Distribuisci un agente della console

NetApp Console setup and administration

NetApp
February 09, 2026

Sommario

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.

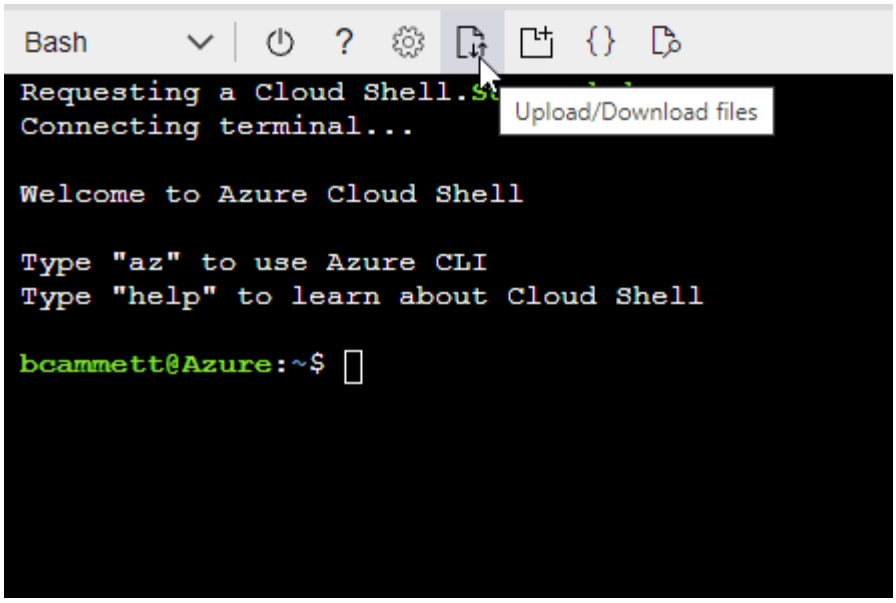
   Esempio

```
"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.

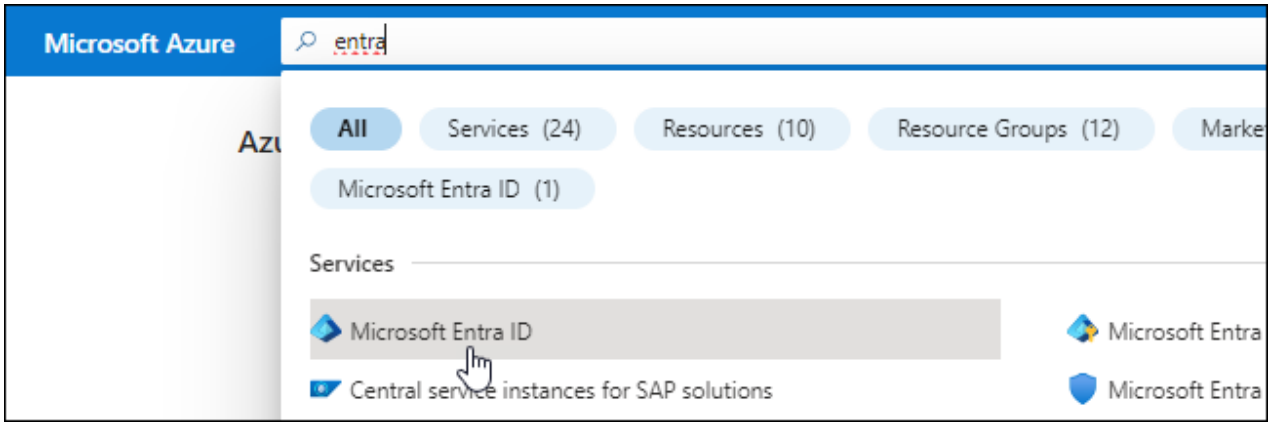
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie alla console.

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**.

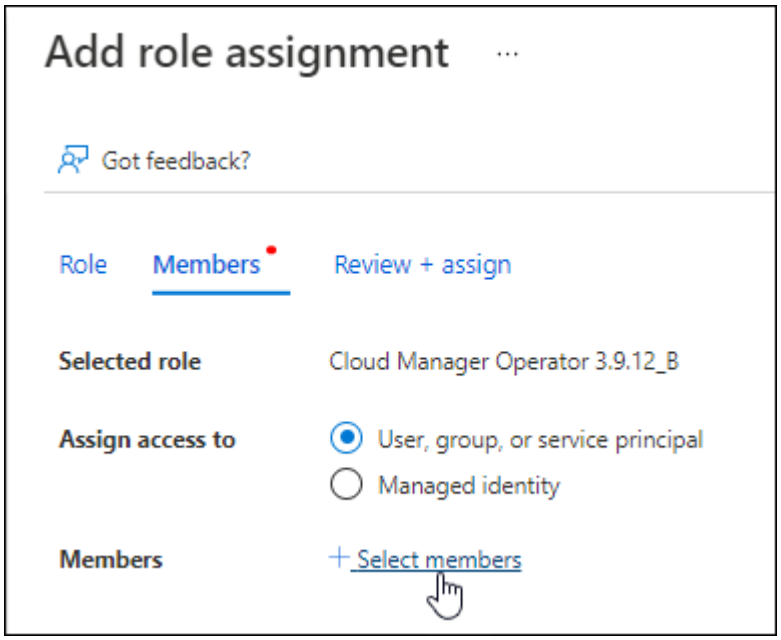
   Hai creato l'applicazione AD e il servizio principale.

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:

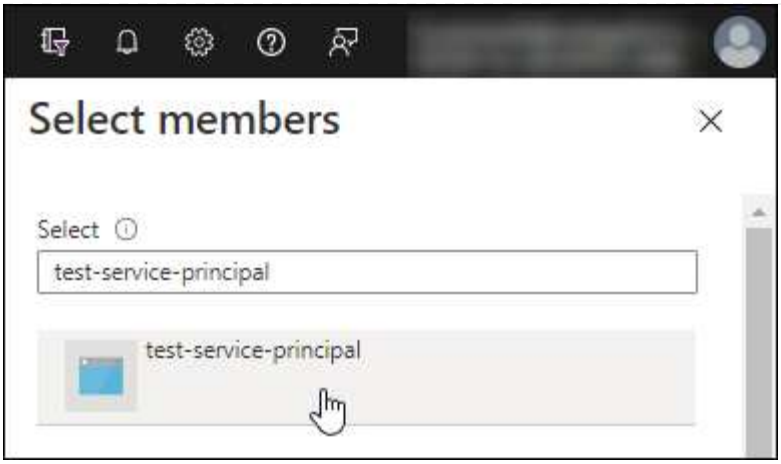
   a. Mantieni selezionato **Utente, gruppo o entità servizio**.

   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**.

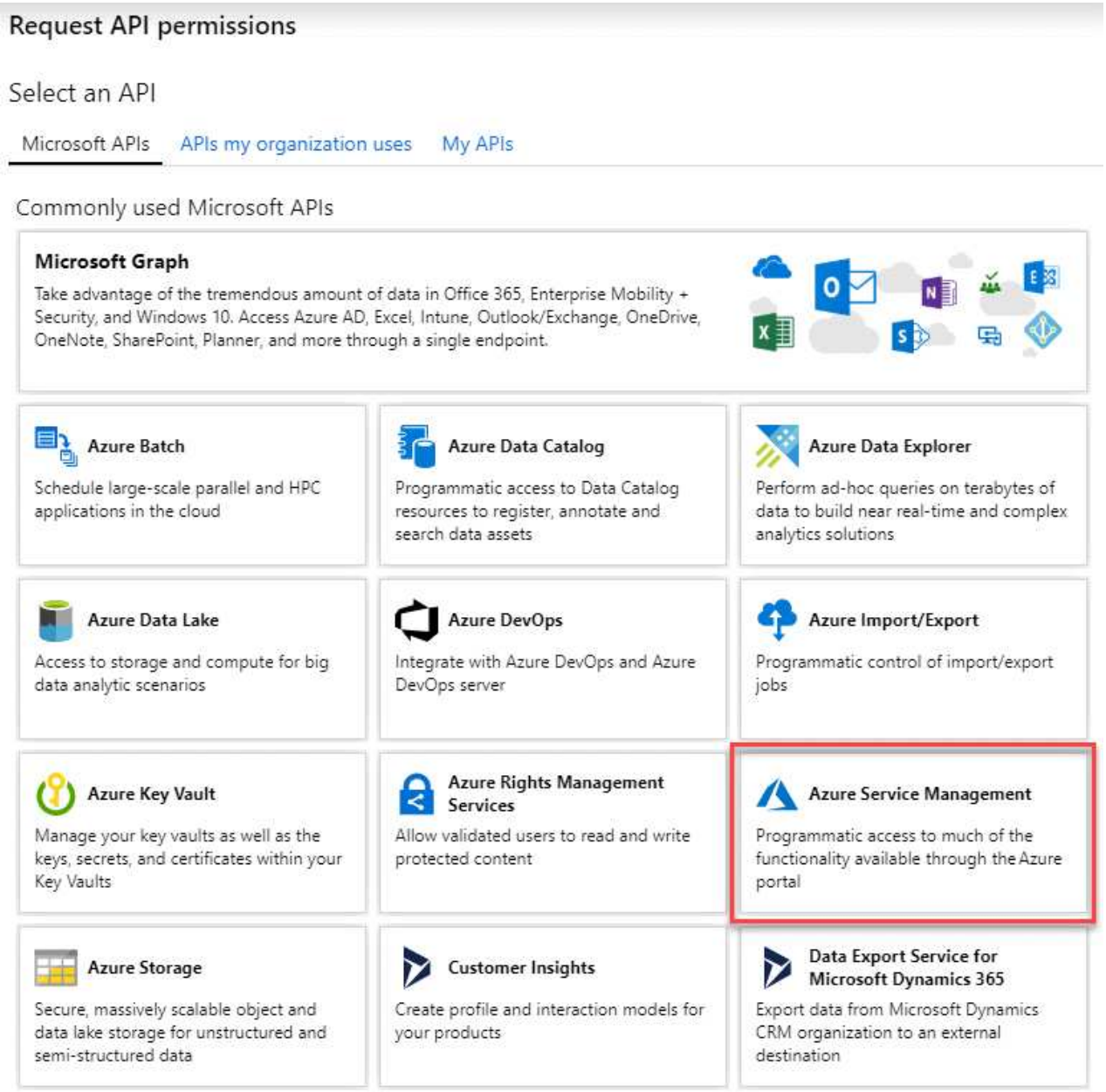
6. Fare clic su **Revisiona + assegna**.

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

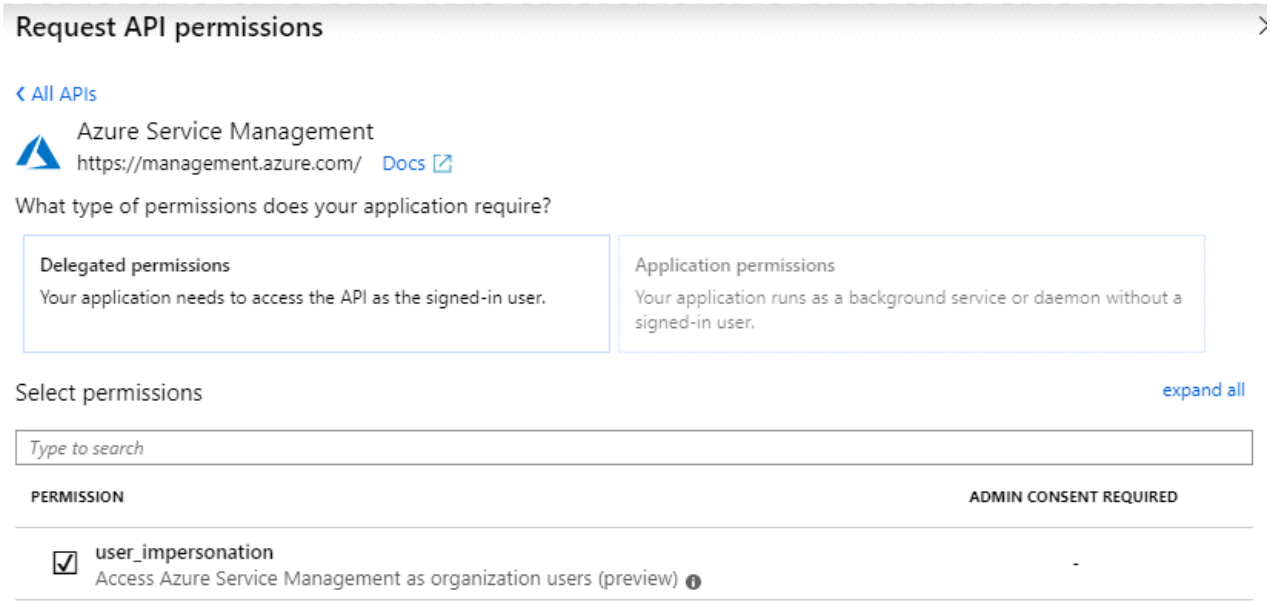
   Se si desidera gestire risorse in più sottoscrizioni di Azure, è necessario associare l'entità servizio a ciascuna di tali sottoscrizioni. Ad esempio, la Console consente di selezionare l'abbonamento che si desidera utilizzare durante la distribuzione Cloud Volumes ONTAP.

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**.

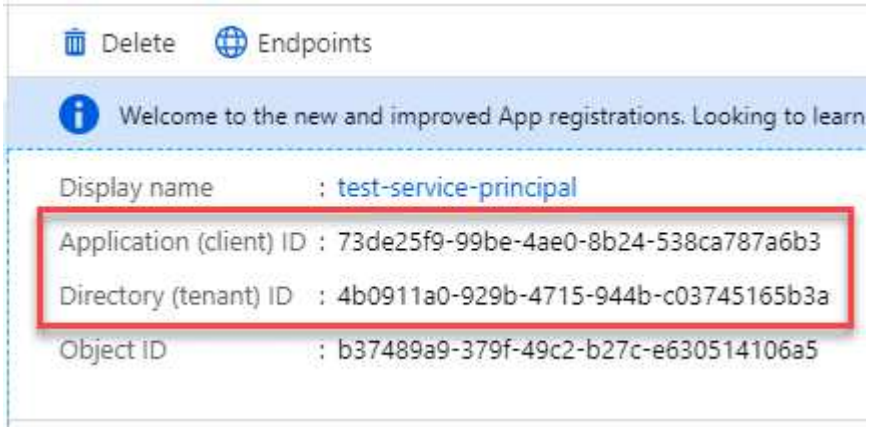


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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.

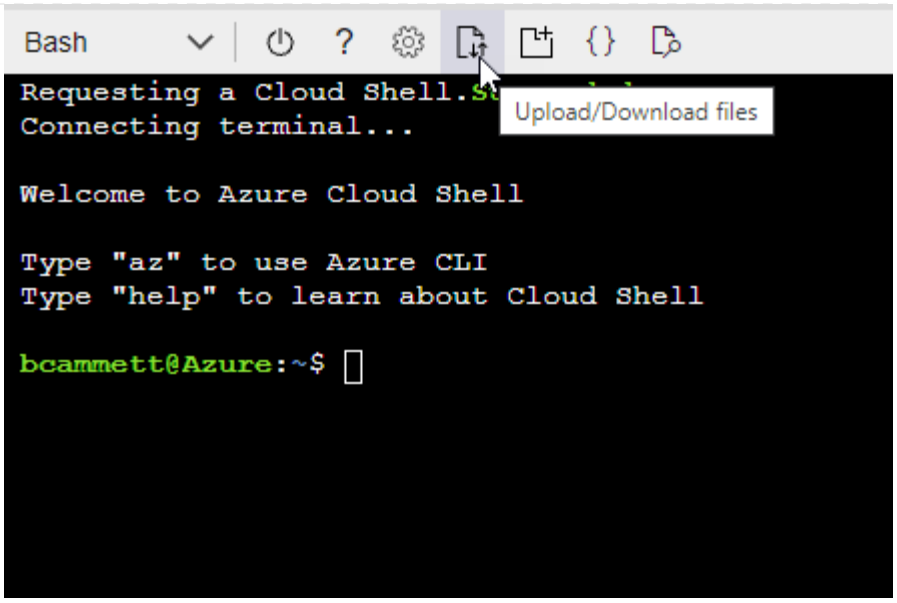
   Esempio

   ```
   "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

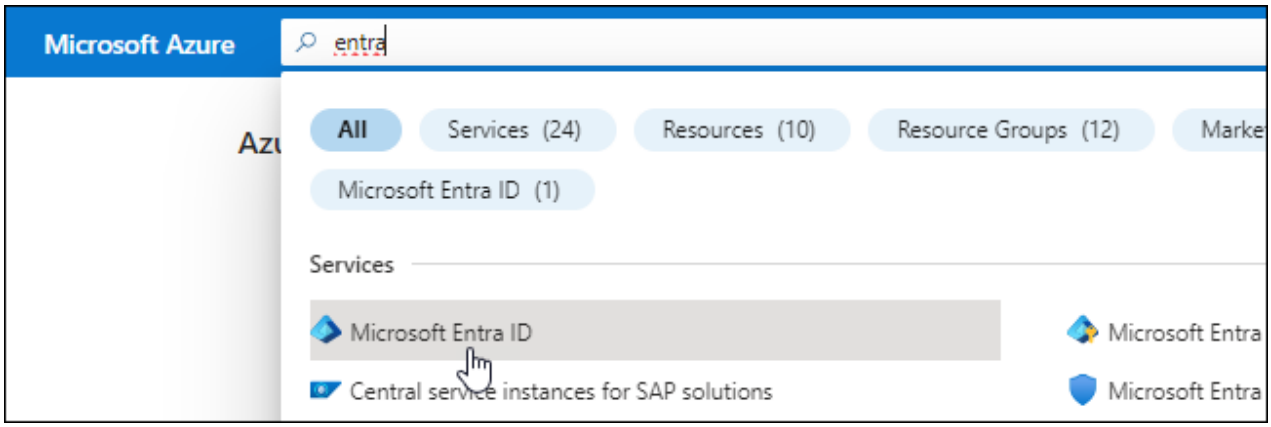
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie alla console.

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 .

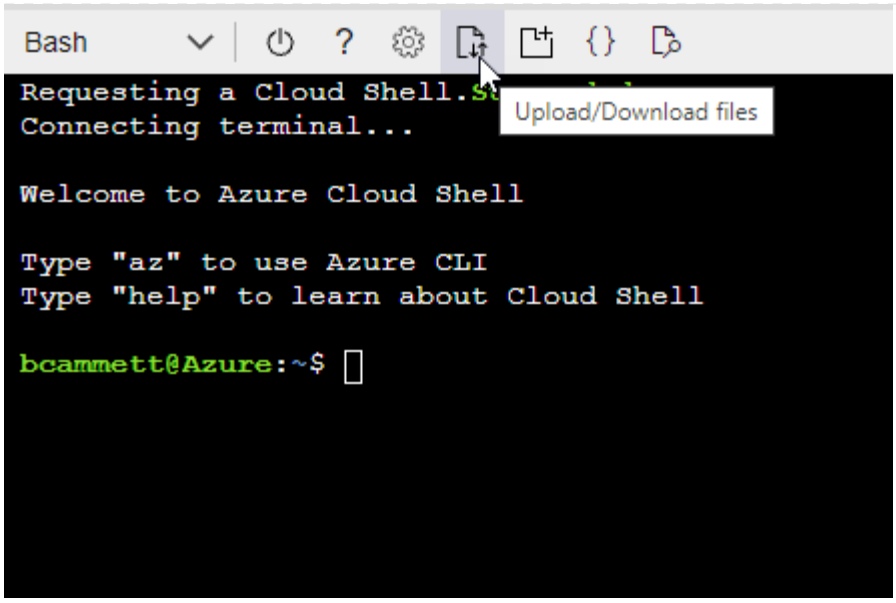
      Esempio

      ```
      "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**.

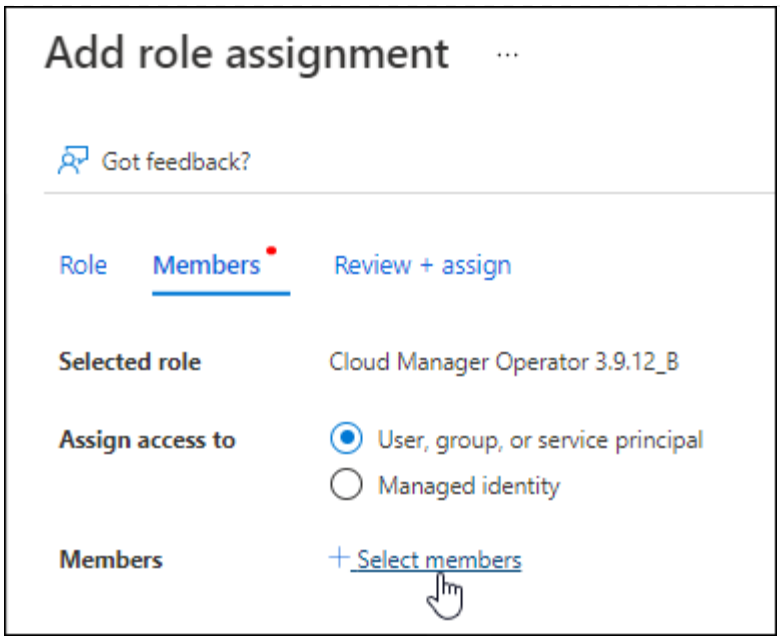
   b. Seleziona l'abbonamento.

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

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

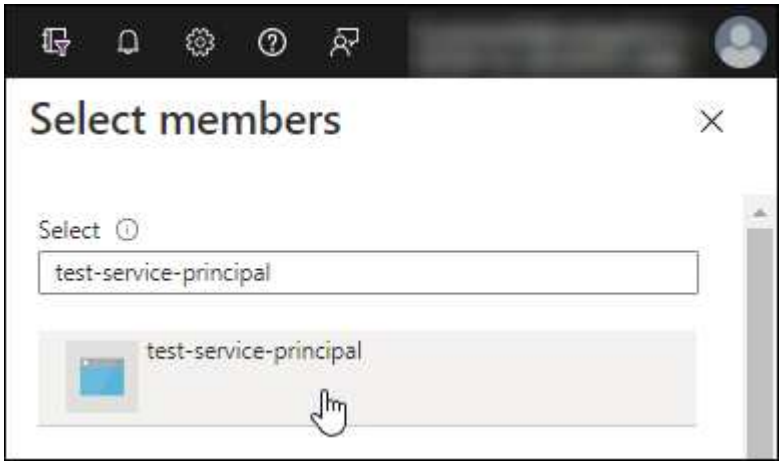
   e. Nella scheda **Membri**, completa i seguenti passaggi:

      - 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**.

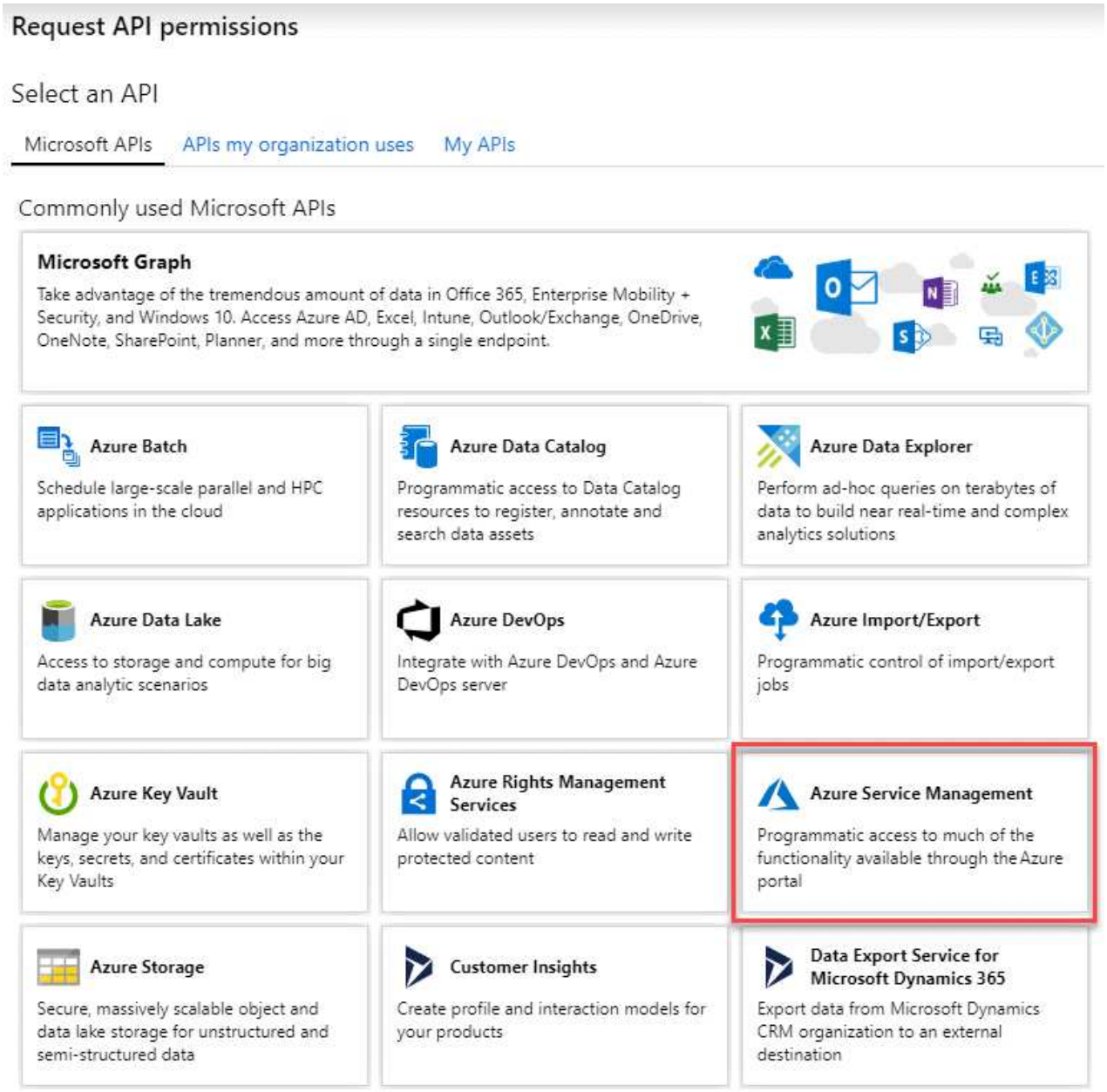
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

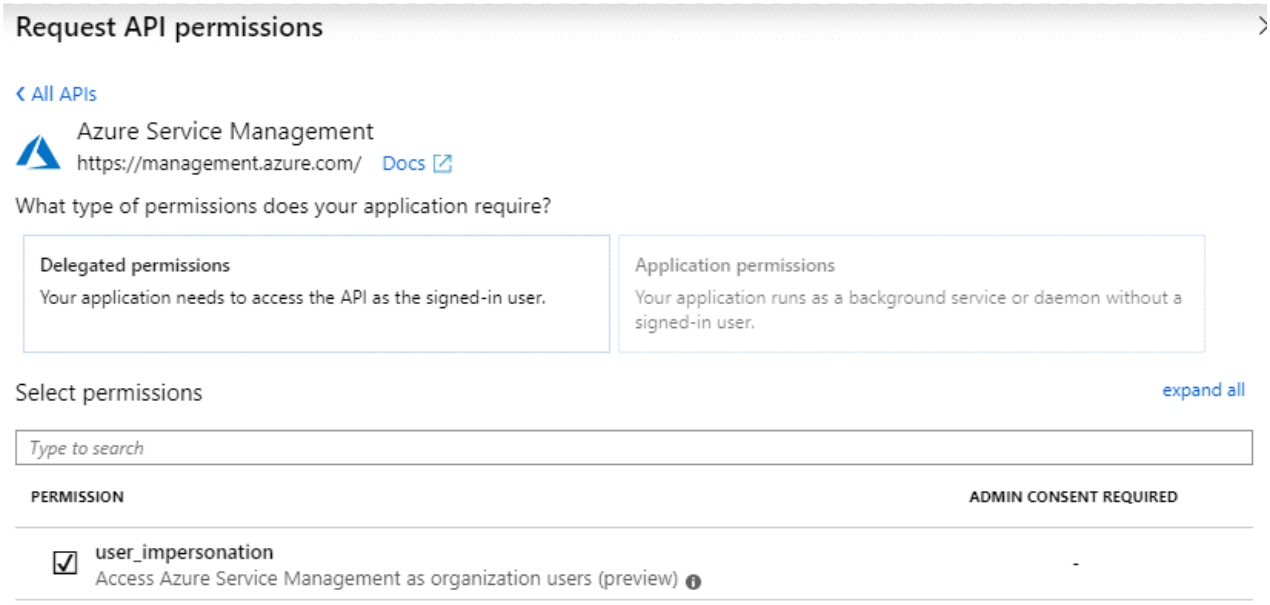
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

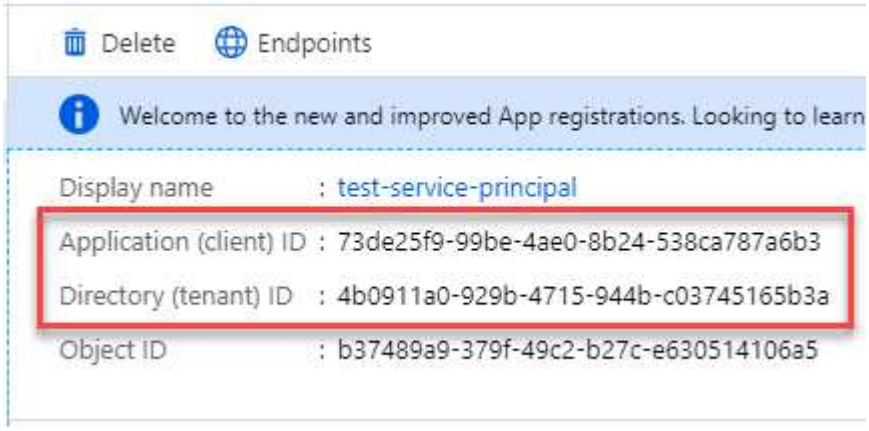


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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

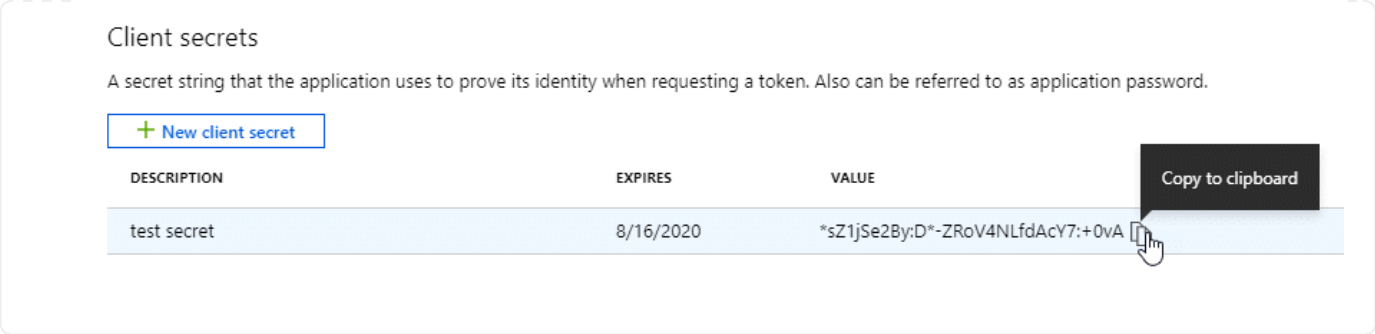
1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)**.



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.

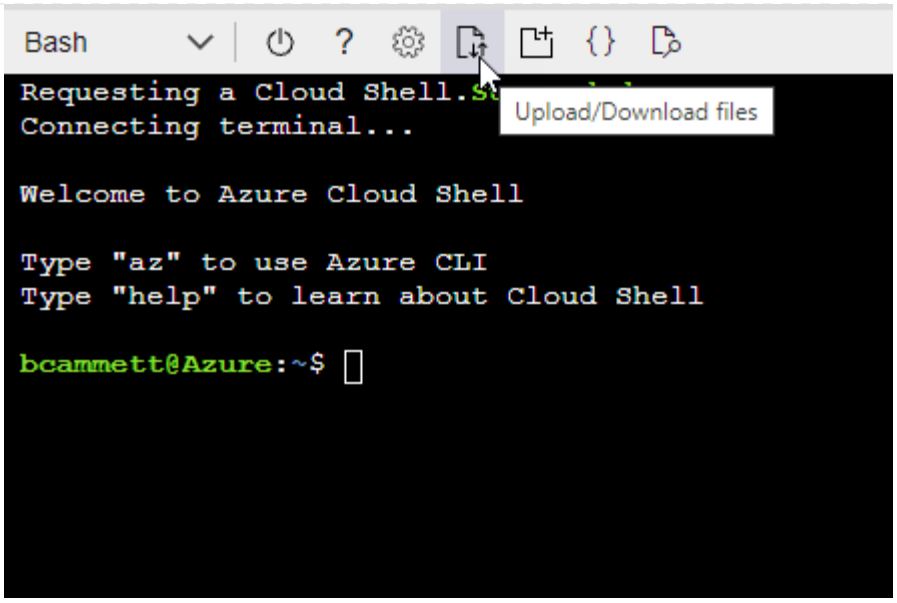
   Esempio

   ```
   "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

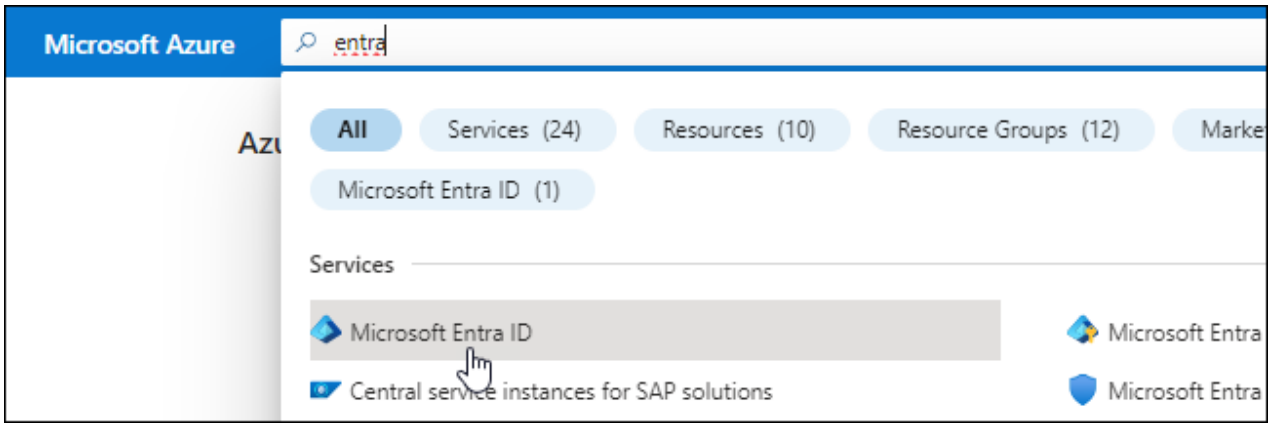
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie all'agente della console.

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 .

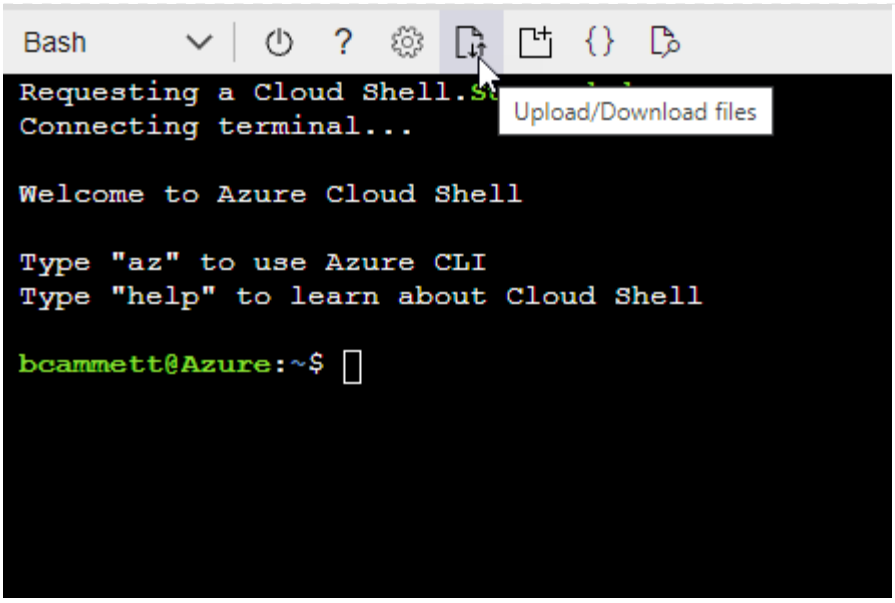
      Esempio

      ```
      "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**.

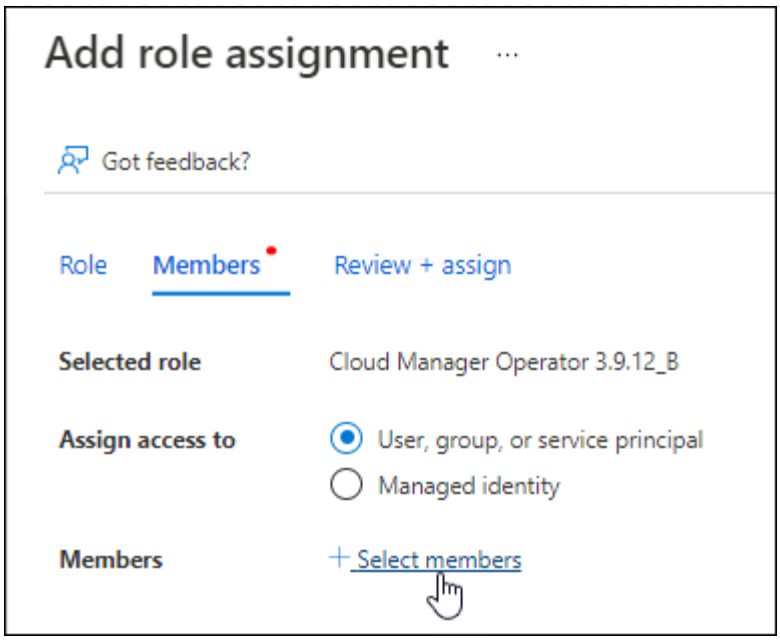
   b. Seleziona l'abbonamento.

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

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

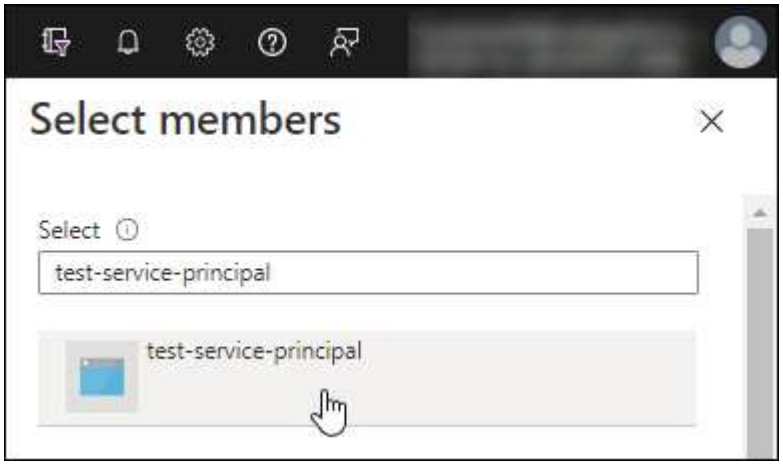
   e. Nella scheda **Membri**, completa i seguenti passaggi:

      - 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**.

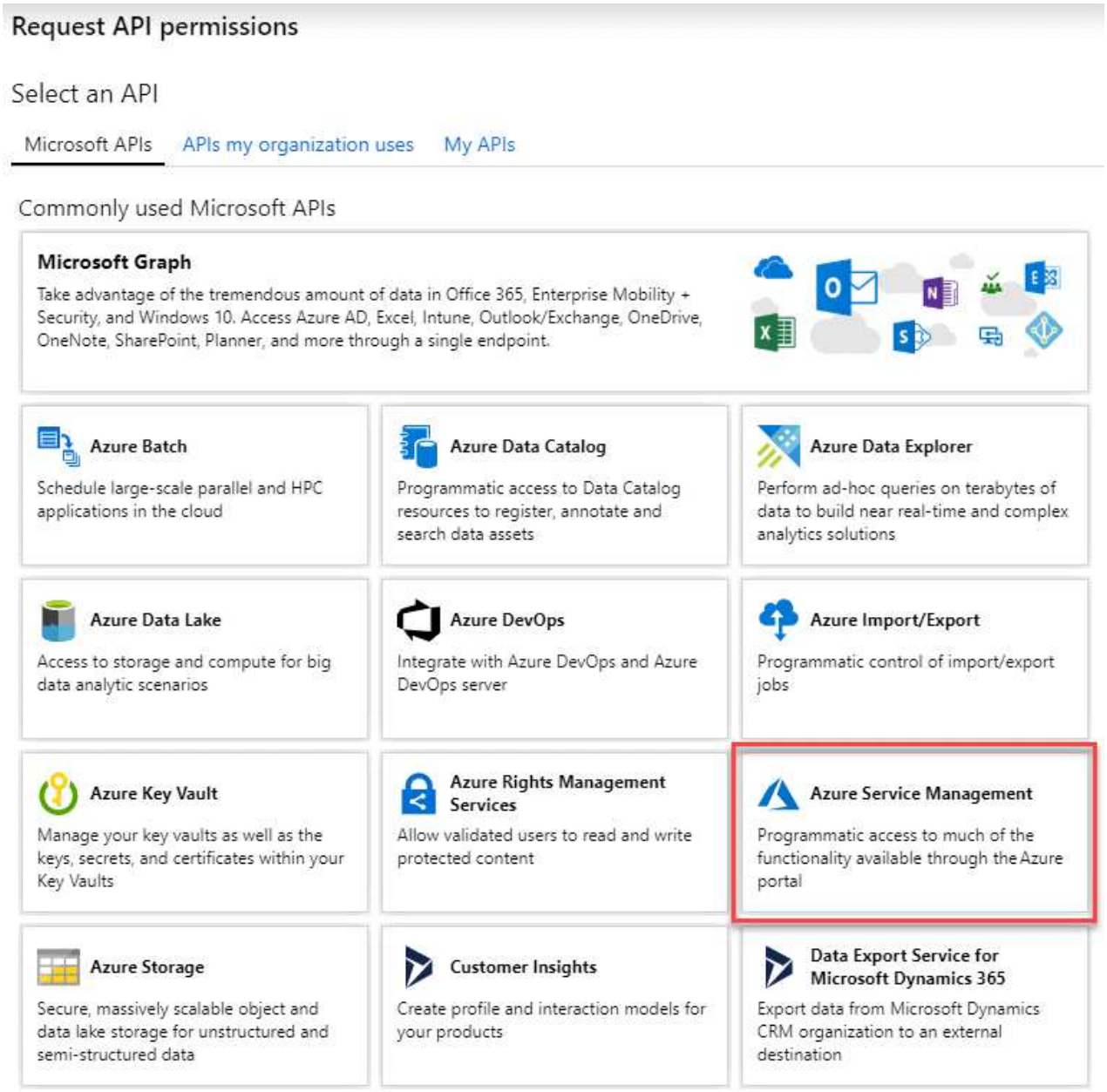
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

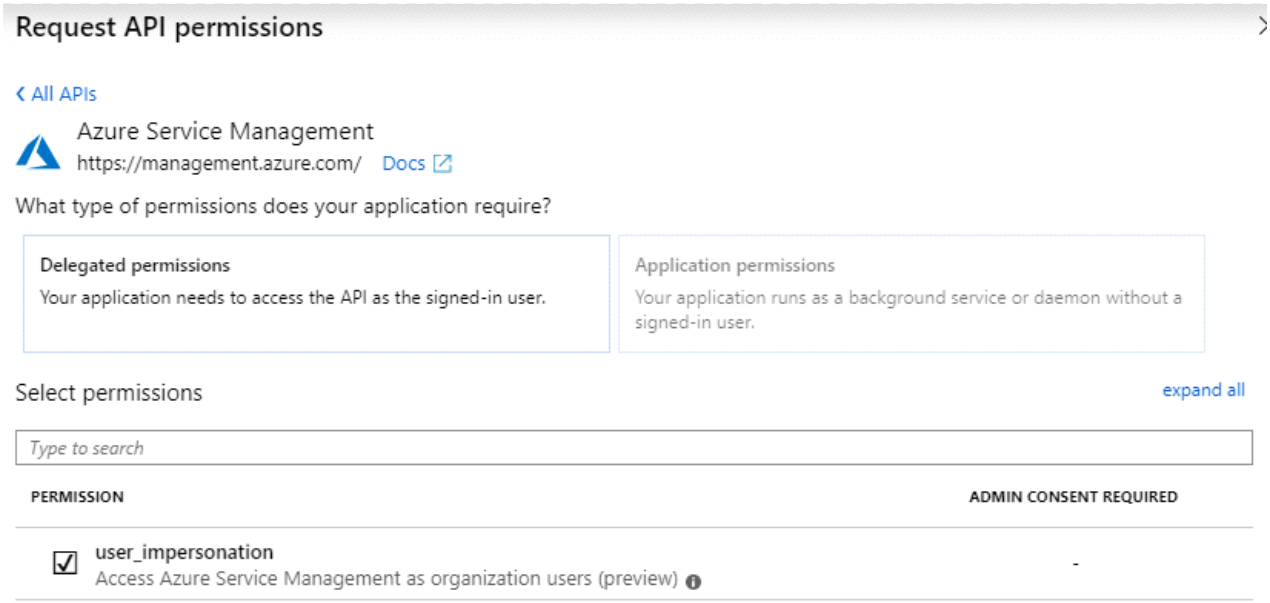
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

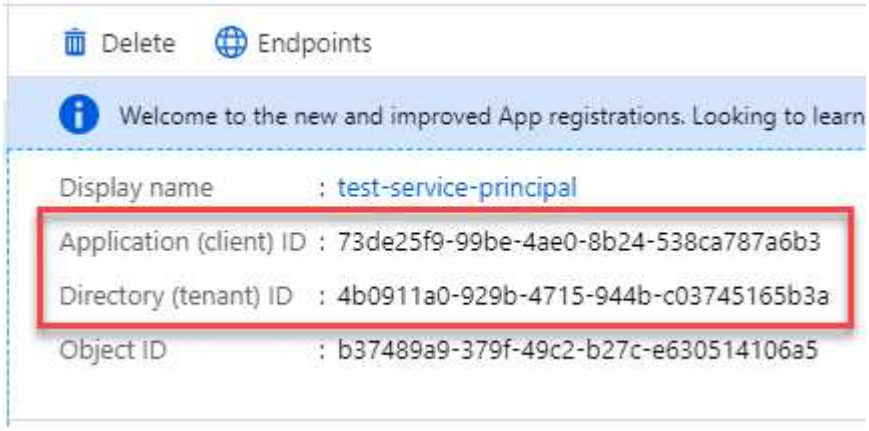


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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.

Installa manualmente l'agente Console in Google Cloud

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

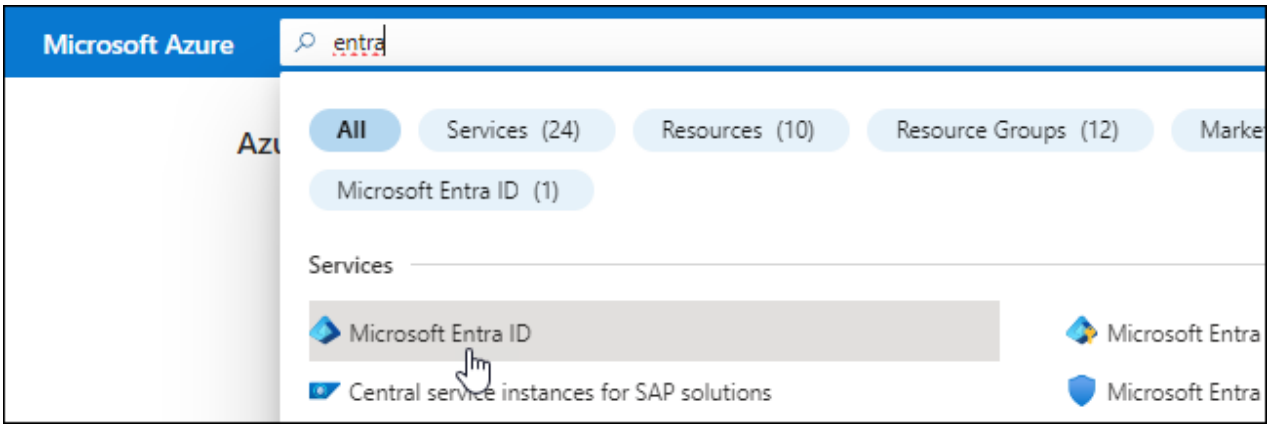
Quando l'agente Console è installato in locale, è necessario fornire all'agente Console le autorizzazioni di Azure impostando un'entità servizio in Microsoft Entra ID e ottenendo le credenziali di Azure necessarie all'agente Console.

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 .

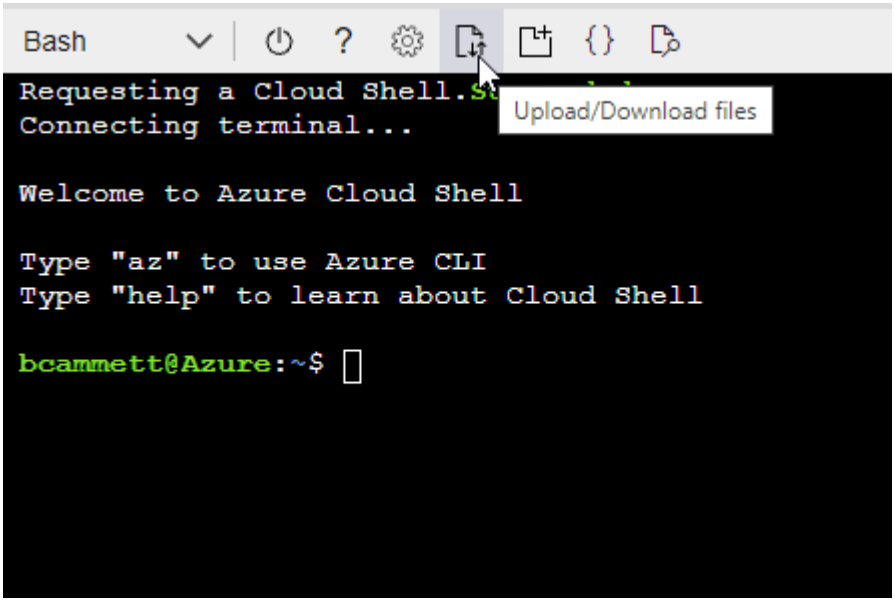
      Esempio

      ```
      "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:

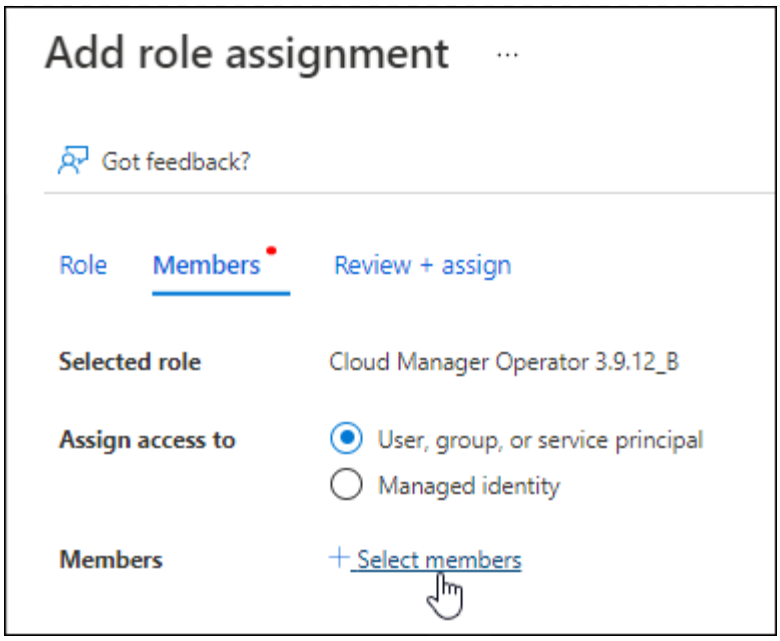
```
az role definition create --role-definition agent_Policy.json
```

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

2. Assegnare l'applicazione al ruolo:

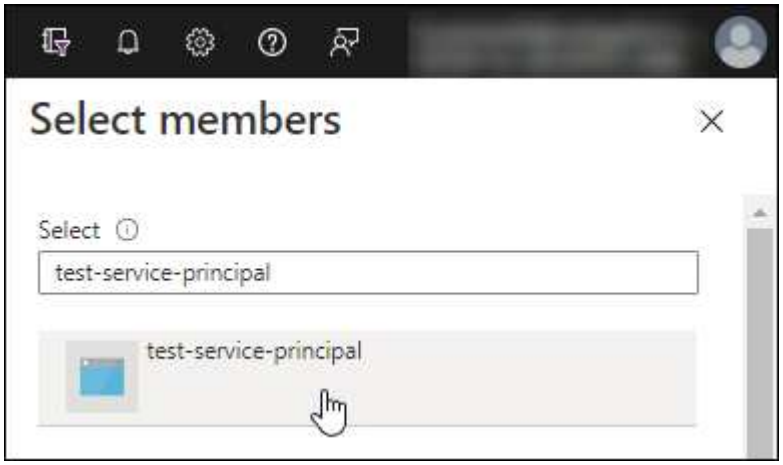
   a. Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
   b. Seleziona l'abbonamento.
   c. Selezionare **Controllo accessi (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.
   e. Nella scheda **Membri**,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

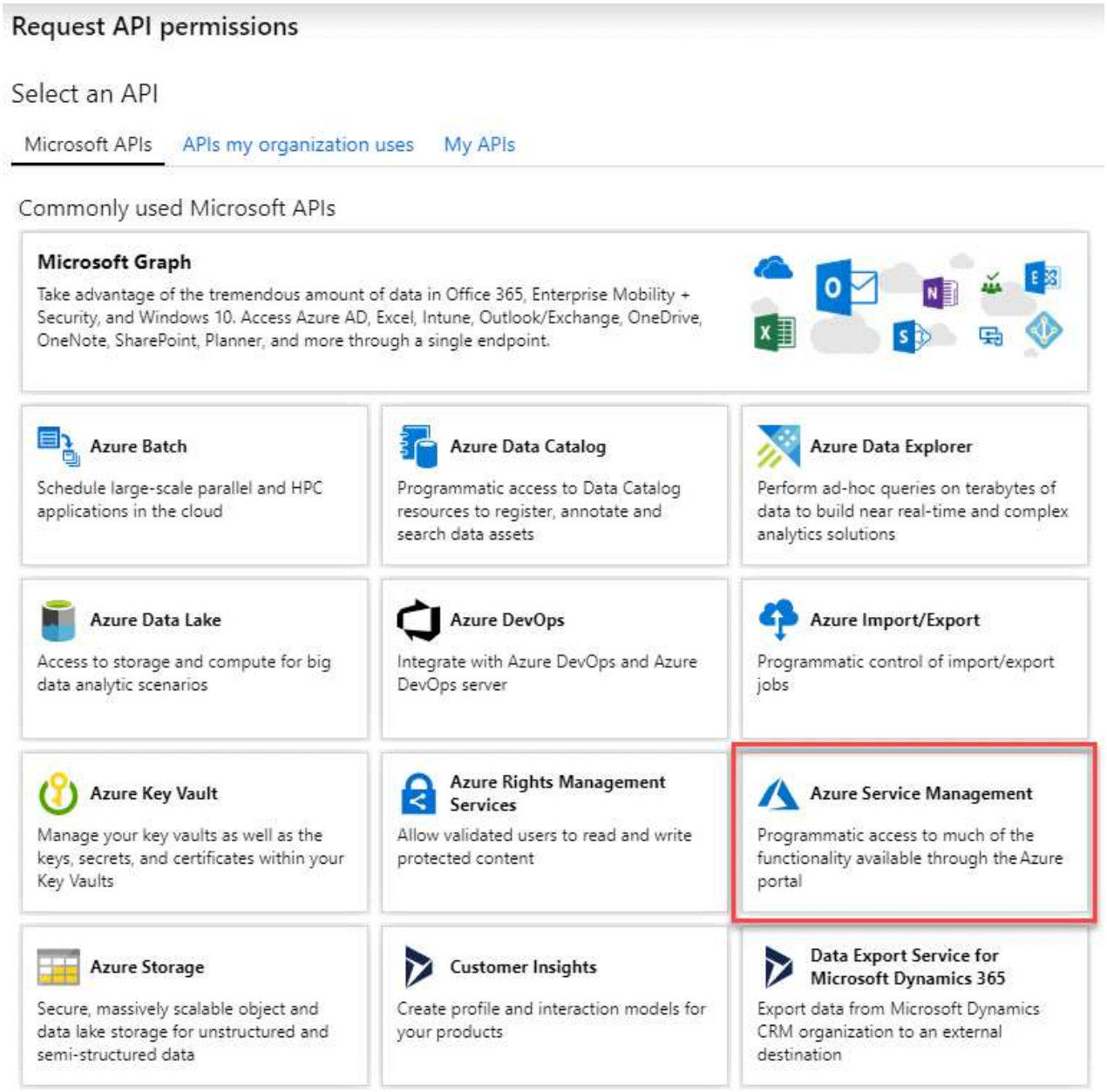
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

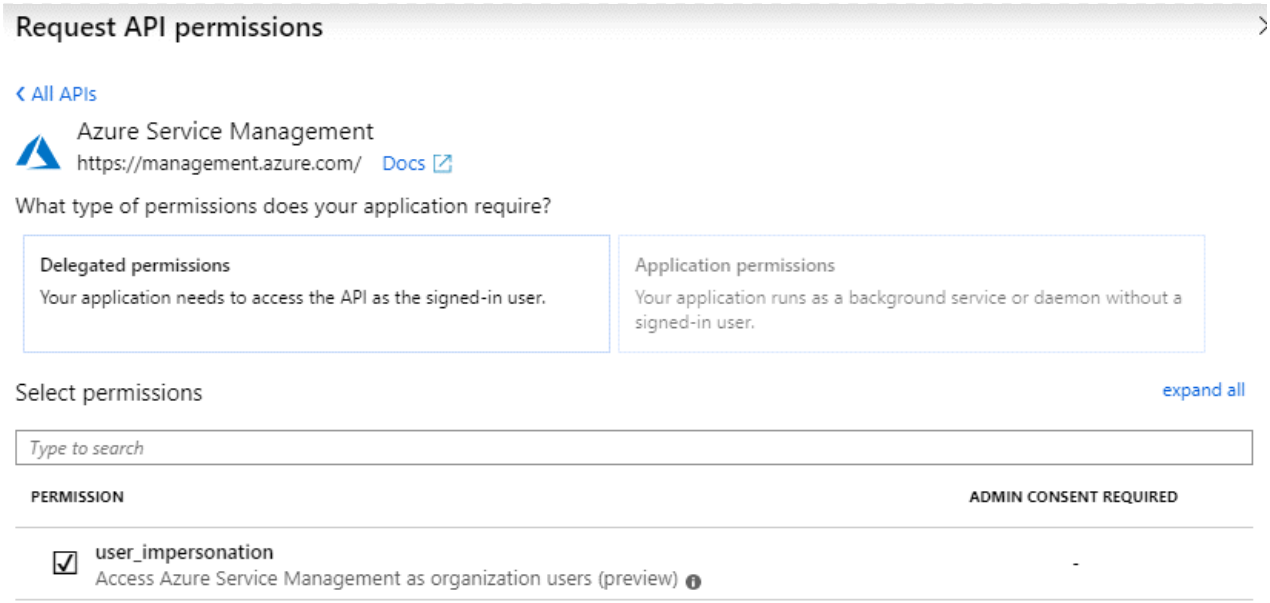
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

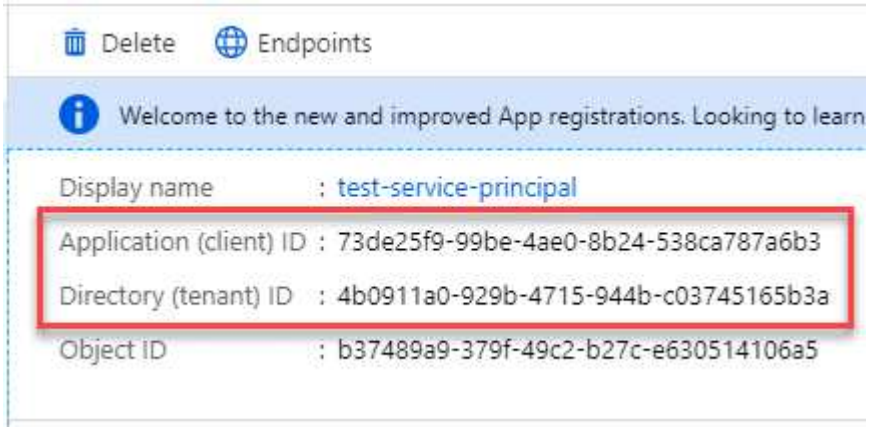


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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

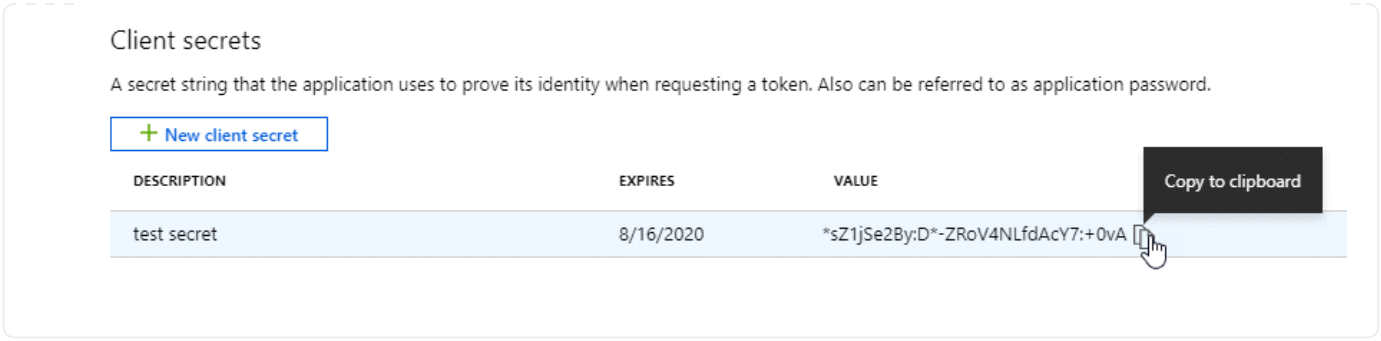
1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)**.



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

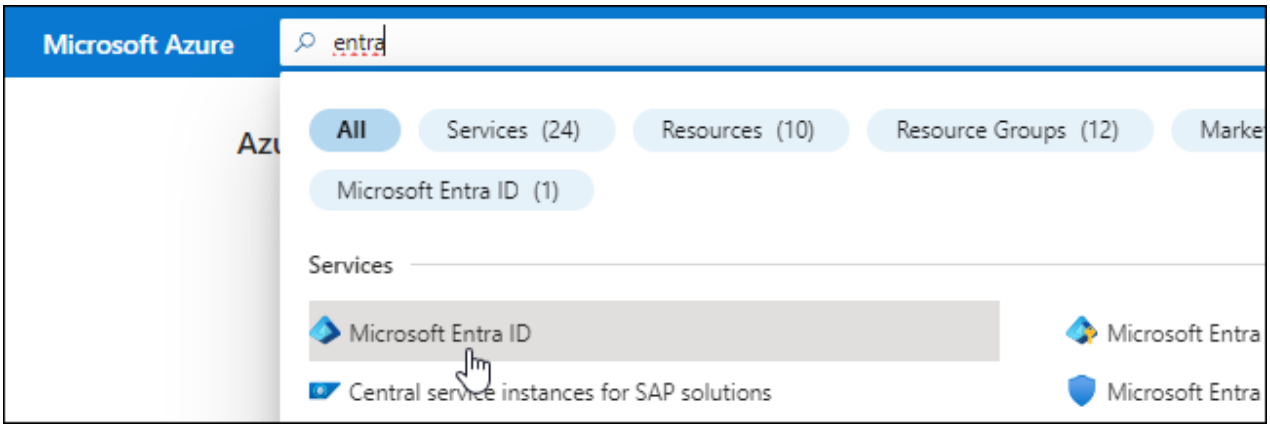
Quando l'agente Console è installato in locale, è necessario concedere all'agente Console le autorizzazioni di Azure impostando un'entità servizio in Microsoft Entra ID e ottenendo le credenziali di Azure necessarie all'agente Console.

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 .

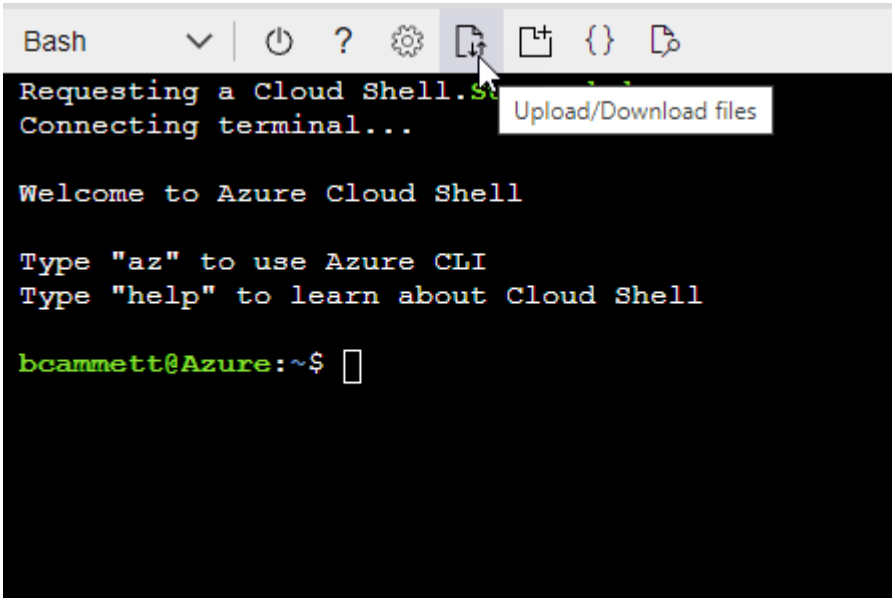
      Esempio

      ```
      "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:

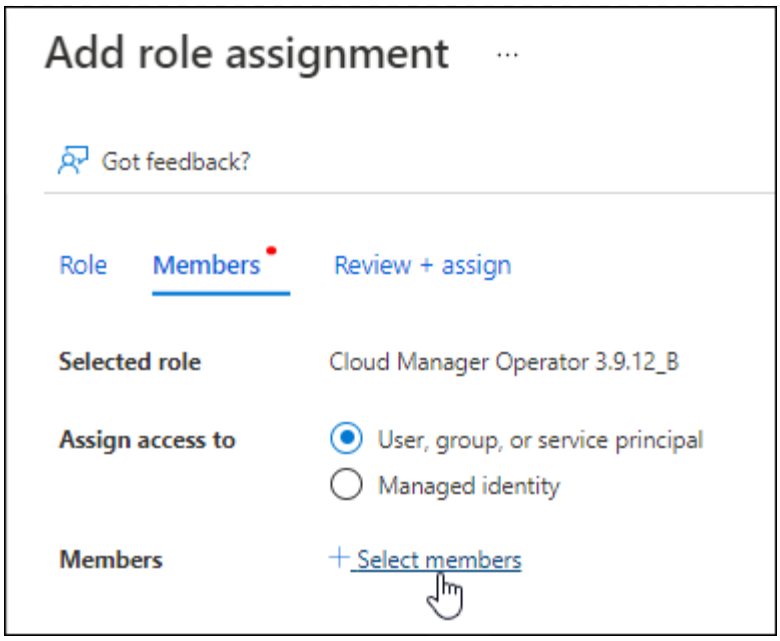
```
az role definition create --role-definition agent_Policy.json
```

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

2. Assegnare l'applicazione al ruolo:

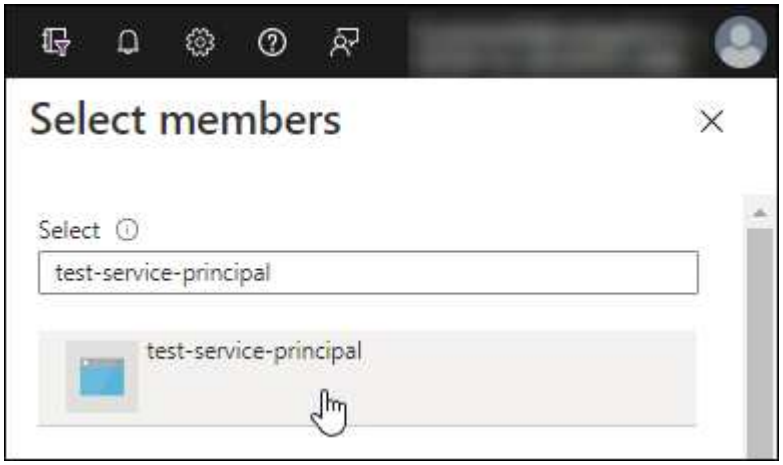
   a. Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
   b. Seleziona l'abbonamento.
   c. Selezionare **Controllo accessi (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.
   e. Nella scheda **Membri**,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

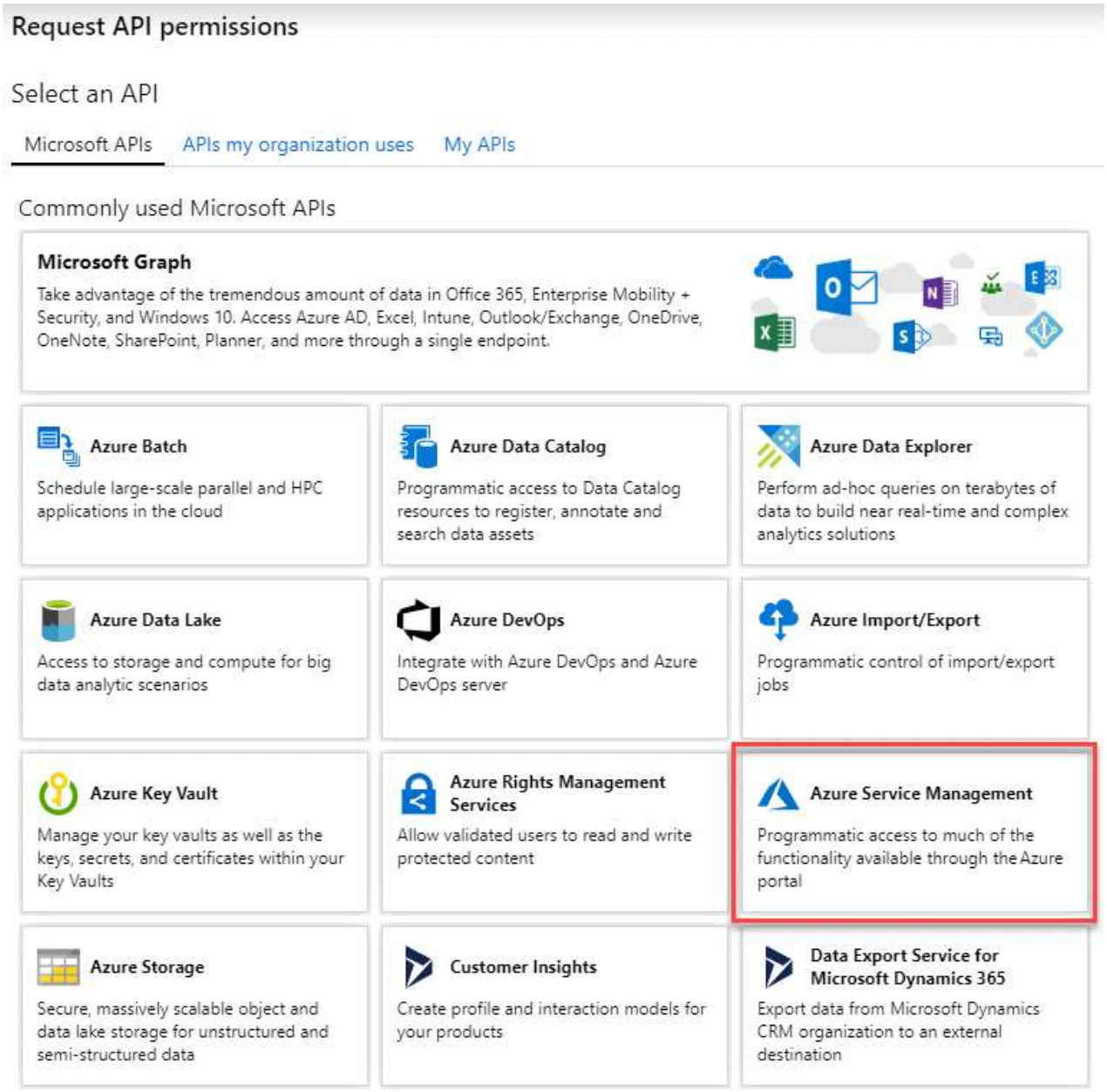
L'entità servizio ora dispone delle autorizzazioni di Azure necessarie per distribuire l'agente della console.

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.

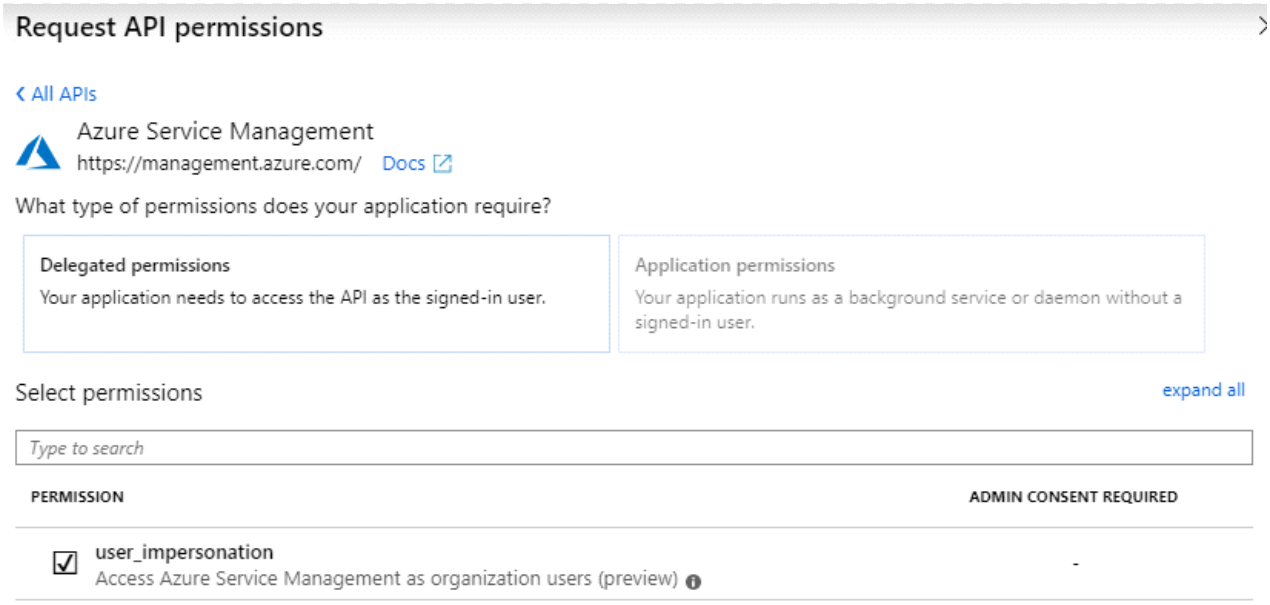
Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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**.

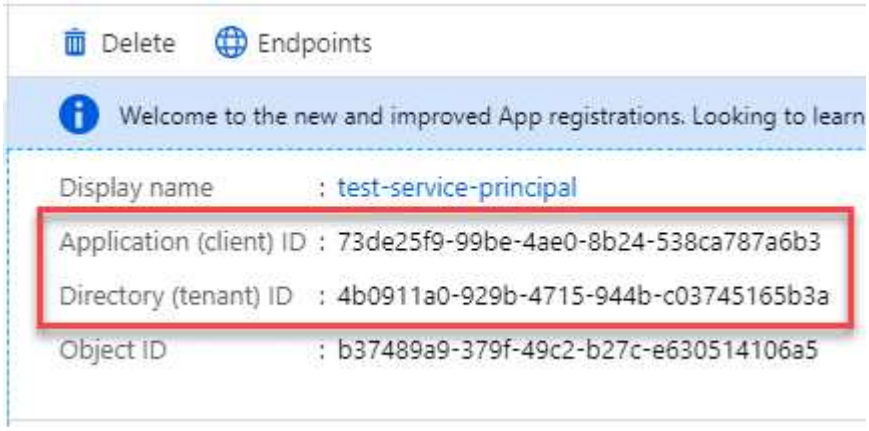


4. Selezionare **Accedi ad Azure Service Management come utenti dell'organizzazione** e quindi selezionare **Aggiungi autorizzazioni**.



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

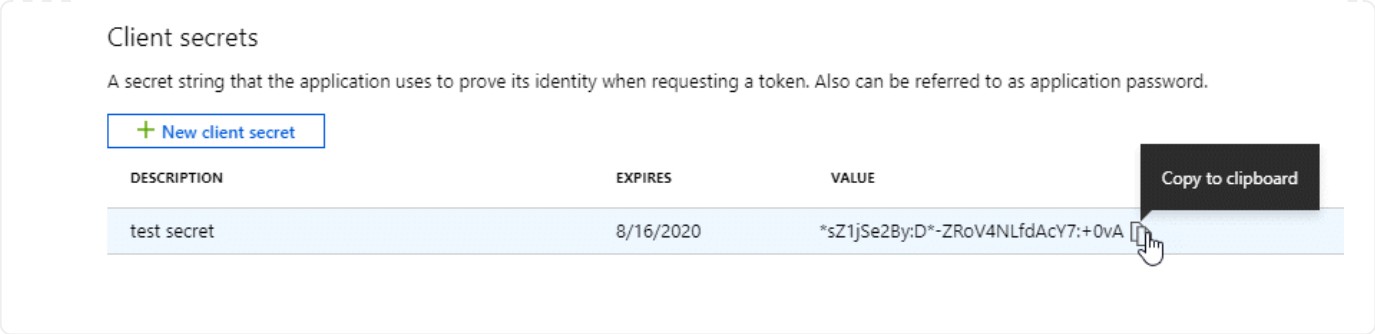
1. Nel servizio **Microsoft Entra ID**, seleziona **Registrazioni app** e seleziona l'applicazione.
2. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)**.



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

Informazioni sul copyright

Informazioni sul marchio commerciale