzare per i servizi dati o per Cloud Volumes ONTAP.

Prima di abilitare un proxy trasparente, assicurati che siano soddisfatti i seguenti requisiti:

- L'agente è installato sulla stessa rete del server proxy trasparente.
- L'ispezione TLS è abilitata sul server proxy.
- Si dispone di un certificato in formato PEM che corrisponde a quello utilizzato sul server proxy trasparente.
- Non utilizzare l'agente Console per nessun servizio dati NetApp diverso da Cloud Volumes ONTAP.

Per configurare un agente esistente affinché utilizzi un server proxy trasparente, è necessario utilizzare lo strumento di manutenzione dell'agente Console, disponibile tramite la riga di comando sull'host dell'agente Console.

Quando si configura un server proxy, l'agente Console si riavvia. Verificare che l'agente della console sia inattivo prima di procedere.

Passi

Assicurarsi di disporre di un file di certificato in formato PEM per il server proxy. Se non si dispone di un certificato, contattare l'amministratore di rete per ottenerne uno.

1. Aprire un'interfaccia della riga di comando sull'host dell'agente Console.
2. Passare alla directory dello strumento di manutenzione dell'agente della console: `/opt/application/netapp/service-manager-2/agent-maint-console`
3. Eseguire il seguente comando per abilitare il proxy trasparente, dove `/home/ubuntu/<certificate-file>.pem` è la directory e il nome del file del certificato che hai per il server proxy:

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

   Assicurarsi che il file del certificato sia in formato PEM e si trovi nella stessa directory del comando oppure specificare il percorso completo del file del certificato.

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

Modificare il proxy trasparente per l'agente della console

È possibile aggiornare il server proxy trasparente esistente di un agente della console utilizzando `proxy update` comando o rimuovere il server proxy trasparente utilizzando il `proxy remove` comando. Per ulteriori informazioni, consultare la documentazione relativa"Console di manutenzione dell'agente" .

> Una volta configurato un proxy, non è possibile modificarne il tipo. Se è necessario modificare il tipo di proxy, è necessario rimuovere l'agente Console e aggiungere un nuovo agente con il nuovo tipo di proxy.

Aggiorna il proxy dell'agente della console se perde l'accesso a Internet

Se la configurazione del proxy per la tua rete cambia, il tuo agente potrebbe perdere l'accesso a Internet. Ad esempio, se qualcuno modifica la password del server proxy o aggiorna il certificato. In questo caso, sarà necessario accedere all'interfaccia utente direttamente dall'host dell'agente della console e aggiornare le impostazioni. Assicurati di avere accesso alla rete dell'host dell'agente della Console e di poter accedere alla Console.

Abilita il traffico API diretto

Se hai configurato un agente Console per utilizzare un server proxy, puoi abilitare il traffico API diretto sull'agente Console per inviare chiamate API direttamente ai servizi del provider cloud senza passare attraverso il proxy. Questa opzione è supportata dagli agenti in esecuzione su AWS, Azure o Google Cloud.

Se si disabilita Azure Private Links con Cloud Volumes ONTAP e si utilizzano endpoint di servizio, abilitare il traffico API diretto. Altrimenti il traffico non verrà instradato correttamente.

"Scopri di più sull'utilizzo di un collegamento privato di Azure o di endpoint di servizio con Cloud Volumes ONTAP"

Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona il menu azioni per un agente della console e seleziona **Modifica agente**.

   Per modificarlo, l'agente della console deve essere attivo.

3. Seleziona **Supporta traffico API diretto**.
4. Selezionare la casella di controllo per abilitare l'opzione, quindi selezionare **Salva**.

Risolvere i problemi dell'agente della console

Per risolvere i problemi con un agente della console, puoi verificare tu stesso i problemi o contattare il supporto NetApp , che potrebbe chiederti l'ID del tuo sistema, la versione dell'agente o gli ultimi messaggi AutoSupport .

Se si dispone di un account del sito di supporto NetApp , è anche possibile visualizzare"Base di conoscenza NetApp ."

Messaggi di errore comuni e risoluzioni

Questa tabella elenca i messaggi di errore più comuni e mostra come risolverli:

Messaggio di errore	Spiegazione	Cosa fare
Impossibile caricare l'interfaccia utente dell'agente della console	L'installazione dell'agente non è riuscita	• Verificare che il servizio Service Manager sia attivo. • Verificare che tutti i contenitori siano in esecuzione. • Assicurati che il tuo firewall consenta l'accesso al servizio sulla porta 8888. • Se i problemi persistono, contatta l'assistenza.
Impossibile accedere all'interfaccia utente dell'agente NetApp	Questo messaggio viene visualizzato quando si tenta di accedere all'indirizzo IP di un agente. L'agente potrebbe non riuscire a inizializzarsi se non dispone dell'accesso di rete corretto o se è instabile.	• Connettersi all'agente della console. • Verificare che il servizio Service Manager • Verificare che l'agente disponga dell'accesso alla rete di cui ha bisogno."Scopri di più sugli endpoint di accesso alla rete richiesti."
Impossibile caricare le impostazioni dell'agente	La Console visualizza questo messaggio quando si tenta di accedere alla pagina delle impostazioni dell'agente.	• Verificare se il contenitore OCCM è in esecuzione e funzionante. • Se il problema persiste, contattare l'assistenza.
Impossibile caricare le informazioni di supporto per l'agente.	Questo messaggio viene visualizzato se l'agente non riesce ad accedere al tuo account di supporto.	• Verificare che l'agente abbia accesso in uscita agli endpoint richiesti."Scopri di più sugli endpoint di accesso alla rete richiesti."

Controllare lo stato dell'agente della console

Utilizzare uno dei seguenti comandi per verificare l'agente della console. Tutti i servizi dovrebbero avere lo stato *In esecuzione*. In caso contrario, contattare l'assistenza NetApp .

Per informazioni più dettagliate sull'accesso alla diagnostica dell'agente Console, vedere i seguenti argomenti:

- "Controllare lo stato dell'agente della console (per le distribuzioni host Linux)"
- "Controllare lo stato dell'agente della console (per le distribuzioni VCenter)"

Docker (per distribuzioni Ubuntu e VCenter)

```
docker ps -a
```

Podman (per distribuzioni RedHat Enterprise Linux)

```
podman ps -a
```

Visualizza la versione dell'agente della console

Visualizza la versione dell'agente della console per confermare l'aggiornamento o condividila con il tuo rappresentante NetApp .

Passi

1. Selezionare **Amministrazione > Supporto > Agenti**.

   La Console visualizza la versione nella parte superiore della pagina.

Verifica l'accesso alla rete

Assicurarsi che l'agente della console disponga dell'accesso alla rete necessario."Scopri di più sui punti di accesso alla rete richiesti."

Eseguire controlli di configurazione sull'agente Console

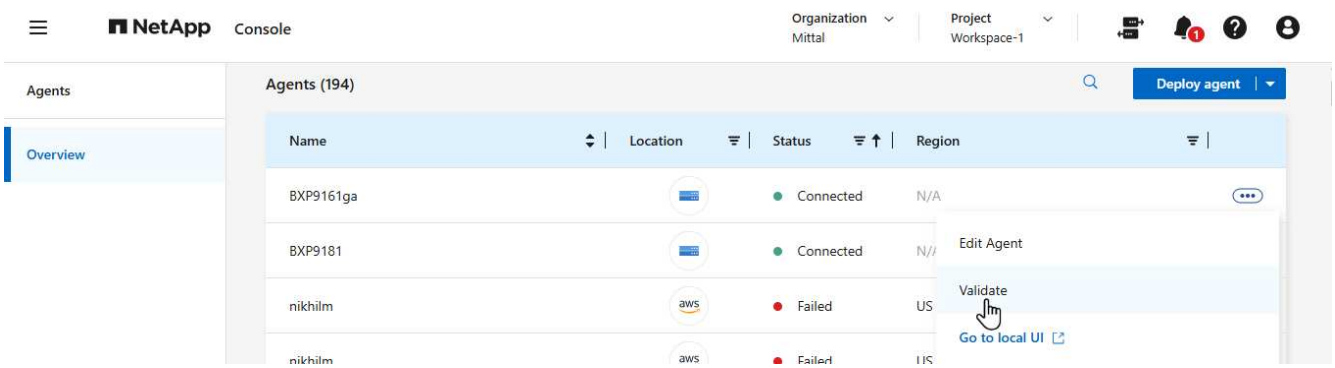
Eseguire controlli di configurazione sugli agenti della Console dalla Console o dalla console di manutenzione dell'agente per assicurarsi che siano connessi.

È anche possibile eseguire controlli di configurazione utilizzando la console di manutenzione dell'agente."Scopri di più sull'utilizzo del comando config-checker validate."

È possibile convalidare solo gli agenti che hanno lo stato **Connesso**.

Passi dalla console

1. Selezionare **Amministrazione > Agenti**.
2. Selezionare il menu azioni per un agente della console che si desidera controllare e scegliere **Convalida**.



La convalida può richiedere fino a 15 minuti. I risultati si vedono quando il lavoro è finito.

Problemi di installazione dell'agente della console

Se l'installazione non riesce, visualizza il report e i registri per risolvere i problemi.

È inoltre possibile accedere al report di convalida in formato JSON e ai log di configurazione direttamente

dall'host dell'agente della console nelle seguenti directory:

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- Per le nuove distribuzioni di agenti, NetApp verifica i seguenti endpoint:"elencato qui" . Questo controllo di configurazione fallisce con un errore se si utilizzano gli endpoint precedenti utilizzati per gli aggiornamenti,"elencato qui" . NetApp consiglia di aggiornare le regole del firewall per consentire l'accesso agli endpoint correnti e bloccare l'accesso agli endpoint precedenti il prima possibile."Scopri come aggiornare la tua rete" .
- Se aggiorni gli endpoint nel firewall, gli agenti esistenti continueranno a funzionare.

Disabilitare i controlli di configurazione per le installazioni manuali

Potrebbero esserci momenti in cui è necessario disattivare i controlli di configurazione che verificano la connettività in uscita durante l'installazione. Ad esempio, quando si installa manualmente un agente nel proprio ambiente Government Cloud, è necessario disabilitare i controlli di configurazione, altrimenti l'installazione non andrà a buon fine.

Passi

È possibile disattivare il controllo della configurazione impostando il flag *skipConfigCheck* nel file *com/opt/application/netapp/service-manager-2/config.json*. Per impostazione predefinita, questo flag è impostato su false e il controllo della configurazione verifica l'accesso in uscita per l'agente. Impostare questo flag su true per disabilitare il controllo. Prima di completare questo passaggio, è necessario acquisire familiarità con la sintassi JSON.

Per riattivare il controllo della configurazione, seguire questi passaggi e impostare il flag *skipConfigCheck* su false.

Passi

1. Accedere all'host dell'agente della console come root o con privilegi sudo.
2. Crea una copia di backup del file */opt/application/netapp/service-manager-2/config.json* per assicurarti di poter annullare le modifiche.
3. Arrestare il servizio Service Manager 2 eseguendo il seguente comando:

```
systemctl stop netapp-service-manager.service
```

1. Modificare il file */opt/application/netapp/service-manager-2/config.json* e cambiare il valore del flag *skipConfigCheck* in true.

```
"skipConfigCheck": true
```

2. Salva il tuo file.
3. Riavviare il servizio Service Manager 2 eseguendo il seguente comando:

```
systemctl restart netapp-service-manager.service
```

Lavora con il supporto NetApp

Se non sei riuscito a risolvere i problemi con l'agente della console, potresti contattare l'assistenza NetApp . Il supporto NetApp potrebbe richiedere l'ID dell'agente della console o l'invio dei registri dell'agente della console, se non li hanno già.

Trova l'ID dell'agente della console

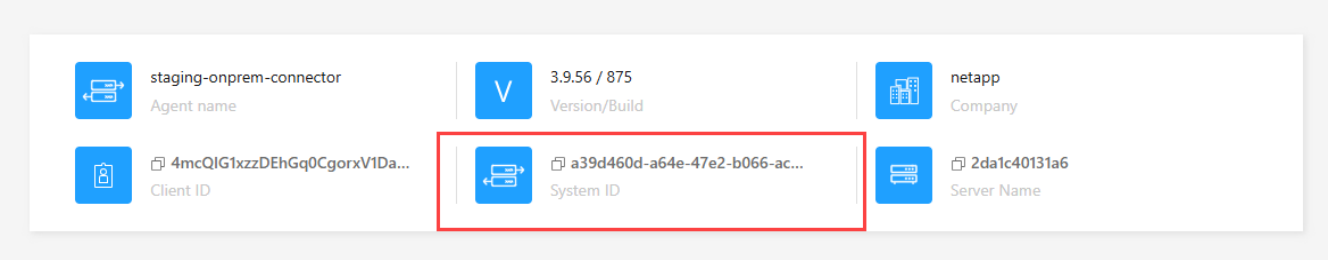
Per iniziare, potrebbe essere necessario l'ID di sistema del tuo agente Console. L'ID viene solitamente utilizzato per scopi di licenza e risoluzione dei problemi.

Passi

1. Selezionare **Amministrazione > Supporto > Agenti**.

   Puoi trovare l'ID del sistema nella parte superiore della pagina.

   Esempio

2. Passa il mouse e clicca sull'ID per copiarlo.

Scarica o invia un messaggio AutoSupport

In caso di problemi, NetApp potrebbe chiederti di inviare un messaggio AutoSupport al supporto NetApp per la risoluzione dei problemi.

A causa del bilanciamento del carico, la NetApp Console impiega fino a cinque ore per inviare messaggi AutoSupport . Per comunicazioni urgenti, scaricare il file e inviarlo manualmente.

Passi

1. Selezionare **Amministrazione > Supporto > Agenti**.
2. A seconda di come desideri inviare le informazioni al supporto NetApp , scegli una delle seguenti opzioni:
   a. Seleziona l'opzione per scaricare il messaggio AutoSupport sul tuo computer locale. Puoi quindi inviarlo al supporto NetApp utilizzando il metodo che preferisci.
   b. Selezionare **Invia AutoSupport** per inviare direttamente il messaggio al supporto NetApp .

Correggi gli errori di download quando utilizzi un gateway Google Cloud NAT

L'agente Console scarica automaticamente gli aggiornamenti software per Cloud Volumes ONTAP. La configurazione potrebbe causare il fallimento del download se si utilizza un gateway Google Cloud NAT. È

possibile correggere questo problema limitando il numero di parti in cui è suddivisa l'immagine software. Questo passaggio deve essere completato utilizzando l'API.

Fare un passo

1. Invia una richiesta PUT a /occm/config con il seguente JSON come corpo:

```
{
  "maxDownloadSessions": 32
}
```

   Il valore per *maxDownloadSessions* può essere 1 o qualsiasi numero intero maggiore di 1. Se il valore è 1, l'immagine scaricata non verrà divisa.

   Si noti che 32 è un valore di esempio. Il valore dipende dalla configurazione NAT e dal numero di sessioni simultanee.

"Scopri di più sulla chiamata API /occm/config"

Ottieni assistenza dalla Knowledge Base NetApp

"Visualizza le informazioni sulla risoluzione dei problemi create dal team di supporto NetApp" .

Disinstallare e rimuovere un agente Console

Disinstallare un agente Console per risolvere i problemi o per rimuoverlo definitivamente dall'host. I passaggi da seguire dipendono dalla modalità di distribuzione utilizzata. Dopo aver rimosso un agente Console dal tuo ambiente, puoi rimuoverlo dalla Console.

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

Disinstallare l'agente quando si utilizza la modalità standard o limitata

Se si utilizza la modalità standard o la modalità limitata (in altre parole, l'host dell'agente ha connettività in uscita), è necessario seguire i passaggi indicati di seguito per disinstallare l'agente.

Passi

1. Connettersi alla VM Linux per l'agente.
2. Dall'host Linux, eseguire lo script di disinstallazione:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent esegue lo script senza chiedere conferma.

Rimuovere gli agenti della console dalla console

Se hai eliminato una VM dell'agente o hai disinstallato l'agente, dovresti rimuoverlo dall'elenco degli agenti nella Console. Dopo aver eliminato una VM dell'agente o aver disinstallato il software dell'agente, l'agente mostra lo stato **Disconnesso** nella Console.

Tenere presente quanto segue sulla rimozione di un agente Console:

- Questa azione non elimina la macchina virtuale.
- Questa azione non può essere annullata: una volta rimosso un agente della console, non è possibile aggiungerlo di nuovo.

Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona il menu azioni per un agente disconnesso e seleziona **Rimuovi agente**.
3. Inserisci il nome dell'agente per confermare e poi seleziona **Rimuovi**.

Gestisci le credenziali del provider cloud

AWS

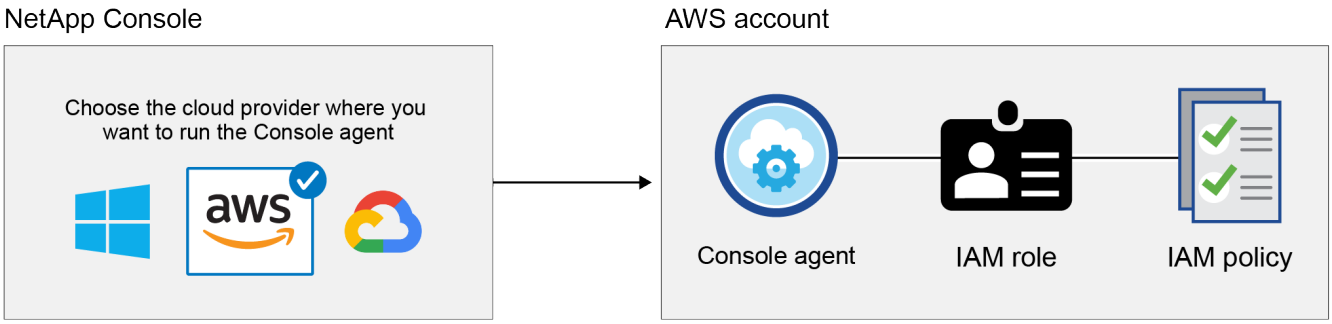
Scopri di più sulle credenziali e le autorizzazioni AWS nella NetApp Console

Puoi gestire le credenziali AWS e gli abbonamenti al marketplace direttamente dalla NetApp Console per garantire una distribuzione sicura di Cloud Volumes ONTAP e di altri servizi dati fornendo le credenziali IAM appropriate durante la distribuzione dell'agente della console e associandole agli abbonamenti ad AWS Marketplace per la fatturazione.

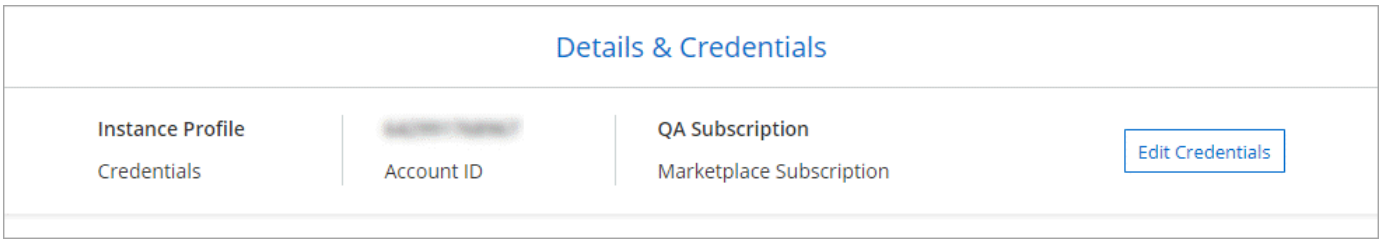
Credenziali AWS iniziali

Quando si distribuisce un agente Console dalla Console, è necessario fornire l'ARN di un ruolo IAM o le chiavi di accesso per un utente IAM. Il metodo di autenticazione deve disporre delle autorizzazioni per distribuire l'agente della console in AWS. Le autorizzazioni richieste sono elencate nel"Criteri di distribuzione degli agenti per AWS" .

Quando la Console avvia l'agente della Console in AWS, crea un ruolo IAM e un profilo per l'agente. Associa inoltre una policy che fornisce all'agente della console le autorizzazioni per gestire risorse e processi all'interno di quell'account AWS. "Esaminare come l'agente utilizza le autorizzazioni".



Se aggiungi un nuovo sistema Cloud Volumes ONTAP , la Console seleziona per impostazione predefinita queste credenziali AWS:



Distribuisci tutti i tuoi sistemi Cloud Volumes ONTAP utilizzando le credenziali AWS iniziali oppure puoi aggiungere credenziali aggiuntive.

Credenziali AWS aggiuntive

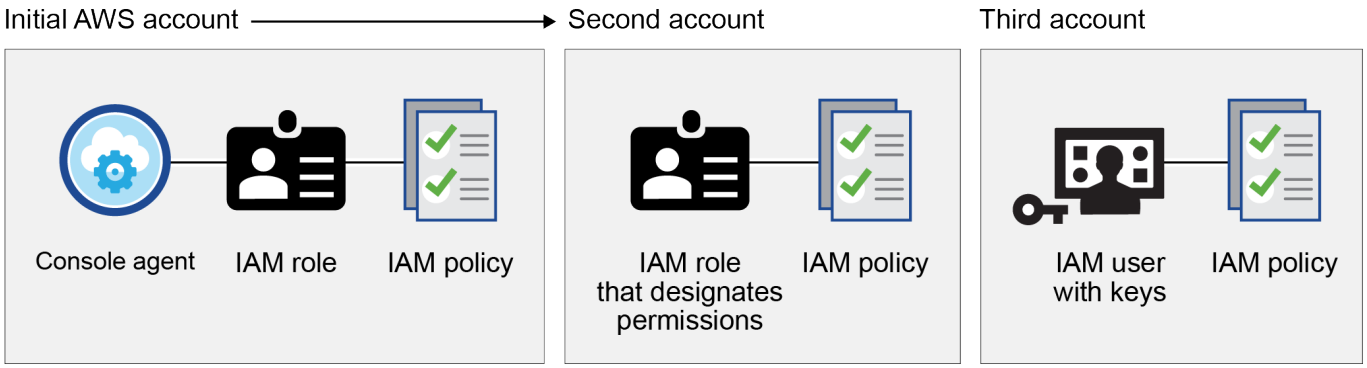
È possibile aggiungere ulteriori credenziali AWS alla Console nei seguenti casi:

- Per utilizzare l'agente della console esistente con un account AWS aggiuntivo
- Per creare un nuovo agente in un account AWS specifico
- Per creare e gestire FSx per i file system ONTAP

Per maggiori dettagli, consultare le sezioni seguenti.

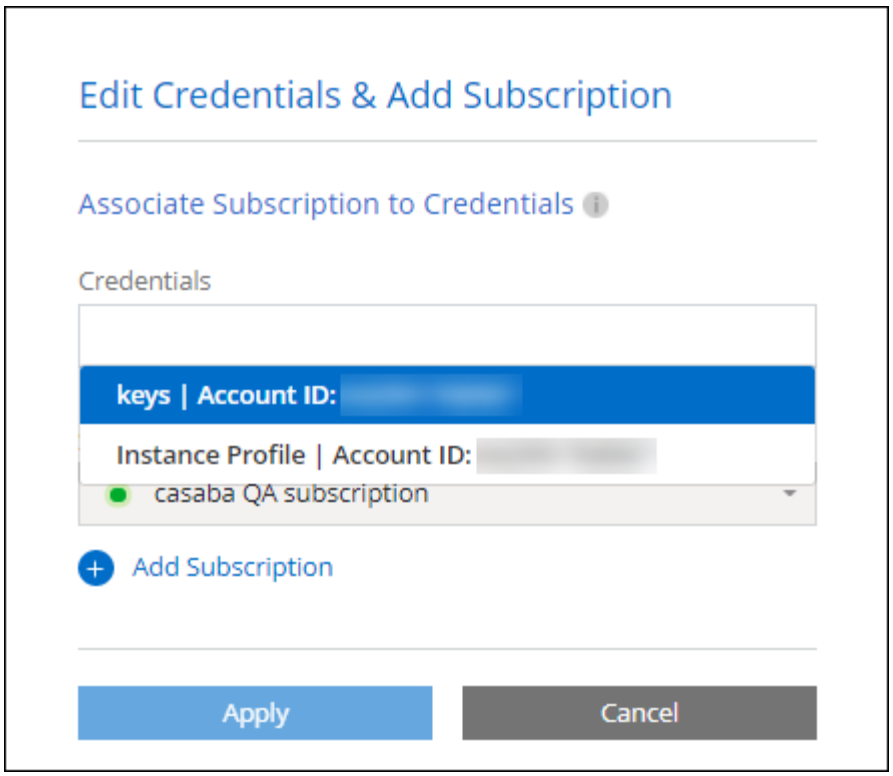
Aggiungi le credenziali AWS per utilizzare un agente della console con un altro account AWS

Per utilizzare la Console con account AWS aggiuntivi, fornire le chiavi AWS o l'ARN di un ruolo in un account attendibile. L'immagine seguente mostra due account aggiuntivi, uno che fornisce autorizzazioni tramite un ruolo IAM in un account attendibile e l'altro tramite le chiavi AWS di un utente IAM:



È possibile aggiungere le credenziali dell'account alla Console specificando l'Amazon Resource Name (ARN) del ruolo IAM o le chiavi AWS per l'utente IAM.

Ad esempio, è possibile passare da una credenziale all'altra quando si crea un nuovo sistema Cloud Volumes ONTAP :



"Scopri come aggiungere le credenziali AWS a un agente esistente."

Aggiungi le credenziali AWS per creare un agente della console

L'aggiunta delle credenziali AWS fornisce le autorizzazioni per creare un agente della console.

"Scopri come aggiungere le credenziali AWS alla Console per creare un agente della Console"

Aggiungi le credenziali AWS per FSx per ONTAP

Aggiungere le credenziali AWS alla Console per fornire le autorizzazioni necessarie per creare e gestire un sistema FSx for ONTAP .

"Scopri come aggiungere le credenziali AWS alla console per Amazon FSx per ONTAP"

Credenziali e abbonamenti al marketplace

È necessario associare le credenziali aggiunte a un agente della console a un abbonamento AWS Marketplace per pagare Cloud Volumes ONTAP a una tariffa oraria (PAYGO) e altri servizi dati NetApp o tramite un contratto annuale. "Scopri come associare un abbonamento AWS".

Tieni presente quanto segue in merito alle credenziali AWS e agli abbonamenti al marketplace:

- È possibile associare un solo abbonamento AWS Marketplace a un set di credenziali AWS
- Puoi sostituire un abbonamento esistente al marketplace con un nuovo abbonamento

Domande frequenti

Le seguenti domande riguardano credenziali e abbonamenti.

Come posso ruotare in modo sicuro le mie credenziali AWS?

Come descritto nelle sezioni precedenti, la Console consente di fornire credenziali AWS in diversi modi: un ruolo IAM associato all'agente della Console, assumendo un ruolo IAM in un account attendibile o fornendo chiavi di accesso AWS.

Con le prime due opzioni, la Console utilizza AWS Security Token Service per ottenere credenziali temporanee che ruotano costantemente. Questo processo è la prassi migliore: è automatico e sicuro.

Se fornisci alla Console le chiavi di accesso AWS, dovresti ruotare le chiavi aggiornandole nella Console a intervalli regolari. Si tratta di un processo completamente manuale.

Posso modificare l'abbonamento AWS Marketplace per i sistemi Cloud Volumes ONTAP ?

Sì, puoi. Quando modifichi l'abbonamento ad AWS Marketplace associato a un set di credenziali, tutti i sistemi Cloud Volumes ONTAP esistenti e nuovi vengono addebitati sul nuovo abbonamento.

"Scopri come associare un abbonamento AWS" .

Posso aggiungere più credenziali AWS, ciascuna con diversi abbonamenti al marketplace?

Tutte le credenziali AWS appartenenti allo stesso account AWS saranno associate allo stesso abbonamento AWS Marketplace.

Se disponi di più credenziali AWS appartenenti a diversi account AWS, tali credenziali possono essere associate allo stesso abbonamento AWS Marketplace o a diversi abbonamenti.

Posso spostare i sistemi Cloud Volumes ONTAP esistenti su un account AWS diverso?

No, non è possibile spostare le risorse AWS associate al sistema Cloud Volumes ONTAP su un account AWS diverso.

Come funzionano le credenziali per le distribuzioni sul marketplace e le distribuzioni on-premise?

Le sezioni precedenti descrivono il metodo di distribuzione consigliato per l'agente Console, ovvero dalla Console. È anche possibile distribuire un agente in AWS da AWS Marketplace e installare manualmente il software dell'agente della console sul proprio host Linux o nel proprio VCenter.

Se si utilizza il Marketplace, le autorizzazioni vengono fornite nello stesso modo. È sufficiente creare e configurare manualmente il ruolo IAM e quindi fornire le autorizzazioni per eventuali account aggiuntivi.

Per le distribuzioni in locale, non è possibile impostare un ruolo IAM per la Console, ma è possibile fornire autorizzazioni utilizzando le chiavi di accesso AWS.

Per informazioni su come impostare le autorizzazioni, fare riferimento alle seguenti pagine:

- Modalità standard
  - "Impostare le autorizzazioni per una distribuzione AWS Marketplace"
  - "Impostare le autorizzazioni per le distribuzioni in locale"
- Modalità limitata
  - "Imposta le autorizzazioni per la modalità limitata"

Aggiungi e gestisci le credenziali AWS in modo da distribuire e gestire le risorse cloud nei tuoi account AWS dalla NetApp Console. Se gestisci più abbonamenti AWS Marketplace, puoi assegnare a ciascuno di essi credenziali AWS diverse dalla pagina Credenziali.

Panoramica

È possibile aggiungere le credenziali AWS a un agente della Console esistente o direttamente alla Console:

- Aggiungi ulteriori credenziali AWS a un agente esistente

  Aggiungi le credenziali AWS a un agente della console per gestire le risorse cloud. Scopri come aggiungere le credenziali AWS a un agente della console .

- Aggiungere le credenziali AWS alla Console per creare un agente della Console

  L'aggiunta di nuove credenziali AWS alla Console fornisce le autorizzazioni necessarie per creare un agente della Console. Scopri come aggiungere le credenziali AWS alla NetApp Console .

- Aggiungere le credenziali AWS alla console per FSx per ONTAP

  Aggiungi nuove credenziali AWS alla Console per creare e gestire FSx per ONTAP. "Scopri come impostare le autorizzazioni per FSx per ONTAP"

Come ruotare le credenziali

La NetApp Console consente di fornire le credenziali AWS in diversi modi: un ruolo IAM associato all'istanza dell'agente, assumendo un ruolo IAM in un account attendibile o fornendo le chiavi di accesso AWS. "Scopri di più sulle credenziali e le autorizzazioni AWS" .

Con le prime due opzioni, la Console utilizza AWS Security Token Service per ottenere credenziali temporanee che ruotano costantemente. Questo processo è la prassi migliore perché è automatico e sicuro.

Ruota manualmente le chiavi di accesso AWS aggiornandole nella Console.

Aggiungere credenziali aggiuntive a un agente della console

Aggiungi ulteriori credenziali AWS a un agente della console in modo che disponga delle autorizzazioni necessarie per gestire risorse e processi all'interno del tuo ambiente cloud pubblico. È possibile fornire l'ARN di un ruolo IAM in un altro account oppure fornire le chiavi di accesso AWS.

"Scopri come la NetApp Console utilizza le credenziali e le autorizzazioni AWS".

Concedi permessi

Concedi le autorizzazioni prima di aggiungere le credenziali AWS a un agente della console. Le autorizzazioni consentono a un agente della console di gestire risorse e processi all'interno di quell'account AWS. È possibile fornire le autorizzazioni con l'ARN di un ruolo in un account attendibile o chiavi AWS.

Se hai distribuito un agente della Console dalla Console, sono state aggiunte automaticamente le credenziali AWS per l'account in cui hai distribuito un agente della Console. In questo modo si garantisce che siano disponibili le autorizzazioni necessarie per la gestione delle risorse.

Scelte

- Concedi autorizzazioni assumendo un ruolo IAM in un altro account
- Concedi le autorizzazioni fornendo le chiavi AWS

Concedi autorizzazioni assumendo un ruolo IAM in un altro account

È possibile impostare una relazione di trust tra l'account AWS di origine in cui è stato distribuito un agente della console e altri account AWS utilizzando i ruoli IAM. Dovresti quindi fornire alla Console l'ARN dei ruoli IAM degli account attendibili.

Se un agente Console è installato in locale, non è possibile utilizzare questo metodo di autenticazione. È necessario utilizzare le chiavi AWS.

Passi

1. Accedere alla console IAM nell'account di destinazione in cui si desidera fornire autorizzazioni a un agente della console.
2. In Gestione accessi, seleziona **Ruoli > Crea ruolo** e segui i passaggi per creare il ruolo.

   Assicurati di fare quanto segue:

   - In **Tipo di entità attendibile**, seleziona **Account AWS**.
   - Seleziona **Un altro account AWS** e inserisci l'ID dell'account in cui risiede un'istanza dell'agente della console.
   - Creare le policy richieste copiando e incollando il contenuto di"le policy IAM per un agente Console" .
3. Copia l'ARN del ruolo IAM in modo da poterlo incollare nella Console in un secondo momento.

Risultato

L'account dispone delle autorizzazioni richieste. Ora puoi aggiungere le credenziali a un agente della console .

Concedi le autorizzazioni fornendo le chiavi AWS

Se si desidera fornire alla Console le chiavi AWS per un utente IAM, è necessario concedere le autorizzazioni richieste a tale utente. La policy IAM della console definisce le azioni e le risorse AWS che la console può utilizzare.

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

Passi

1. Dalla console IAM, creare policy copiando e incollando il contenuto di"le policy IAM per un agente Console" .

   "Documentazione AWS: creazione di policy IAM"

2. Associare i criteri a un ruolo IAM o a un utente IAM.
   - "Documentazione AWS: creazione di ruoli IAM"
   - "Documentazione AWS: aggiunta e rimozione di policy IAM"

Aggiungi le credenziali a un agente esistente

Dopo aver fornito a un account AWS le autorizzazioni necessarie, puoi aggiungere le credenziali per tale account a un agente esistente. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in quell'account utilizzando lo stesso agente.

> Potrebbero volerci alcuni minuti prima che le nuove credenziali del tuo provider cloud diventino disponibili.

Passi

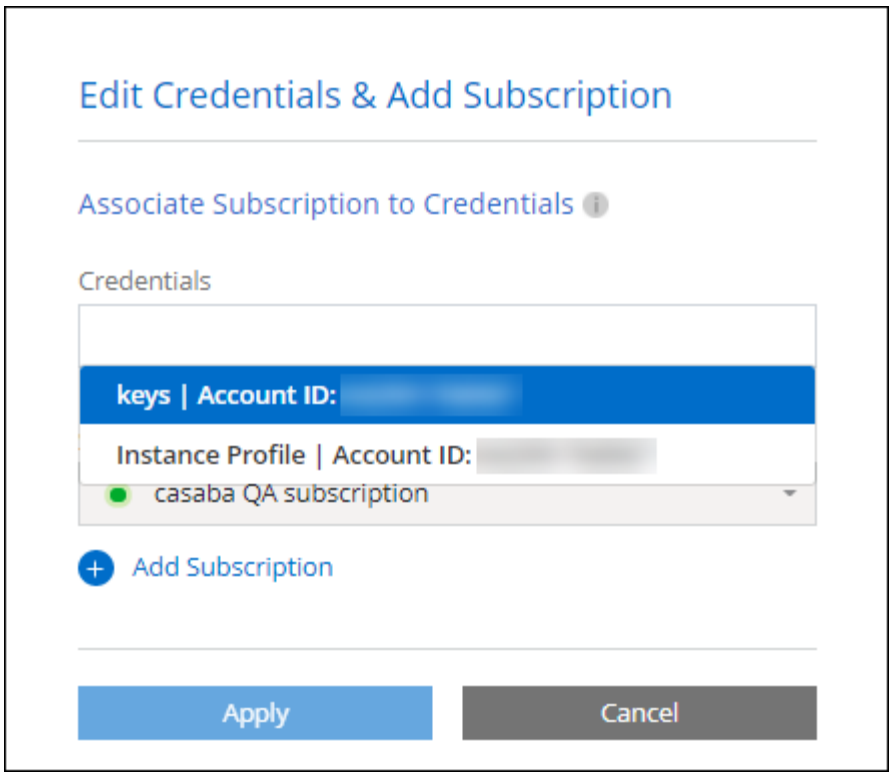
1. Utilizzare la barra di navigazione superiore per selezionare un agente della console a cui si desidera aggiungere le credenziali.
2. Nella barra di navigazione a sinistra, seleziona **Amministrazione > Credenziali**.
3. Nella pagina **Credenziali dell'organizzazione**, seleziona **Aggiungi credenziali** e segui i passaggi della procedura guidata.
   a. **Posizione delle credenziali**: seleziona **Amazon Web Services > Agente**.
   b. **Definisci credenziali**: fornisci l'ARN (Amazon Resource Name) di un ruolo IAM attendibile oppure 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.

      Per pagare i servizi con una tariffa oraria (PAYGO) o con un contratto annuale, è necessario associare le credenziali AWS al proprio abbonamento ad AWS Marketplace.

   d. **Revisione**: conferma i dettagli sulle nuove credenziali e seleziona **Aggiungi**.

Risultato

Ora puoi passare a un set di credenziali diverso dalla pagina Dettagli e credenziali quando aggiungi un abbonamento alla Console.



Aggiungere le credenziali alla Console per creare un agente Console

Aggiungere le credenziali AWS fornendo l'ARN di un ruolo IAM che fornisce le autorizzazioni necessarie per creare un agente della console. Puoi scegliere queste credenziali quando crei un nuovo agente.

Impostare il ruolo IAM

Impostare un ruolo IAM che consenta al livello SaaS (Software as a Service) della NetApp Console di assumere tale ruolo.

Passi

1. Accedere alla console IAM nell'account di destinazione.
2. In Gestione accessi, seleziona **Ruoli > Crea ruolo** e segui i passaggi per creare il ruolo.

   Assicurati di fare quanto segue:

   - In **Tipo di entità attendibile**, seleziona **Account AWS**.
   - Seleziona **Un altro account AWS** e inserisci l'ID di NetApp Console SaaS: 952013314444
   - Specificamente per Amazon FSx for NetApp ONTAP , modificare la policy **Relazioni di trust** per includere "AWS": "arn:aws:iam::952013314444:root".

     Ad esempio, la policy dovrebbe apparire così:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
Fare riferimento a "Documentazione di AWS Identity and Access Management (IAM)" per ulteriori informazioni sull'accesso alle risorse tra account in IAM.

- Creare un criterio che includa le autorizzazioni necessarie per creare un agente Console.
  - "Visualizza le autorizzazioni necessarie per FSx per ONTAP"
  - "Visualizza la politica di distribuzione dell'agente"

3. Copia l'ARN del ruolo IAM in modo da poterlo incollare nella Console nel passaggio successivo.

Risultato

Il ruolo IAM ora dispone delle autorizzazioni necessarie. Ora puoi aggiungerlo alla Console.

Aggiungi le credenziali

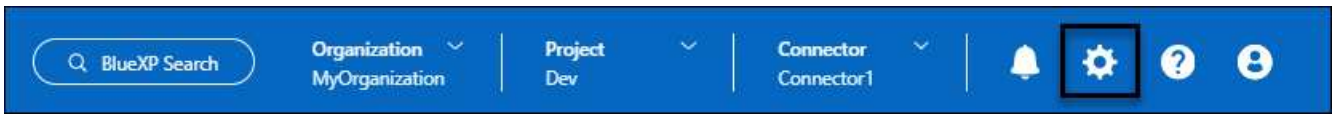
Dopo aver fornito al ruolo IAM le autorizzazioni richieste, aggiungere l'ARN del ruolo alla Console.

Prima di iniziare

Se hai appena creato il ruolo IAM, potrebbero volerci alcuni minuti prima che sia disponibile per l'uso. Attendi qualche minuto prima di aggiungere le credenziali alla Console.

Passi

1. Selezionare **Amministrazione > Credenziali**.



2. Nella pagina **Credenziali dell'organizzazione**, seleziona **Aggiungi credenziali** e segui i passaggi della procedura guidata.
   a. **Posizione delle credenziali**: seleziona **Amazon Web Services > Console**.
   b. **Definisci credenziali**: fornisci l'ARN (Amazon Resource Name) del ruolo IAM.
   c. **Revisione**: conferma i dettagli sulle nuove credenziali e seleziona **Aggiungi**.

Aggiungere le credenziali alla console per Amazon FSx per ONTAP

Per i dettagli, fare riferimento al "la documentazione della console per Amazon FSx per ONTAP"

Configurare un abbonamento AWS

Dopo aver aggiunto le credenziali AWS, puoi configurare un abbonamento ad AWS Marketplace con tali credenziali. L'abbonamento consente di pagare i servizi dati NetApp e Cloud Volumes ONTAP a una tariffa oraria (PAYGO) o tramite un contratto annuale.

Esistono due scenari in cui potresti configurare un abbonamento ad AWS Marketplace dopo aver già aggiunto le credenziali:

- Non hai configurato un abbonamento quando hai aggiunto inizialmente le credenziali.
- Desideri modificare l'abbonamento AWS Marketplace configurato con le credenziali AWS.

  La sostituzione dell'attuale abbonamento al marketplace con un nuovo abbonamento modifica l'abbonamento al marketplace per tutti i sistemi Cloud Volumes ONTAP esistenti e per tutti i nuovi sistemi.

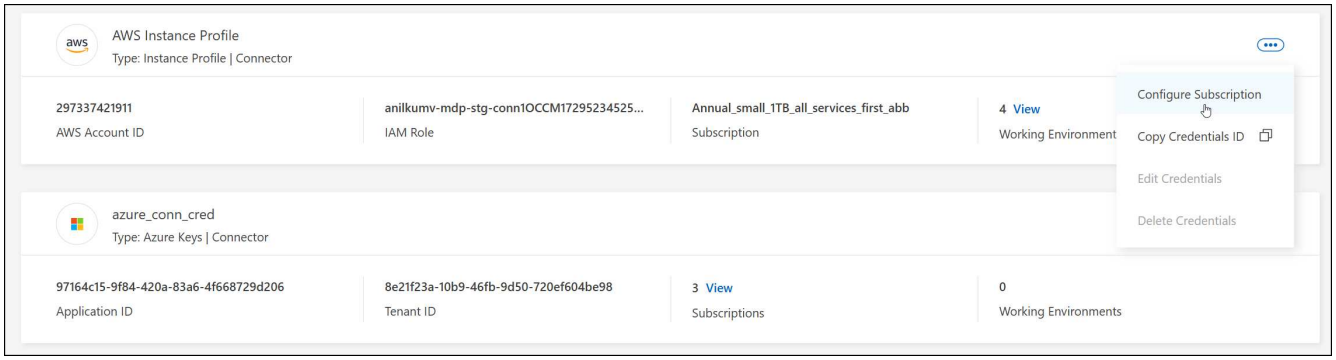
Prima di iniziare

Prima di poter configurare un abbonamento, è necessario creare un agente Console. "Scopri come creare un agente Console" .

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**.

Associa un abbonamento esistente alla tua organizzazione

Quando ti abboni ad AWS Marketplace, l'ultimo passaggio del processo consiste nell'associare l'abbonamento alla tua organizzazione. Se non hai completato questo passaggio, non potrai utilizzare l'abbonamento con la tua organizzazione.

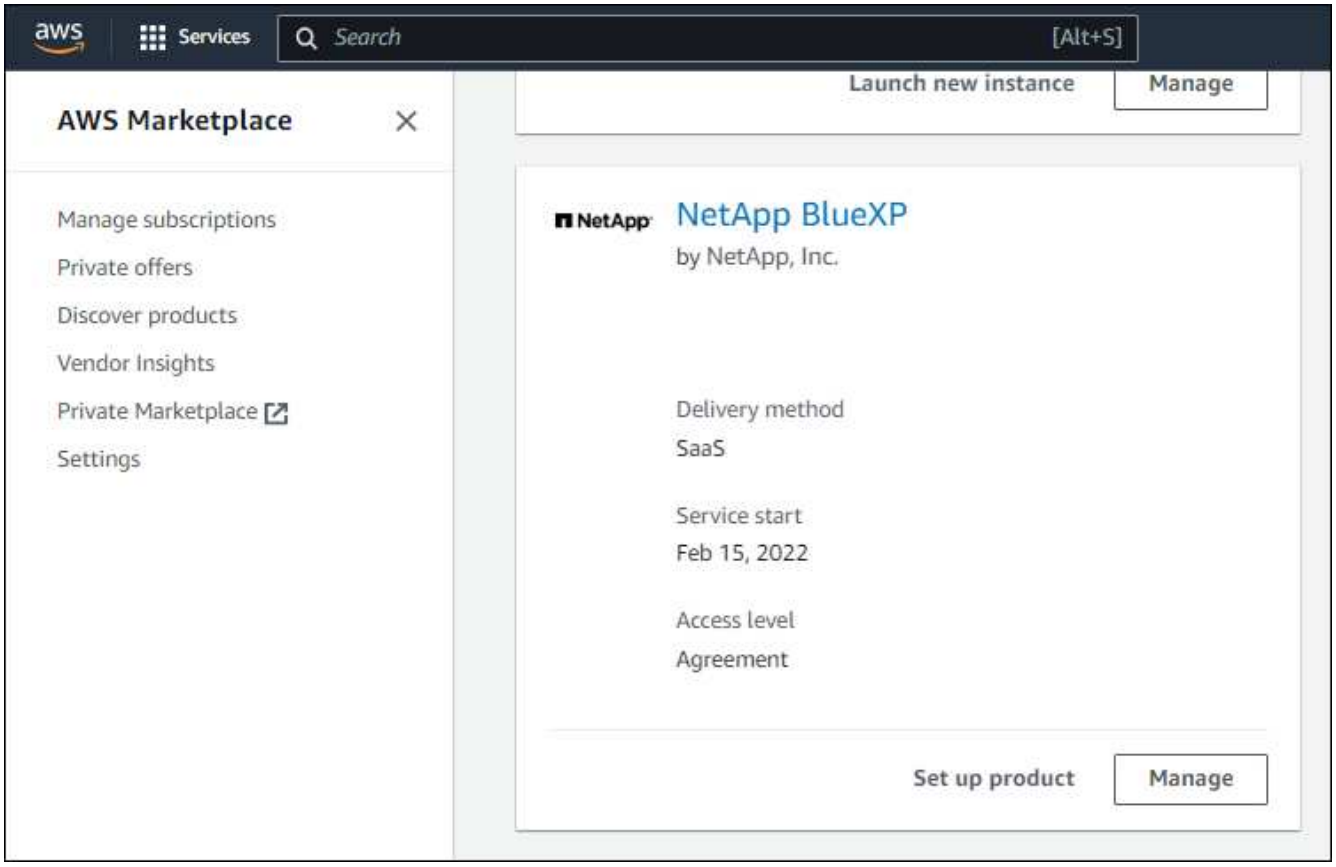
- "Scopri di più sulle modalità di distribuzione della console"
- "Scopri di più sulla gestione dell'identità e dell'accesso alla console"

Segui i passaggi indicati di seguito se hai sottoscritto un abbonamento a NetApp Intelligent Services da AWS Marketplace, ma hai saltato il passaggio per associare l'abbonamento al tuo account.

Passi

1. Verifica di non aver associato il tuo abbonamento all'organizzazione della tua Console.
   a. Dal menu di navigazione, seleziona **Amministrazione > Licenses and subscriptions**.
   b. Seleziona **Abbonamenti**.
   c. Verifica che il tuo abbonamento non venga visualizzato.

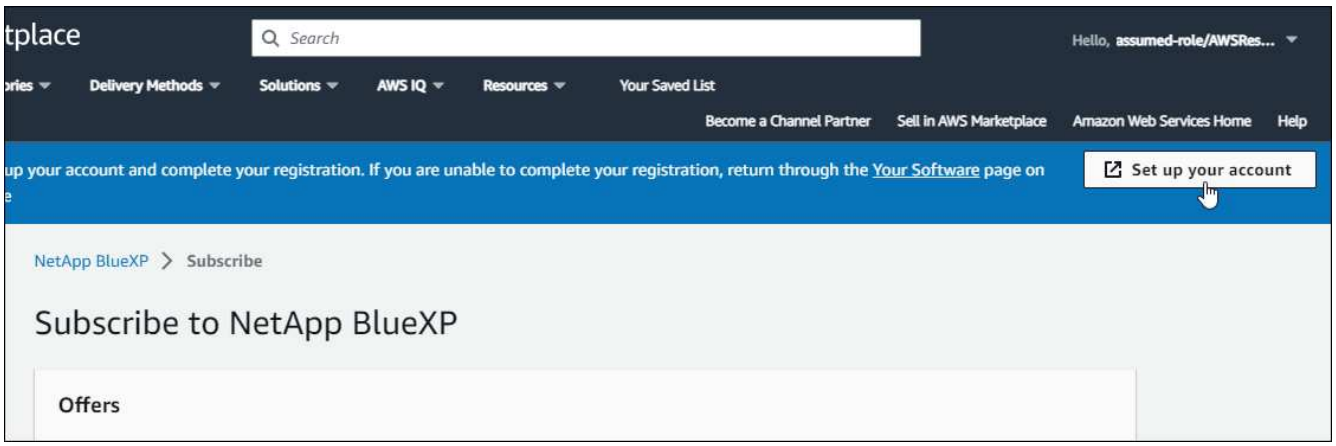
      Vedrai solo gli abbonamenti associati all'organizzazione o all'account che stai visualizzando. Se non vedi il tuo abbonamento, procedi come segue.
2. Accedi alla console AWS e vai su **Abbonamenti AWS Marketplace**.
3. Trova l'abbonamento.



4. Seleziona **Configura prodotto**.

   La pagina dell'offerta di abbonamento dovrebbe caricarsi in una nuova scheda o finestra del browser.

5. Seleziona **Configura il tuo account**.



   La pagina **Assegnazione abbonamento** su netapp.com dovrebbe caricarsi in una nuova scheda o finestra del browser.

   Tieni presente che potrebbe esserti richiesto di accedere prima alla Console.

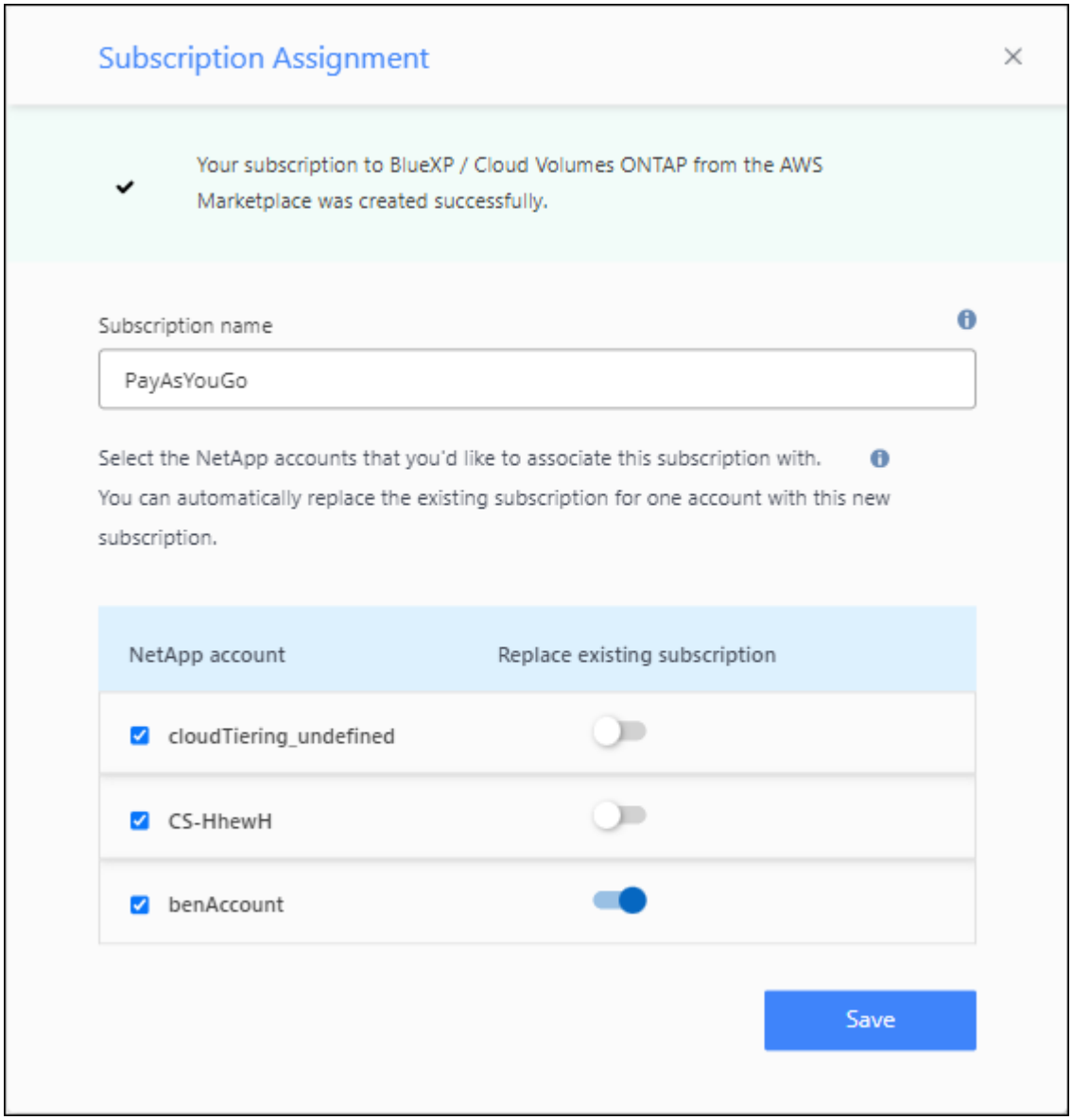
6. Dalla pagina **Assegnazione abbonamento**:

   - 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.

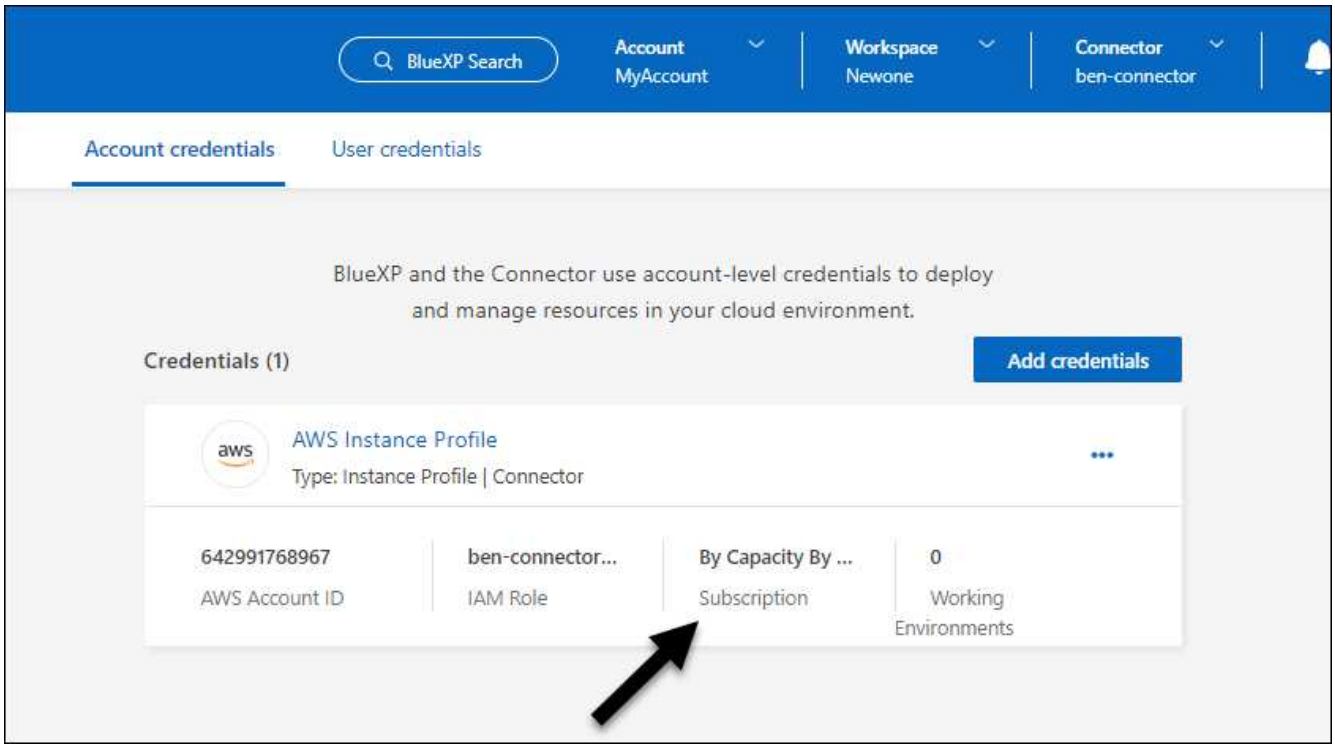
  Per tutte le altre organizzazioni o account, sarà necessario associare manualmente l'abbonamento ripetendo questi passaggi.



7. Verifica che l'abbonamento sia associato alla tua organizzazione.
   a. Dal menu di navigazione, seleziona **Amministrazione > Licenze e abbonamenti**.
   b. Seleziona **Abbonamenti**.
   c. Verifica che il tuo abbonamento venga visualizzato.
8. Verifica che l'abbonamento sia associato alle tue credenziali AWS.
   a. Selezionare **Amministrazione > Credenziali**.

b. Nella pagina **Credenziali dell'organizzazione**, verifica che l'abbonamento sia associato alle tue credenziali AWS.

   Ecco un esempio.



Modifica credenziali

Modifica le tue credenziali AWS cambiando il tipo di account (chiavi AWS o ruolo di assunzione), modificando il nome o aggiornando le credenziali stesse (le chiavi o l'ARN del ruolo).

Non è possibile modificare le credenziali per un profilo di istanza associato a un'istanza dell'agente della console o a un'istanza Amazon FSx for ONTAP . È possibile rinominare le credenziali solo per un'istanza FSx for ONTAP .

Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Nella pagina **Credenziali dell'organizzazione**, seleziona il menu azioni per un set di credenziali, quindi seleziona **Modifica credenziali**.
3. Apporta le modifiche desiderate e seleziona **Applica**.

Elimina le credenziali

Se non hai più bisogno di un set di credenziali, puoi eliminarlo. È possibile eliminare solo le credenziali non associate a un sistema.

Non è possibile eliminare le credenziali per un profilo di istanza associato a un agente Console.

Passi

1. Selezionare **Amministrazione > Credenziali**.

2. Nella pagina **Credenziali dell'organizzazione** o **Credenziali dell'account**, seleziona il menu delle azioni per un set di credenziali, quindi seleziona **Elimina credenziali**.
3. Selezionare **Elimina** per confermare.

Azzurro

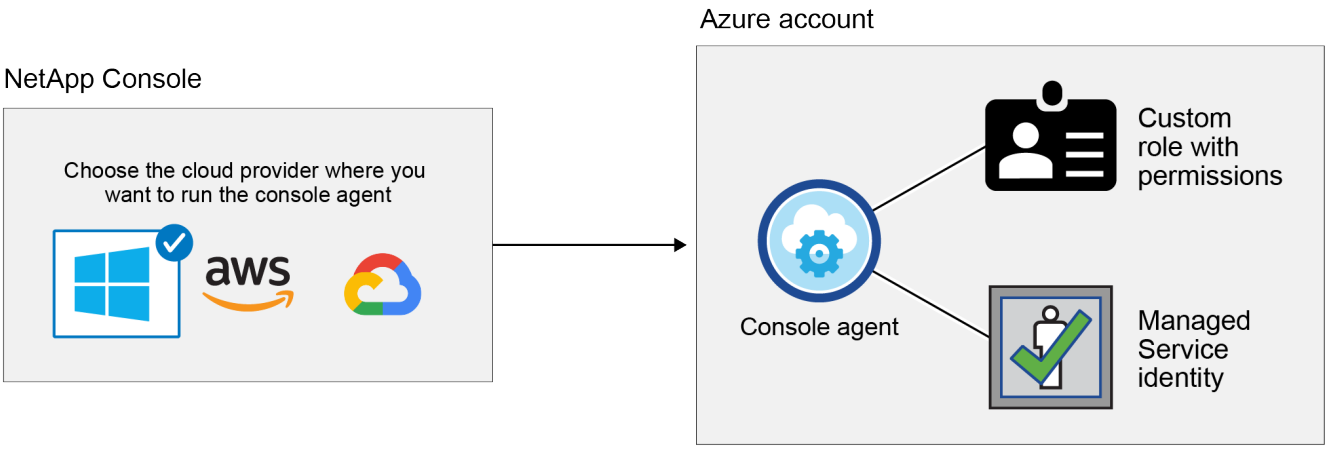
Scopri di più sulle credenziali e le autorizzazioni di Azure nella NetApp Console

Scopri come la NetApp Console utilizza le credenziali di Azure per eseguire azioni per tuo conto e come tali credenziali sono associate agli abbonamenti del marketplace. La comprensione di questi dettagli può essere utile quando si gestiscono le credenziali per una o più sottoscrizioni di Azure. Ad esempio, potresti voler sapere quando aggiungere ulteriori credenziali di Azure alla console.

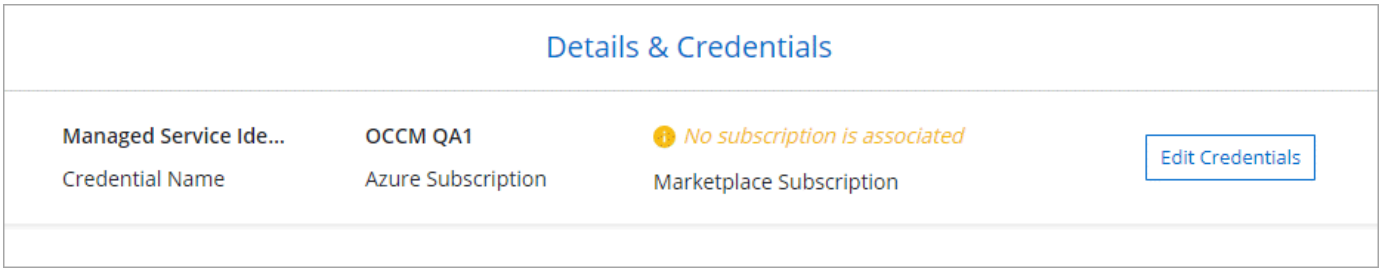
Credenziali iniziali di Azure

Quando si distribuisce un agente Console dalla Console, è necessario utilizzare un account Azure o un'entità servizio che disponga delle autorizzazioni per distribuire la macchina virtuale dell'agente Console. Le autorizzazioni richieste sono elencate nel"Criteri di distribuzione degli agenti per Azure" .

Quando la console distribuisce la macchina virtuale dell'agente console in Azure, abilita un "identità gestita assegnata dal sistema" sulla macchina virtuale, crea un ruolo personalizzato e lo assegna alla macchina virtuale. Il ruolo fornisce alla Console le autorizzazioni necessarie per gestire risorse e processi all'interno di tale sottoscrizione di Azure. "Esaminare come la Console utilizza le autorizzazioni" .



Se si crea un nuovo sistema per Cloud Volumes ONTAP, la console seleziona per impostazione predefinita queste credenziali di Azure:



È possibile distribuire tutti i sistemi Cloud Volumes ONTAP utilizzando le credenziali iniziali di Azure oppure è

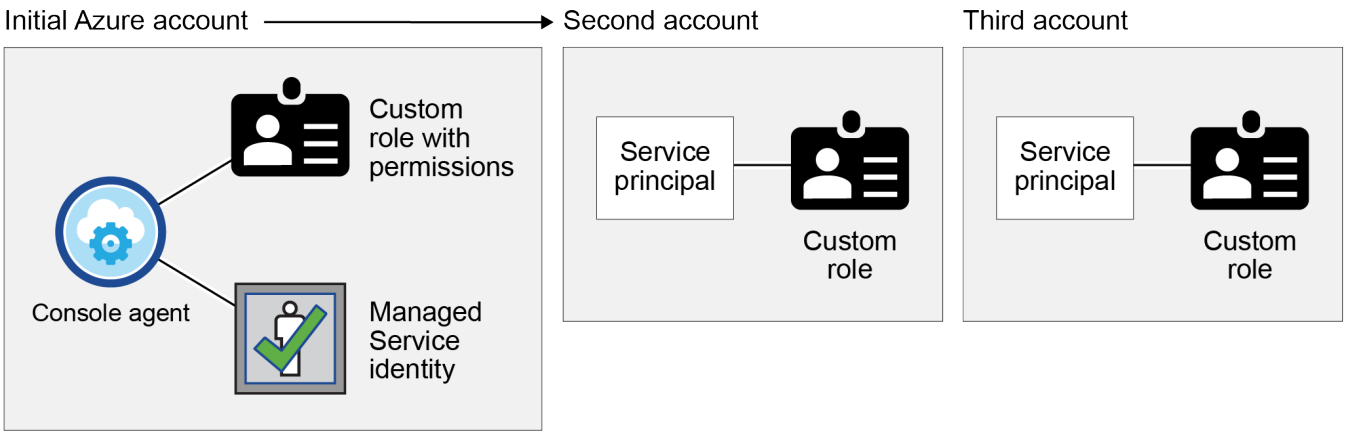
possibile aggiungere credenziali aggiuntive.

Abbonamenti Azure aggiuntivi per un'identità gestita

L'identità gestita assegnata dal sistema alla VM dell'agente Console è associata alla sottoscrizione in cui è stato avviato l'agente Console. Se si desidera selezionare una sottoscrizione Azure diversa, è necessario"associare l'identità gestita a tali abbonamenti" .

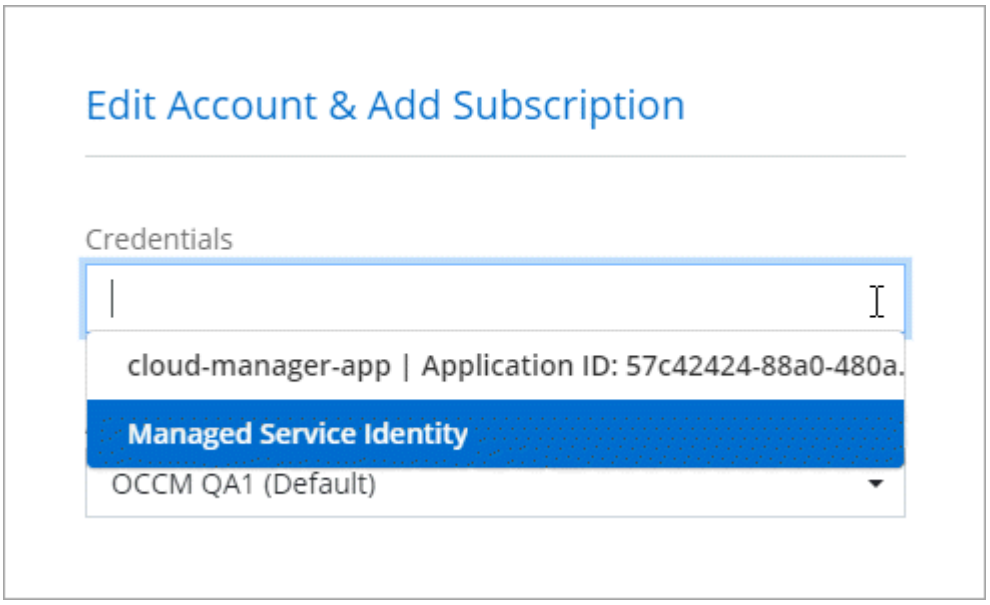
Credenziali Azure aggiuntive

Se si desidera utilizzare credenziali di Azure diverse con la console, è necessario concedere le autorizzazioni richieste tramite"creazione e configurazione di un'entità servizio in Microsoft Entra ID" per ogni account Azure. L'immagine seguente mostra due account aggiuntivi, ciascuno configurato con un'entità servizio e un ruolo personalizzato che fornisce autorizzazioni:



Allora lo faresti"aggiungere le credenziali dell'account alla Console" fornendo dettagli sul principale del servizio AD.

Ad esempio, è possibile passare da una credenziale all'altra quando si crea un nuovo sistema Cloud Volumes ONTAP :



Credenziali e abbonamenti al marketplace

Le credenziali aggiunte a un agente della console devono essere associate a una sottoscrizione di Azure Marketplace, in modo da poter pagare Cloud Volumes ONTAP a una tariffa oraria (PAYGO) o tramite servizi dati NetApp o tramite un contratto annuale.

"Scopri come associare una sottoscrizione Azure" .

Tieni presente quanto segue in merito alle credenziali di Azure e agli abbonamenti al Marketplace:

- È possibile associare una sola sottoscrizione di Azure Marketplace a un set di credenziali di Azure
- Puoi sostituire un abbonamento esistente al marketplace con un nuovo abbonamento

Domande frequenti

La seguente domanda riguarda le credenziali e gli abbonamenti.

Posso modificare l'abbonamento ad Azure Marketplace per i sistemi Cloud Volumes ONTAP ?

Sì, puoi. Quando si modifica l'abbonamento ad Azure Marketplace associato a un set di credenziali di Azure, tutti i sistemi Cloud Volumes ONTAP esistenti e nuovi verranno addebitati sul nuovo abbonamento.

"Scopri come associare una sottoscrizione Azure" .

Posso aggiungere più credenziali di Azure, ciascuna con diversi abbonamenti al marketplace?

Tutte le credenziali di Azure che appartengono allo stesso abbonamento di Azure saranno associate allo stesso abbonamento di Azure Marketplace.

Se si dispone di più credenziali di Azure appartenenti a diverse sottoscrizioni di Azure, tali credenziali possono essere associate alla stessa sottoscrizione di Azure Marketplace o a diverse sottoscrizioni di Marketplace.

Posso spostare i sistemi Cloud Volumes ONTAP esistenti in un abbonamento Azure diverso?

No, non è possibile spostare le risorse di Azure associate al sistema Cloud Volumes ONTAP in una sottoscrizione di Azure diversa.

Come funzionano le credenziali per le distribuzioni sul marketplace e le distribuzioni on-premise?

Le sezioni precedenti descrivono il metodo di distribuzione consigliato per l'agente Console, ovvero dalla Console. È anche possibile distribuire un agente console in Azure da Azure Marketplace e installare il software dell'agente console sul proprio host Linux.

Se si utilizza Marketplace, è possibile fornire autorizzazioni assegnando un ruolo personalizzato alla macchina virtuale dell'agente della console e a un'identità gestita assegnata dal sistema, oppure è possibile utilizzare un'entità servizio Microsoft Entra.

Per le distribuzioni on-premise, non è possibile impostare un'identità gestita per l'agente della console, ma è possibile fornire autorizzazioni utilizzando un'entità servizio.

Per informazioni su come impostare le autorizzazioni, fare riferimento alle seguenti pagine:

- Modalità standard
  - "Impostare le autorizzazioni per una distribuzione di Azure Marketplace"

- "Impostare le autorizzazioni per le distribuzioni in locale"

- Modalità limitata
  - "Imposta le autorizzazioni per la modalità limitata"

Gestisci le credenziali di Azure e gli abbonamenti al marketplace per NetApp Console

Aggiungi e gestisci le credenziali di Azure in modo che la NetApp Console disponga delle autorizzazioni necessarie per distribuire e gestire le risorse cloud nelle tue sottoscrizioni di Azure. Se gestisci più abbonamenti ad Azure Marketplace, puoi assegnare a ciascuno di essi credenziali Azure diverse dalla pagina Credenziali.

Panoramica

Esistono due modi per aggiungere ulteriori sottoscrizioni e credenziali di Azure nella Console.

1. Associare ulteriori sottoscrizioni di Azure all'identità gestita di Azure.
2. Per distribuire Cloud Volumes ONTAP utilizzando credenziali di Azure diverse, concedi le autorizzazioni di Azure utilizzando un'entità servizio e aggiungi le relative credenziali alla console.

Associare ulteriori sottoscrizioni di Azure a un'identità gestita

La console consente di scegliere le credenziali di Azure e la sottoscrizione di Azure in cui si desidera distribuire Cloud Volumes ONTAP. Non è possibile selezionare una sottoscrizione di Azure diversa per il profilo di identità gestita a meno che non si associ "identità gestita" con quegli abbonamenti.

Informazioni su questo compito

Un'identità gestita è"l'account Azure iniziale" quando si distribuisce un agente Console dalla Console. Quando si distribuisce l'agente Console, la Console assegna il ruolo di Operatore Console alla macchina virtuale dell'agente Console.

Passi

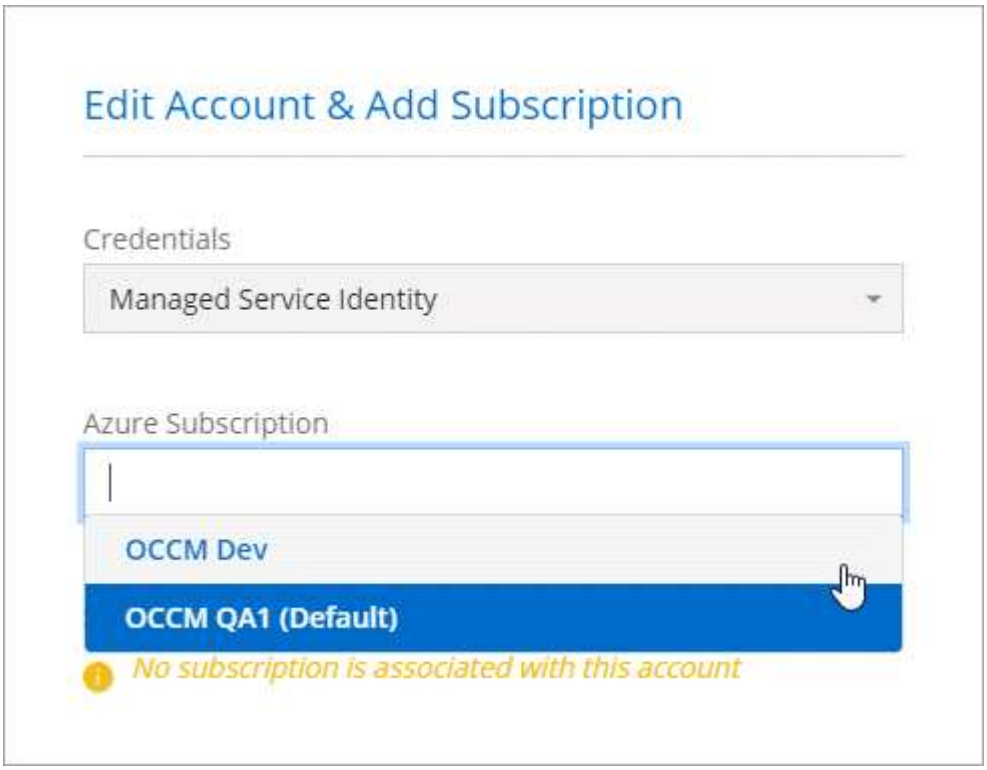
1. Accedi al portale di Azure.
2. Aprire il servizio **Abbonamenti** e quindi selezionare l'abbonamento in cui si desidera distribuire Cloud Volumes ONTAP.
3. Selezionare **Controllo accessi (IAM)**.
   a. Selezionare **Aggiungi** > **Aggiungi assegnazione ruolo** e quindi aggiungere le autorizzazioni:
      - Selezionare il ruolo **Operatore console**.

        Console Operator è il nome predefinito fornito in un criterio dell'agente Console. Se hai scelto un nome diverso per il ruolo, seleziona quel nome.

      - Assegna l'accesso a una **Macchina Virtuale**.
      - Selezionare la sottoscrizione in cui è stata creata una macchina virtuale dell'agente Console.
      - Selezionare una macchina virtuale agente Console.
      - Seleziona **Salva**.
4. Ripetere questi passaggi per ulteriori abbonamenti.

Risultato

Quando si crea un nuovo sistema, ora è possibile selezionare tra più sottoscrizioni Azure per il profilo di identità gestita.



Aggiungi ulteriori credenziali di Azure alla NetApp Console

Quando si distribuisce un agente Console dalla Console, la Console abilita un'identità gestita assegnata dal sistema sulla macchina virtuale che dispone delle autorizzazioni richieste. La console seleziona queste credenziali di Azure per impostazione predefinita quando si crea un nuovo sistema per Cloud Volumes ONTAP.

Se si installa manualmente un software agente Console su un sistema esistente, non viene aggiunto un set iniziale di credenziali. "Scopri di più sulle credenziali e le autorizzazioni di Azure" .

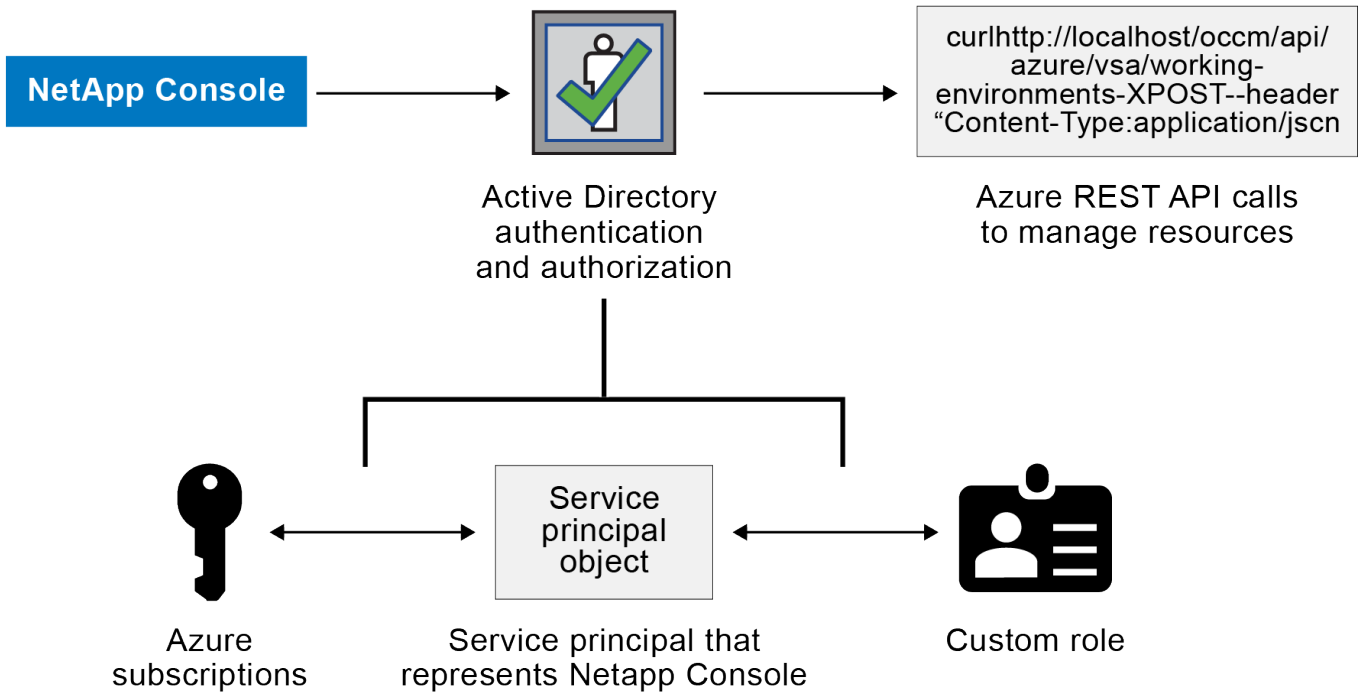
Se si desidera distribuire Cloud Volumes ONTAP utilizzando credenziali Azure *diverse*, è necessario concedere le autorizzazioni richieste creando e configurando un'entità servizio in Microsoft Entra ID per ciascun account Azure. È quindi possibile aggiungere le nuove credenziali alla Console.

Concedi le autorizzazioni di Azure utilizzando un'entità servizio

La console necessita delle autorizzazioni per eseguire azioni in Azure. È possibile concedere le autorizzazioni necessarie a un account Azure creando e configurando un'entità servizio in Microsoft Entra ID e ottenendo le credenziali di Azure necessarie alla console.

Informazioni su questo compito

L'immagine seguente illustra come la console ottiene le autorizzazioni per eseguire operazioni in Azure. Un oggetto entità servizio, associato a una o più sottoscrizioni di Azure, rappresenta la console nell'ID Microsoft Entra e viene assegnato a un ruolo personalizzato che consente le autorizzazioni richieste.



Passi

1. Creare un’applicazione Microsoft Entra .
2. Assegnare l’applicazione a un ruolo .
3. Aggiungere autorizzazioni API di gestione dei servizi Windows Azure .
4. Ottieni l’ID dell’applicazione e l’ID della directory .
5. Crea un segreto client .

Creare un’applicazione Microsoft Entra

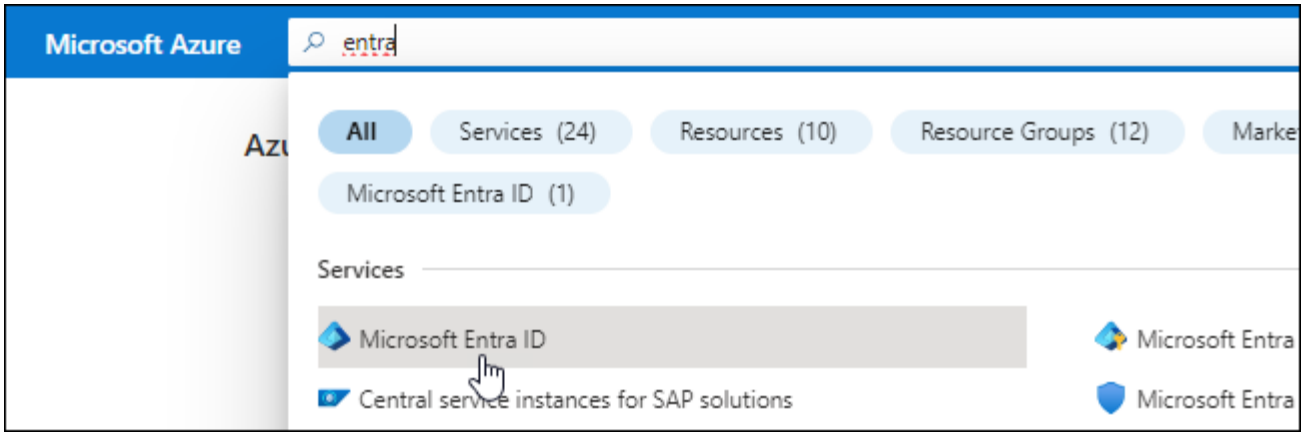
Creare un’applicazione Microsoft Entra e un’entità servizio che la console può utilizzare per il controllo degli accessi basato sui ruoli.

Passi

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

È necessario associare l'entità servizio a una o più sottoscrizioni di Azure e assegnarle il ruolo personalizzato "Operatore console" in modo che la console disponga delle autorizzazioni in Azure.

Passi

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 .

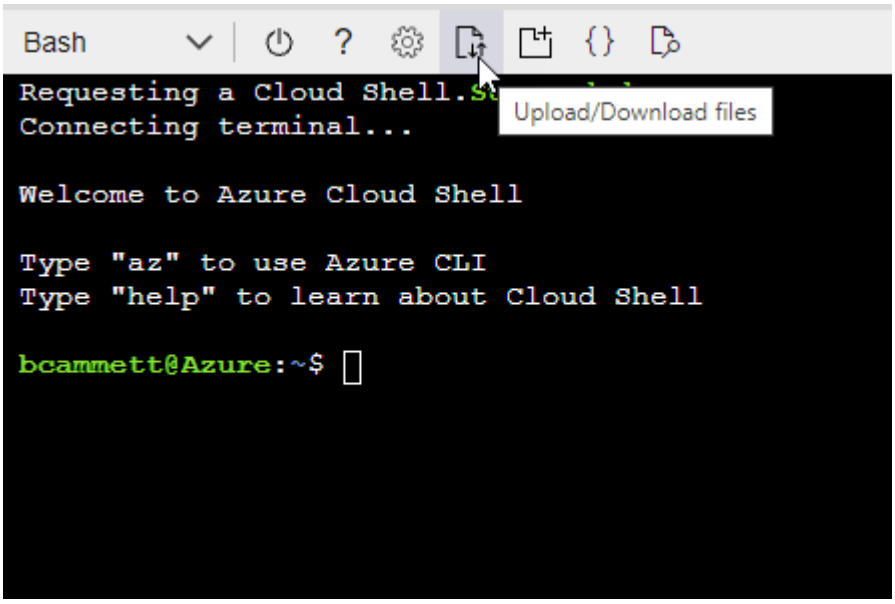
      Esempio

```
"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
```

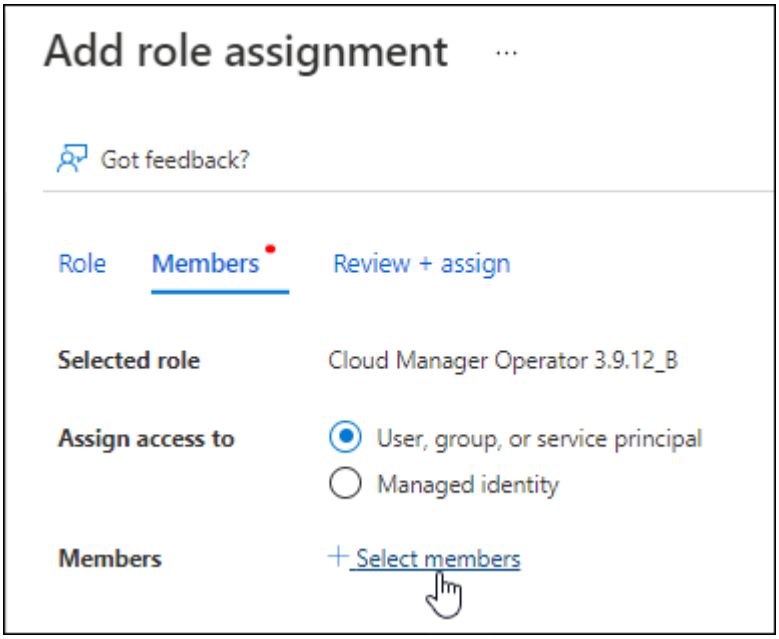
Ora dovresti avere un ruolo personalizzato denominato Operatore Console che puoi assegnare alla macchina virtuale dell'agente Console.

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:

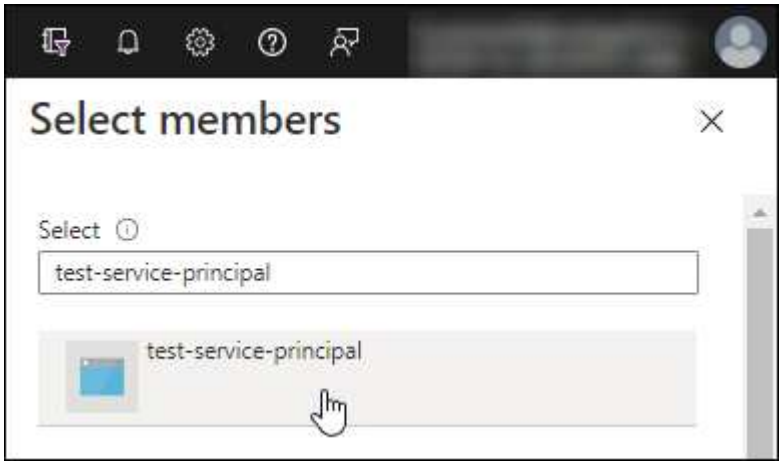
- Mantieni selezionato **Utente, gruppo o entità servizio**.

- 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.

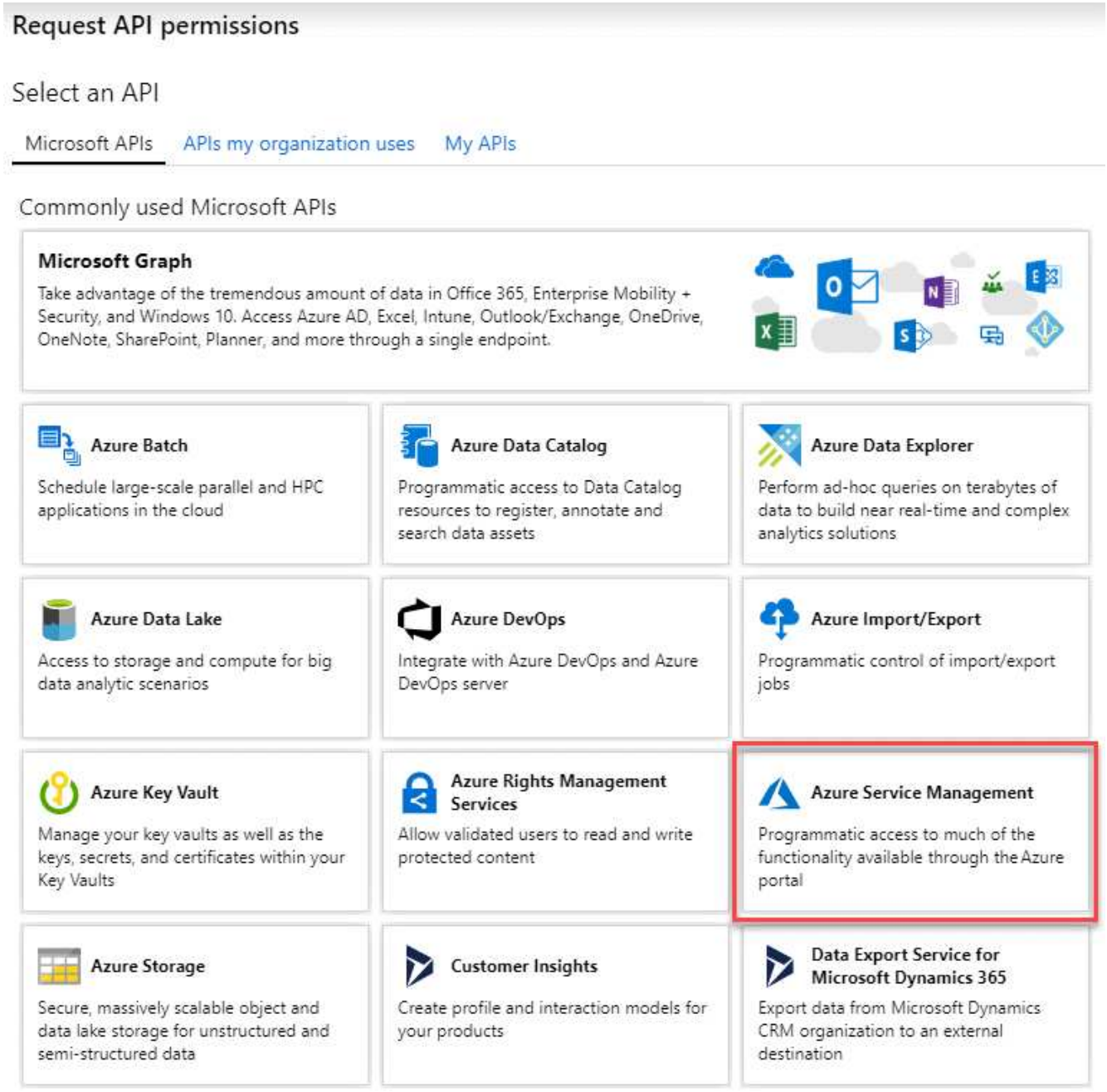
Se si desidera distribuire Cloud Volumes ONTAP da più sottoscrizioni di Azure, è necessario associare l'entità servizio a ciascuna di tali sottoscrizioni. Nella NetApp Console, puoi selezionare l'abbonamento che desideri utilizzare durante la distribuzione Cloud Volumes ONTAP.

Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

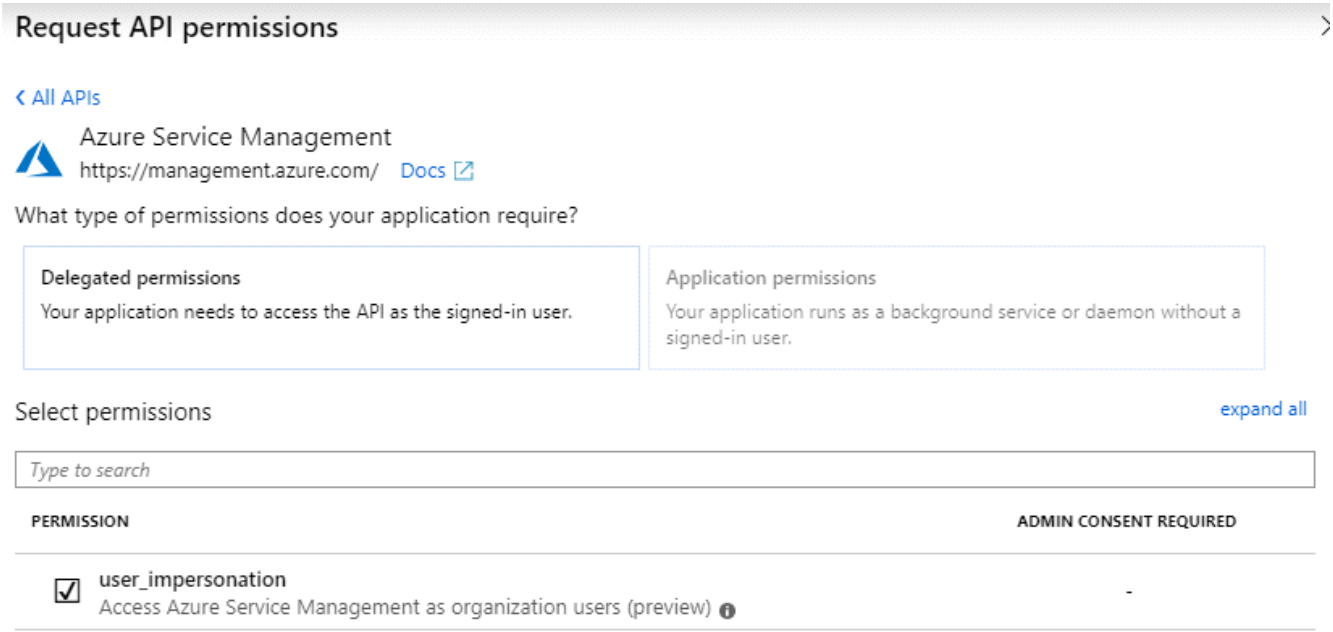
È necessario assegnare le autorizzazioni "Windows Azure Service Management API" all'entità servizio.

Passi

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**.

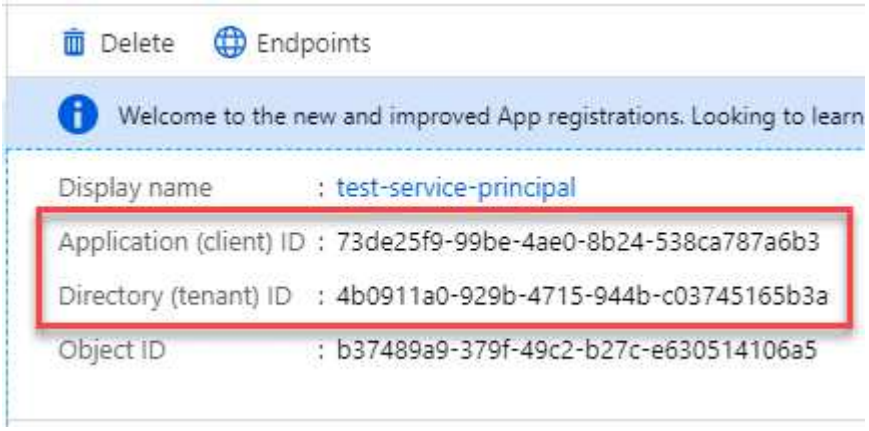


Ottieni l'ID dell'applicazione e l'ID della directory

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.

Passi

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

Creare un segreto client e fornirne il valore alla Console per l'autenticazione con l'ID Microsoft Entra.

Passi

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.

Aggiungere le credenziali alla Console

Dopo aver fornito a un account Azure le autorizzazioni necessarie, è possibile aggiungere le credenziali per tale account alla Console. Completando questo passaggio sarà possibile avviare Cloud Volumes ONTAP utilizzando credenziali Azure diverse.

Prima di iniziare

Se hai appena creato queste credenziali nel tuo provider cloud, potrebbero volerci alcuni minuti prima che siano disponibili per l'uso. Attendi qualche minuto prima di aggiungere le credenziali alla Console.

Prima di iniziare

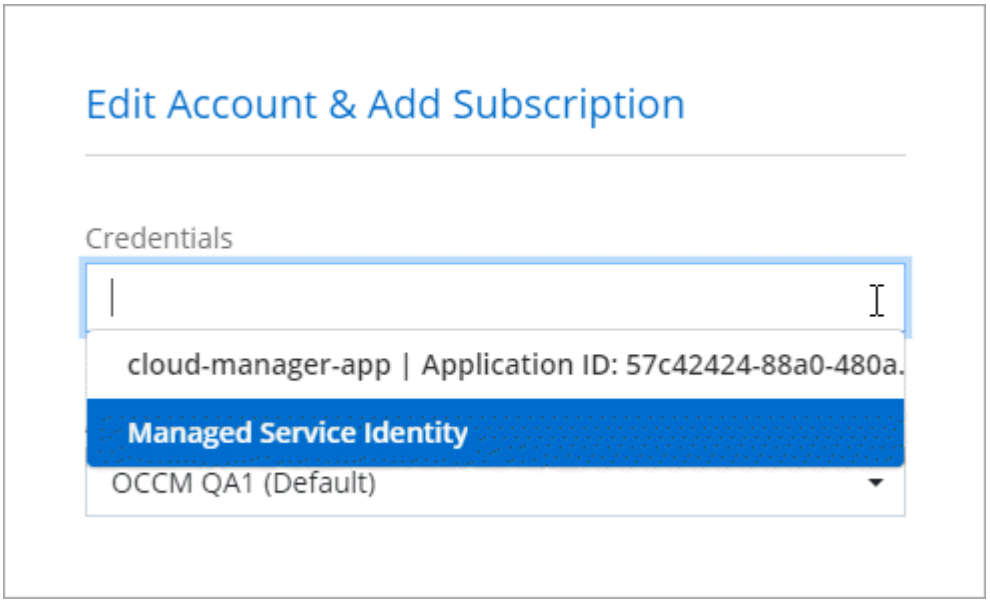
Prima di poter modificare le impostazioni della console, è necessario creare un agente della console. "Scopri come creare un agente Console" .

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

Puoi passare a un set di credenziali diverso dalla pagina Dettagli e credenziali "quando si aggiunge un sistema alla Console"



Gestisci le credenziali esistenti

Gestisci le credenziali di Azure che hai già aggiunto alla Console associando una sottoscrizione al Marketplace, modificando le credenziali ed eliminandole.

Associare una sottoscrizione di Azure Marketplace alle credenziali

Dopo aver aggiunto le credenziali di Azure alla console, è possibile associare a tali credenziali un abbonamento ad Azure Marketplace. È possibile utilizzare l'abbonamento per creare un sistema Cloud Volumes ONTAP con pagamento in base al consumo e accedere ai servizi dati NetApp .

Esistono due scenari in cui potresti associare una sottoscrizione ad Azure Marketplace dopo aver già aggiunto le credenziali alla Console:

- Non hai associato un abbonamento quando hai aggiunto inizialmente le credenziali alla Console.
- Si desidera modificare la sottoscrizione di Azure Marketplace associata alle credenziali di Azure.

  La sostituzione dell'attuale abbonamento al marketplace lo aggiorna per i sistemi Cloud Volumes ONTAP esistenti e nuovi.

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**.

Modifica credenziali

Modifica le tue credenziali di Azure nella Console. Ad esempio, è possibile aggiornare il segreto client se è stato creato un nuovo segreto per l'applicazione del servizio principale.

Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Selezionare **Credenziali dell'organizzazione**.
3. Selezionare il menu azioni per un set di credenziali, quindi selezionare **Modifica credenziali**.
4. Apporta le modifiche desiderate e seleziona **Applica**.

Elimina le credenziali

Se non hai più bisogno di un set di credenziali, puoi eliminarlo. È possibile eliminare solo le credenziali non associate a un sistema.

Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Selezionare **Credenziali dell'organizzazione**.
3. Nella pagina **Credenziali dell'organizzazione**, seleziona il menu azioni per un set di credenziali, quindi seleziona **Elimina credenziali**.
4. Selezionare **Elimina** per confermare.

Google Cloud

Scopri di più sui progetti e sulle autorizzazioni di Google Cloud

Scopri come la NetApp Console utilizza le credenziali di Google Cloud per eseguire azioni per tuo conto e come tali credenziali sono associate agli abbonamenti al marketplace. Comprendere questi dettagli può essere utile quando si gestiscono le credenziali per uno o più progetti Google Cloud. Ad esempio, potresti voler ottenere informazioni sull'account di servizio associato alla VM dell'agente Console.

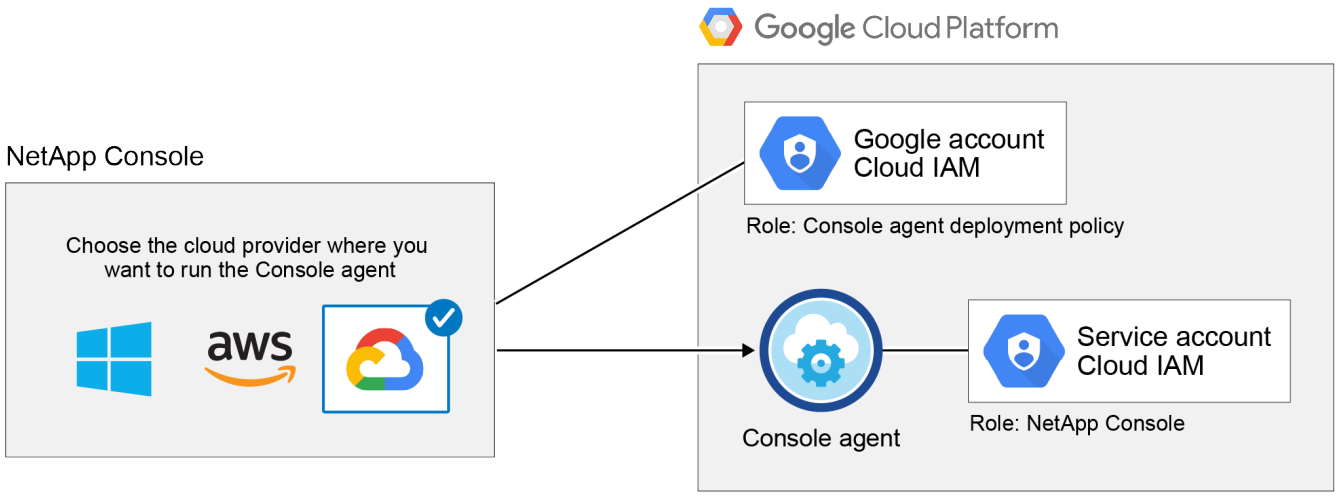
Progetto e autorizzazioni per NetApp Console

Prima di poter utilizzare la Console per gestire le risorse nel tuo progetto Google Cloud, devi prima distribuire un agente Console. L'agente non può essere in esecuzione presso la tua sede o presso un altro provider cloud.

Prima di distribuire un agente Console direttamente dalla Console, è necessario disporre di due set di autorizzazioni:

1. È necessario distribuire un agente Console utilizzando un account Google che disponga delle autorizzazioni per avviare l'agente Console dalla Console.
2. Quando si distribuisce l'agente Console, viene richiesto di selezionare un "account di servizio" per l'agente La console ottiene le autorizzazioni dall'account di servizio per creare e gestire i sistemi Cloud Volumes ONTAP , per gestire i backup utilizzando il backup e il ripristino NetApp e altro ancora. Le autorizzazioni vengono fornite associando un ruolo personalizzato all'account di servizio.

L'immagine seguente illustra i requisiti di autorizzazione descritti nei numeri 1 e 2 sopra:



Per informazioni su come impostare le autorizzazioni, fare riferimento alle seguenti pagine:

- "Imposta le autorizzazioni di Google Cloud per la modalità standard"
- "Imposta le autorizzazioni per la modalità limitata"

Credenziali e abbonamenti al marketplace

Quando distribuisci un agente Console in Google Cloud, la Console crea un set predefinito di credenziali per l'account del servizio Google Cloud nel progetto in cui risiede l'agente Console. Per poter pagare i servizi dati

Cloud Volumes ONTAP e NetApp , queste credenziali devono essere associate a un abbonamento a Google Cloud Marketplace.

"Scopri come associare un abbonamento a Google Cloud Marketplace" .

Tieni presente quanto segue in merito alle credenziali di Google Cloud e agli abbonamenti al marketplace:

- È possibile associare un solo set di credenziali Google Cloud a un agente Console
- È possibile associare solo un abbonamento a Google Cloud Marketplace alle credenziali
- Puoi sostituire un abbonamento esistente al marketplace con un nuovo abbonamento

Progetto per Cloud Volumes ONTAP

Cloud Volumes ONTAP può risiedere nello stesso progetto dell'agente Console oppure in un progetto diverso. Per distribuire Cloud Volumes ONTAP in un progetto diverso, è necessario prima aggiungere l'account del servizio agente Console e il ruolo a quel progetto.

- "Scopri come configurare l'account di servizio"
- "Scopri come distribuire Cloud Volumes ONTAP in Google Cloud e selezionare un progetto"

Gestisci le credenziali e gli abbonamenti di Google Cloud per NetApp Console

È possibile gestire le credenziali di Google Cloud associate a una istanza di macchine virtuali Console agent associando un abbonamento al marketplace e risolvendo i problemi del processo di abbonamento. Entrambe queste attività garantiscono che sia possibile utilizzare l'abbonamento al marketplace per pagare i servizi dati.

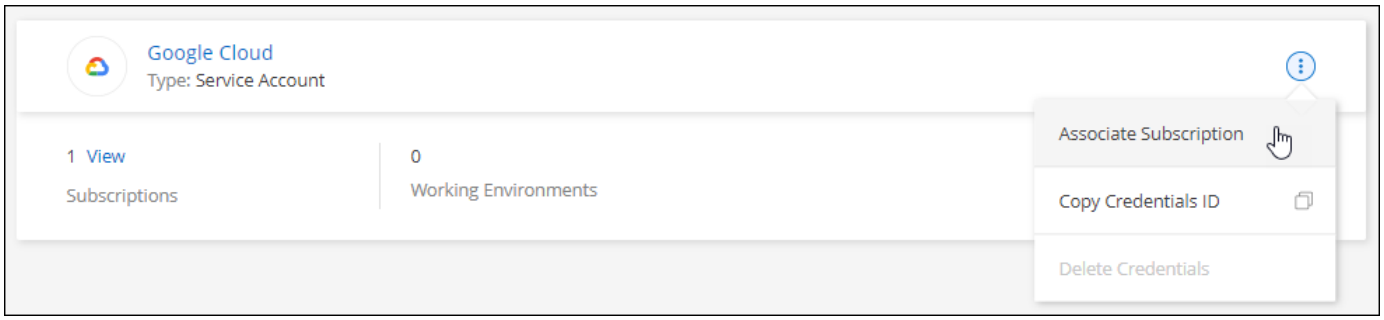
Associa un abbonamento Marketplace alle credenziali di Google Cloud

Quando si distribuisce un agente Console in Google Cloud, la Console crea un set predefinito di credenziali associate a una istanza di macchine virtuali agente Console. In qualsiasi momento, è possibile modificare l'abbonamento a Google Cloud Marketplace associato a queste credenziali. L'abbonamento consente di creare un sistema Cloud Volumes ONTAP pay-as-you-go e di utilizzare altri servizi dati.

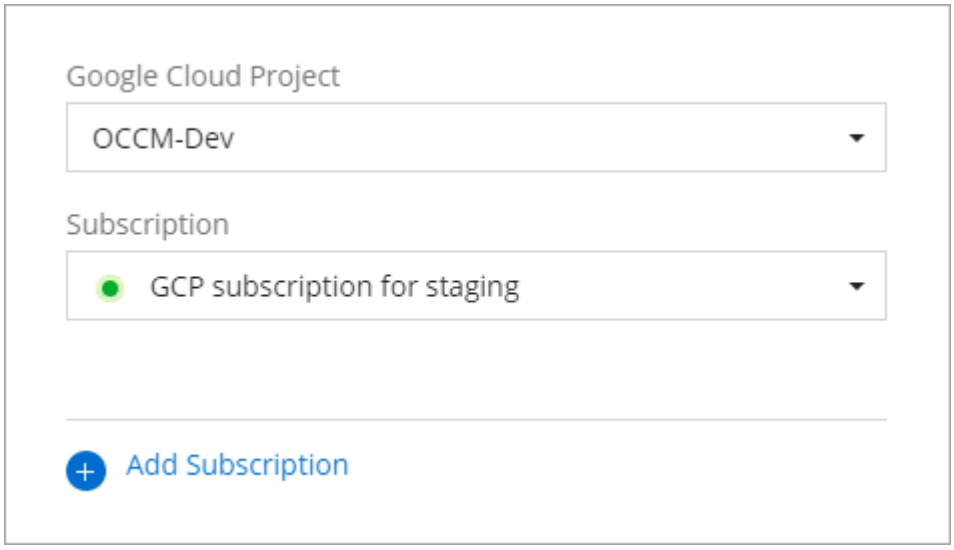
La sostituzione dell'attuale abbonamento al marketplace con un nuovo abbonamento modifica l'abbonamento al marketplace per tutti i sistemi Cloud Volumes ONTAP esistenti e per tutti i nuovi sistemi.

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**.



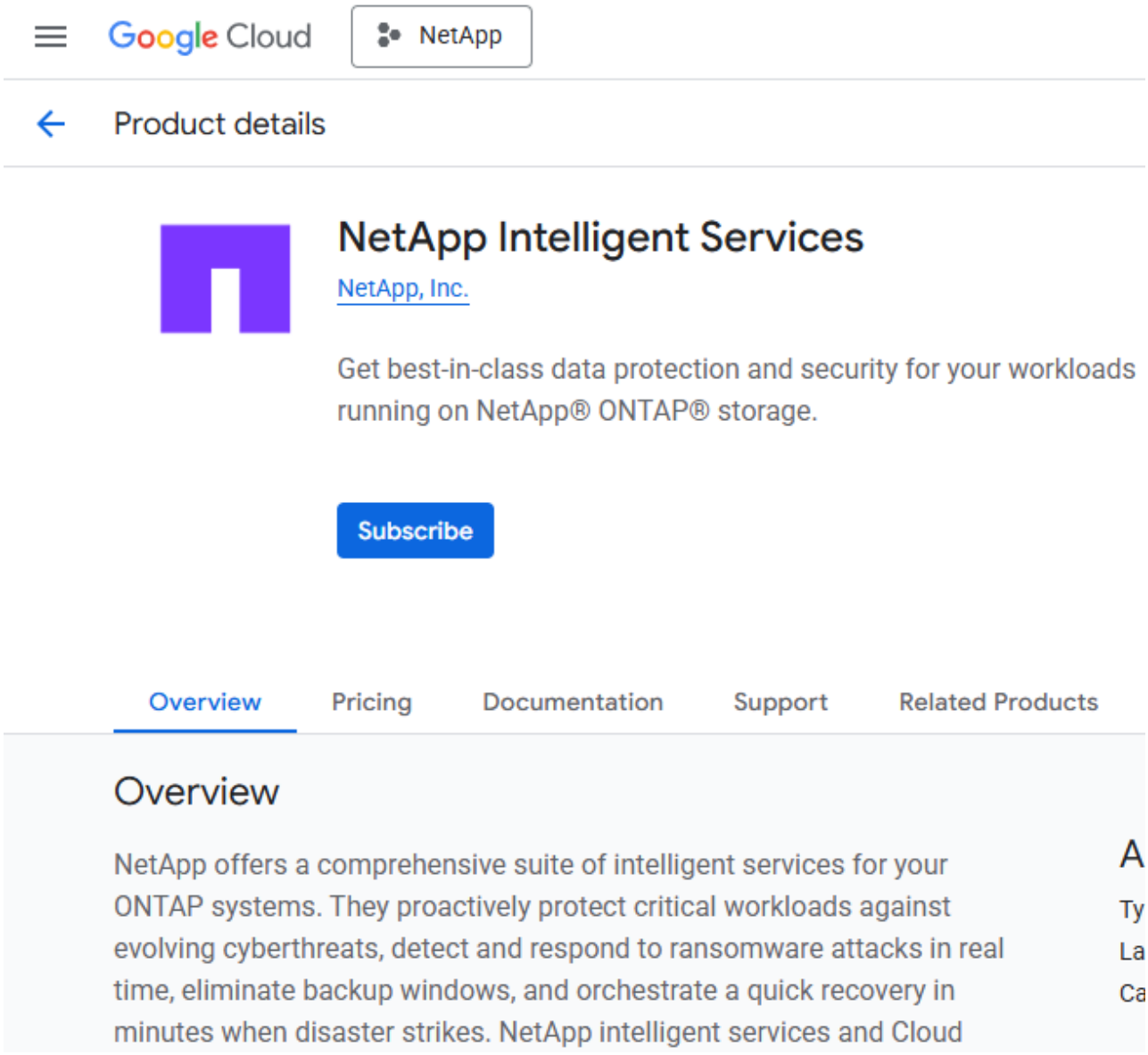
1. Per configurare un abbonamento esistente con le credenziali selezionate, seleziona un progetto Google Cloud e un abbonamento dall'elenco a discesa, quindi seleziona **Configura**.



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.

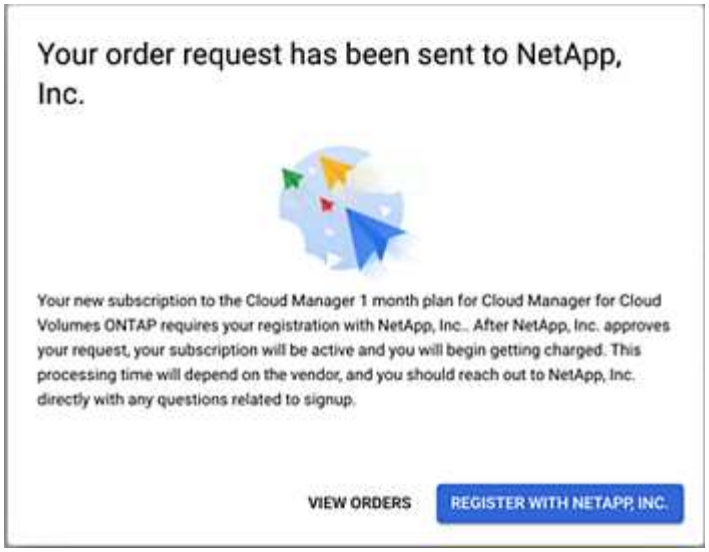


b. Seleziona **Iscriviti**.
c. Seleziona l'account di fatturazione appropriato e accetta i termini e le condizioni.
d. Seleziona **Iscriviti**.

   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.

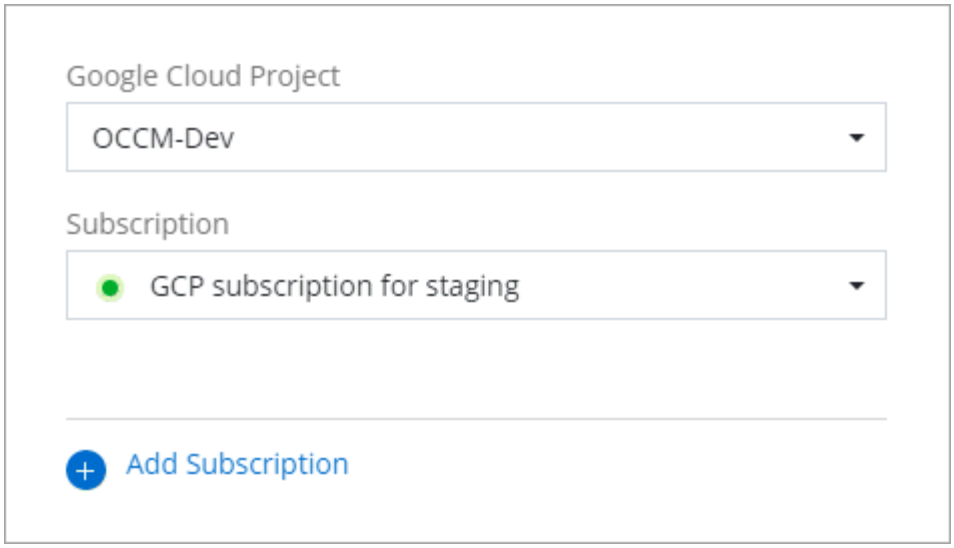
- Seleziona l'organizzazione della Console a cui desideri associare questo abbonamento.
- Nel campo **Sostituisci abbonamento esistente**, scegli se desideri sostituire automaticamente l'abbonamento esistente per un'organizzazione con questo nuovo abbonamento.

  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.

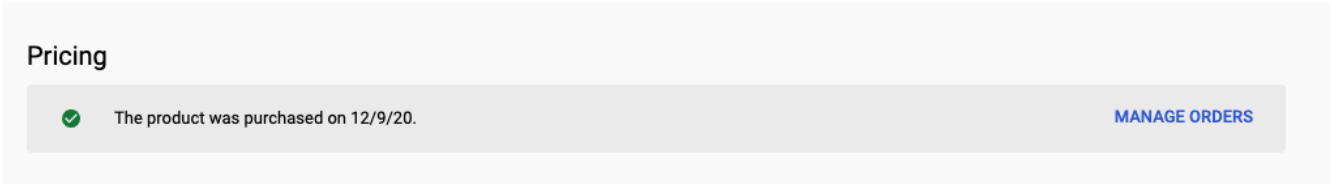


Risolvi i problemi del processo di abbonamento al Marketplace

A volte, l'abbonamento ai servizi dati NetApp tramite Google Cloud Marketplace può risultare frammentato a causa di autorizzazioni errate o del mancato rispetto accidentale del reindirizzamento alla Console. Se ciò accade, utilizzare i seguenti passaggi per completare il processo di abbonamento.

Passi

1. Vai su "Pagina NetApp su Google Cloud Marketplace" per verificare lo stato dell'ordine. Se la pagina riporta la dicitura **Gestisci sul fornitore**, scorri verso il basso e seleziona **Gestisci ordini**.



   - Se l'ordine mostra un segno di spunta verde e ciò è inaspettato, è possibile che qualcun altro nell'organizzazione che utilizza lo stesso account di fatturazione sia già abbonato. Se ciò è inaspettato o hai bisogno dei dettagli di questo abbonamento, contatta il tuo team di vendita NetApp.

   - Se l'ordine mostra un orologio e lo stato **Pending**, torna alla pagina del marketplace e seleziona **Manage on Provider** per completare il processo come documentato sopra.

Gestione dell’identità e degli accessi

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

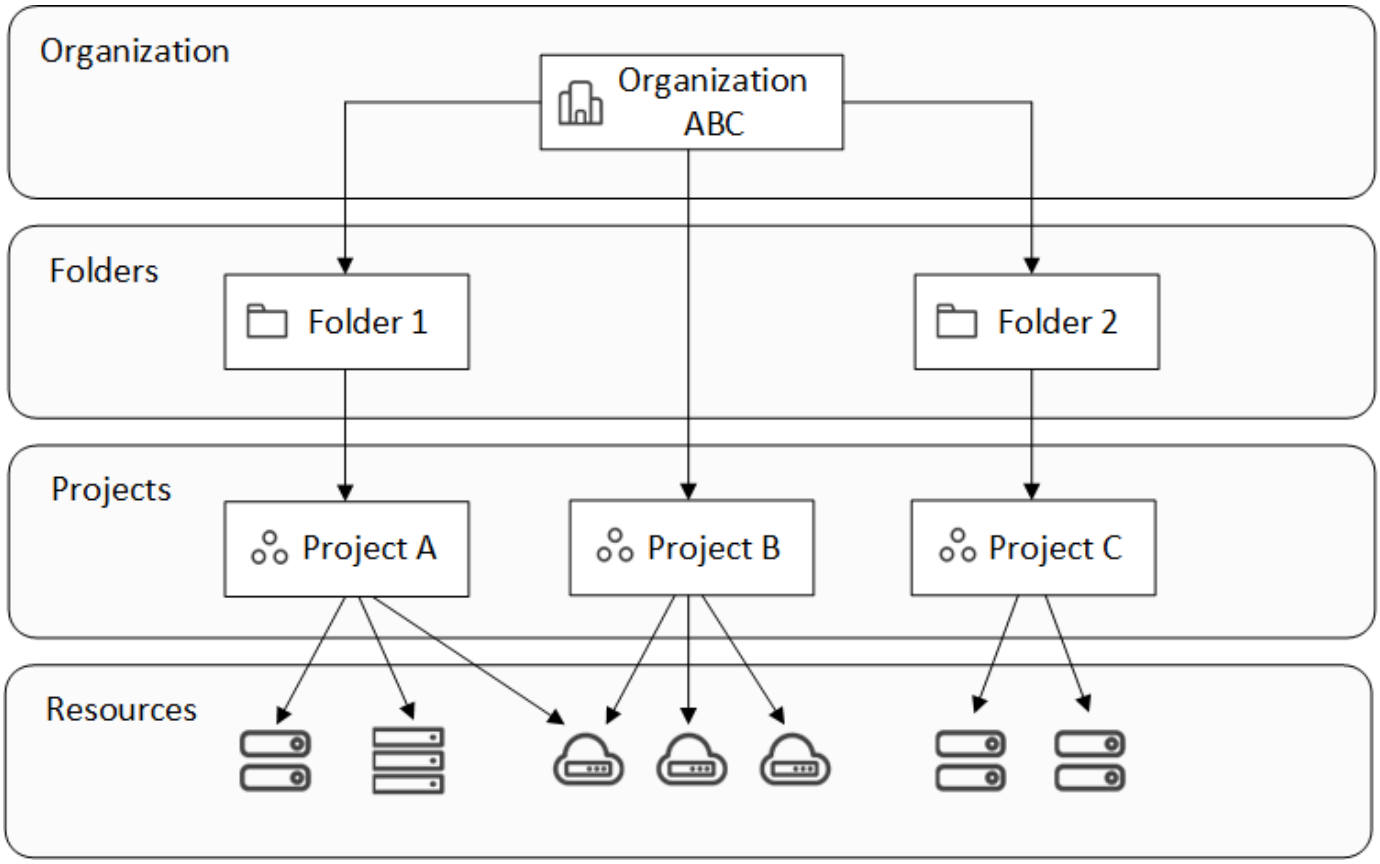
Utilizza la gestione delle identità e degli accessi (IAM) di NetApp Console per organizzare le tue risorse NetApp e controllare l’accesso in base alla struttura aziendale, in base a sede, reparto o progetto.

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

Assegna ruoli di accesso a livello di organizzazione, cartella o progetto in modo che gli utenti abbiano il giusto accesso alle risorse.

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

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



]

Componenti di gestione dell’identità e dell’accesso

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

Progetti e cartelle all'interno della tua organizzazione

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

Organizzazione

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

Progetti

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

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

"Scopri come aggiungere progetti alla tua organizzazione."

Cartelle

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

"Scopri come aggiungere cartelle alla tua organizzazione."

Risorse

Una *risorsa* è un'entità di cui la Console è a conoscenza e che può essere assegnata a un progetto. Le *risorse* includono sistemi storage, abbonamenti Keystone, alcuni carichi di lavoro di NetApp Backup and Recovery, nonché agenti della Console.

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

+

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

+

"Scopri come associare le risorse ai progetti."

Sistemi di archiviazione e abbonamenti Keystone

I sistemi storage sono le risorse principali che gestisci in NetApp Console. NetApp Console supporta la gestione sia dei sistemi storage on-premises che di cloud storage. Devi aggiungere un sistema storage a un progetto affinché possa essere accessibile a coloro che sono assegnati al progetto.

Sistemi storage

I sistemi storage vengono automaticamente associati al progetto in cui vengono aggiunti, ma puoi associarli ad altri progetti o cartelle dalla pagina **Resources**. Non puoi associare i sistemi storage FSx for NetApp ONTAP a progetti o cartelle, ma puoi visualizzarli nella pagina **Systems** o da Workloads.

Abbonamenti Keystone

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

Carichi di lavoro di Backup and Recovery (Oracle e Microsoft SQL Server)

Anche alcuni carichi di lavoro di Backup and Recovery sono considerati risorse. È possibile assegnare agli utenti le autorizzazioni per accedere a Backup and Recovery

Agenti della console

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

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

"Scopri come associare gli agenti ai progetti."

Membri e ruoli

Membri

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

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

"Scopri come aggiungere membri alla tua organizzazione."

Ruoli di accesso

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

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

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

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

"Scopri di più sui ruoli di accesso" .

Esempi di strategia IAM

Strategia per piccole organizzazioni

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

Esempio: ABC Corporation (team di 5 persone)

- **Struttura:** Unica organizzazione con 3 progetti (Produzione, Sviluppo, Backup)
- **Ruoli:**
  - 2 membri senior: ruolo di **Super amministratore** per accesso amministrativo completo
  - 3 membri del team: ruolo di **Super viewer** per il monitoraggio senza diritti di modifica
- **Strategia dell'agente:** Singolo agente associato a tutti i progetti per l'accesso alle risorse condivise
- **Vantaggi:** Amministrazione semplificata, ridotta complessità dei ruoli, adatto a team che necessitano di un ampio accesso

Strategia aziendale multiregionale

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

Esempio: XYZ Corporation (multinazionale)

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

Strategia di specializzazione dipartimentale

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

Esempio: TechCorp (azienda tecnologica di medie dimensioni)

- **Struttura:** Organizzazione > Cartelle dipartimentali (IT, Sicurezza, Sviluppo) > Risorse specifiche del progetto
- **Ruoli specializzati:**
  - Team di sicurezza: ruoli di **amministratore di Ransomware Resilience** e **visualizzatore di**

classificazione

- Team di backup: **Super amministratore di backup e ripristino** per operazioni di backup complete
- Team di sviluppo: **Amministratore di archiviazione** per la gestione dell'ambiente di test
- Team di conformità: **Analista di supporto operativo** per il monitoraggio e la gestione dei casi di supporto

- **Strategia dell'agente:** Agenti collegati a progetti dipartimentali in base alla proprietà delle risorse
- **Vantaggi:** Controllo degli accessi personalizzato, maggiore efficienza operativa e chiara responsabilità per attività specializzate

Passaggi successivi con IAM nella NetApp Console

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

Inizia con l'identità e l'accesso nella NetApp Console

Quando ti registri alla NetApp Console, ti verrà chiesto di creare una nuova organizzazione. L'organizzazione comprende un membro (un amministratore dell'organizzazione) e un progetto predefinito. Per configurare la gestione delle identità e degli accessi (IAM) in base alle esigenze aziendali, è necessario personalizzare la gerarchia dell'organizzazione, aggiungere altri membri, aggiungere o scoprire risorse e associare tali risorse all'interno della gerarchia.

Per gestire l'identità e l'accesso della tua organizzazione, hai bisogno delle autorizzazioni **Org admin** o **Super admin**. Con le autorizzazioni di **Amministratore cartella o progetto**, puoi gestire solo le cartelle e i progetti a cui hai accesso.

Per creare una nuova organizzazione, segui questi passaggi. L'ordine può variare in base alle esigenze della tua organizzazione.

1 Modifica il progetto predefinito o aggiungilo alla gerarchia della tua organizzazione

Utilizza il progetto predefinito oppure crea progetti e cartelle aggiuntivi in base alla gerarchia aziendale.

"Scopri come organizzare le tue risorse con cartelle e progetti" .

2 Associare i membri alla tua organizzazione

Dopo che gli utenti si sono registrati a NetApp Console, devi aggiungerli esplicitamente alla tua organizzazione Console. Hai anche la possibilità di aggiungere account di servizio alla tua organizzazione.

"Scopri come gestire i membri e i loro permessi" .

3 Aggiungi o scopri risorse

Aggiungere o scoprire risorse (sistemi) nella Console. I membri dell'organizzazione gestiscono i sistemi

dall'interno di un progetto.

Scopri come creare o scoprire risorse:

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Sistemi della serie E"
- "Cluster ONTAP on-premise"
- "StorageGRID"

Associare risorse a progetti aggiuntivi

L'aggiunta o la scoperta di un sistema nella Console associa automaticamente la risorsa al progetto attualmente selezionato. Per rendere quella risorsa disponibile per un altro progetto nella tua organizzazione, associala al rispettivo progetto. Se per gestire la risorsa viene utilizzato un agente Console, associare l'agente Console al rispettivo progetto.

- "Scopri come gestire la gerarchia delle risorse della tua organizzazione" .
- "Scopri come associare un agente Console a una cartella o a un progetto" .

Informazioni correlate

- "Scopri di più sulla gestione dell'identità e degli accessi nella NetApp Console"
- "Scopri di più sull'API per l'identità e l'accesso"

Imposta l'organizzazione della tua console

Aggiungi cartelle e progetti alla tua organizzazione NetApp Console

Aggiungi cartelle e progetti adatti alla struttura della tua attività. Dopo aver creato cartelle e progetti, puoi associarvi risorse e gestire l'accesso dei membri a tali progetti.

La Console crea automaticamente un progetto per te quando crei una nuova organizzazione. La maggior parte delle organizzazioni ha bisogno di più di un progetto e di cartelle per tenere tutto organizzato. "Scopri di più sulla gerarchia delle risorse nella NetApp Console".

Utilizzo di cartelle e progetti per organizzare le risorse

Nella NetApp Console, un'organizzazione contiene cartelle e progetti che ti aiutano a organizzare le tue risorse. Le cartelle ti aiutano a raggruppare progetti correlati e i progetti ti aiutano a gestire le risorse e l'accesso dei membri.

Cartelle

Le cartelle ti aiutano a organizzare i progetti correlati. È possibile creare cartelle nidificate per rappresentare diversi livelli della struttura della propria organizzazione. Ad esempio, potresti creare una cartella di primo livello per ogni unità aziendale e quindi creare sottocartelle per i diversi team all'interno di tale unità aziendale. Quindi si creano progetti all'interno delle cartelle.

Le cartelle consentono inoltre di gestire l'accesso dei membri in modo più efficiente utilizzando l'ereditarietà dei

ruoli. Quando si assegnano ruoli ai membri a livello di cartella, questi ereditano le autorizzazioni per tutti i progetti e le cartelle figlio.

Le cartelle sono uno strumento organizzativo e non sono visibili ai membri che non dispongono di autorizzazioni IAM, come i ruoli di amministratore dell'organizzazione, amministratore di cartelle o progetti o super amministratore. I membri accedono ai progetti, non alle cartelle.

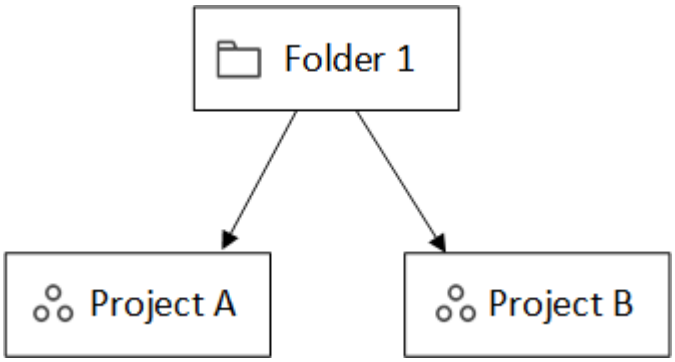
Gli amministratori dell'organizzazione possono delegare le responsabilità amministrative creando cartelle. Dopo aver creato una cartella, un amministratore dell'organizzazione può assegnare a un membro i ruoli di amministratore della cartella o del progetto per cartelle specifiche. Questi membri possono quindi gestire tutti i progetti all'interno di quella cartella senza avere accesso all'intera organizzazione.

Le cartelle possono avere altre cartelle o progetti come elementi secondari, ma non possono avere risorse direttamente associate. Le risorse devono essere associate a un progetto.

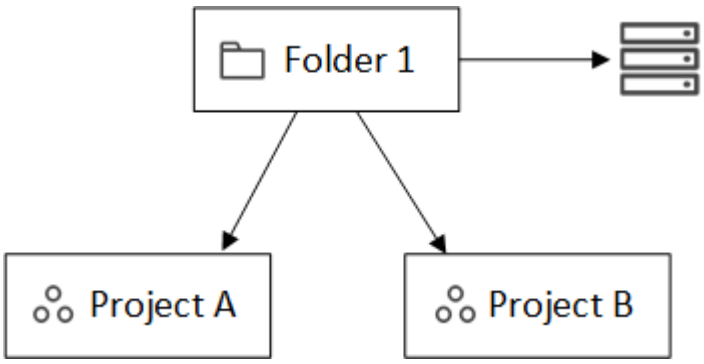
Quando associare una risorsa a una cartella

Un *amministratore dell'organizzazione* può associare una risorsa a una cartella in modo che un *amministratore della cartella o del progetto* possa collegarla ai progetti appropriati nella cartella.

Ad esempio, supponiamo di avere una cartella che contiene due progetti:

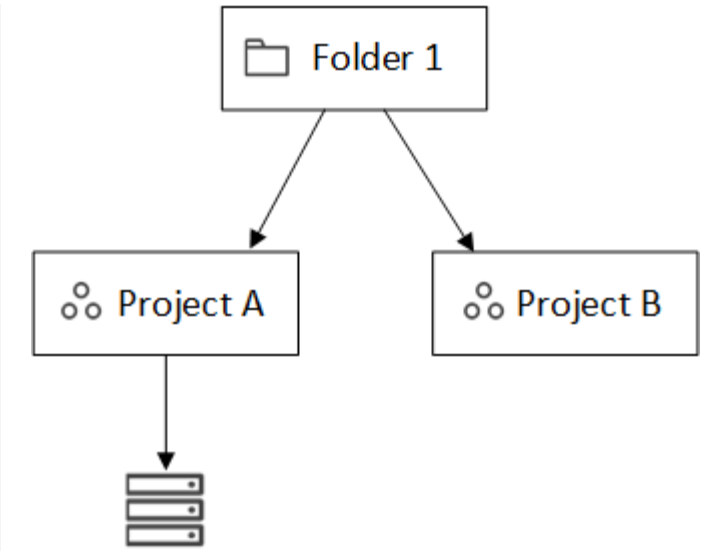


L'*amministratore dell'organizzazione* può associare una risorsa alla cartella:



L'associazione di una risorsa a una cartella non la rende accessibile a tutti i progetti; solo l'amministratore della cartella o del progetto può vederla. L'amministratore della cartella o del progetto decide quali progetti possono accedervi e associa la risorsa ai progetti appropriati.

In questo esempio, l'amministratore associa la risorsa al Progetto A:



I membri che dispongono delle autorizzazioni per il progetto A possono ora accedere alla risorsa.

Progetti

Associare le risorse ai progetti per consentire ai membri di gestirli. Per la gestione e l'accesso degli utenti, le risorse devono essere associate a un progetto.

Un'organizzazione può avere uno o più progetti. Un progetto può trovarsi direttamente sotto l'organizzazione o all'interno di una cartella. Se un agente viene utilizzato per scoprire risorse all'interno di un progetto, è necessario associare l'agente anche a quel progetto.

Gli utenti possono navigare tra i progetti assegnati nella pagina **Sistemi** per gestire le risorse associate a ciascun progetto.

Aggiungi una cartella o un progetto

Aggiungi progetti per gestire risorse e cartelle per raggruppare progetti correlati. Quando si crea una nuova organizzazione, la Console include un progetto.

Puoi creare fino a sette livelli di cartelle e progetti nella struttura delle risorse della tua organizzazione. Crea cartelle nidificate per organizzare le tue risorse in base alle tue esigenze.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Organizzazione**.
3. Dalla pagina **Organizzazione**, seleziona **Aggiungi cartella o progetto**.
4. Selezionare **Cartella** o **Progetto**.
5. Inserisci i dettagli della cartella o del progetto:
   - **Nome e posizione**: inserisci un nome e scegli una posizione per la cartella o il progetto. È possibile posizionare cartelle o progetti sotto l'organizzazione o all'interno di un'altra cartella.
   - **Risorse**: seleziona le risorse che desideri associare a questa cartella o progetto. Se non hai ancora aggiunto sistemi di archiviazione alla Console, puoi eseguire questo passaggio in un secondo momento.

I membri non possono accedere alle risorse in una cartella finché tali risorse non vengono assegnate a un progetto. Utilizzare le cartelle per conservare temporaneamente le risorse finché non si creano i progetti necessari. Ciò può aiutare l'amministratore dell'organizzazione a delegare l'assegnazione delle risorse a un amministratore di cartelle o di progetti, che poi assegna le risorse ai progetti all'interno della cartella.

- **Accesso**: seleziona **Aggiungi un membro** per assegnare l'accesso e un ruolo. Puoi aggiungere o rimuovere membri dal progetto o dalla cartella in qualsiasi momento.

  "Scopri di più sui ruoli di accesso" .

6. Selezionare **Aggiungi**.

Rinomina una cartella o un progetto

Rinominare una cartella o un progetto in base alle proprie esigenze. La ridenominazione non influisce sulle risorse associate o sull'accesso dei membri.

Passi

1. Dalla pagina **Organizzazione**, vai a un progetto o a una cartella nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica progetto**.
2. Nella pagina **Modifica**, inserisci un nuovo nome e seleziona **Applica**.

Elimina una cartella o un progetto

Elimina le cartelle e i progetti di cui non hai più bisogno, ad esempio dopo la ristrutturazione del team o il completamento del progetto.

Prima di eliminare una cartella o un progetto, assicurati che non contenga risorse. Scopri come rimuovere le risorse.

Passi

1. Dalla pagina **Organizzazione**, vai a un progetto o a una cartella nella tabella, seleziona ••• e quindi seleziona **Elimina**.
2. Conferma che vuoi eliminare la cartella o il progetto.

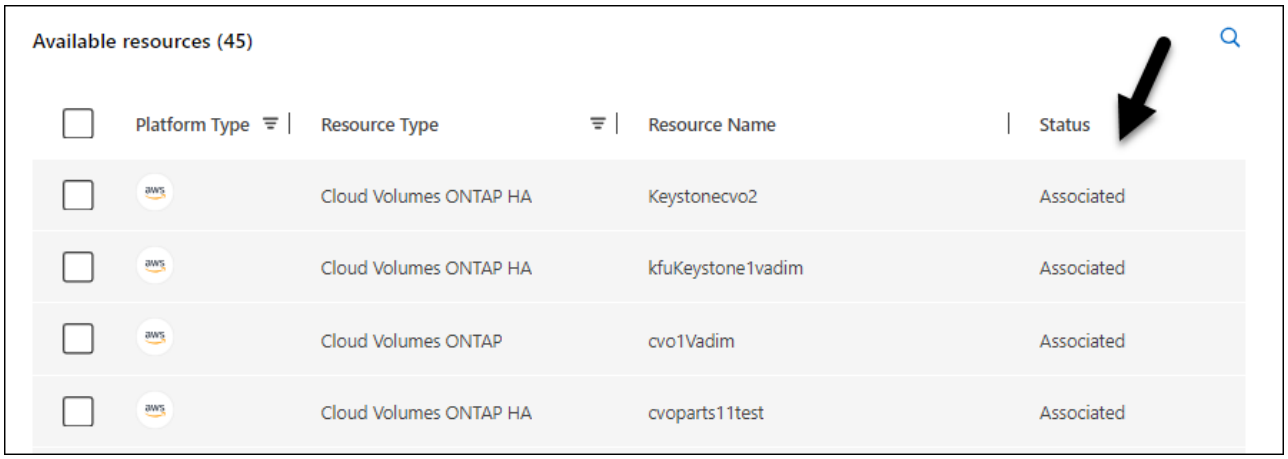
Visualizza le risorse associate a una cartella o a un progetto

Visualizza quali risorse e membri sono associati a una cartella o a un progetto.

Passi

1. Dalla pagina **Organizzazione**, vai a un progetto o a una cartella nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica progetto**.

2. Nella pagina **Modifica**, puoi visualizzare i dettagli sulla cartella o sul progetto selezionato espandendo le sezioni **Risorse** o **Accesso**.
   - Selezionare **Risorse** per visualizzare le risorse associate. Nella tabella, la colonna **Stato** identifica le risorse associate alla cartella o al progetto.



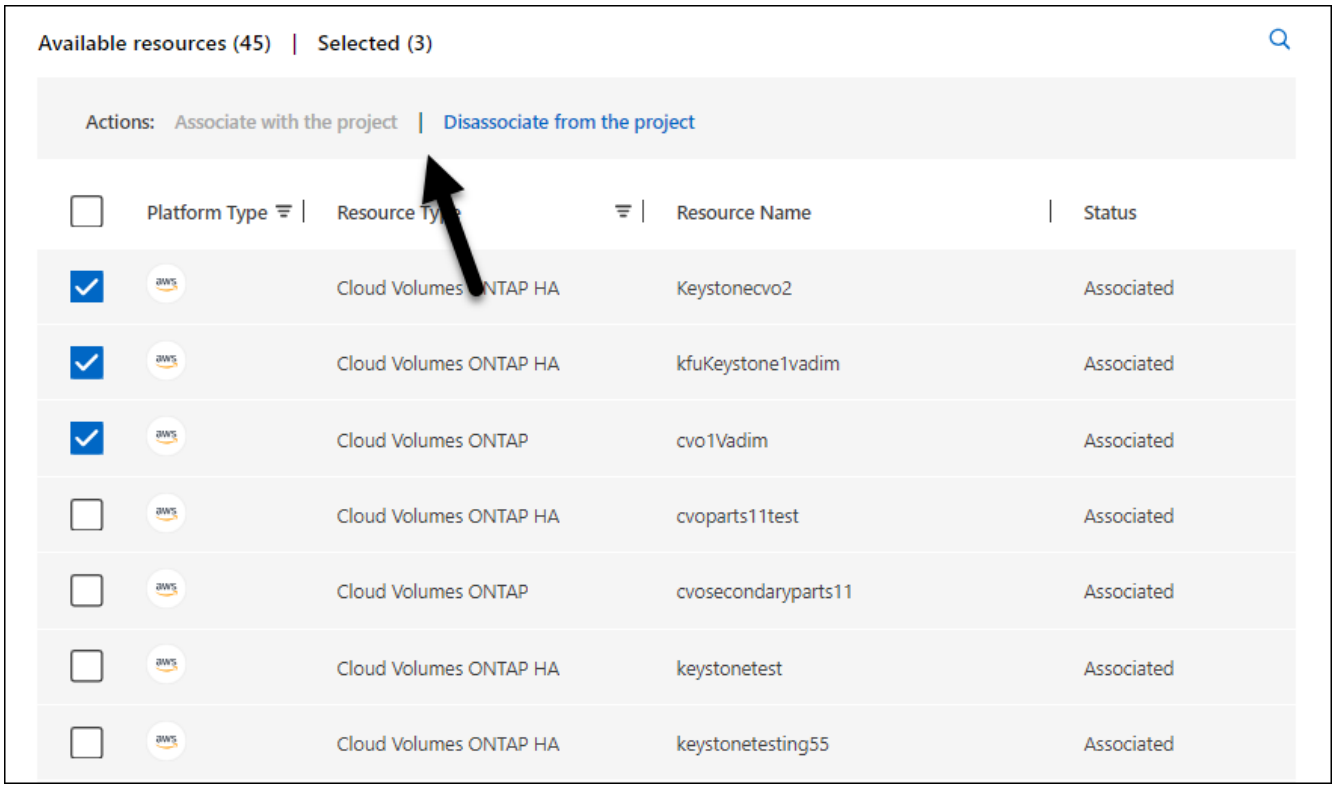
Modificare le risorse associate a una cartella o a un progetto

È possibile modificare le risorse associate a una cartella o a un progetto in base alle esigenze della propria organizzazione.

Passi

1. Dalla pagina **Organizzazione**, vai a un progetto o a una cartella nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica progetto**.
2. Nella pagina **Modifica**, seleziona **Risorse**.

   Nella tabella, la colonna **Stato** identifica le risorse associate alla cartella o al progetto.
3. Seleziona le risorse che desideri associare o dissociare.
4. In base alle risorse selezionate, seleziona **Associa al progetto** o **Disassocia dal progetto**.



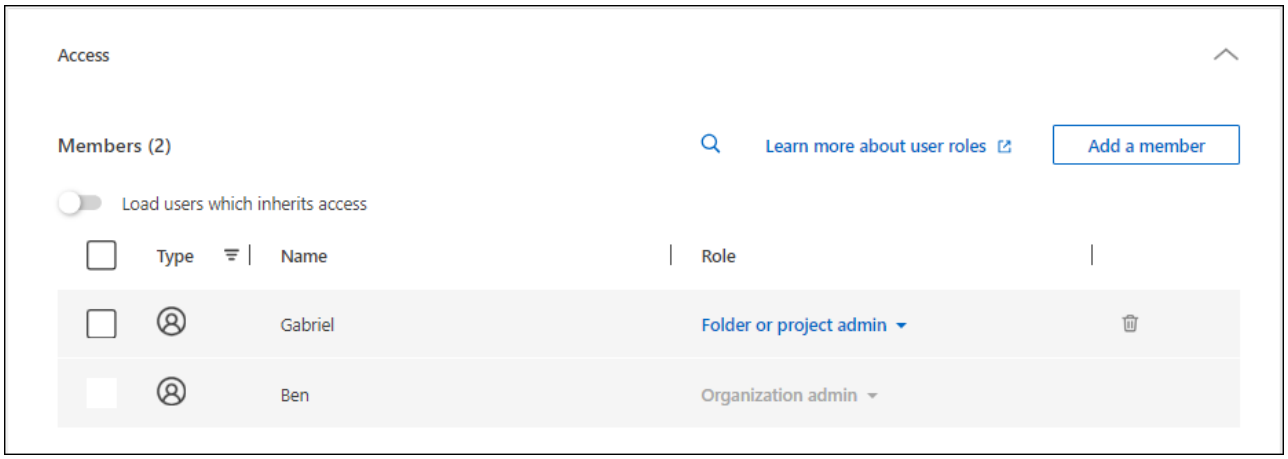
5. Selezionare **Applica**.

Visualizza i membri associati a una cartella o a un progetto

È possibile visualizzare i membri associati a una cartella o a un progetto dalla pagina **Organizzazione**.

Passi

1. Dalla pagina **Organizzazione**, vai a un progetto o a una cartella nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica progetto**.
2. Nella pagina **Modifica**, seleziona **Accesso** per visualizzare l'elenco dei membri che hanno accesso alla cartella o al progetto selezionato.
   - Selezionare **Accesso** per visualizzare i membri che hanno accesso alla cartella o al progetto.



Modificare l’accesso dei membri a una cartella o a un progetto

Modificare l’accesso dei membri per controllare l’accesso alle risorse. Ricorda che i ruoli assegnati a livello di cartella vengono ereditati da tutti i progetti e le cartelle figlio.

Non è possibile modificare l’accesso dei membri ai livelli inferiori se è ereditato dal livello di cartella o di organizzazione. Modificare l’autorizzazione del membro al livello gerarchico superiore per modificare l’accesso In alternativa, è possibile "gestire i permessi dalla pagina Membri".

Passi

1. Dalla pagina **Organizzazione**, vai a un progetto o a una cartella nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica progetto**.
2. Nella pagina **Modifica**, seleziona **Accesso** per visualizzare l’elenco dei membri che hanno accesso alla cartella o al progetto selezionato.
3. Modifica l’accesso dei membri:
   - **Aggiungi un membro**: seleziona il membro che desideri aggiungere alla cartella o al progetto e assegnagli un ruolo.
   - **Modifica il ruolo di un membro**: per tutti i membri con un ruolo diverso da Amministratore dell’organizzazione, seleziona il ruolo esistente e poi scegli un nuovo ruolo.
   - **Rimuovi accesso membro**: puoi rimuovere l’accesso ai membri che hanno un ruolo definito nella cartella o nel progetto che stai visualizzando.
4. Selezionare **Applica**.

Informazioni correlate

- "Scopri di più su identità e accesso nella NetApp Console"
- "Inizia con identità e accesso"
- "Scopri di più sull’API di identità e accesso"

Aggiungere risorse a cartelle e progetti nella NetApp Console

Controlla l’accesso degli utenti alle risorse aggiungendoli a progetti e cartelle nell’organizzazione NetApp Console . Concedere l’accesso agli utenti a livello di progetto.

Una *risorsa* è un’entità di cui la Console è a conoscenza, ad esempio una risorsa di archiviazione, un agente della Console o un carico di lavoro di backup e ripristino.

È possibile visualizzare e gestire le risorse dalla pagina **Risorse** nella Console.

Tipi di risorse della console

È possibile associare diversi tipi di risorse ai progetti nell’organizzazione NetApp Console :

Risorse di archiviazione

Le risorse di archiviazione sono il tipo di risorsa più comune nella tua organizzazione e rappresentano sia sistemi di archiviazione locali che cloud. Quando aggiungi un sistema di archiviazione alla Console, puoi aggiungerlo a una cartella o a un progetto. Fino a quel momento, la Console lo contrassegna come non scoperto e non lo visualizza nella pagina **Risorse**.

Agenti della console

Se hai utilizzato un agente Console per individuare i sistemi di archiviazione, aggiungi l'agente alla stessa cartella o progetto. Ciò consente agli utenti di eseguire funzioni abilitate dall'agente, come servizi dati o gestione dell'archiviazione nativa della console. È possibile aggiungere agenti a cartelle o progetti dalla pagina **Agenti** nella Console. "Scopri come associare un agente Console a una cartella o a un progetto".

Abbonamenti Keystone

Se nella tua organizzazione sono presenti abbonamenti Keystone , puoi visualizzarli nella pagina **Risorse**. È possibile associare gli abbonamenti Keystone a cartelle o progetti per consentire l'accesso ai membri che dispongono delle autorizzazioni per tali cartelle o progetti.

Visualizza le risorse nella tua organizzazione

Puoi visualizzare sia le risorse scoperte che quelle non scoperte associate alla tua organizzazione. Il sistema trova le risorse di archiviazione e le contrassegna come non rilevate finché non le aggiungi alla Console.

La console esclude le risorse Amazon FSx for NetApp ONTAP dalla pagina Risorse perché gli utenti non possono associarle a un ruolo. È possibile visualizzare queste risorse nella pagina **Sistemi** o da Carichi di lavoro.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Risorse**.
3. Seleziona **Ricerca avanzata e filtri**.
4. Utilizza le opzioni disponibili per trovare una risorsa:
   - **Cerca per nome della risorsa**: inserisci una stringa di testo e seleziona **Aggiungi**.
   - **Piattaforma**: seleziona una o più piattaforme, ad esempio Amazon Web Services.
   - **Risorse**: seleziona una o più risorse, ad esempio Cloud Volumes ONTAP.
   - **Organizzazione, cartella o progetto**: seleziona l'intera organizzazione, una cartella specifica o un progetto specifico.
5. Seleziona **Cerca**.

Associare una risorsa a cartelle e progetti

Associa una risorsa a una cartella o a un progetto per renderla disponibile ai membri che dispongono delle autorizzazioni per quella cartella o quel progetto.

Passi

1. Dalla pagina **Risorse**, vai a una risorsa nella tabella, seleziona ••• e quindi seleziona **Associa a cartelle o progetti**.
2. Seleziona una cartella o un progetto, quindi seleziona **Accetta**.
3. Per associare una cartella o un progetto aggiuntivo, seleziona **Aggiungi cartella o progetto** e poi seleziona la cartella o il progetto.

   Tieni presente che puoi selezionare solo le cartelle e i progetti per i quali disponi dei permessi di amministratore.

4. Seleziona **Risorse associate**.

- Se hai associato la risorsa a dei progetti, i membri che dispongono delle autorizzazioni per tali progetti ora possono accedere alla risorsa dalla Console.
- Se hai associato la risorsa a una cartella, un *amministratore di cartella o di progetto* può ora accedere alla risorsa e associarla a un progetto all'interno della cartella. "Scopri come associare una risorsa a una cartella".

Dopo aver finito

Se si individua una risorsa utilizzando un agente Console, associare l'agente Console al progetto per concedere l'accesso. In caso contrario, l'agente della console e la risorsa associata non saranno accessibili ai membri senza il ruolo di *Amministratore organizzazione*.

"Scopri come associare un agente Console a una cartella o a un progetto".

Visualizza le cartelle e i progetti associati a una risorsa

È possibile visualizzare le cartelle e i progetti associati a una determinata risorsa.

Se hai bisogno di scoprire quali membri dell'organizzazione hanno accesso alla risorsa, puoi"visualizzare i membri che hanno accesso alle cartelle e ai progetti associati alla risorsa" .

Passi

1. Dalla pagina **Risorse**, vai a una risorsa nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.

L'esempio seguente mostra una risorsa associata a un progetto.

Per vedere quali membri dell'organizzazione hanno accesso alla risorsa,"visualizza i membri con accesso alle cartelle e ai progetti associati" .

Rimuovere una risorsa da una cartella o da un progetto

Per rimuovere una risorsa da una cartella o da un progetto, rimuovere la sua associazione. Ciò impedisce ai membri di gestire la risorsa in quella cartella o progetto.

Per rimuovere una risorsa rilevata dall'intera organizzazione, vai alla pagina **Sistemi** e rimuovi il sistema.

Passi

1. Dalla pagina **Risorse**, vai a una risorsa nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
2. Per rimuovere una risorsa da una cartella o da un progetto, seleziona accanto alla cartella o al progetto.

3. Selezionare **Elimina** per rimuovere l'associazione.

Informazioni correlate

- "Scopri di più su identità e accesso nella NetApp Console"
- "Inizia con l'identità e l'accesso nella NetApp Console"
- "Scopri di più sull'API per l'identità e l'accesso"

Associare un agente Console ad altre cartelle e progetti

Associare gli agenti della console a progetti specifici per abilitare la gestione delle risorse e l'accesso al servizio dati. Per accedere al team, le risorse scoperte tramite un agente della console devono essere associate sia alla risorsa che all'agente agli stessi rispettivi progetti.

I super amministratori e gli amministratori dell'organizzazione possono creare agenti e associare qualsiasi agente a qualsiasi progetto o cartella. Gli amministratori di cartelle o progetti possono associare gli agenti esistenti solo alle cartelle e ai progetti per i quali dispongono delle autorizzazioni. "Scopri di più sulle azioni che un *amministratore di cartella o di progetto* può completare".

Passi

1. Selezionare **Amministrazione > Identità e accesso** > **Agenti**.
2. Nella tabella, trova l'agente Console che desideri associare.

   Utilizzare la ricerca sopra la tabella per trovare un agente Console specifico o filtrare la tabella in base alla gerarchia delle risorse.

3. Per visualizzare le cartelle e i progetti collegati all'agente Console, selezionare ••• e poi seleziona **Visualizza dettagli**.

   La pagina visualizza i dettagli sulle cartelle e sui progetti associati all'agente Console.

4. Seleziona **Associa a cartella o progetto**.
5. Seleziona una cartella o un progetto, quindi seleziona **Accetta**.
6. Per associare l'agente Console a una cartella o a un progetto aggiuntivo, selezionare **Aggiungi una cartella o un progetto**, quindi selezionare la cartella o il progetto.
7. Selezionare **Agente associato**.

Dopo aver finito

Associare le risorse dell'agente Console alle stesse cartelle e progetti dalla pagina **Risorse**.

"Scopri come associare una risorsa a cartelle e progetti" .

Informazioni correlate

- "Scopri di più sugli agenti NetApp Console"
- "Scopri di più sulla gestione dell'identità e degli accessi NetApp Console"
- "Inizia con identità e accesso"
- "Scopri di più sull'API per la gestione dell'identità e degli accessi"

Aggiungi utenti alla tua organizzazione Console

Aggiungere utenti a un'organizzazione NetApp Console

All'interno della Console, puoi concedere agli utenti l'accesso a progetti o cartelle in base a un ruolo di accesso. Un *ruolo di accesso* contiene un set di autorizzazioni che consente a un membro (account utente o di servizio) di eseguire azioni specifiche al livello assegnato della gerarchia delle risorse.

Ruoli di accesso richiesti

Super amministratore, amministratore dell'organizzazione o amministratore di cartelle o progetti (per le cartelle e i progetti che amministrano). "Scopri di più sui ruoli di accesso".

Scopri come viene concesso l'accesso nella NetApp Console

NetApp Console utilizza il controllo degli accessi basato sui ruoli (RBAC) per gestire le autorizzazioni. Assegnare ruoli agli utenti individualmente o tramite gruppi federati. Ogni ruolo definisce le azioni consentite per risorse specifiche.

Tenere presente quanto segue in merito alla concessione dell'accesso nella NetApp Console:

- Tutti gli utenti devono prima registrarsi alla NetApp Console prima di poter ottenere l'accesso alle risorse
- È necessario assegnare esplicitamente un ruolo a ciascun utente nella Console prima che possa accedere alle risorse, anche se è membro di un gruppo federato a cui è stato assegnato un ruolo.
- È possibile aggiungere account di servizio direttamente dalla Console e assegnare loro ruoli.

Aggiungi membri alla tua organizzazione

NetApp Console supporta tre tipi di membri: account utente, account di servizio e gruppi federati.

Gli utenti devono registrarsi a NetApp Console prima di poterli aggiungere e assegnare un ruolo, anche se fanno parte di un gruppo federato. Crea account di servizio direttamente nella Console.

Per poter accedere alle risorse, a tutti i membri deve essere assegnato esplicitamente almeno un ruolo.

Quando aggiungi un membro, scegli il livello della risorsa (organizzazione, cartella o progetto) e assegna un ruolo o più ruoli con le autorizzazioni necessarie.

Aggiungi un utente

Gli utenti si iscrivono alla NetApp Console, ma un amministratore dell'organizzazione o un amministratore di cartella o di progetto deve aggiungerli a un'organizzazione, una cartella o un progetto affinché possano accedere alle risorse.

Prima di iniziare:

L'utente deve essersi già registrato alla NetApp Console. Se non si sono ancora registrati, indirizzali a "iscriviti alla NetApp Console."

Se si aggiunge un utente che fa parte di un gruppo federato, assicurarsi che l'utente si sia già registrato alla NetApp Console e che gli sia stato assegnato esplicitamente un ruolo nella Console. NetApp consiglia di assegnare un ruolo di accesso minimo, ad esempio Visualizzatore dell'organizzazione.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Seleziona **Aggiungi un membro**.
4. Per **Tipo di membro**, mantenere selezionato **Utente**.
5. Per **Email dell'utente**, inserisci l'indirizzo email dell'utente associato all'accesso che ha creato.
6. Utilizzare la sezione **Seleziona un'organizzazione, una cartella o un progetto** per scegliere il livello della gerarchia delle risorse per il quale il membro deve disporre delle autorizzazioni.

   Notare quanto segue:

   - Puoi selezionare solo le cartelle e i progetti per i quali disponi delle autorizzazioni.
   - Quando selezioni un'organizzazione o una cartella, concedi al membro le autorizzazioni per tutti i suoi contenuti.
   - È possibile assegnare il ruolo di **Amministratore organizzazione** solo a livello di organizzazione.
7. **Seleziona una categoria**, quindi seleziona un **Ruolo** che fornisca al membro le autorizzazioni per le risorse associate all'organizzazione, alla cartella o al progetto selezionato.

   "Scopri di più sui ruoli di accesso" .
8. Per consentire l'accesso a più cartelle, progetti o ruoli, seleziona **Aggiungi ruolo**, scegli la cartella, il progetto o la categoria di ruolo e seleziona un ruolo.
9. Selezionare **Aggiungi**.

   La Console invia le istruzioni all'utente tramite e-mail.

Aggiungi un account di servizio

Gli account di servizio consentono di automatizzare le attività e di connettersi in modo sicuro alle API della console. Scegli un ID client e un segreto per configurazioni semplici oppure JWT (JSON Web Token) per una maggiore sicurezza in ambienti automatizzati o cloud-native. Seleziona il metodo che soddisfa i tuoi requisiti di sicurezza.

Prima di iniziare:

Per l'autenticazione JWT, prepara la tua chiave pubblica o il tuo certificato.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Seleziona **Aggiungi un membro**.
4. Per **Tipo di membro**, seleziona **Account di servizio**.
5. Inserisci un nome per l'account di servizio.
6. Per utilizzare l'autenticazione JWT, seleziona **Usa autenticazione JWT con chiave privata** e carica la tua chiave RSA pubblica o il certificato. Ignora se utilizzi ID client e segreto.

   Il tuo certificato X.509. Deve essere in formato PEM, CRT o CER.

a. Imposta le notifiche di scadenza per il tuo certificato. Scegli tra sette giorni o 30 giorni. Le notifiche di scadenza vengono inviate tramite e-mail e visualizzate nella Console agli utenti con il ruolo di Super amministratore o Amministratore dell'organizzazione.

7. Utilizzare la sezione **Seleziona un'organizzazione, una cartella o un progetto** per scegliere il livello della gerarchia delle risorse per il quale il membro deve disporre delle autorizzazioni.

   Notare quanto segue:

   - Puoi selezionare solo le cartelle e i progetti per i quali disponi delle autorizzazioni.
   - Selezionando un'organizzazione o una cartella, al membro vengono concesse autorizzazioni su tutti i suoi contenuti.
   - È possibile assegnare il ruolo di **Amministratore organizzazione** solo a livello di organizzazione.

8. Seleziona una **Categoria**, quindi seleziona un **Ruolo** che conceda al membro le autorizzazioni per le risorse nell'organizzazione, nella cartella o nel progetto selezionato.

   "Scopri di più sui ruoli di accesso" .

9. Per consentire l'accesso a più cartelle, progetti o ruoli, seleziona **Aggiungi ruolo**, scegli la cartella, il progetto o la categoria di ruolo e seleziona un ruolo.
10. Se non hai scelto di utilizzare l'autenticazione JWT, scarica o copia l'ID client e il segreto client.

    La console mostra il segreto del client solo una volta. Copialo in modo sicuro: potrai ricrearlo in seguito se lo perdi.

11. Se hai scelto l'autenticazione JWT, scarica o copia l'ID client e il pubblico JWT. La Console visualizza queste informazioni una sola volta e non consente di recuperarle in seguito.
12. Selezionare **Chiudi**.

Aggiungi un gruppo federato alla tua organizzazione

Puoi aggiungere un gruppo federato dal tuo provider di identità (IdP) alla tua organizzazione e assegnargli uno o più ruoli. I membri del gruppo federato ereditano i ruoli assegnati al gruppo nella Console.

Prima di poter assegnare un ruolo a un gruppo federato, assicurati di aver soddisfatto i seguenti requisiti:

- Imposta la federazione tra il tuo IdP e la Console. "Scopri come impostare una federazione."
- Il gruppo deve già esistere nel tuo IdP e deve avere accesso all'app Console.
- Gli utenti appartenenti al gruppo devono essersi già registrati alla NetApp Console e aver ricevuto un ruolo esplicito nella Console. NetApp consiglia di assegnare un ruolo di accesso minimo, ad esempio Visualizzatore dell'organizzazione.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Seleziona **Aggiungi un membro**.
4. Per **Tipo di membro**, seleziona **Gruppo federato**.
5. Seleziona la federazione di cui il gruppo è membro
6. Per **Nome gruppo**, inserisci il nome esatto del gruppo nel tuo IdP.

7. Utilizzare la sezione **Seleziona un'organizzazione, una cartella o un progetto** per scegliere il livello della gerarchia delle risorse per il quale il membro deve disporre delle autorizzazioni.

   Notare quanto segue:

   - Puoi selezionare solo le cartelle e i progetti per i quali disponi delle autorizzazioni.
   - Selezionando un'organizzazione o una cartella, al membro vengono concesse autorizzazioni su tutti i suoi contenuti.
   - È possibile assegnare il ruolo di **Amministratore organizzazione** solo a livello di organizzazione.

8. Seleziona una **Categoria**, quindi seleziona un **Ruolo** che conceda al membro le autorizzazioni per le risorse nell'organizzazione, nella cartella o nel progetto selezionato.

   "Scopri di più sui ruoli di accesso" .

9. Per consentire l'accesso a più cartelle, progetti o ruoli, seleziona **Aggiungi ruolo**, scegli la cartella, il progetto o la categoria di ruolo e seleziona un ruolo.

Informazioni correlate

- "Scopri di più sulla gestione dell'identità e degli accessi nella NetApp Console"
- "Inizia con identità e accesso"
- "Ruoli di accesso NetApp Console"
- "Scopri di più sull'API per l'identità e l'accesso"

Gestire l'accesso e la sicurezza degli utenti

Scopri di più sul controllo degli accessi basato sui ruoli (RBAC) NetApp Console

Gestisci l'accesso degli utenti alla NetApp Console con il controllo degli accessi basato sui ruoli (RBAC), assegnando ruoli predefiniti a livello di organizzazione, cartella o progetto. Ogni ruolo concede autorizzazioni specifiche che definiscono quali azioni gli utenti possono eseguire nell'ambito loro assegnato.

NetApp progetta i ruoli della console con privilegi minimi, in modo che ogni ruolo includa solo le autorizzazioni necessarie per le sue attività. Questo approccio aumenta la sicurezza limitando l'accesso a ciò di cui ogni membro ha bisogno.

Dopo aver organizzato le risorse in cartelle e progetti, assegna ai membri dell'organizzazione uno o più ruoli per cartelle o progetti specifici, che consentano loro di svolgere solo le proprie responsabilità.

Ad esempio, è possibile assegnare a un membro il ruolo di amministratore di Ransomware Resilience per un livello di progetto specifico, consentendogli di eseguire operazioni di Ransomware Resilience per le risorse all'interno di quel progetto, senza concedergli un accesso più ampio all'intera organizzazione. Allo stesso utente può essere concesso il ruolo per diversi progetti all'interno della tua organizzazione.

È possibile assegnare agli utenti più ruoli per lo stesso ambito o per ambiti diversi, a seconda delle loro responsabilità. Ad esempio, un'organizzazione più piccola potrebbe avere lo stesso utente che gestisce sia le attività di Ransomware Resilience sia quelle di Backup e ripristino a livello di organizzazione, mentre un'organizzazione più grande potrebbe avere utenti diversi assegnati a ciascun ruolo a livello di progetto.

Tipi di membri dell'organizzazione della console

Esistono tre tipi di membri in un'organizzazione NetApp Console : * *Account utente*: singoli utenti che accedono a NetApp Console per gestire le risorse. Gli utenti devono registrarsi alla NetApp Console prima di poter essere aggiunti a un'organizzazione. * *Account di servizio*: account non umani utilizzati dalle applicazioni o dai servizi per interagire con la NetApp Console tramite API. Puoi aggiungere account di servizio direttamente all'organizzazione della tua Console. * *Gruppi federati*: gruppi sincronizzati dal tuo provider di identità (IdP) che ti consentono di gestire l'accesso di più utenti collettivamente. Ogni utente all'interno di un gruppo federato deve essersi registrato alla NetApp Console ed essere stato aggiunto all'organizzazione con un ruolo di accesso prima di poter accedere alle risorse concesse al gruppo.

"Scopri come aggiungere membri alla tua organizzazione."

Ruoli predefiniti nella NetApp Console

NetApp Console include ruoli predefiniti che è possibile assegnare ai membri dell'organizzazione. Ogni ruolo include autorizzazioni che specificano quali azioni un membro può eseguire nell'ambito assegnatogli (organizzazione, cartella o progetto).

I ruoli NetApp Console utilizzano principi di privilegi minimi che garantiscono che i membri abbiano solo le autorizzazioni necessarie per le loro attività e categorizzano i ruoli in base al tipo di accesso che forniscono:

- Ruoli della piattaforma: fornire autorizzazioni di amministrazione della console
- Ruoli dei servizi dati: fornire autorizzazioni per la gestione di servizi dati specifici, come Ransomware Resilience e Backup e ripristino
- Ruoli dell'applicazione: fornire autorizzazioni per la gestione dell'archiviazione e per il controllo degli eventi e degli avvisi della console

È possibile assegnare più ruoli a un membro in base alle sue responsabilità. Ad esempio, potresti assegnare a un membro sia il ruolo di amministratore Ransomware Resilience sia il ruolo di amministratore Backup e ripristino per un progetto specifico.

"Scopri i ruoli predefiniti disponibili nella NetApp Console".

Gestisci l'accesso dei membri nella NetApp Console

Gestisci l'accesso dei membri nella tua organizzazione Console. Assegnare ruoli per impostare le autorizzazioni. Rimuovi i membri quando se ne vanno.

Ruoli di accesso richiesti

Super amministratore, amministratore dell'organizzazione o amministratore di cartelle o progetti (per le cartelle e i progetti che amministrano). Link:reference-iam-predefined-roles.html[Scopri di più sui ruoli di accesso].

È possibile assegnare ruoli di accesso in base al progetto o alla cartella. Ad esempio, assegnare un ruolo a un utente per due progetti specifici o assegnare il ruolo a livello di cartella per assegnare a un utente il ruolo di amministratore di Ransomware Resilience per tutti i progetti in una cartella

Aggiungi le tue cartelle e i tuoi progetti prima di assegnare l'accesso agli utenti. "Scopri come aggiungere cartelle e progetti."

Scopri come viene concesso l'accesso nella NetApp Console

NetApp Console utilizza un modello di controllo degli accessi basato sui ruoli (RBAC) per gestire le

autorizzazioni degli utenti. È possibile assegnare ruoli predefiniti ai membri individualmente o tramite gruppi federati. È possibile aggiungere e assegnare ruoli agli account di servizio, nonché ai gruppi federati. Ogni ruolo definisce quali azioni un membro può eseguire sulle risorse associate.

Tenere presente quanto segue in merito alla concessione dell'accesso nella NetApp Console:

- Tutti gli utenti devono prima registrarsi alla NetApp Console prima di poter ottenere l'accesso alle risorse.
- È necessario assegnare esplicitamente un ruolo a ciascun utente nella Console prima che possa accedere alle risorse, anche se è membro di un gruppo federato a cui è stato assegnato un ruolo.
- È possibile aggiungere account di servizio direttamente dalla Console e assegnare loro ruoli.

Utilizzo dell'ereditarietà dei ruoli

Quando si assegna un ruolo a livello di organizzazione, cartella o progetto in NetApp Console, tale ruolo viene automaticamente ereditato da tutte le risorse nell'ambito selezionato. Ad esempio, i ruoli a livello di cartella si applicano a tutti i progetti contenuti, mentre i ruoli a livello di progetto si applicano a tutte le risorse all'interno di quel progetto.

Visualizza i membri dell'organizzazione

Per capire quali risorse e autorizzazioni sono disponibili per un membro, puoi visualizzare i ruoli assegnati al membro ai diversi livelli della gerarchia delle risorse della tua organizzazione."Scopri come utilizzare i ruoli per controllare l'accesso alle risorse della Console."

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.

   Nella tabella **Membri** sono elencati i membri della tua organizzazione.

3. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.

Visualizza i ruoli assegnati a un membro

Puoi verificare quali ruoli sono attualmente assegnati loro.

Se si dispone del ruolo di *Amministratore cartella o progetto*, la pagina visualizza tutti i membri dell'organizzazione. Tuttavia, puoi visualizzare e gestire le autorizzazioni dei membri solo per le cartelle e i progetti per i quali disponi delle autorizzazioni. "Scopri di più sulle azioni che un *amministratore di cartella o di progetto* può completare" .

1. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
2. Nella tabella, espandi la riga corrispondente all'organizzazione, alla cartella o al progetto in cui desideri visualizzare il ruolo assegnato al membro e seleziona **Visualizza** nella colonna **Ruolo**.

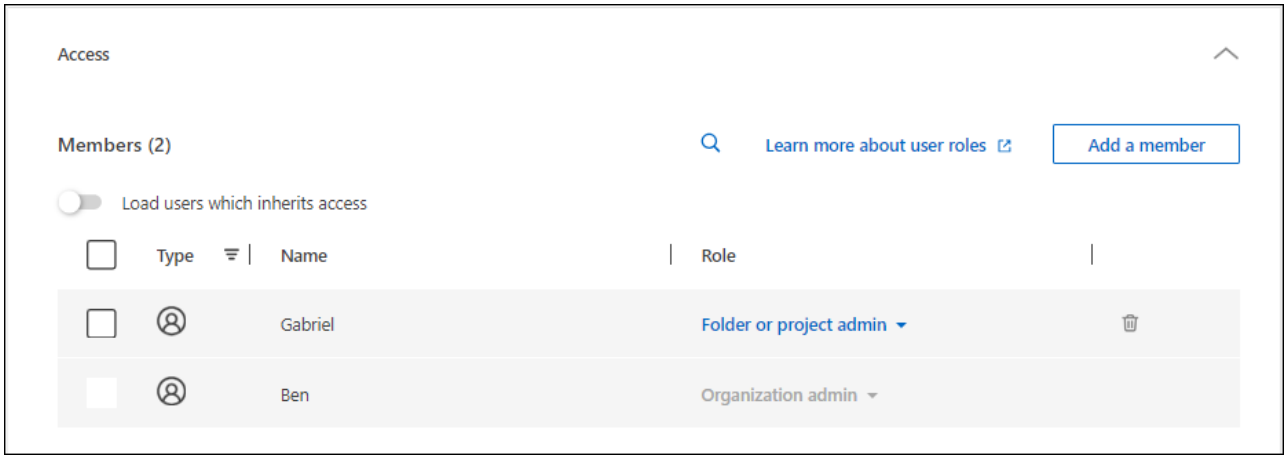
Visualizza i membri associati a una cartella o a un progetto

Puoi visualizzare i membri che hanno accesso a una cartella o a un progetto specifico.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Organizzazione**.

3. Dalla pagina **Organizzazione**, vai a un progetto o a una cartella nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica progetto**.
   - Selezionare **Accesso** per visualizzare i membri che hanno accesso alla cartella o al progetto.



Assegna o modifica l'accesso dei membri

Dopo che un utente si è registrato a NetApp Console, puoi aggiungerlo alla tua organizzazione e assegnargli un ruolo per fornire l'accesso alle risorse. "Scopri come aggiungere membri alla tua organizzazione."

È possibile modificare l'accesso di un membro aggiungendo o rimuovendo ruoli in base alle esigenze.

Aggiungere un ruolo di accesso a un membro

Solitamente si assegna un ruolo quando si aggiunge un membro all'organizzazione, ma è possibile aggiornarlo in qualsiasi momento rimuovendo o aggiungendo ruoli.

Puoi assegnare a un utente un ruolo di accesso per la tua organizzazione, cartella o progetto.

I membri possono avere più ruoli all'interno dello stesso progetto e in progetti diversi. Ad esempio, le organizzazioni più piccole potrebbero assegnare tutti i ruoli di accesso disponibili allo stesso utente, mentre le organizzazioni più grandi potrebbero far svolgere agli utenti attività più specializzate. In alternativa, è possibile assegnare a un utente il ruolo di amministratore di Ransomware Resilience a livello di organizzazione. In questo esempio, l'utente sarebbe in grado di eseguire attività di Ransomware Resilience su tutti i progetti all'interno della tua organizzazione.

La strategia del ruolo di accesso deve essere in linea con il modo in cui hai organizzato le tue risorse NetApp .

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Selezionare una delle schede dei membri: **Utenti**, **Account di servizio** o **Gruppi federati**.
4. Seleziona il menu azioni ••• accanto al membro a cui vuoi assegnare un ruolo e seleziona **Aggiungi un ruolo**.
5. Per aggiungere un ruolo, completare i passaggi nella finestra di dialogo:
   - **Seleziona un'organizzazione, una cartella o un progetto**: scegli il livello della gerarchia delle risorse per il quale il membro deve avere le autorizzazioni.

Se selezioni l'organizzazione o una cartella, il membro avrà autorizzazioni per tutto ciò che risiede all'interno dell'organizzazione o della cartella.

- **Seleziona una categoria**: Scegli una categoria di ruolo. "Scopri di più sui ruoli di accesso" .
- Seleziona un **Ruolo**: scegli un ruolo che fornisca al membro le autorizzazioni per le risorse associate all'organizzazione, alla cartella o al progetto selezionato.
- **Aggiungi ruolo**: se desideri concedere l'accesso a cartelle o progetti aggiuntivi all'interno della tua organizzazione, seleziona **Aggiungi ruolo**, specifica un'altra cartella, un altro progetto o una categoria di ruolo, quindi seleziona una categoria di ruolo e un ruolo corrispondente.

6. Seleziona **Aggiungi nuovi ruoli**.

Modificare il ruolo assegnato a un membro

Modifica i ruoli di un membro per aggiornarne l'accesso.

Agli utenti deve essere assegnato almeno un ruolo. Non è possibile rimuovere tutti i ruoli da un utente. Se devi rimuovere tutti i ruoli, devi eliminare l'utente dalla tua organizzazione.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Selezionare una delle schede dei membri: **Utenti**, **Account di servizio** o **Gruppi federati**.
4. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
5. Nella tabella, espandi la riga corrispondente all'organizzazione, alla cartella o al progetto in cui desideri modificare il ruolo assegnato al membro e seleziona **Visualizza** nella colonna **Ruolo** per visualizzare i ruoli assegnati a questo membro.
6. È possibile modificare un ruolo esistente per un membro o rimuovere un ruolo.
   a. Per modificare il ruolo di un membro, seleziona **Modifica** accanto al ruolo che desideri modificare. È possibile modificare un ruolo solo in un ruolo all'interno della stessa categoria di ruoli. Ad esempio, è possibile passare da un ruolo di servizio dati a un altro. Conferma la modifica.
   b. Per annullare l'assegnazione del ruolo a un membro, selezionare 🗑 accanto al ruolo per rimuovere il rispettivo ruolo dal membro. Ti verrà chiesto di confermare la rimozione.

Rimuovi un membro dalla tua organizzazione

Rimuovi un membro se abbandona la tua organizzazione.

Quando si rimuove un membro, il sistema revoca le autorizzazioni della Console, ma conserva i relativi account Console e NetApp Support Site.

Membri federati

- Gli utenti federati perdono automaticamente l'accesso alla NetApp Console quando vengono rimossi dal tuo IdP. Tuttavia, dovresti comunque rimuoverli dall'organizzazione della tua Console per mantenere aggiornato l'elenco dei membri.
- Se rimuovi un utente da un gruppo federato nel tuo IdP, l'utente perderà l'accesso alla Console associato a quel gruppo. Tuttavia, mantengono comunque qualsiasi accesso associato a un ruolo esplicito loro assegnato nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Selezionare una delle schede dei membri: **Utenti**, **Account di servizio** o **Gruppi federati**.
4. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• quindi seleziona **Elimina utente**.
5. Conferma che desideri rimuovere il membro dalla tua organizzazione.

Sicurezza dell'utente

Proteggi l'accesso degli utenti alla tua organizzazione NetApp Console gestendo le impostazioni di sicurezza dei membri. È possibile reimpostare le password utente, gestire l'autenticazione a più fattori (MFA) e ricreare le credenziali dell'account di servizio.

Ruoli di accesso richiesti

Super amministratore, amministratore dell'organizzazione o amministratore di cartelle o progetti (per le cartelle e i progetti che amministrano). Link:reference-iam-predefined-roles.html[Scopri di più sui ruoli di accesso].

Reimposta le password utente (solo utenti locali)

Gli amministratori dell'organizzazione non possono reimpostare le password degli utenti locali. Possono tuttavia chiedere agli utenti di reimpostare autonomamente le proprie password.

Chiedere all'utente di reimpostare la propria password dalla pagina di accesso della Console selezionando **Password dimenticata?**.

Questa opzione non è disponibile per gli utenti di un'organizzazione federata.

Gestire l'autenticazione a più fattori (MFA) di un utente

Se un utente perde l'accesso al proprio dispositivo MFA, è possibile rimuovere o disabilitare la configurazione MFA.

L'autenticazione a più fattori è disponibile solo per gli utenti locali. Gli utenti federati non possono abilitare MFA.

Gli utenti devono configurare nuovamente l'MFA quando effettuano l'accesso dopo la rimozione. Se l'utente perde temporaneamente l'accesso al proprio dispositivo MFA, può utilizzare il codice di ripristino salvato per effettuare l'accesso.

Se non hanno il codice di ripristino, disattivare temporaneamente l'MFA per consentire l'accesso. Quando si disattiva l'MFA per un utente, questa viene disattivata solo per otto ore e poi riattivata automaticamente. All'utente è consentito un solo accesso durante tale periodo senza MFA. Dopo otto ore, l'utente deve utilizzare MFA per effettuare l'accesso.

Per gestire l'autenticazione a più fattori di un utente, è necessario disporre di un indirizzo email nello stesso dominio dell'utente interessato.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.

2. Seleziona **Membri**.

   Nella tabella **Membri** sono elencati i membri della tua organizzazione.

3. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e quindi seleziona **Gestisci autenticazione a più fattori**.
4. Scegliere se rimuovere o disabilitare la configurazione MFA dell'utente.

Ricreare le credenziali per un account di servizio

Puoi creare nuove credenziali per un servizio se le perdi o devi aggiornarle.

La creazione di nuove credenziali elimina quelle vecchie. Non è possibile utilizzare le vecchie credenziali.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Nella tabella **Membri**, vai a un account di servizio, seleziona ••• e poi seleziona **Ricrea segreti**.
4. Seleziona **Ricrea**.
5. Scarica o copia l'ID client e il segreto client.

   La console mostra il segreto del client solo una volta. Assicuratevi di copiarlo o scaricarlo e conservarlo in modo sicuro.

Ruoli di accesso NetApp Console

Scopri di più sui ruoli di accesso NetApp Console

La gestione delle identità e degli accessi (IAM) nella NetApp Console fornisce ruoli predefiniti che puoi assegnare ai membri della tua organizzazione nei diversi livelli della gerarchia delle risorse. Prima di assegnare questi ruoli, è necessario comprendere le autorizzazioni incluse in ciascun ruolo. I ruoli rientrano nelle seguenti categorie: piattaforma, applicazione e servizio dati.

Ruoli della piattaforma

I ruoli della piattaforma concedono autorizzazioni di amministrazione NetApp Console , tra cui l'assegnazione dei ruoli e la gestione degli utenti. La console ha diversi ruoli di piattaforma.

Ruolo della piattaforma	Responsabilità
"Amministratore dell'organizzazione"	Consente all'utente l'accesso illimitato a tutti i progetti e le cartelle all'interno di un'organizzazione, di aggiungere membri a qualsiasi progetto o cartella, nonché di eseguire qualsiasi attività e utilizzare qualsiasi servizio dati a cui non sia associato un ruolo esplicito. Gli utenti con questo ruolo gestiscono la tua organizzazione creando cartelle e progetti, assegnando ruoli, aggiungendo utenti e gestendo i sistemi, se dispongono delle credenziali appropriate. Questo è l'unico ruolo di accesso che può creare agenti Console.

Ruolo della piattaforma	Responsabilità
"Amministratore di cartelle o progetti"	Consente all'utente l'accesso illimitato ai progetti e alle cartelle assegnati. Possono aggiungere membri alle cartelle o ai progetti che gestiscono, nonché eseguire qualsiasi attività e utilizzare qualsiasi servizio dati o applicazione sulle risorse all'interno della cartella o del progetto a loro assegnato. Gli amministratori di cartelle o progetti non possono creare agenti della console.
"Amministratore della Federazione"	Consente a un utente di creare e gestire federazioni con la Console, che abilita l'accesso singolo (SSO).
"Visualizzatore della federazione"	Consente a un utente di visualizzare le federazioni esistenti con la Console. Non è possibile creare o gestire federazioni.
"Amministratore della partnership"	Consente all'utente di creare e gestire partnership.
"Visualizzatore di partnership"	Consente all'utente di visualizzare le partnership esistenti. Non è possibile creare o gestire partnership.
"Super amministratore"	Fornisce all'utente un sottoinsieme di ruoli amministrativi. Questo ruolo è pensato per le organizzazioni più piccole che potrebbero non aver bisogno di distribuire le responsabilità della console tra più utenti.
"Super spettatore"	Assegna all'utente un sottoinsieme di ruoli di visualizzazione. Questo ruolo è pensato per le organizzazioni più piccole che potrebbero non aver bisogno di distribuire le responsabilità della console tra più utenti.

Ruoli applicativi

Di seguito è riportato un elenco dei ruoli nella categoria applicazione. Ogni ruolo concede autorizzazioni specifiche nell'ambito designato. Gli utenti che non possiedono il ruolo di piattaforma o applicazione richiesto non possono accedere alla rispettiva applicazione.

Ruolo applicativo	Responsabilità
"Amministratore di Google Cloud NetApp Volumes"	Gli utenti con il ruolo Google Cloud NetApp Volumes possono scoprire e gestire Google Cloud NetApp Volumes.
"Visualizzatore Google Cloud NetApp Volumes"	Gli utenti con il ruolo utente Google Cloud NetApp Volumes possono visualizzare Google Cloud NetApp Volumes.
"Amministratore Keystone"	Gli utenti con il ruolo di amministratore Keystone possono creare richieste di servizio. Consente agli utenti di monitorare e visualizzare l'utilizzo, le risorse e i dettagli amministrativi all'interno del tenant Keystone a cui accedono.
"Visualizzatore Keystone"	Gli utenti con il ruolo di visualizzatore Keystone NON POSSONO creare richieste di servizio. Consente agli utenti di monitorare e visualizzare i consumi, le risorse e le informazioni amministrative all'interno del tenant Keystone a cui accedono.
Ruolo di configurazione del mediatore ONTAP	Gli account di servizio con il ruolo di configurazione ONTAP Mediator possono creare richieste di servizio. Questo ruolo è richiesto in un account di servizio per configurare un'istanza di"Mediatore cloud ONTAP" .
"Analista di supporto operativo"	Fornisce accesso ad avvisi e strumenti di monitoraggio e la possibilità di inserire e gestire casi di supporto.

Ruolo applicativo	Responsabilità
"Amministratore di archiviazione"	Gestire le funzioni di governance e integrità dello storage, individuare le risorse di storage e modificare ed eliminare i sistemi esistenti.
"Visualizzatore di archiviazione"	Visualizza le funzioni di governance e di integrità dello storage, nonché le risorse di storage precedentemente scoperte. Impossibile scoprire, modificare o eliminare i sistemi di archiviazione esistenti.
"Specialista in salute del sistema"	Gestire le funzioni di archiviazione, integrità e governance; tutte le autorizzazioni dell'amministratore di archiviazione, tranne quella di non poter modificare o eliminare i sistemi esistenti.

Ruoli del servizio dati

Di seguito è riportato un elenco dei ruoli nella categoria dei servizi dati. Ogni ruolo concede autorizzazioni specifiche nell'ambito designato. Gli utenti che non dispongono del ruolo di servizio dati richiesto o di un ruolo di piattaforma non potranno accedere al servizio dati.

Ruolo del servizio dati	Responsabilità
"Super amministratore di backup e ripristino"	Eseguire qualsiasi azione in NetApp Backup and Recovery.
"Amministratore di backup e ripristino"	Eseguire backup su snapshot locali, replicare su storage secondario ed eseguire backup su storage di oggetti.
"Backup e ripristino ripristino amministratore"	Ripristinare i carichi di lavoro nel backup e nel ripristino.
"Amministratore clone di backup e ripristino"	Clona applicazioni e dati nel Backup e Ripristino.
"Visualizzatore di backup e ripristino"	Visualizza le informazioni di backup e ripristino.
"Amministratore del ripristino di emergenza"	Eseguire qualsiasi azione nel servizio NetApp Disaster Recovery .
"Amministratore del failover del ripristino di emergenza"	Eseguire failover e migrazioni.
"Amministratore dell'applicazione Disaster Recovery"	Crea piani di replicazione, modifica i piani di replicazione e avvia i failover di prova.
"Visualizzatore di Disaster Recovery"	Visualizza solo le informazioni.
Visualizzatore di classificazione	Consente agli utenti di visualizzare i risultati della scansione NetApp Data Classification . Gli utenti con questo ruolo possono visualizzare le informazioni sulla conformità e generare report per le risorse per le quali hanno l'autorizzazione ad accedere. Questi utenti non possono abilitare o disabilitare la scansione di volumi, bucket o schemi di database. La classificazione non ha un ruolo amministrativo.
"Amministratore di Ransomware Resilience"	Gestisci le azioni nelle schede Proteggi, Avvisi, Ripristina, Impostazioni e Report di NetApp Ransomware Resilience.

Ruolo del servizio dati	Responsabilità
"Visualizzatore di resilienza ransomware"	Visualizza i dati del carico di lavoro, visualizza i dati degli avvisi, scarica i dati di ripristino e scarica i report in Ransomware Resilience.
"Comportamento utente di Ransomware Resilience amministratore"	Configura, gestisci e visualizza il rilevamento, gli avvisi e il monitoraggio dei comportamenti sospetti degli utenti in Ransomware Resilience.
"Visualizzatore del comportamento dell'utente di Ransomware Resilience"	Visualizza avvisi e approfondimenti sui comportamenti sospetti degli utenti in Ransomware Resilience.
Amministratore SnapCenter	Offre la possibilità di eseguire il backup di snapshot da cluster ONTAP locali utilizzando NetApp Backup and Recovery per le applicazioni. Un membro che ha questo ruolo può completare le seguenti azioni: * Completare qualsiasi azione da Backup e ripristino > Applicazioni * Gestire tutti i sistemi nei progetti e nelle cartelle per i quali dispone delle autorizzazioni * Utilizzare tutti i servizi NetApp Console SnapCenter non ha un ruolo di visualizzatore.

Link correlati

- "Scopri di più sulla gestione dell'identità e degli accessi NetApp Console"
- "Inizia con NetApp Console IAM"
- "Gestisci i membri NetApp Console e le relative autorizzazioni"
- "Scopri di più sull'API per NetApp Console IAM"

Ruoli di accesso alla piattaforma NetApp Console

Assegna ruoli di piattaforma agli utenti per concedere autorizzazioni per gestire la NetApp Console, assegnare ruoli, aggiungere utenti, creare agenti della console e gestire federazioni.

Esempio di ruoli organizzativi per una grande organizzazione multinazionale

XYZ Corporation organizza l'accesso all'archiviazione dei dati per regione (Nord America, Europa e Asia-Pacifico), garantendo un controllo regionale con supervisione centralizzata.

L'**amministratore dell'organizzazione** nella console di XYZ Corporation crea un'organizzazione iniziale e cartelle separate per ogni regione. L'**amministratore della cartella o del progetto** di ogni regione organizza i progetti (con le risorse associate) all'interno della cartella della regione.

Gli amministratori regionali con il ruolo di **Amministratore cartella o progetto** gestiscono attivamente le proprie cartelle aggiungendo risorse e utenti. Questi amministratori regionali possono anche aggiungere, rimuovere o rinominare le cartelle e i progetti che gestiscono. L'**amministratore dell'organizzazione** eredita le autorizzazioni per tutte le nuove risorse, mantenendo la visibilità dell'utilizzo dello spazio di archiviazione nell'intera organizzazione.

All'interno della stessa organizzazione, a un utente viene assegnato il ruolo di **Amministratore federazione** per gestire la federazione dell'organizzazione con il proprio IdP aziendale. Questo utente può aggiungere o rimuovere organizzazioni federate, ma non può gestire utenti o risorse all'interno dell'organizzazione. L'**amministratore dell'organizzazione** assegna a un utente il ruolo di **Visualizzatore federazione** per controllare lo stato della federazione e visualizzare le organizzazioni federate.

Le tabelle seguenti indicano le azioni che ciascun ruolo della piattaforma Console può eseguire.

Ruoli di amministrazione dell'organizzazione

Compito	Amministratore dell'organizzazione	Amministratore di cartelle o progetti
Crea agenti	SÌ	NO
Crea, modifica o elimina sistemi dalla Console (aggiungi o scopri sistemi)	SÌ	SÌ
Crea cartelle e progetti, inclusa l'eliminazione	SÌ	NO
Rinomina cartelle e progetti esistenti	SÌ	SÌ
Assegna ruoli e aggiungi utenti	SÌ	SÌ
Associare risorse a cartelle e progetti	SÌ	SÌ
Associare agenti a cartelle e progetti	SÌ	NO
Rimuovere gli agenti dalle cartelle e dai progetti	SÌ	NO
Gestire gli agenti (modificare certificati, impostazioni e così via)	SÌ	NO
Gestisci le credenziali da Amministrazione > Credenziali	SÌ	SÌ
Crea, gestisci e visualizza le federazioni	SÌ	NO
Registrati per ricevere supporto e invia casi tramite la Console	SÌ	SÌ
Utilizzare servizi dati non associati a un ruolo di accesso esplicito	SÌ	SÌ
Visualizza la pagina Audit e le notifiche	SÌ	SÌ

Ruoli della Federazione

Compito	Amministratore della Federazione	Visualizzatore della federazione
Creare una federazione	SÌ	NO
Verificare un dominio	SÌ	NO
Aggiungere un dominio a una federazione	SÌ	NO
Disattivare ed eliminare le federazioni	SÌ	NO
Federazioni di prova	SÌ	NO
Visualizza le federazioni e i loro dettagli	SÌ	SÌ

Ruoli di partnership

Compito	Amministratore della partnership	Visualizzatore di partnership
Può creare una partnership	SÌ	NO

Compito	Amministratore della partnership	Visualizzatore di partnership
Assegnare ruoli ai membri partner	SÌ	NO
Può aggiungere membri a una partnership	SÌ	NO
Può visualizzare i dettagli della partnership dell'organizzazione	SÌ	SÌ

Ruoli di super amministratore e visualizzatore

Il ruolo di **Super amministratore** fornisce accesso completo alla gestione delle funzionalità della Console, dell'archiviazione e dei servizi dati. Questo ruolo è adatto a coloro che supervisionano l'amministrazione e la governance. Al contrario, il ruolo **Super viewer** offre un accesso di sola lettura, ideale per revisori o stakeholder che necessitano di visibilità senza apportare modifiche.

Le organizzazioni dovrebbero utilizzare l'accesso **Super amministratore** con parsimonia per ridurre al minimo i rischi per la sicurezza e allinearsi al principio del privilegio minimo. La maggior parte delle organizzazioni dovrebbe assegnare ruoli ben definiti, con solo le autorizzazioni necessarie, per ridurre i rischi e migliorare la verificabilità.

Esempio per i ruoli super

ABC Corporation dispone di un piccolo team di cinque persone che sfrutta la NetApp Console per la gestione dei servizi dati e dello storage. Invece di distribuire più ruoli, assegnano il ruolo di **Super amministratore** a due membri senior del team che gestiscono tutte le attività amministrative, tra cui la gestione degli utenti e la configurazione delle risorse. Ai restanti tre membri del team viene assegnato il ruolo di **Super visualizzatore**, che consente loro di monitorare lo stato dell'archiviazione e del servizio dati senza la possibilità di modificare le impostazioni.

Ruolo	Ruoli ereditati
Super amministratore	• Amministratore dell'organizzazione • Amministratore di cartelle o progetti • Amministratore della Federazione • Amministratore della partnership • Amministratore di Ransomware Resilience • Amministratore del ripristino di emergenza • Super amministratore di backup • Amministratore di archiviazione • Amministratore Keystone • Amministratore di Google Cloud NetApp Volumes

Ruolo	Ruoli ereditati
Super spettatore	• Visualizzatore dell'organizzazione • Visualizzatore della federazione • Visualizzatore di partnership • Visualizzatore di resilienza ransomware • Visualizzatore di ripristino di emergenza • Visualizzatore di backup • Visualizzatore di archiviazione • Visualizzatore Keystone • Visualizzatore Google Cloud NetApp Volumes

Ruoli applicativi

Ruoli Google Cloud NetApp Volumes nella NetApp Console

È possibile assegnare il seguente ruolo agli utenti per consentire loro di accedere a Google Cloud NetApp Volumes nella NetApp Console.

Google Cloud NetApp Volumes utilizza il seguente ruolo:

- * Amministratore Google Cloud NetApp Volumes *: scopri e gestisci Google Cloud NetApp Volumes nella Console.
- * Visualizzatore Google Cloud NetApp Volumes *: visualizza Google Cloud NetApp Volumes nella Console.

Ruoli di accesso Keystone nella NetApp Console

I ruoli Keystone forniscono l'accesso alle dashboard Keystone e consentono agli utenti di visualizzare e gestire il proprio abbonamento Keystone . Esistono due ruoli Keystone : amministratore Keystone e visualizzatore Keystone . La differenza principale tra i due ruoli riguarda le azioni che possono intraprendere in Keystone. Il ruolo di amministratore Keystone è l'unico a cui è consentito creare richieste di servizio o modificare abbonamenti.

Esempio di ruoli Keystone nella NetApp Console

XYZ Corporation dispone di quattro tecnici di archiviazione provenienti da reparti diversi che visualizzano le informazioni sugli abbonamenti Keystone . Sebbene tutti questi utenti debbano monitorare l'abbonamento Keystone , solo il responsabile del team è autorizzato a effettuare richieste di assistenza. A tre membri del team viene assegnato il ruolo di * Keystone viewer*, mentre al responsabile del team viene assegnato il ruolo di * Keystone admin*, in modo che vi sia un punto di controllo sulle richieste di servizio per l'azienda.

La tabella seguente indica le azioni che ciascun ruolo Keystone può eseguire.

Caratteristica e azione	Amministratore Keystone	Visualizzatore Keystone
Visualizza le seguenti schede: Abbonamento, Risorse, Monitoraggio e Amministrazione	SÌ	SÌ
* Pagina di abbonamento Keystone *:		
Visualizza gli abbonamenti	SÌ	SÌ
Modificare o rinnovare gli abbonamenti	SÌ	NO
* Pagina delle risorse Keystone *:		
Visualizza risorse	SÌ	SÌ
Gestire le risorse	SÌ	NO
* Pagina degli avvisi Keystone *:		
Visualizza avvisi	SÌ	SÌ
Gestisci gli avvisi	SÌ	NO
Crea avvisi per te stesso	SÌ	SÌ
* Licenses and subscriptions*:		
Può visualizzare licenze e abbonamenti	SÌ	SÌ
* Pagina dei report Keystone *:		
Scarica i report	SÌ	SÌ
Gestisci i report	SÌ	SÌ
Crea report per te stesso	SÌ	SÌ
Richieste di servizio:		
Crea richieste di servizio	SÌ	NO
Visualizza le richieste di servizio create da qualsiasi utente all'interno dell'organizzazione	SÌ	SÌ

Ruolo di accesso dell'analista del supporto operativo per NetApp Console

È possibile assegnare agli utenti il ruolo di analista del supporto operativo per consentire loro di accedere ad avvisi e monitoraggio. Gli utenti con questo ruolo possono anche aprire casi di supporto.

Analista di supporto operativo

Compito	Può eseguire
Gestisci le tue credenziali utente da Impostazioni > Credenziali	SÌ
Visualizza le risorse scoperte	SÌ
Registrati per ricevere supporto e invia casi tramite la Console	SÌ
Visualizza la pagina Audit e le notifiche	SÌ
Visualizza, scarica e configura gli avvisi	SÌ

Ruoli di accesso all'archiviazione per NetApp Console

È possibile assegnare i seguenti ruoli agli utenti per consentire loro di accedere alle funzionalità di gestione dello storage nella NetApp Console. È possibile assegnare agli utenti un ruolo amministrativo per gestire l'archiviazione o un ruolo di visualizzatore per il monitoraggio.

Questi ruoli non sono disponibili dall'API di partnership NetApp Console .

Gli amministratori possono assegnare ruoli di archiviazione agli utenti per le seguenti risorse e funzionalità di archiviazione:

Risorse di archiviazione:

- Cluster ONTAP on-premise
- StorageGRID
- Serie E

Servizi e funzionalità della console:

- Consulente digitale
- Aggiornamenti software
- Pianificazione del ciclo di vita
- Sostenibilità

Esempio di ruoli di archiviazione nella NetApp Console

XYZ Corporation, una multinazionale, dispone di un ampio team di ingegneri e amministratori di storage. Consentono a questo team di gestire le risorse di archiviazione per le proprie regioni, limitando al contempo l'accesso alle attività principali della Console, come la gestione degli utenti, la creazione degli agenti e la gestione delle licenze.

All'interno di un team di 12 persone, a due utenti viene assegnato il ruolo di **Visualizzatore di archiviazione**, che consente loro di monitorare le risorse di archiviazione associate ai progetti della Console a cui sono assegnati. Ai restanti nove viene assegnato il ruolo di **Amministratore di storage**, che include la possibilità di gestire gli aggiornamenti software, accedere a ONTAP System Manager tramite la Console e scoprire le

risorse di storage (aggiungere sistemi). A una persona del team viene assegnato il ruolo di **Specialista dell'integrità del sistema**, in modo che possa gestire l'integrità delle risorse di storage nella propria regione, ma non modificare o eliminare alcun sistema. Questa persona può anche eseguire aggiornamenti software sulle risorse di archiviazione per i progetti a lei assegnati.

L'organizzazione dispone di altri due utenti con il ruolo di **Amministratore organizzazione** che possono gestire tutti gli aspetti della Console, tra cui la gestione degli utenti, la creazione degli agenti e la gestione delle licenze, nonché di diversi utenti con il ruolo di **Amministratore cartella o progetto** che possono eseguire attività di amministrazione della Console per le cartelle e i progetti a cui sono assegnati.

Nella tabella seguente vengono illustrate le azioni eseguite da ciascun ruolo di archiviazione.

Caratteristica e azione	Amministratore di archiviazione	Specialista in salute del sistema	Visualizzatore di archiviazione
Gestione dell'archiviazione:			
Scoprire nuove risorse (creare sistemi)	SÌ	SÌ	NO
Visualizza i sistemi scoperti	SÌ	SÌ	NO
Elimina i sistemi dalla Console	SÌ	NO	NO
Modificare i sistemi	SÌ	NO	NO
Crea agenti	NO	NO	NO
Consulente digitale			
Visualizza tutte le pagine e le funzioni	SÌ	SÌ	SÌ
* Licenses and subscriptions*			
Visualizza tutte le pagine e le funzioni	NO	NO	NO
Aggiornamenti software			
Visualizza la landing page e i consigli	SÌ	SÌ	SÌ
Esaminare le potenziali raccomandazioni sulla versione e i principali vantaggi	SÌ	SÌ	SÌ
Visualizza i dettagli di aggiornamento per un cluster	SÌ	SÌ	SÌ
Esegui controlli pre-aggiornamento e scarica il piano di aggiornamento	SÌ	SÌ	SÌ
Installa gli aggiornamenti software	SÌ	SÌ	NO
Pianificazione del ciclo di vita			
Esaminare lo stato di pianificazione della capacità	SÌ	SÌ	SÌ

Caratteristica e azione	Amministratore di archiviazione	Specialista in salute del sistema	Visualizzatore di archiviazione
Scegli l'azione successiva (migliore pratica, livello)	SÌ	NO	NO
Trasferisci i dati inattivi nell'archiviazione cloud e libera spazio di archiviazione	SÌ	SÌ	NO
Imposta promemoria	SÌ	SÌ	SÌ
Sostenibilità			
Visualizza dashboard e consigli	SÌ	SÌ	SÌ
Scarica i dati del report	SÌ	SÌ	SÌ
Modifica la percentuale di mitigazione del carbonio	SÌ	SÌ	NO
Correggi le raccomandazioni	SÌ	SÌ	NO
Rinviare le raccomandazioni	SÌ	SÌ	NO
Accesso al gestore del sistema			
Può inserire le credenziali	SÌ	SÌ	NO
Credenziali			
Credenziali utente	SÌ	SÌ	NO

Ruoli dei servizi dati

Ruoli NetApp Backup and Recovery nella NetApp Console

È possibile assegnare i seguenti ruoli agli utenti per consentire loro di accedere a NetApp Backup and Recovery all'interno della Console. I ruoli di backup e ripristino offrono la flessibilità di assegnare agli utenti un ruolo specifico per le attività che devono svolgere all'interno della tua organizzazione. Il modo in cui si assegnano i ruoli dipende dalle proprie pratiche aziendali e di gestione dell'archiviazione.

Il servizio utilizza i seguenti ruoli specifici di NetApp Backup and Recovery.

- **Super amministratore di Backup e Recovery**: esegue qualsiasi azione in NetApp Backup and Recovery.
- **Amministratore di backup e ripristino**: esegue backup su snapshot locali, replica su storage secondario ed esegue il backup su azioni di storage di oggetti in NetApp Backup and Recovery.
- **Amministratore di Backup e ripristino**: ripristina i carichi di lavoro utilizzando NetApp Backup and Recovery.
- **Amministratore di backup e ripristino Clone**: clona applicazioni e dati utilizzando NetApp Backup and Recovery.

- **Visualizzatore di backup e ripristino**: visualizza le informazioni in NetApp Backup and Recovery, ma non esegue alcuna azione.

Per i dettagli su tutti i ruoli di accesso NetApp Console , vedere "la documentazione di configurazione e amministrazione della console" .

Ruoli utilizzati per azioni comuni

La tabella seguente indica le azioni che ciascun ruolo NetApp Backup and Recovery può eseguire per tutti i carichi di lavoro.

Caratteristica e azione	Super amministratore di backup e ripristino	Backup e ripristino amministratore del backup	Backup e ripristino ripristino amministratore	Amministratore clone di backup e ripristino	Visualizzatore di backup e ripristino
Aggiungi, modifica o elimina host	SÌ	NO	NO	NO	NO
Installa i plugin	SÌ	NO	NO	NO	NO
Aggiungi credenziali (host, istanza, vCenter)	SÌ	NO	NO	NO	NO
Visualizza la dashboard e tutte le schede	SÌ	SÌ	SÌ	SÌ	SÌ
Inizia la prova gratuita	SÌ	NO	NO	NO	NO
Avviare la scoperta dei carichi di lavoro	NO	SÌ	SÌ	SÌ	NO
Visualizza le informazioni sulla licenza	SÌ	SÌ	SÌ	SÌ	SÌ
Attiva la licenza	SÌ	NO	NO	NO	NO
Visualizza gli host	SÌ	SÌ	SÌ	SÌ	SÌ
Orari:					
Attivare gli orari	SÌ	SÌ	SÌ	SÌ	NO
Sospendere gli orari	SÌ	SÌ	SÌ	SÌ	NO
Politiche e protezione:					
Visualizza i piani di protezione	SÌ	SÌ	SÌ	SÌ	SÌ

Caratteristica e azione	Super amministratore di backup e ripristino	Backup e ripristino amministratore del backup	Backup e ripristino ripristino amministratore	Amministratore clone di backup e ripristino	Visualizzatore di backup e ripristino
Creare, modificare o eliminare piani di protezione	SÌ	SÌ	NO	NO	NO
Ripristinare i carichi di lavoro	SÌ	NO	SÌ	NO	NO
Crea, dividi o elimina cloni	SÌ	NO	NO	SÌ	NO
Crea, modifica o elimina una policy	SÌ	SÌ	NO	NO	NO
Segnalazioni:					
Visualizza i report	SÌ	SÌ	SÌ	SÌ	SÌ
Crea report	SÌ	SÌ	SÌ	SÌ	NO
Elimina i report	SÌ	NO	NO	NO	NO
Importa da SnapCenter e gestisci l'host:					
Visualizza i dati SnapCenter importati	SÌ	SÌ	SÌ	SÌ	SÌ
Importa dati da SnapCenter	SÌ	SÌ	NO	NO	NO
Gestisci (migra) l'host	SÌ	SÌ	NO	NO	NO
Configura impostazioni:					
Configurare la directory dei registri	SÌ	SÌ	SÌ	NO	NO
Associare o rimuovere le credenziali dell'istanza	SÌ	SÌ	SÌ	NO	NO
Secchi:					
Visualizza i bucket	SÌ	SÌ	SÌ	SÌ	SÌ
Crea, modifica o elimina bucket	SÌ	SÌ	NO	NO	NO

Ruoli utilizzati per azioni specifiche del carico di lavoro

La tabella seguente indica le azioni che ciascun ruolo NetApp Backup and Recovery può eseguire per carichi di lavoro specifici.

Carichi di lavoro Kubernetes

Questa tabella indica le azioni che ciascun ruolo NetApp Backup and Recovery può eseguire per azioni specifiche dei carichi di lavoro Kubernetes.

Caratteristica e azione	Super amministratore di backup e ripristino	Backup e ripristino amministratore del backup	Backup e ripristino ripristino amministratore	Visualizzatore di backup e ripristino
Visualizza cluster, namespace, classi di archiviazione e risorse API	SÌ	SÌ	SÌ	SÌ
Aggiungi nuovi cluster Kubernetes	SÌ	SÌ	NO	NO
Aggiorna le configurazioni del cluster	SÌ	NO	NO	NO
Rimuovere i cluster dalla gestione	SÌ	NO	NO	NO
Visualizza le applicazioni	SÌ	SÌ	SÌ	SÌ
Creare e definire nuove applicazioni	SÌ	SÌ	NO	NO
Aggiorna le configurazioni dell'applicazione	SÌ	SÌ	NO	NO
Rimuovere le applicazioni dalla gestione	SÌ	SÌ	NO	NO
Visualizza le risorse protette e lo stato del backup	SÌ	SÌ	SÌ	SÌ
Crea backup e proteggi le applicazioni con policy	SÌ	SÌ	NO	NO
Rimuovi la protezione dalle app ed elimina i backup	SÌ	SÌ	NO	NO
Visualizza i punti di ripristino e i risultati del visualizzatore delle risorse	SÌ	SÌ	SÌ	SÌ

Caratteristica e azione	Super amministratore di backup e ripristino	Backup e ripristino amministratore del backup	Backup e ripristino ripristino amministratore	Visualizzatore di backup e ripristino
Ripristina le applicazioni dai punti di ripristino	SÌ	NO	SÌ	NO
Visualizza le policy di backup di Kubernetes	SÌ	SÌ	SÌ	SÌ
Creare policy di backup di Kubernetes	SÌ	SÌ	SÌ	NO
Aggiorna i criteri di backup	SÌ	SÌ	SÌ	NO
Elimina i criteri di backup	SÌ	SÌ	SÌ	NO
Visualizza gli hook di esecuzione e le sorgenti degli hook	SÌ	SÌ	SÌ	SÌ
Creare hook di esecuzione e sorgenti di hook	SÌ	SÌ	SÌ	NO
Aggiorna gli hook di esecuzione e le sorgenti degli hook	SÌ	SÌ	SÌ	NO
Eliminare gli hook di esecuzione e le sorgenti degli hook	SÌ	SÌ	SÌ	NO
Visualizza i modelli di hook di esecuzione	SÌ	SÌ	SÌ	SÌ
Creare modelli di hook di esecuzione	SÌ	SÌ	SÌ	NO
Aggiorna i modelli di hook di esecuzione	SÌ	SÌ	SÌ	NO
Elimina i modelli di hook di esecuzione	SÌ	SÌ	SÌ	NO
Visualizza i dashboard di riepilogo e analisi del carico di lavoro	SÌ	SÌ	SÌ	SÌ
Visualizza i bucket StorageGRID e le destinazioni di archiviazione	SÌ	SÌ	SÌ	SÌ

Ruoli NetApp Disaster Recovery nella NetApp Console

È possibile assegnare i seguenti ruoli agli utenti per consentire loro di accedere a NetApp

Disaster Recovery all'interno della Console. I ruoli di Disaster Recovery offrono la flessibilità di assegnare agli utenti un ruolo specifico per le attività che devono svolgere all'interno della tua organizzazione. Il modo in cui si assegnano i ruoli dipende dalle proprie pratiche aziendali e di gestione dell'archiviazione.

Il ripristino di emergenza utilizza i seguenti ruoli:

- **Amministratore del ripristino di emergenza**: Esegui qualsiasi azione.
- **Amministratore failover di disaster recovery**: esegue failover e migrazioni.
- **Amministratore dell'applicazione di ripristino di emergenza**: crea piani di replica. Modificare i piani di replicazione. Avviare i failover di prova.
- **Visualizzatore di ripristino di emergenza**: visualizza solo le informazioni.

La tabella seguente indica le azioni che ciascun ruolo può eseguire.

Caratteristica e azione	Amministratore del ripristino di emergenza	Amministratore del failover del ripristino di emergenza	Amministratore dell'applicazione di ripristino di emergenza	Visualizzatore di ripristino di emergenza
Visualizza la dashboard e tutte le schede	SÌ	SÌ	SÌ	SÌ
Inizia la prova gratuita	SÌ	NO	NO	NO
Avviare la scoperta dei carichi di lavoro	SÌ	NO	NO	NO
Visualizza le informazioni sulla licenza	SÌ	SÌ	SÌ	SÌ
Attiva la licenza	SÌ	NO	SÌ	NO
Nella scheda Siti:				
Visualizza i siti	SÌ	SÌ	SÌ	SÌ
Aggiungere, modificare o eliminare siti	SÌ	NO	NO	NO
Nella scheda Piani di replicazione:				
Visualizza i piani di replicazione	SÌ	SÌ	SÌ	SÌ
Visualizza i dettagli del piano di replicazione	SÌ	SÌ	SÌ	SÌ
Creare o modificare piani di replicazione	SÌ	SÌ	SÌ	NO
Crea report	SÌ	NO	NO	NO
Visualizza istantanee	SÌ	SÌ	SÌ	SÌ

Caratteristica e azione	Amministratore del ripristino di emergenza	Amministratore del failover del ripristino di emergenza	Amministratore dell'applicazione di ripristino di emergenza	Visualizzatore di ripristino di emergenza
Eseguire test di failover	SÌ	SÌ	SÌ	NO
Eseguire failover	SÌ	SÌ	NO	NO
Eseguire failback	SÌ	SÌ	NO	NO
Eseguire migrazioni	SÌ	SÌ	NO	NO
Nella scheda Gruppi di risorse:				
Visualizza gruppi di risorse	SÌ	SÌ	SÌ	SÌ
Crea, modifica o elimina gruppi di risorse	SÌ	NO	SÌ	NO
Nella scheda Monitoraggio lavori:				
Visualizza i lavori	SÌ	NO	SÌ	SÌ
Annulla lavori	SÌ	SÌ	SÌ	NO

Ruoli di accesso alla resilienza ransomware per NetApp Console

I ruoli di Ransomware Resilience forniscono agli utenti l'accesso a NetApp Ransomware Resilience. Ransomware Resilience supporta i seguenti ruoli:

Ruoli di base

- Amministratore di Ransomware Resilience: configura le impostazioni di Ransomware Resilience; esamina e rispondi agli avvisi di crittografia
- Visualizzatore di resilienza ransomware: visualizza incidenti di crittografia, report e impostazioni di rilevamento

Ruoli di attività comportamentali dell'utente"Rilevamento di attività sospette degli utenti" Gli avvisi forniscono visibilità sui dati, ad esempio sugli eventi di attività dei file; questi avvisi includono i nomi dei file e le azioni sui file (ad esempio Lettura, Scrittura, Eliminazione, Rinomina) eseguite dall'utente. Per limitare la visibilità di questi dati, solo gli utenti con questi ruoli possono gestire o visualizzare questi avvisi.

- Comportamento utente Ransomware Resilience - Attiva il rilevamento delle attività sospette degli utenti, indaga e rispondi agli avvisi di attività sospette degli utenti
- Visualizzatore del comportamento utente di Ransomware Resilience: visualizza gli avvisi sulle attività sospette degli utenti

I ruoli di comportamento dell'utente non sono ruoli autonomi; sono progettati per essere aggiunti ai ruoli di amministratore o visualizzatore di Ransomware Resilience. Per maggiori informazioni, vedere Ruoli comportamentali dell'utente.

Per descrizioni dettagliate di ciascun ruolo, consultare le tabelle seguenti.

Ruoli di base

Nella tabella seguente vengono descritte le azioni disponibili per i ruoli di amministratore e visualizzatore di Ransomware Resilience.

Caratteristica e azione	Amministratore di Ransomware Resilience	Visualizzatore di resilienza ransomware
Visualizza la dashboard e tutte le schede	SÌ	SÌ
Nella dashboard, aggiorna lo stato della raccomandazione	SÌ	NO
Inizia la prova gratuita	SÌ	NO
Avviare la scoperta dei carichi di lavoro	SÌ	NO
Avviare la riscoperta dei carichi di lavoro	SÌ	NO
Nella scheda Proteggi:		
Aggiungere, modificare o eliminare piani di protezione per le policy di *crittografia*	SÌ	NO
Proteggere i carichi di lavoro	SÌ	NO
Identificare l'esposizione ai dati sensibili con la classificazione dei dati	SÌ	NO
Elencare i piani di protezione e i dettagli	SÌ	SÌ
Elenca i gruppi di protezione	SÌ	SÌ
Visualizza i dettagli del gruppo di protezione	SÌ	SÌ
Crea, modifica o elimina gruppi di protezione	SÌ	NO
Scarica i dati	SÌ	SÌ
Nella scheda Avvisi:		
Visualizza gli avvisi di crittografia e i dettagli degli avvisi	SÌ	SÌ
Modifica lo stato dell'incidente di crittografia	SÌ	NO
Segnala l'avviso di crittografia per il ripristino	SÌ	NO
Visualizza i dettagli dell'incidente di crittografia	SÌ	SÌ

Caratteristica e azione	Amministratore di Ransomware Resilience	Visualizzatore di resilienza ransomware
Ignorare o risolvere gli incidenti di crittografia	SÌ	NO
Ottieni l'elenco completo dei file interessati dall'evento di crittografia	SÌ	NO
Scarica i dati degli avvisi degli eventi di crittografia	SÌ	SÌ
Blocca utente (con configurazione agente Workload Security)	SÌ	NO
Nella scheda Recupera:		
Scarica i file interessati dall'evento di crittografia	SÌ	NO
Ripristina il carico di lavoro dall'evento di crittografia	SÌ	NO
Scarica i dati di recupero dall'evento di crittografia	SÌ	SÌ
Scarica i report dall'evento di crittografia	SÌ	SÌ
Nella scheda Impostazioni:		
Aggiungere o modificare le destinazioni di backup	SÌ	NO
Elenca le destinazioni di backup	SÌ	SÌ
Visualizza gli obiettivi SIEM connessi	SÌ	SÌ
Aggiungere o modificare gli obiettivi SIEM	SÌ	NO
Configurare l'esercitazione di preparazione	SÌ	NO
Avvia, reimposta o modifica l'esercitazione di preparazione	SÌ	NO
Esaminare lo stato di preparazione dell'esercitazione	SÌ	SÌ
Aggiorna la configurazione di rilevamento	SÌ	NO
Visualizza la configurazione di rilevamento	SÌ	SÌ
Nella scheda Report:		
Scarica i report	SÌ	SÌ

Ruoli comportamentali dell'utente

Per configurare le impostazioni relative al comportamento sospetto degli utenti e rispondere agli avvisi, un utente deve disporre del ruolo di amministratore del comportamento utente di Ransomware Resilience. Per visualizzare solo gli avvisi relativi a comportamenti sospetti degli utenti, l'utente deve disporre del ruolo di visualizzatore del comportamento utente Ransomware Resilience.

I ruoli di comportamento dell'utente dovrebbero essere conferiti agli utenti con privilegi di amministratore o visualizzatore di Ransomware Resilience esistenti che necessitano di accesso a"impostazioni e avvisi di attività utente sospette" . Ad esempio, un utente con il ruolo di amministratore Ransomware Resilience dovrebbe ricevere il ruolo di amministratore del comportamento utente Ransomware Resilience per configurare gli agenti di attività utente e bloccare o sbloccare gli utenti. Il ruolo di amministratore del comportamento utente di Ransomware Resilience non deve essere conferito a un visualizzatore di Ransomware Resilience.

Per attivare il rilevamento delle attività sospette degli utenti, è necessario disporre del ruolo di amministratore dell'organizzazione della console.

Nella tabella seguente vengono descritte le azioni disponibili per i ruoli di amministratore e visualizzatore del comportamento utente di Ransomware Resilience.

Caratteristica e azione	Comportamento utente di Ransomware Resilience amministratore	Visualizzatore del comportamento dell'utente di Ransomware Resilience
Nella scheda Impostazioni:		
Crea, modifica o elimina l'agente di attività utente	SÌ	NO
Crea o elimina il connettore della directory utente	SÌ	NO
Metti in pausa o riprendi il raccoglitore dati	SÌ	NO
Eseguire un'esercitazione di preparazione alla violazione dei dati	SÌ	NO
Nella scheda Proteggi:		
Aggiungere, modificare o eliminare piani di protezione per le policy relative al *comportamento sospetto degli utenti*	SÌ	NO
Nella scheda Avvisi:		
Visualizza gli avvisi sulle attività degli utenti e i dettagli degli avvisi	SÌ	SÌ
Modifica lo stato dell'incidente dell'attività dell'utente	SÌ	NO
Contrassegna l'avviso di attività dell'utente per il ripristino	SÌ	NO
Visualizza i dettagli dell'incidente relativo all'attività dell'utente	SÌ	SÌ

Caratteristica e azione	Comportamento utente di Ransomware Resilience amministratore	Visualizzatore del comportamento dell'utente di Ransomware Resilience
Ignora o risolvi gli incidenti relativi alle attività degli utenti	SÌ	NO
Ottieni l'elenco completo dei file interessati dall'utente sospetto	SÌ	SÌ
Scarica i dati degli avvisi sugli eventi di attività dell'utente	SÌ	SÌ
Blocca o sblocca l'utente	SÌ	NO
Nella scheda Recupera:		
Scarica i file interessati dall'evento di attività dell'utente	SÌ	NO
Ripristina il carico di lavoro dall'evento di attività dell'utente	SÌ	NO
Scarica i dati di recupero dall'evento di attività dell'utente	SÌ	SÌ
Scarica i report dagli eventi di attività dell'utente	SÌ	SÌ

API di identità e accesso

ID organizzazione e progetto

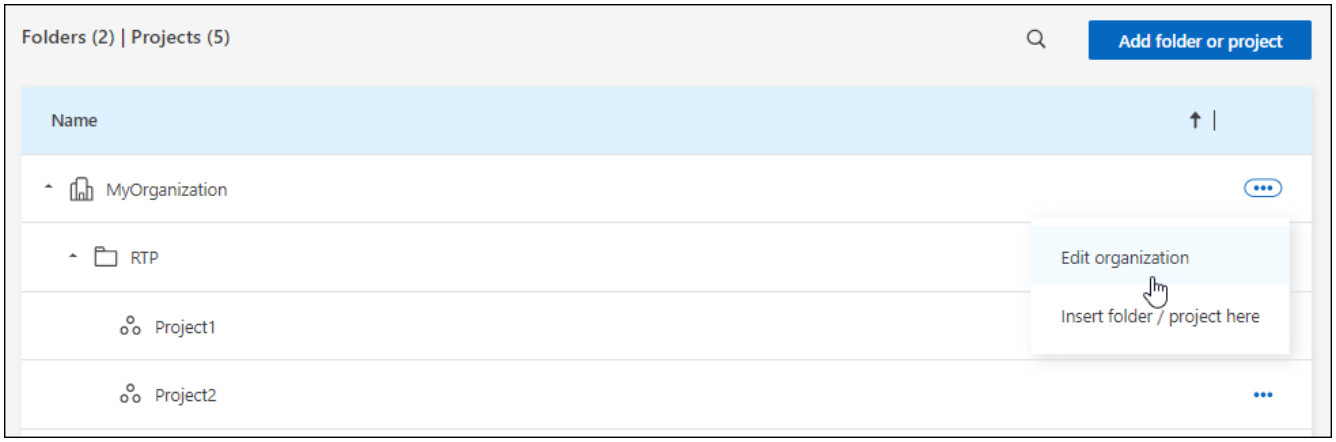
L'organizzazione NetApp Console ha un nome e un ID. Puoi scegliere un nome per la tua organizzazione che ti aiuti a identificarla. Potrebbe essere necessario recuperare anche l'ID dell'organizzazione per determinate integrazioni.

Rinomina la tua organizzazione

Puoi rinominare la tua organizzazione. Questa funzione è utile se si supporta più di un'organizzazione.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Organizzazione**.
3. Dalla pagina **Organizzazione**, vai alla prima riga della tabella, seleziona ••• e quindi seleziona **Modifica organizzazione**.



4. Inserisci un nuovo nome per l'organizzazione e seleziona **Applica**.

Ottieni l'ID dell'organizzazione

L'ID organizzazione viene utilizzato per determinate integrazioni con la Console.

Puoi visualizzare l'ID dell'organizzazione dalla pagina Organizzazioni e copiarlo negli appunti per le tue esigenze.

Passi

1. Selezionare **Amministrazione > Identità e accesso** > **Organizzazione**.
2. Nella pagina **Organizzazione**, cerca l'ID della tua organizzazione nella barra di riepilogo e copialo negli appunti. Puoi salvarlo per utilizzarlo in seguito oppure copiarlo direttamente dove ti serve.

Ottieni l'ID per un progetto

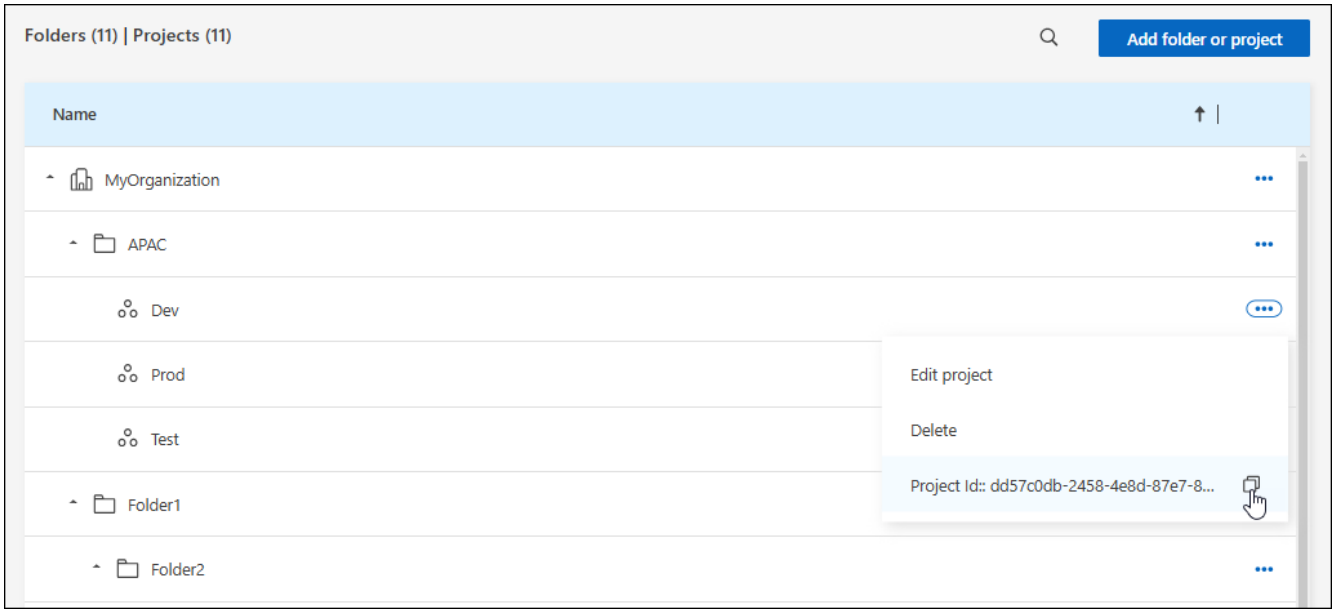
Se utilizzi l'API, dovrai ottenere l'ID per un progetto. Ad esempio, quando si crea un sistema Cloud Volumes ONTAP .

Passi

1. Dalla pagina **Organizzazione**, vai a un progetto nella tabella e seleziona •••

   Viene visualizzato l'ID del progetto.

2. Per copiare l'ID, selezionare il pulsante Copia.



Informazioni correlate

- "Scopri di più sulla gestione dell'identità e degli accessi"
- "Inizia con identità e accesso"
- "Scopri di più sull'API per l'identità e l'accesso"

Sicurezza e conformità

Federazione delle identità

Abilita l'accesso singolo utilizzando la federazione delle identità con NetApp Console

L'accesso Single Sign-On (federazione) semplifica il processo di accesso e migliora la sicurezza consentendo agli utenti di accedere alla NetApp Console utilizzando le proprie credenziali aziendali. Puoi abilitare l'accesso Single Sign-On (SSO) con il tuo provider di identità (IdP) o con il sito di supporto NetApp .

Ruolo richiesto

Amministratore dell'organizzazione, amministratore della federazione, visualizzatore della federazione."Scopri di più sui ruoli di accesso."

Single sign-on con il NetApp Support Site

La federazione con il sito di supporto NetApp consente agli utenti di accedere alla console, Active IQ Digital Advisor e ad altre app associate utilizzando le stesse credenziali.

Se esegui la federazione con il sito di supporto NetApp , non puoi eseguirla anche con il tuo provider di gestione dell'identità aziendale. Scegli quello più adatto alla tua organizzazione.

Passi

1. Scarica e completa il "Modulo di richiesta di federazione NetApp" .
2. Inviare il modulo all'indirizzo email specificato nel modulo.

Il team di supporto NetApp esamina ed elabora la tua richiesta.

Single sign-on con il tuo identity provider

È possibile impostare una connessione federata con il proprio provider di identità per abilitare l'accesso Single Sign-On (SSO) per la Console. Il processo prevede la configurazione del provider di identità in modo che consideri NetApp affidabile come fornitore di servizi e la successiva creazione della connessione nella Console.

Se in precedenza hai configurato la federazione utilizzando NetApp Cloud Central (un'applicazione esterna alla Console), devi importare la federazione utilizzando la pagina Federazione per gestirla all'interno della Console."Scopri come importare la tua federazione."

Provider di identità supportati

NetApp supporta i seguenti protocolli e provider di identità per la federazione:

Protocolli

- Provider di identità Security Assertion Markup Language (SAML)
- Servizi federativi di Active Directory (AD FS)

Fornitori di identità

- ID di accesso Microsoft
- PingFederate

Federazione con flusso di lavoro NetApp Console

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

Puoi effettuare la federazione con il tuo dominio di posta elettronica o con un dominio diverso di tua proprietà. Per federarti con un dominio diverso dal tuo dominio di posta elettronica, verifica innanzitutto di essere il proprietario del dominio.

Verifica il tuo dominio (se non stai utilizzando il tuo dominio di posta elettronica)

Per federarti con un dominio diverso dal tuo dominio di posta elettronica, verifica di esserne il proprietario. Puoi federare il tuo dominio di posta elettronica senza ulteriori passaggi.

Configura il tuo IdP in modo che consideri NetApp come fornitore di servizi attendibile

Configura il tuo provider di identità in modo che si fidi NetApp creando una nuova applicazione e fornendo dettagli come l'URL ACS, l'ID entità o altre informazioni sulle credenziali. Le informazioni sul fornitore di servizi variano a seconda del fornitore di identità, pertanto per maggiori dettagli fare riferimento alla documentazione del proprio fornitore di identità specifico. Per completare questo passaggio dovrai collaborare con l'amministratore dell'IdP.

Crea la connessione federata nella Console

Fornisci l'URL o il file dei metadati SAML dal tuo provider di identità per creare la connessione. Queste informazioni vengono utilizzate per stabilire la relazione di trust tra la Console e il tuo provider di identità. Le informazioni fornite dipendono dall'IdP utilizzato. Ad esempio, se si utilizza l'ID Microsoft Entra, è necessario fornire l'ID client, il segreto e il dominio.

4 Prova la tua federazione nella Console

Testa la tua connessione federata prima di abilitarla. Utilizzare l'opzione di test nella pagina Federazione nella Console per verificare che l'utente di prova possa autenticarsi correttamente. Se il test ha esito positivo, è possibile abilitare la connessione.

5 Abilita la tua connessione nella Console

Dopo aver abilitato la connessione, gli utenti potranno accedere alla Console utilizzando le proprie credenziali aziendali.

Per iniziare, rivedi l'argomento relativo al tuo protocollo o IdP:

- "Impostare una connessione federata con AD FS"
- "Imposta una connessione federata con Microsoft Entra ID"
- "Imposta una connessione federata con PingFederate"
- "Impostare una connessione federata con un provider di identità SAML"

Verifica del dominio

Verifica il dominio email per la tua connessione federata

Se desideri federarti con un dominio diverso dal tuo dominio di posta elettronica, devi prima verificare di essere il proprietario del dominio. Per la federazione è possibile utilizzare solo domini verificati.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

La verifica del tuo dominio comporta l'aggiunta di un record TXT alle impostazioni DNS del tuo dominio. Questo record viene utilizzato per dimostrare che sei il proprietario del dominio e consente alla NetApp Console di considerare attendibile il dominio per la federazione. Potrebbe essere necessario coordinarsi con l'amministratore IT o di rete per completare questo passaggio.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Seleziona **Verifica la proprietà del dominio**.
5. Inserisci il dominio che vuoi verificare e seleziona **Continua**.
6. Copiare il record TXT fornito.

7. Vai alle impostazioni DNS del tuo dominio e configura il valore TXT fornito come record TXT per il tuo dominio. Se necessario, collaborare con l'amministratore IT o di rete.
8. Dopo aver aggiunto il record TXT, tornare alla Console e selezionare **Verifica**.

Configurare le federazioni

Federare la NetApp Console con Active Directory Federation Services (AD FS)

Federa i tuoi servizi di federazione di Active Directory (AD FS) con la NetApp Console per abilitare l'accesso singolo (SSO) per la NetApp Console. Ciò consente agli utenti di accedere alla Console utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . NetApp consiglia di scegliere l'una o l'altra opzione, ma non entrambe.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa, configura il provider di identità in modo che consideri attendibile la NetApp Console come provider di servizi. Quindi, crea una connessione nella Console utilizzando la configurazione del tuo provider di identità.

È possibile configurare la federazione con il server AD FS per abilitare l'accesso Single Sign-On (SSO) per NetApp Console. Il processo prevede la configurazione di AD FS in modo che consideri attendibile la Console come fornitore di servizi e quindi la creazione della connessione nella NetApp Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
    a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
    b. Inserisci il nome della federazione che stai configurando.
    c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
5. Selezionare **Avanti**.
6. Per il metodo di connessione, seleziona **Protocollo** e poi seleziona **Active Directory Federation Services (AD FS)**.
7. Selezionare **Avanti**.
8. Crea un trust della relying party nel tuo server AD FS. È possibile utilizzare PowerShell o configurarlo manualmente sul server AD FS. Per informazioni dettagliate su come creare un trust relying party, consultare la documentazione di AD FS.
    a. Creare il trust utilizzando PowerShell utilizzando il seguente script:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

b. In alternativa, è possibile creare manualmente il trust nella console di gestione di AD FS. Utilizzare i seguenti valori NetApp Console durante la creazione del trust:

   - Quando si crea il Relying Trust Identifier, utilizzare il valore **YOUR_TENANT**: `netapp-cloud-account`
   - Quando selezioni **Abilita supporto per WS-Federation**, usa il valore **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`

c. Dopo aver creato il trust, copia l'URL dei metadati dal tuo server AD FS o scarica il file dei metadati della federazione. Questo URL o file ti servirà per completare la connessione nella Console.

NetApp consiglia di utilizzare l'URL dei metadati per consentire alla NetApp Console di recuperare automaticamente la configurazione AD FS più recente. Se scarichi il file dei metadati della federazione, dovrai aggiornarlo manualmente nella NetApp Console ogni volta che vengono apportate modifiche alla configurazione di AD FS.

9. Torna alla Console e seleziona **Avanti** per creare la connessione.
10. Creare la connessione con AD FS.
    a. Inserisci l'URL di AD FS copiato dal server AD FS nel passaggio precedente oppure carica il file dei metadati di federazione scaricato dal server AD FS.
11. Seleziona **Crea connessione**. La creazione della connessione potrebbe richiedere alcuni secondi.
12. Selezionare **Avanti**.
13. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

    Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

14. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
15. Imposta le notifiche.

    Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

16. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
17. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Federati con il tuo provider IdP Microsoft Entra ID per abilitare l'accesso Single Sign-On (SSO) per NetApp Console. Ciò consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . NetApp consiglia di scegliere l'una o l'altra opzione, ma non entrambe.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

È possibile impostare una connessione federata con Microsoft Entra ID per abilitare l'accesso Single Sign-On (SSO) per la Console. Il processo prevede la configurazione del tuo ID Microsoft Entra in modo che consideri attendibile la Console come fornitore di servizi e quindi la creazione della connessione nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.

Dettagli del dominio

1. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
2. Selezionare **Avanti**.

Metodo di connessione

1. Per il metodo di connessione, seleziona **Provider** e poi seleziona **Microsoft Entra ID**.
2. Selezionare **Avanti**.

Istruzioni di configurazione

1. Configura il tuo ID Microsoft Entra per considerare NetApp attendibile come fornitore di servizi. Devi eseguire questo passaggio sul tuo server Microsoft Entra ID.
   a. Utilizzare i seguenti valori durante la registrazione dell'app Microsoft Entra ID per considerare attendibile la console:
      - Per l'URL di reindirizzamento, utilizzare `https://services.cloud.netapp.com`
      - Per l'**URL di risposta**, usa `https://netapp-cloud-account.auth0.com/login/callback`

b. Crea un segreto client per la tua app Microsoft Entra ID. Per completare la federazione sarà necessario fornire l'ID client, il segreto client e il nome di dominio ID Entra.

2. Torna alla Console e seleziona **Avanti** per creare la connessione.

Crea connessione

1. Crea la connessione con Microsoft Entra ID
   a. Inserisci l'ID client e il segreto client creati nel passaggio precedente.
   b. Inserisci il nome di dominio dell'ID Microsoft Entra.
2. Seleziona **Crea connessione**. Il sistema crea la connessione in pochi secondi.

Testare e abilitare la connessione

1. Selezionare **Avanti**.
2. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

   Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

3. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
4. Imposta le notifiche.

   Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

5. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
6. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Federare la NetApp Console con PingFederate

Federati con il tuo provider IdP PingFederate per abilitare l'accesso singolo (SSO) per la NetApp Console. Ciò consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . NetApp consiglia di scegliere l'una o l'altra opzione, ma non entrambe.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

È possibile impostare una connessione federata con PingFederate per abilitare l'accesso singolo (SSO) per la Console. Il processo prevede la configurazione del server PingFederate in modo che consideri attendibile la Console come fornitore di servizi e quindi la creazione della connessione nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
5. Selezionare **Avanti**.
6. Per il metodo di connessione, seleziona **Provider** e poi seleziona **PingFederate**.
7. Selezionare **Avanti**.
8. Configura il tuo server PingFederate in modo che consideri NetApp affidabile come fornitore di servizi. Devi eseguire questo passaggio sul tuo server PingFederate.
   a. Utilizzare i seguenti valori quando si configura PingFederate per considerare attendibile la NetApp Console:
      - Per l'URL di risposta o l'URL del servizio consumatori di asserzione (ACS), utilizzare `https://netapp-cloud-account.auth0.com/login/callback`
      - Per l'URL di disconnessione, utilizzare `https://netapp-cloud-account.auth0.com/logout`
      - Per **ID pubblico/entità**, utilizzare `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` dove <fed-domain-name-pingfederate> è il nome di dominio della federazione. Ad esempio, se il tuo dominio è `example.com` , l'ID Pubblico/Entità sarebbe `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Copia l'URL del server PingFederate. Questo URL sarà necessario quando si crea la connessione nella Console.
   c. Scarica il certificato X.509 dal tuo server PingFederate. Deve essere in formato PEM codificato in Base64 (.pem, .crt, .cer).
9. Torna alla Console e seleziona **Avanti** per creare la connessione.
10. Crea la connessione con PingFederate
    a. Inserisci l'URL del server PingFederate che hai copiato nel passaggio precedente.
    b. Carica il certificato di firma X.509. Il certificato deve essere in formato PEM, CER o CRT.
11. Seleziona **Crea connessione**. Il sistema crea la connessione in pochi secondi.
12. Selezionare **Avanti**.
13. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

14. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
15. Imposta le notifiche.

    Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

16. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
17. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Federare con un provider di identità SAML

Federati con il tuo provider IdP SAML 2.0 per abilitare l'accesso Single Sign-On (SSO) per la console NEtApp. Ciò consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruolo richiesto

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . Non è possibile federarsi con entrambi.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

È possibile impostare una connessione federata con il provider SAML 2.0 per abilitare l'accesso Single Sign-On (SSO) per la Console. Il processo prevede la configurazione del provider in modo che consideri attendibile NetApp come fornitore di servizi e la successiva creazione della connessione nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
5. Selezionare **Avanti**.
6. Per il metodo di connessione, seleziona **Protocollo** e poi seleziona **Provider di identità SAML**.

7. Selezionare **Avanti**.
8. Configura il tuo provider di identità SAML in modo che consideri attendibile NetApp come fornitore di servizi. È necessario eseguire questo passaggio sul server del provider SAML.
   a. Assicurati che il tuo IdP abbia l'attributo `email` impostato sull'indirizzo email dell'utente. Ciò è necessario affinché la Console identifichi correttamente gli utenti:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. Utilizzare i seguenti valori quando si registra l'applicazione SAML con la Console:
   - Per l'URL di risposta o l'URL del servizio consumatori di asserzione (ACS), utilizzare `https://netapp-cloud-account.auth0.com/login/callback`
   - Per l'URL di disconnessione, utilizzare `https://netapp-cloud-account.auth0.com/logout`
   - Per **ID pubblico/entità**, utilizzare `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` dove <fed-domain-name-saml> è il nome di dominio che si desidera utilizzare per la federazione. Ad esempio, se il tuo dominio è `example.com` , l'ID Pubblico/Entità sarebbe `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
2. Dopo aver creato il trust, copia i seguenti valori dal server del tuo provider SAML:
   - URL di accesso
   - URL di disconnessione (facoltativo)
3. Scarica il certificato X.509 dal server del tuo provider SAML. Deve essere in formato PEM, CER o CRT.
   a. Torna alla Console e seleziona **Avanti** per creare la connessione.
   b. Creare la connessione con SAML.
4. Inserisci l'**URL di accesso** del tuo server SAML.
5. Carica il certificato X.509 che hai scaricato dal server del tuo provider SAML.
6. Facoltativamente, inserisci l'**URL di disconnessione** del tuo server SAML.
   a. Seleziona **Crea connessione**. Il sistema crea la connessione in pochi secondi.
   b. Selezionare **Avanti**.
   c. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

> Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

d. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.

e. Imposta le notifiche.

   Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

f. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.

g. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Gestire le federazioni

Gestisci le federazioni nella NetApp Console

Puoi gestire la tua federazione nella NetApp Console. Puoi disattivarlo, aggiornare le credenziali scadute e anche disattivarlo se non ti serve più.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi anche aggiungere un ulteriore dominio verificato a una federazione esistente, il che ti consente di utilizzare più domini per la tua connessione federata.

- Se hai configurato la federazione utilizzando NetApp Cloud Central, importala tramite la pagina **Federazione** per gestirla nella Console."Scopri come importare la tua federazione"
- È possibile visualizzare gli eventi di gestione della federazione, come l'abilitazione, la disabilitazione e l'aggiornamento delle federazioni, nella pagina Audit. "Scopri di più sulle operazioni di monitoraggio nella NetApp Console."

Abilitare una federazione

Se hai creato una federazione ma non è abilitata, puoi abilitarla tramite la pagina **Federazione**. L'abilitazione di una federazione consente agli utenti associati alla federazione di accedere alla Console utilizzando le proprie credenziali aziendali. Creare e testare correttamente la federazione prima di abilitarla.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Seleziona il menu azioni ••• accanto alla federazione che vuoi abilitare e seleziona **Abilita**.

Aggiungi un dominio verificato a una federazione esistente

È possibile aggiungere un dominio verificato a una federazione esistente nella Console per utilizzare più domini con lo stesso provider di identità (IdP).

Prima di poterlo aggiungere a una federazione, è necessario aver già verificato il dominio nella Console. Se non hai ancora verificato il dominio, puoi farlo seguendo i passaggi in"Verifica il tuo dominio nella Console" .

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Seleziona il menu azioni: accanto alla federazione a cui vuoi aggiungere un dominio verificato e seleziona **Aggiorna domini**. Nella finestra di dialogo **Aggiorna domini** viene visualizzato il dominio già associato a questa federazione.
4. Seleziona un dominio verificato dall'elenco dei domini disponibili.
5. Selezionare **Aggiorna**. I nuovi utenti del dominio possono ottenere l'accesso alla Console federata entro 30 secondi.

Aggiornamento di una connessione federata in scadenza

È possibile aggiornare i dettagli di una federazione nella Console. Ad esempio, sarà necessario aggiornare la federazione se le credenziali, come un certificato o un segreto client, scadono. Se necessario, aggiorna la data di notifica per ricordarti di aggiornare la connessione prima che scada.

Aggiornare prima la Console prima di aggiornare l'IdP per evitare problemi di accesso. Rimani connesso alla Console durante il processo.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Selezionare il menu azioni (tre punti verticali) accanto alla federazione che si desidera aggiornare e selezionare **Aggiorna federazione**.
4. Aggiornare i dettagli della federazione secondo necessità.
5. Selezionare **Aggiorna**.

Testare una federazione esistente

Testare la connessione di una federazione esistente per verificarne il funzionamento. Ciò può aiutarti a identificare eventuali problemi con la federazione e a risolverli.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Seleziona il menu azioni: accanto alla federazione a cui vuoi aggiungere un dominio verificato e seleziona **Test connessione**.
4. Selezionare **Test**. Il sistema ti chiederà di accedere con le tue credenziali aziendali. Se la connessione riesce, verrai reindirizzato alla NetApp Console. Se la connessione fallisce, viene visualizzato un messaggio di errore che indica il problema con la federazione.
5. Selezionare **Fine** per tornare alla scheda **Federazione**.

Disattivare una federazione

Se non hai più bisogno di una federazione, puoi disattivarla. Ciò impedisce agli utenti associati alla federazione di accedere alla Console utilizzando le proprie credenziali aziendali. Se necessario, potrai riattivare la federazione in un secondo momento.

Disattivare una federazione prima di eliminarla, ad esempio quando si dismette l'IdP o si interrompe la federazione. Ciò consente di riattivarlo in seguito, se necessario.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Seleziona il menu azioni ⋮ accanto alla federazione a cui vuoi aggiungere un dominio verificato e seleziona **Disabilita**.

Elimina una federazione

Se non hai più bisogno di una federazione, puoi eliminarla. In questo modo si rimuove la federazione e si impedisce agli utenti ad essa associati di accedere alla Console utilizzando le proprie credenziali aziendali. Ad esempio, se l'IdP viene dismesso o se la federazione non è più necessaria.

Non è possibile recuperare una federazione dopo averla eliminata. Devi creare una nuova federazione.

ⓘ È necessario disattivare una federazione prima di poterla eliminare. Non è possibile ripristinare una federazione dopo averla eliminata.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazioni** per visualizzare la pagina **Federazioni**.
3. Seleziona il menu azioni ⋮ accanto alla federazione a cui vuoi aggiungere un dominio verificato e seleziona **Elimina**.

Importa la tua federazione nella NetApp Console

Se in precedenza hai configurato la federazione tramite NetApp Cloud Central (un'applicazione esterna alla NetApp Console), la pagina Federazione ti chiederà di importare la tua connessione federata esistente nella Console, in modo da poterla gestire nella nuova interfaccia. Potrai quindi sfruttare i miglioramenti più recenti senza dover ricreare la tua connessione federata.

ⓘ Dopo aver importato la federazione esistente, puoi gestirla dalla pagina **Federazioni**."Scopri di più sulla gestione delle federazioni."

Ruolo richiesto

Amministratore dell'organizzazione o amministratore della federazione."Scopri di più sui ruoli di accesso."

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Selezionare **Importa federazione**.

Applica le autorizzazioni ONTAP per ONTAP Advanced View (ONTAP System Manager)

Per impostazione predefinita, le credenziali dell'agente della console consentono agli utenti di accedere alla Visualizzazione avanzata (ONTAP System Manager). In alternativa, è possibile richiedere agli utenti le credenziali ONTAP . Ciò garantisce che le autorizzazioni ONTAP di un utente vengano applicate quando lavora con cluster ONTAP sia in Cloud Volumes ONTAP che in cluster ONTAP on-premises.

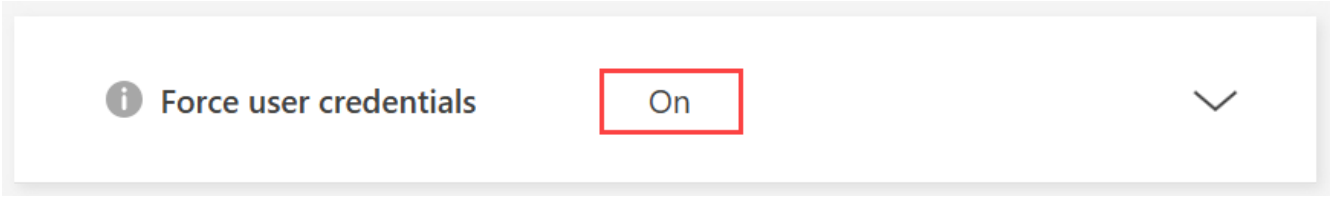
Per modificare le impostazioni dell'agente della console, è necessario disporre del ruolo di amministratore dell'organizzazione.

Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona il menu azioni per un agente della console e seleziona **Modifica agente**.

   Per modificarlo, l'agente della console deve essere attivo.

3. Espandi l'opzione **Forza credenziali**.
4. Selezionare la casella di controllo per abilitare l'opzione **Forza credenziali**, quindi selezionare **Salva**.
5. Verificare che l'opzione **Forza credenziali** sia abilitata.



Abilita la modalità di sola lettura per un'organizzazione NetApp Console

Come misura di sicurezza, puoi abilitare la modalità di sola lettura per la tua organizzazione NetApp Console . In modalità di sola lettura, gli utenti possono visualizzare risorse e impostazioni, ma non possono apportare modifiche.

In modalità di sola lettura, gli utenti con ruoli di amministratore devono elevare manualmente le proprie autorizzazioni per apportare modifiche, il che garantisce che le modifiche siano intenzionali.

Ruoli di accesso richiesti

Super amministratore o amministratore dell'organizzazione.

Abilita la modalità di sola lettura per l'organizzazione della tua console

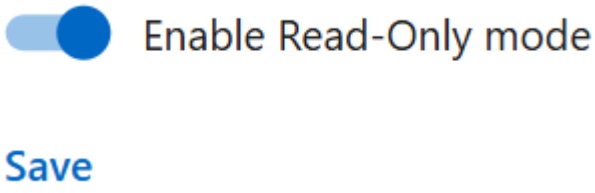
Abilita la modalità di sola lettura per limitare le modifiche all'organizzazione della tua Console. Tutti gli utenti possono comunque visualizzare le risorse. Gli utenti con ruoli di amministratore non possono eseguire alcuna azione nella Console senza elevare manualmente le proprie autorizzazioni.

Quando la modalità di sola lettura è abilitata, gli utenti visualizzano un banner che li informa che l'organizzazione è in modalità di sola lettura. Gli utenti devono accedere alle Impostazioni utente per elevare il

proprio ruolo.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Dalla scheda **Organizzazioni**, seleziona **Modifica impostazioni organizzazione** per l'organizzazione che desideri impostare in modalità di sola lettura.
3. Nella sezione **Modalità di sola lettura**, abilita la modalità di sola lettura spostando l'interruttore sulla posizione **On** e quindi seleziona **Salva**.



Registrati a NetApp Console come amministratore iniziale dell'organizzazione

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

Passi

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

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

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

      Nel modulo di registrazione sono ammessi solo caratteri inglesi.

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

      Verifica il tuo indirizzo email per completare la registrazione.

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

+ Se sei un amministratore alle prime armi, segui la procedura guidata per aggiungere spazio di archiviazione, creare un agente della console e altro ancora. "Scopri come utilizzare l'Assistente Console."

Prossimi passi

In qualità di amministratore, dopo aver completato i passaggi inclusi in Console Assistant, dovresti pianificare

la tua strategia di identità e accesso, aggiungere utenti alla tua organizzazione e assegnare ruoli. "Scopri di più sulla gestione dell'identità e degli accessi per NetApp Console"

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

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

Passi

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

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

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

      Nel modulo di registrazione sono ammessi solo caratteri inglesi.

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

      Verifica il tuo indirizzo email per completare la registrazione.

4. Dopo aver effettuato l'accesso, leggere e accettare il Contratto di licenza con l'utente finale.
5. Se il sistema ti chiede di creare un'organizzazione, chiudi la finestra di dialogo e contatta un amministratore della Console affinché possa aggiungerti all'organizzazione della Console e concederti l'accesso. "Scopri come contattare un amministratore dell'organizzazione."

Prossimi passi

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

Gestire le partnership organizzative

Partnership organizzative in NetApp Console

La creazione di partnership tra organizzazioni nella NetApp Console consente ai partner di gestire in modo sicuro le risorse NetApp oltre i confini aziendali, semplificando la collaborazione e migliorando la sicurezza.

Ruoli richiesti

Amministratore della partnership"Scopri di più sui ruoli di accesso."

Le partnership consentono una gestione sicura delle risorse NetApp tra le organizzazioni utilizzando relazioni basate sui ruoli nella Console. L'organizzazione che avvia l'operazione concede l'accesso alle proprie risorse, mentre l'organizzazione che accetta fornisce gli utenti o gli account di servizio a cui concedere l'accesso. Le partnership vengono stabilite tramite un flusso di lavoro self-service, che offre all'organizzazione che le avvia il

controllo completo sulle risorse condivise, sui ruoli assegnati e sulla possibilità di integrare, gestire o revocare l'accesso dei partner in base alle necessità.

I clienti possono autorizzare MSP o rivenditori a gestire gli ambienti NetApp senza dover eseguire configurazioni complesse. I clienti possono controllare a quali cluster i partner possono accedere e quali ruoli hanno, e possono revocare l'accesso in qualsiasi momento per mantenere la sicurezza e la conformità.

In qualità di partner, ottieni visibilità e controllo centralizzati su tutti gli ambienti dei clienti. È possibile passare facilmente all'organizzazione di un cliente per gestire le risorse, eseguire servizi dati e monitorare lo stato entro limiti definiti, riducendo gli strumenti personalizzati e garantendo l'allineamento con le policy di ciascun cliente.

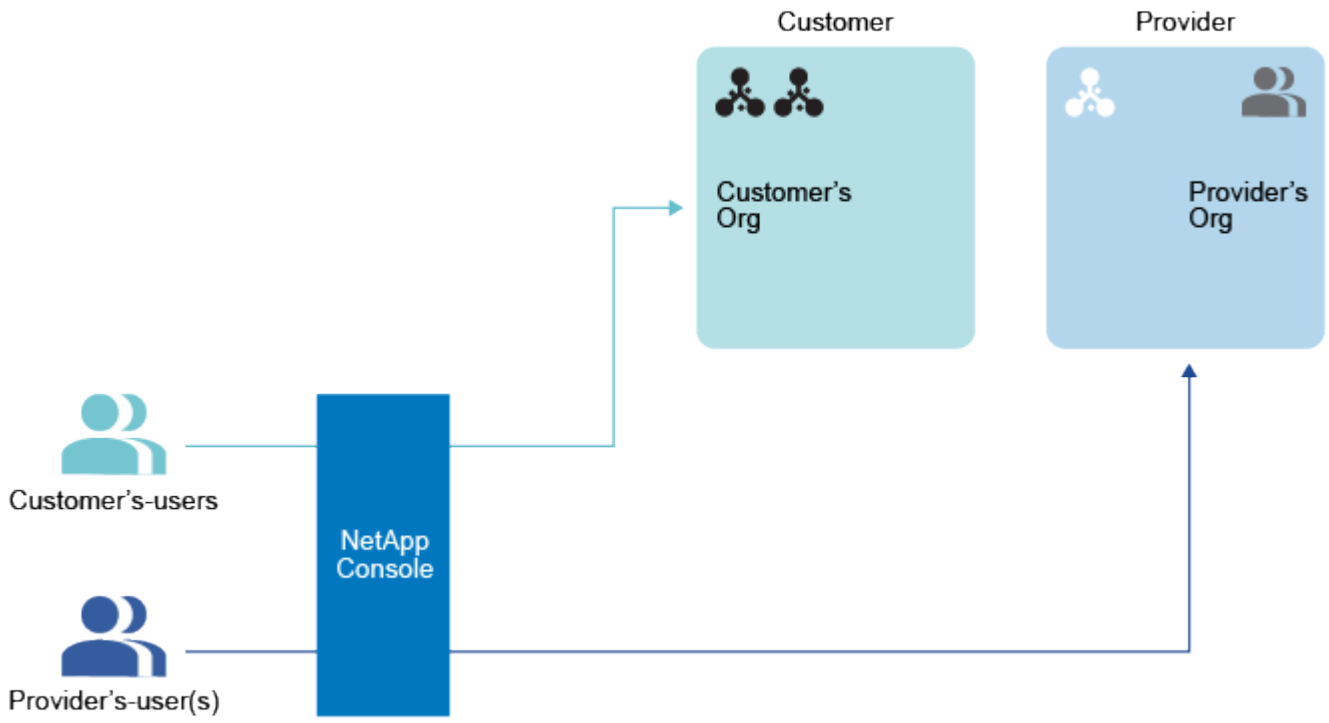
1 Assegnare a uno o più utenti il ruolo di amministratore della partnership

Assegna a uno o più utenti, sia nell'organizzazione di avvio che in quella di ricezione, il ruolo Partnership admin per creare e gestire le partnership. Puoi assegnare il ruolo Partnership viewer agli utenti che devono solo visualizzare le partnership e non gestirle.

2 Condividi l'ID della tua organizzazione con l'organizzazione che ha avviato l'operazione

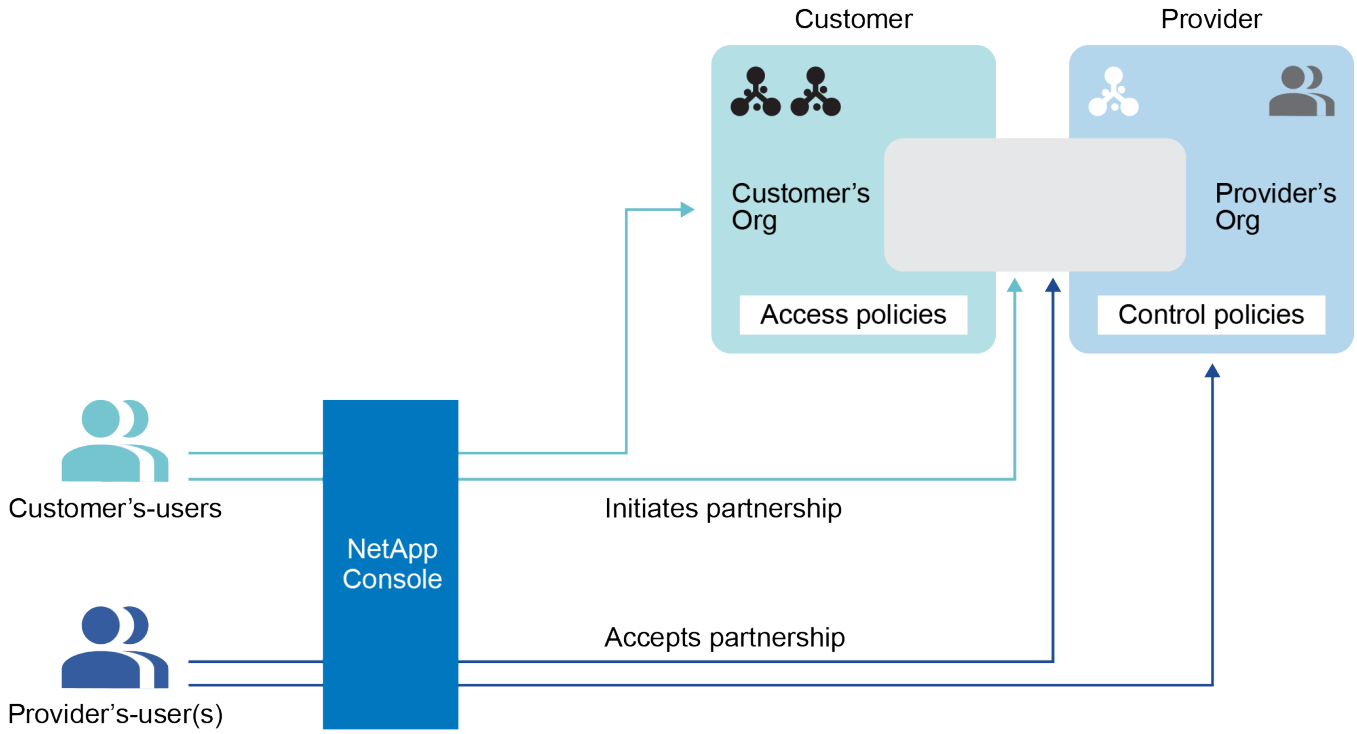
Per avviare una partnership, l'iniziatore deve conoscere l'ID dell'organizzazione di destinazione. Solo la rispettiva organizzazione può accedere a questo ID organizzazione. Condividilo direttamente con l'organizzazione che lo ha avviato al di fuori della NetApp Console tramite e-mail o un altro metodo.

L'organizzazione che avvia l'iniziativa è l'organizzazione che concede l'accesso alle proprie risorse.



3 Avviare la partnership all'interno di NetApp Console

L'organizzazione che avvia la partnership lo fa dall'interno della NetApp Console inviando una richiesta di partnership.



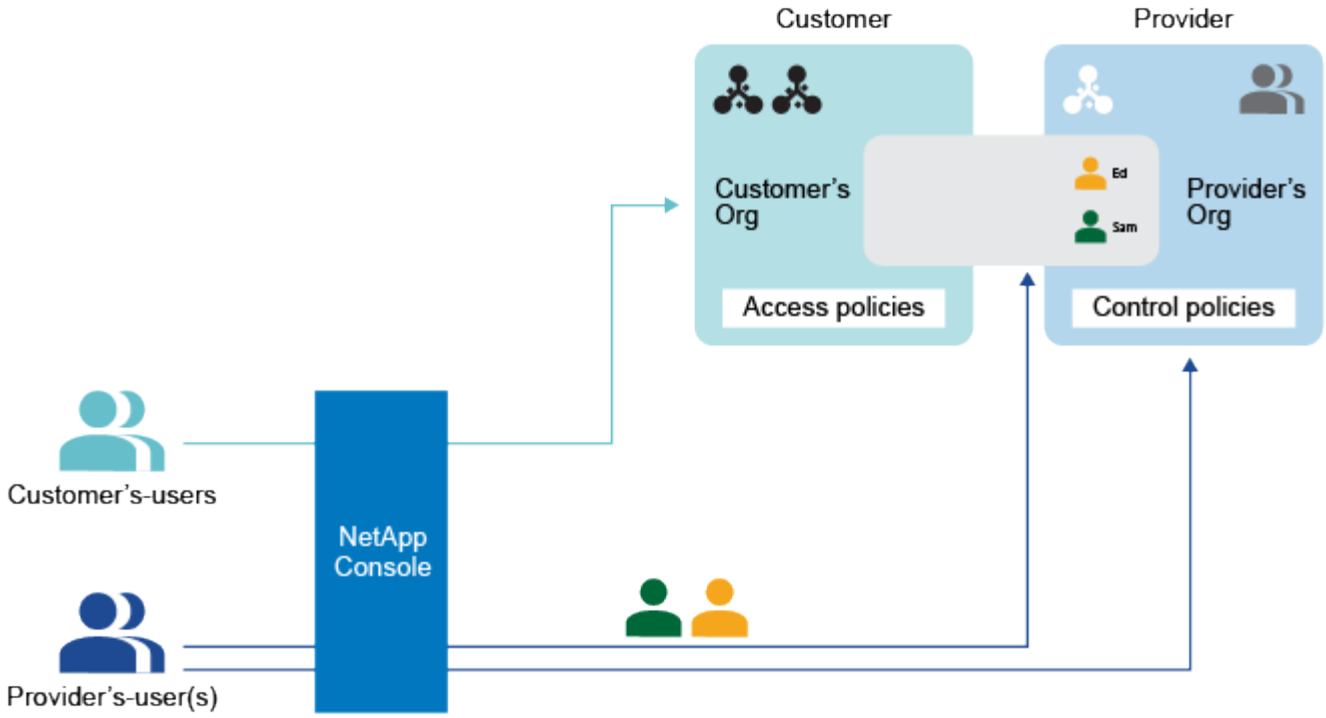
4 **Approvare la partnership**

L'organizzazione ricevente deve accettare la richiesta.

L'organizzazione ricevente è l'organizzazione a cui viene concesso l'accesso alle risorse.

5 **Assegnare gli utenti alla partnership**

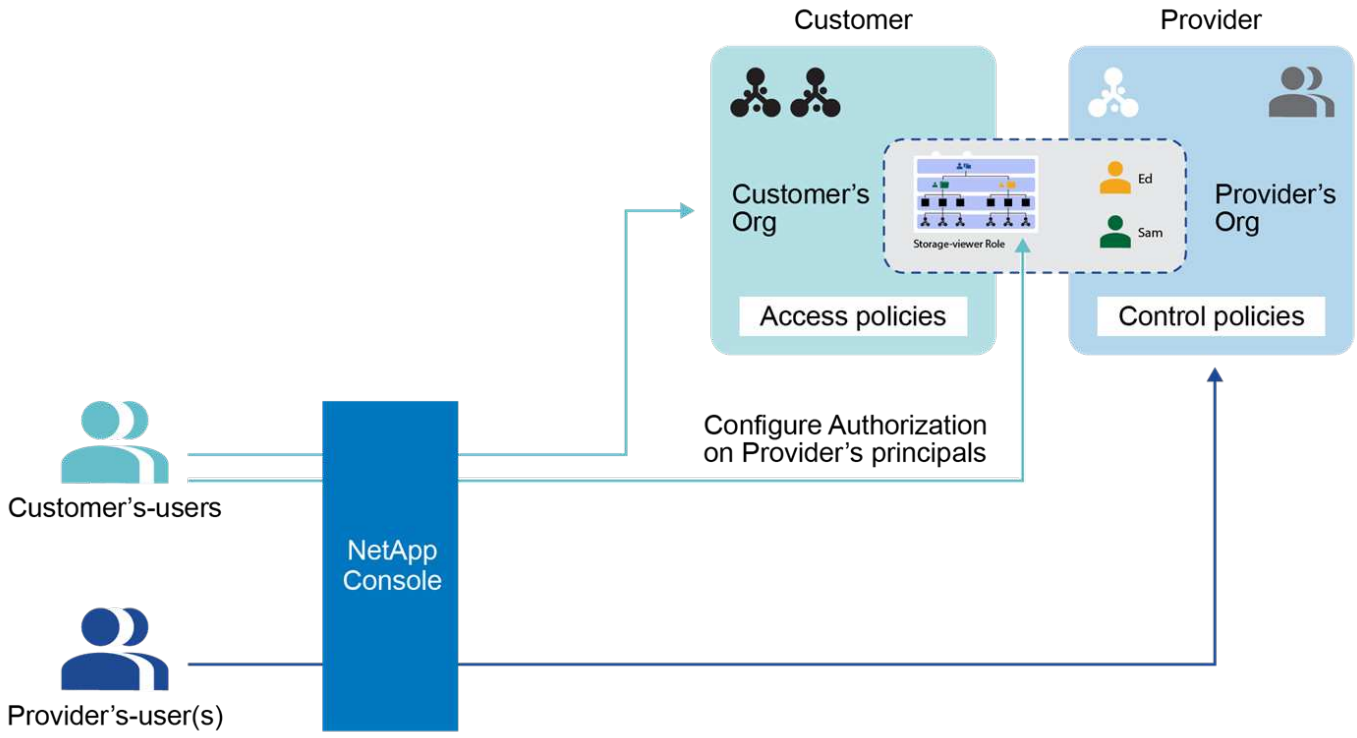
L'organizzazione ricevente assegna utenti o account di servizio specifici dalla tua organizzazione alla partnership. L'organizzazione che avvia l'operazione assegna i ruoli a questi utenti.



6 **Concedi agli utenti assegnati l'accesso alle risorse**

Se sei l'organizzazione che avvia la partnership, puoi concedere l'accesso a risorse specifiche agli utenti assegnati alla partnership. Puoi revocare l'accesso in qualsiasi momento.

Ciò è possibile assegnando ruoli a progetti o cartelle specifici all'interno della propria organizzazione.



Gestisci le partnership nella NetApp Console

Crea partnership per stabilire connessioni sicure e gestite tra la tua organizzazione e partner fidati per una gestione collaborativa delle risorse NetApp .

Le partnership consentono di gestire in modo sicuro le risorse NetApp oltre i confini, con relazioni basate sui ruoli nella Console. L'organizzazione che avvia l'operazione concede l'accesso alle proprie risorse, mentre l'organizzazione che accetta fornisce gli utenti o gli account di servizio a cui concedere l'accesso. Le partnership vengono stabilite tramite un flusso di lavoro self-service, che offre all'organizzazione che le avvia il controllo completo sulle risorse condivise, sui ruoli assegnati e sulla possibilità di integrare, gestire o revocare l'accesso dei partner in base alle necessità.

Ruoli richiesti

Il ruolo di **Amministratore partnership** è necessario per creare e gestire le partnership. Il **Visualizzatore partnership** può visualizzare la pagina Partnership."Scopri di più sui ruoli di accesso."

Avviare una partnership organizzativa

Puoi richiedere una partnership con un'altra organizzazione se conosci il suo ID organizzazione. L'organizzazione ricevente approva la richiesta prima che la partnership possa procedere.

Prima di iniziare, assicurati di avere l'ID organizzazione dell'organizzazione partner e di aver ricevuto il ruolo di **Amministratore della partnership**.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Partnership**.
3. Seleziona **Aggiungi partnership**.
4. Nella finestra di dialogo **Crea partnership**, immettere l'ID dell'organizzazione partner del partner richiesto e selezionare **Aggiungi**.

   La richiesta di partnership viene inviata all'organizzazione partner per l'approvazione. Puoi visualizzare lo stato della richiesta di partnership nella pagina **Partnership**.

Approvare una partnership organizzativa

La richiesta di partenariato tra organizzazioni deve essere accettata dall'organizzazione ricevente prima che il partenariato possa procedere. Per approvare e gestire le partnership è necessario disporre del ruolo di **Amministratore partnership**.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Partnership**.
3. Selezionare la scheda **Partnership ricevuta**.
4. Passare alla partnership ricevuta che si desidera approvare e selezionare ••• e quindi seleziona **Approva**.
5. Esaminare i dettagli della partnership, tra cui il nome e l'ID dell'organizzazione che ha richiesto la partnership, quindi selezionare **Avanti.**
6. Facoltativo, aggiungi i membri dell'organizzazione alla partnership e seleziona **Applica**.

Puoi aggiungere altri membri in qualsiasi momento tramite la pagina **Partnership**.

> Tutti i membri aggiunti diventano visibili nell'organizzazione del partner, dove il partner può assegnarli alle risorse.

Risultato

La partnership che hai approvato ora mostra lo stato **Costituita**. Gli utenti con i ruoli **Amministratore partnership** o **Visualizzatore partnership** in entrambe le organizzazioni possono visualizzare la partnership.

Visualizza lo stato della partnership

Visualizza lo stato delle tue partnership.

Ruolo richiesto

Amministratore della partnership, Visualizzatore della partnership."Scopri di più sui ruoli di accesso."

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Partnership**.
3. Selezionare la scheda **Partnership avviate** o **Partnership ricevute**.
4. Esaminare la tabella corrispondente che mostra le partnership e i relativi stati.

Disattivare una partnership organizzativa

Per disattivare una partnership è necessario essere membri dell'organizzazione che ha avviato la collaborazione. La disattivazione di una partnership revoca immediatamente l'accesso a tutte le risorse della tua organizzazione che erano condivise con l'organizzazione partner.

Ruolo richiesto

Amministratore della partnership."Scopri di più sui ruoli di accesso."

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Partnership**.
3. Selezionare la scheda **Partnership avviate**.
4. Esaminare la tabella corrispondente che mostra le partnership e i relativi stati.
5. Passare alla partnership avviata che si desidera disattivare e selezionare ••• e quindi seleziona **Disabilita**.

Gestire i membri di un'organizzazione di partnership

È possibile aggiungere utenti a una partnership aggiungendoli all'organizzazione partner. Dopo aver aggiunto gli utenti, l'organizzazione partner è tenuta ad assegnare loro ruoli per risorse specifiche nella propria organizzazione.

Ruoli richiesti

Il ruolo di **Amministratore partnership** è necessario per creare e gestire le partnership. Il **Visualizzatore partnership** può visualizzare la pagina Partnership."Scopri di più sui ruoli di accesso."

Puoi rimuovere gli utenti da una partnership in qualsiasi momento. La rimozione di un utente da una partnership revoca immediatamente il suo accesso a tutte le risorse nell'organizzazione partner.

Aggiungere membri a una partnership

Quando si aggiungono membri a una partnership, l'**amministratore della partnership** dell'organizzazione partner deve assegnare loro ruoli per risorse specifiche nella propria organizzazione prima che possano accedere a tali risorse.

Dopo aver aggiunto membri a una partnership, i membri vengono visualizzati come membri nell'organizzazione partner, dove il partner può assegnarli alle risorse.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Partnership**.
3. Selezionare la scheda **Partnership ricevuta**.
4. Seleziona il menu azioni ••• accanto alla partnership consolidata di cui vuoi aggiungere i membri e seleziona **Aggiungi membri**.
5. Scegli uno o più membri da aggiungere alla partnership e seleziona **Aggiungi**.

Rimuovere i membri da una partnership

Puoi rimuovere i membri da una partnership in qualsiasi momento. La rimozione di un utente da una partnership revoca immediatamente il suo accesso a tutte le risorse nell'organizzazione partner.

Se si desidera modificare il ruolo di un membro o le risorse a cui può accedere, l'amministratore della partnership dell'organizzazione partner deve apportare tali modifiche.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Partnership**.
3. Selezionare la scheda **Partnership ricevuta**.
4. Seleziona il menu azioni ••• accanto al membro che vuoi rimuovere e seleziona **Rimuovi associazione**.
5. Confermare l'azione selezionando **Rimuovi** nella finestra di dialogo.

Visualizza le informazioni sul ruolo di un utente

È possibile visualizzare il ruolo assegnato a un utente e le risorse associate.

Non è possibile modificare il ruolo associato a un utente. In caso di domande sulle risorse o sul ruolo fornito, contattare l'amministratore dell'organizzazione partner.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Partnership**.
3. Selezionare la scheda **Partnership ricevuta**.
4. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
5. Nella tabella, espandi la riga corrispondente all'organizzazione, alla cartella o al progetto in cui desideri visualizzare il ruolo assegnato al membro e seleziona il numero nella colonna **Ruolo**.

Fornire l’accesso alle risorse agli utenti della partnership

Puoi concedere l’accesso agli utenti partner assegnando loro ruoli specifici per cartelle e progetti all’interno della tua organizzazione.

Ruoli richiesti

Amministratore della partnership."Scopri di più sui ruoli di accesso."

Un’organizzazione partner deve prima aggiungere membri alla partnership prima che tu possa assegnare loro ruoli per le risorse nella tua organizzazione."Scopri come aggiungere membri a una partnership."

Comprendere i ruoli degli utenti della partnership

Puoi gestire i ruoli dei membri delle organizzazioni partner nello stesso modo in cui gestisci i tuoi. Tuttavia, non tutti i ruoli sono disponibili per gli utenti in partnership. In particolare, non è possibile concedere agli utenti partner un ruolo che consenta gli aggiornamenti software. L’aggiornamento del software ONTAP richiede in genere l’accesso diretto alla rete.

È possibile assegnare i seguenti ruoli agli utenti partner:

- "Amministratore dell’organizzazione"
- "Amministratore di cartelle o progetti"
- "Amministratore della Federazione"
- "Visualizzatore della federazione"
- "Amministratore di backup e ripristino"
- "Visualizzatore di backup"
- "Ripristina amministratore"
- "Clona amministratore"
- "Amministratore del ripristino di emergenza"
- "Amministratore del failover del ripristino di emergenza"
- "Amministratore dell’applicazione di ripristino di emergenza"
- "Visualizzatore di ripristino di emergenza"
- "Analista di supporto alle operazioni"
- "Visualizzatore di classificazione"

"Scopri di più sui ruoli predefiniti"

Aggiungere un ruolo a un utente partner

Puoi fornire l’accesso alle risorse della tua organizzazione aggiungendo un ruolo a un membro. Quando si assegna un ruolo, si specifica una risorsa e un ruolo. È possibile assegnare più di un ruolo a un utente.

Ad esempio, se si dispone di due progetti e si desidera che lo stesso utente abbia il ruolo di amministratore di backup e ripristino per entrambi, è necessario assegnare il ruolo all’utente per ciascun progetto. Allo stesso modo, se si desidera assegnare a un utente due ruoli diversi per lo stesso progetto, è necessario assegnare ciascun ruolo separatamente.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Partnership**.
3. Selezionare la scheda **Partnership avviata**.
4. Seleziona il menu azioni ••• accanto alla partnership consolidata che desideri visualizzare e seleziona **Visualizza dettagli**.

   L'elenco **Membro** mostra i membri che l'organizzazione partner ha aggiunto alla partnership.

5. Seleziona il menu azioni ••• accanto al membro a cui vuoi assegnare un ruolo e seleziona **Aggiungi un ruolo**.
6. Per aggiungere un ruolo, completare i passaggi nella finestra di dialogo:
   - **Seleziona un'organizzazione, una cartella o un progetto**: scegli il livello della gerarchia delle risorse per il quale il membro deve avere le autorizzazioni.

     Se selezioni l'organizzazione o una cartella, il membro avrà autorizzazioni per tutto ciò che risiede all'interno dell'organizzazione o della cartella.

   - **Seleziona una categoria**: Scegli una categoria di ruolo. "Scopri di più sui ruoli di accesso" .
   - Seleziona un **Ruolo**: scegli un ruolo che fornisca al membro le autorizzazioni per le risorse associate all'organizzazione, alla cartella o al progetto selezionato.
   - **Aggiungi ruolo**: se desideri concedere l'accesso a cartelle o progetti aggiuntivi all'interno della tua organizzazione, seleziona **Aggiungi ruolo**, specifica un'altra cartella, un altro progetto o una categoria di ruolo, quindi seleziona una categoria di ruolo e un ruolo corrispondente.
7. Seleziona **Aggiungi nuovi ruoli**.

Modificare o rimuovere un ruolo da un utente partner

Puoi modificare o rimuovere un ruolo assegnato a un membro di un'organizzazione partner.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Partnership**.
3. Selezionare la scheda **Partnership avviata**.
4. Seleziona il menu azioni ••• accanto alla partnership consolidata che desideri visualizzare e seleziona **Visualizza dettagli**.

   L'elenco **Membro** mostra i membri che l'organizzazione partner ha aggiunto alla partnership.

5. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
6. Nella tabella, espandi la riga corrispondente all'organizzazione, alla cartella o al progetto in cui desideri modificare il ruolo assegnato al membro e seleziona **Visualizza** nella colonna **Ruolo** per visualizzare i ruoli assegnati a questo membro.
7. È possibile modificare un ruolo esistente per un membro o rimuovere un ruolo.
   a. Per modificare il ruolo di un membro, seleziona **Modifica** accanto al ruolo che desideri modificare. È possibile modificare un ruolo solo in un ruolo all'interno della stessa categoria di ruoli. Ad esempio, è possibile passare da un ruolo di servizio dati a un altro. Conferma la modifica.
   b. Per annullare l'assegnazione del ruolo a un membro, selezionare 🗑 accanto al ruolo per rimuovere il rispettivo ruolo dal membro. Ti verrà chiesto di confermare la rimozione.

Lavorare in un’organizzazione partner

Una volta assegnato un ruolo in un’organizzazione partner, puoi passare a quell’organizzazione ed eseguire le azioni per cui sei autorizzato a farlo.

Utilizza il menu Organizzazione per passare dalla tua organizzazione a qualsiasi organizzazione partner a cui hai accesso."Scopri di più sul passaggio da un’organizzazione all’altra e da un progetto all’altro."

Potrai visualizzare le risorse che sono state condivise con te nell’organizzazione partner ed eseguire azioni in base al ruolo che ti è stato assegnato. Collabora con l’amministratore della tua partnership per assicurarti di avere il ruolo appropriato per le risorse a cui devi accedere.

Monitorare le operazioni NetApp Console

È possibile monitorare lo stato delle operazioni eseguite dalla Console per verificare se ci sono problemi da risolvere. Puoi visualizzare lo stato dalla pagina Audit, dal Centro notifiche oppure ricevere notifiche via email.

La tabella mette a confronto le funzionalità della pagina Audit e del Centro notifiche.

Centro notifiche	Pagina di controllo
Mostra lo stato di alto livello per eventi e azioni	Fornisce dettagli per ogni evento o azione per ulteriori indagini
Mostra lo stato della sessione di accesso corrente (le informazioni non vengono visualizzate nel Centro notifiche dopo la disconnessione)	Mantiene lo stato dell’ultimo mese
Mostra solo le azioni avviate nell’interfaccia utente	Mostra tutte le azioni dall’interfaccia utente o dalle API
Mostra le azioni avviate dall’utente	Mostra tutte le azioni, sia avviate dall’utente che dal sistema
Filtra i risultati per importanza	Filtra per servizio, azione, utente, stato e altro ancora
Fornisce la possibilità di inviare notifiche via e-mail agli utenti e ad altri	Nessuna funzionalità di posta elettronica

Controlla l’attività dell’utente dalla pagina Audit

Utilizzare la pagina Audit per identificare chi ha eseguito un’azione o il suo stato.

La pagina Audit mostra le azioni completate dagli utenti per gestire la tua organizzazione o il tuo account. Ciò include azioni di gestione quali l’associazione di utenti, la creazione di sistemi, la creazione di agenti e altro ancora.

Puoi anche verificare chi ha aggiunto un membro a un’organizzazione o se un progetto è stato eliminato correttamente.

Passi

1. Selezionare **Amministrazione > Audit**.
2. Utilizza i filtri sopra la tabella per modificare le azioni da visualizzare nella tabella.

Ad esempio, puoi utilizzare il filtro **Servizio** per mostrare le azioni relative a un servizio specifico oppure puoi utilizzare il filtro **Utente** per mostrare le azioni relative a un account utente specifico.

Scarica i registri di controllo dalla pagina Audit

È possibile scaricare i registri di controllo dalla pagina Controllo in un file CSV. Ciò consente di tenere traccia delle azioni eseguite dagli utenti nella tua organizzazione. Il file CSV include tutte le colonne presenti nel file CSV scaricato, indipendentemente dai filtri o dalle colonne visualizzate nella pagina Audit.

Passi

1. Nella pagina **Audit**, seleziona l'icona di download nell'angolo in alto a destra della tabella.

Monitorare le attività tramite il Centro notifiche

Le notifiche monitorano le operazioni della Console per confermarne il successo. Consentono di visualizzare lo stato di numerose azioni della Console avviate durante la sessione di accesso corrente. Non tutti i servizi della console segnalano informazioni nel Centro notifiche.

È possibile visualizzare le notifiche selezionando la campanella delle notifiche () nella barra dei menu. Il colore della piccola bolla nella campana indica la notifica di gravità più alta attiva. Quindi, se vedi una bolla rossa, significa che c'è una notifica importante che dovresti leggere.

È anche possibile configurare la Console in modo che invii determinati tipi di notifiche tramite e-mail, in modo da essere informati sulle attività importanti del sistema anche quando non si è effettuato l'accesso al sistema. Le e-mail possono essere inviate a tutti gli utenti che fanno parte della tua organizzazione o a qualsiasi altro destinatario che debba essere a conoscenza di determinati tipi di attività del sistema. Scopri comeimposta le impostazioni di notifica e-mail .

Confronto tra il Centro notifiche e gli avvisi

Il Centro notifiche consente di visualizzare lo stato delle operazioni avviate e di impostare notifiche di avviso per determinati tipi di attività di sistema. Nel frattempo, gli avvisi consentono di visualizzare problemi o potenziali rischi nel tuo ambiente di archiviazione ONTAP in relazione a capacità, disponibilità, prestazioni, protezione e sicurezza.

"Scopri di più sugli avvisi NetApp Console"

Tipi di notifica

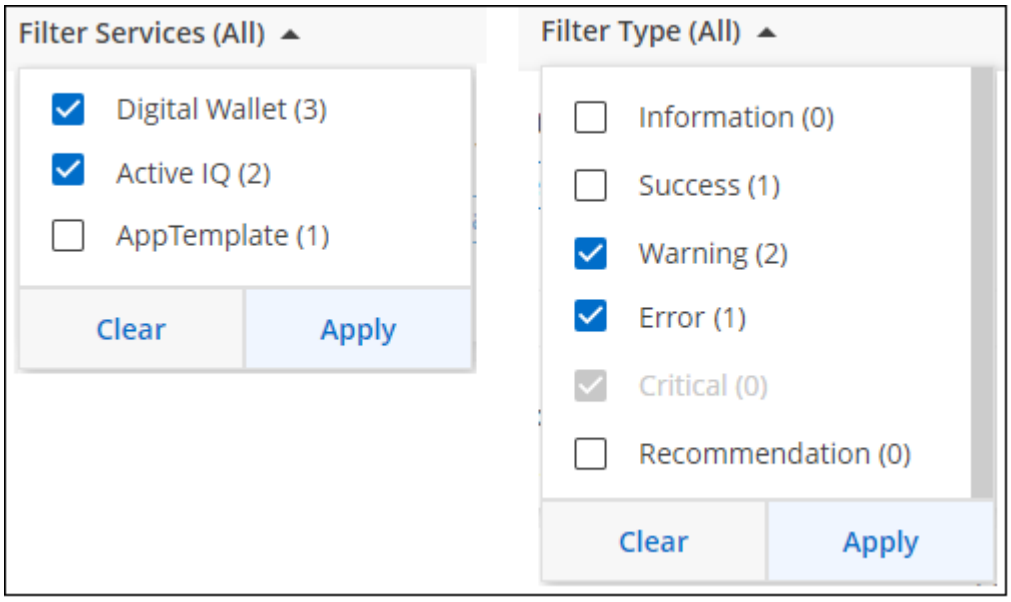
La Console classifica le notifiche nelle seguenti categorie:

Tipo di notifica	Descrizione
Critico	Si è verificato un problema che potrebbe causare l'interruzione del servizio se non si interviene immediatamente con misure correttive.
Errore	Un'azione o un processo si è concluso con un fallimento o potrebbe portare al fallimento se non vengono adottate misure correttive.
Avvertimento	Un problema di cui dovresti essere a conoscenza per assicurarti che non raggiunga la gravità critica. Le notifiche di questa gravità non causano interruzioni del servizio e potrebbero non essere necessarie misure correttive immediate.

Tipo di notifica	Descrizione
Raccomandazione	Una raccomandazione di sistema che ti invita a intraprendere un'azione per migliorare il sistema o un determinato servizio; ad esempio: risparmio sui costi, suggerimento per nuovi servizi, configurazione di sicurezza consigliata, ecc.
Informazioni	Un messaggio che fornisce informazioni aggiuntive su un'azione o un processo.
Successo	Un'azione o un processo completato con successo.

Filtra le notifiche

Per impostazione predefinita, tutte le notifiche attive verranno visualizzate nel Centro notifiche. Puoi filtrare le notifiche che vedi per visualizzare solo quelle che ritieni importanti. È possibile filtrare per "Servizio" e per "Tipo" di notifica.



Ad esempio, se vuoi visualizzare solo le notifiche "Errore" e "Avviso" per le operazioni della Console, seleziona tali voci e vedrai solo quei tipi di notifiche.

Ignora le notifiche

Puoi rimuovere le notifiche dalla pagina se non hai più bisogno di vederle. È possibile ignorare le notifiche singolarmente o tutte contemporaneamente.

Per ignorare tutte le notifiche, nel Centro notifiche, seleziona ⋮ e seleziona **Ignora tutto**.

Per ignorare singole notifiche, passa il cursore sulla notifica e seleziona **Ignora**.

Imposta le impostazioni di notifica via email

Puoi inviare tipi specifici di notifiche tramite e-mail, in modo da essere informato sulle attività importanti del sistema anche quando non hai effettuato l'accesso. Le e-mail possono essere inviate a tutti gli utenti che fanno parte della tua organizzazione o del tuo account, oppure a qualsiasi altro destinatario che debba essere a conoscenza di determinati tipi di attività del sistema.

- La console invia notifiche e-mail per l'agente, le licenze e gli abbonamenti, NetApp Copy and Sync e NetApp Backup and Recovery.
- L'invio di notifiche e-mail non è supportato quando l'agente Console è installato in un sito senza accesso a Internet.

I filtri impostati nel Centro notifiche non determinano i tipi di notifiche che ricevi via e-mail. Per impostazione predefinita, qualsiasi amministratore dell'organizzazione riceverà email per tutte le notifiche "Critiche" e "Raccomandate". Queste notifiche sono valide per tutti i servizi: non è possibile scegliere di ricevere notifiche solo per determinati servizi, ad esempio agenti o NetApp Backup and Recovery.

Tutti gli altri utenti e destinatari sono configurati per non ricevere alcuna email di notifica, quindi sarà necessario configurare le impostazioni di notifica per tutti gli utenti aggiuntivi.

Per personalizzare le impostazioni delle notifiche è necessario disporre del ruolo di amministratore dell'organizzazione.

Passi

1. Selezionare **Amministrazione > Impostazioni notifiche**.
2. Selezionare **Utenti dell'organizzazione** o **Destinatari aggiuntivi**.

   La pagina **Destinatari aggiuntivi** consente di configurare la Console in modo che invii notifiche alle persone che sono membri della tua organizzazione Console.

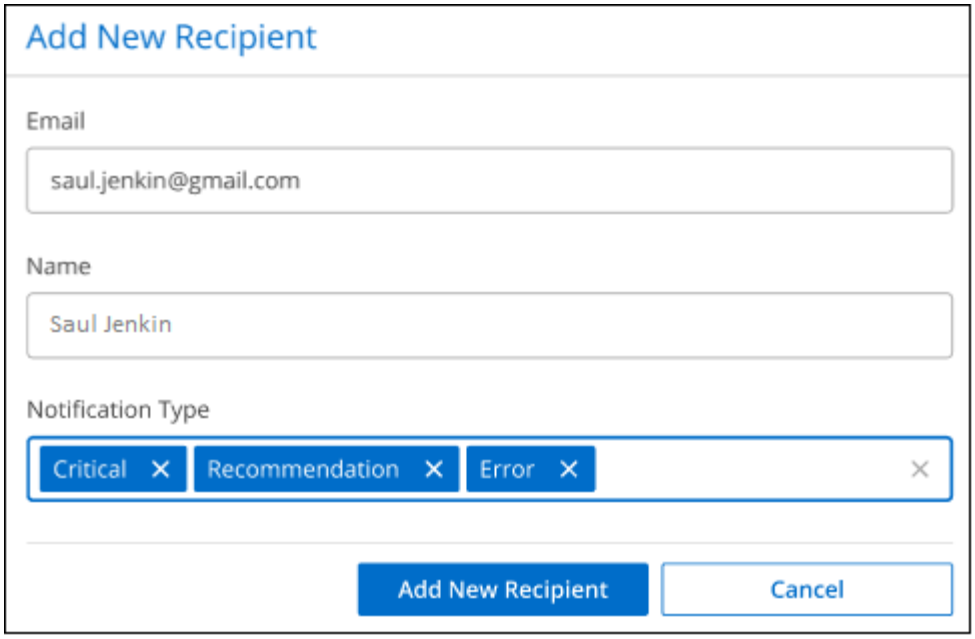
3. Seleziona uno o più utenti dalla pagina *Utenti dell'organizzazione* o dalla pagina *Destinatari aggiuntivi* e scegli il tipo di notifiche da inviare:
   - Per apportare modifiche per un singolo utente, seleziona il menu nella colonna Notifiche per quell'utente, seleziona i tipi di notifiche da inviare e seleziona **Applica**.
   - Per apportare modifiche per più utenti, seleziona la casella per ciascun utente, seleziona **Gestisci notifiche e-mail**, seleziona i tipi di notifiche da inviare e seleziona **Applica**.

Aggiungi altri destinatari e-mail

Gli utenti che compaiono nella pagina *Utenti dell'organizzazione* vengono automaticamente inseriti tra gli utenti della tua organizzazione o del tuo account. Nella pagina *Destinatari aggiuntivi* puoi aggiungere indirizzi email per altre persone o gruppi che non hanno accesso alla Console, ma che devono essere informati su determinati tipi di avvisi e notifiche.

Passi

1. Dalla pagina **Impostazioni notifiche**, seleziona **Aggiungi nuovi destinatari**.



2. Inserisci il nome, l'indirizzo email e seleziona i tipi di notifiche che il destinatario riceverà, quindi seleziona **Aggiungi nuovo destinatario**.

Informazioni sul copyright

Informazioni sul marchio commerciale