



## **Agenti della console**

NetApp Console setup and administration

NetApp  
January 27, 2026

# Sommario

Agenti della console . . . . .	1
Scopri di più sugli agenti NetApp Console . . . . .	1
Gli agenti della console devono essere operativi in ogni momento . . . . .	3
Posizioni supportate . . . . .	3
Comunicazione con i provider cloud . . . . .	3
Modalità limitata . . . . .	3
Come installare un agente Console . . . . .	3
Autorizzazioni del provider cloud . . . . .	4
Aggiornamenti degli agenti . . . . .	4
Manutenzione del sistema operativo e della VM . . . . .	4
Sistemi e agenti multipli . . . . .	5
Distribuisci un agente della console . . . . .	5
AWS . . . . .	5
Azzurro . . . . .	33
Google Cloud . . . . .	83
Installa un agente in locale . . . . .	118
Mantieni gli agenti della console . . . . .	157
Gestire un host VCenter o ESXi per l'agente della console . . . . .	157
Installa un certificato firmato da una CA per l'accesso alla console basata sul Web . . . . .	160
Configurare un agente Console per utilizzare un server proxy . . . . .	162
Risolvere i problemi dell'agente della console . . . . .	165
Disinstallare e rimuovere un agente Console . . . . .	170
Gestisci le credenziali del provider cloud . . . . .	171
AWS . . . . .	171
Azzurro . . . . .	185
Google Cloud . . . . .	199

# Agenti della console

## Scopri di più sugli agenti NetApp Console

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

Un agente Console consente di:

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

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

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

	Disponibile con agente	Disponibile senza agente
<b>Sistemi di archiviazione supportati:</b>		
Amazon FSx per ONTAP	Sì (funzionalità di scoperta e gestione)	Sì (solo scoperta)
Archiviazione Amazon S3	Sì	NO
Archiviazione BLOB di Azure	Sì	Sì
Azure NetApp Files	Sì	Sì
Cloud Volumes ONTAP	Sì	NO
Sistemi della serie E	Sì	NO
Google Cloud NetApp Volumes	Sì	Sì
Bucket di archiviazione di Google Cloud	Sì	NO

	<b>Disponibile con agente</b>	<b>Disponibile senza agente</b>
Sistemi StorageGRID	Sì	NO
Cluster ONTAP on-premise (gestione e individuazione avanzate)	Sì (gestione avanzata e scoperta)	No (solo scoperta di base)
<b>Servizi di gestione dello storage disponibili:</b>		
Avvisi	Sì	NO
Hub di automazione	Sì	Sì
Digital Advisor (Active IQ)	Sì	NO
Gestione delle licenze e degli abbonamenti	Sì	NO
Efficienza economica	Sì	NO
Metriche della dashboard della home page	Sì <sup>2</sup>	NO
Pianificazione del ciclo di vita	Sì	No <sup>1</sup>
Sostenibilità	Sì	NO
Aggiornamenti software	Sì	Sì
Carichi di lavoro NetApp	Sì	Sì
<b>Servizi dati disponibili:</b>		
NetApp Backup and Recovery	Sì	NO
Classificazione dei dati	Sì	NO
NetApp Cloud Tiering	Sì	NO
NetApp Copy and Sync	Sì	NO
NetApp Disaster Recovery	Sì	NO
NetApp Ransomware Resilience	Sì	NO
NetApp Volume Caching	Sì	NO

<sup>1</sup> È possibile visualizzare la pianificazione del ciclo di vita senza un agente della console, ma è necessario un

agente della console per avviare le azioni.

<sup>2</sup> Per ottenere metriche precise nella home page sono necessari agenti della console opportunamente dimensionati e configurati.

## Gli agenti della console devono essere operativi in ogni momento

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

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

## Posizioni supportate

È possibile installare gli agenti nelle seguenti posizioni:

- Servizi Web Amazon
- Microsoft Azure

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

- Google Cloud

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

- Presso la vostra sede

## Comunicazione con i provider cloud

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

## Modalità limitata

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

["Scopri di più sulle modalità di distribuzione NetApp Console"](#) .

## Come installare un agente Console

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

- "["Scopri di più sulle modalità di distribuzione NetApp Console"](#)"
- "["Inizia a usare NetApp Console in modalità standard"](#)"
- "["Inizia a usare NetApp Console in modalità limitata"](#)"

## Autorizzazioni del provider cloud

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

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

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

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

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

- ["Scopri come l'agente della console utilizza le autorizzazioni AWS"](#)
- ["Scopri come l'agente Console utilizza le autorizzazioni di Azure"](#)
- ["Scopri come l'agente della console utilizza le autorizzazioni di Google Cloud"](#)

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

## Aggiornamenti degli agenti

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

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

## Manutenzione del sistema operativo e della VM

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

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

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

[L'agente della console deve essere operativo in ogni momento .](#)

## Sistemi e agenti multipli

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

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

Ecco alcuni esempi di distribuzioni di agenti:

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

## Distribuisci un agente della console

### AWS

#### Opzioni di installazione dell'agente console in AWS

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

Sono disponibili le seguenti opzioni di installazione:

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

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

- "[Create 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): <ul style="list-style-type: none"><li>• Formazione delle nuvole</li><li>• Elastic Compute Cloud (EC2)</li><li>• Gestione dell'identità e degli accessi (IAM)</li><li>• Servizio di gestione delle chiavi (KMS)</li><li>• Servizio token di sicurezza (STS)</li><li>• Servizio di archiviazione semplice (S3)</li></ul>	Per gestire le risorse AWS. L'endpoint dipende dalla tua regione AWS. <a href="#">"Per i dettagli, fare riferimento alla documentazione AWS"</a>
Amazon FsX per NetApp ONTAP: <ul style="list-style-type: none"><li>• api.workloads.netapp.com</li></ul>	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 .
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.

Punti finali	Scopo
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \ <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a> .</li> <li>• Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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, deselectare 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
<p>Servizi AWS (amazonaws.com):</p> <ul style="list-style-type: none"><li>• Formazione delle nuvole</li><li>• Elastic Compute Cloud (EC2)</li><li>• Gestione dell'identità e degli accessi (IAM)</li><li>• Servizio di gestione delle chiavi (KMS)</li><li>• Servizio token di sicurezza (STS)</li><li>• Servizio di archiviazione semplice (S3)</li></ul>	<p>Per gestire le risorse AWS. L'endpoint dipende dalla tua regione AWS. "<a href="#">Per i dettagli, fare riferimento alla documentazione AWS</a>"</p>

Punti finali	Scopo
Amazon FsX per NetApp ONTAP: • <a href="https://api.workloads.netapp.com">api.workloads.netapp.com</a>	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 .
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.

Punti finali	Scopo
<ul style="list-style-type: none"> <li>\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \</li> <li><a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a></li> </ul>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>• Quando si distribuisce un nuovo agente, il controllo di convalida verifica la connettività agli endpoint correnti. Se usi "<a href="#">punti finali precedenti</a>" , il controllo di convalida fallisce. Per evitare questo errore, saltare il controllo di convalida.</li> </ul> <p>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a> .</p> <ul style="list-style-type: none"> <li>• Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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.

## Abilità 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		<p>9,6</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	<p>4.0.0 o versione successiva con la console in modalità standard o modalità limitata</p>	<p>Podman versione 5.4.0 con podman-compose 1.5.0.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>
Supportato in modalità di applicazione o modalità permissiva		<p>da 9,1 a 9,4</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	<p>3.9.50 o versione successiva con la Console in modalità standard o modalità limitata</p>	<p>Podman versione 4.9.4 con podman-compose 1.5.0.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>

Sistema operativo	Versioni del sistema operativo supportate	Versioni dell'agente supportate	Strumento contenitore richiesto	SELinux
Supportato in modalità di applicazione o modalità permissiva		<p>da 8,6 a 8,10</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	3.9.50 o versione successiva con la Console in modalità standard o modalità limitata	<p>Podman versione 4.6.1 o 4.9.4 con podman-compose 1.0.6.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>
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, dovrà cambiare 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): <ul style="list-style-type: none"><li>• Formazione delle nuvole</li><li>• Elastic Compute Cloud (EC2)</li><li>• Gestione dell'identità e degli accessi (IAM)</li><li>• Servizio di gestione delle chiavi (KMS)</li><li>• Servizio token di sicurezza (STS)</li><li>• Servizio di archiviazione semplice (S3)</li></ul>	Per gestire le risorse AWS. L'endpoint dipende dalla tua regione AWS. <a href="#">"Per i dettagli, fare riferimento alla documentazione AWS"</a>
Amazon FsX per NetApp ONTAP: <ul style="list-style-type: none"><li>• api.workloads.netapp.com</li></ul>	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 .
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.

Punti finali	Scopo
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \ <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>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.</li> <li>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a> .</li> <li>Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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, dovrà modificare la porta aardvark-dns.

- a. Eseguire l'SSH sulla macchina virtuale dell'agente Console.
- b. Aprire il file `/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://<em>ipaddress</em>>

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, ["seguì 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.

- "[Create 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.

<b>Punti finali</b>	<b>Scopo</b>
\ <a href="https://management.azure.com">https://management.azure.com</a> \ <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> \ <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> \ <a href="https://core.windows.net">https://core.windows.net</a>	Per gestire le risorse nelle aree pubbliche di Azure.

Punti finali	Scopo
\ <a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> \ <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> \ <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> \ <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	Per gestire le risorse nelle regioni di Azure Cina.
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.

Punti finali	Scopo
<ul style="list-style-type: none"> <li>\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \</li> <li><a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a></li> </ul>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>• Quando si distribuisce un nuovo agente, il controllo di convalida verifica la connettività agli endpoint correnti. Se usi "<a href="#">punti finali precedenti</a>" , il controllo di convalida fallisce. Per evitare questo errore, saltare il controllo di convalida.</li> <li>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. "<a href="#">Scopri come aggiornare l'elenco degli endpoint</a>" .</li> <li>• Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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.

## Abilità 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.

```
"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/read",
"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

```

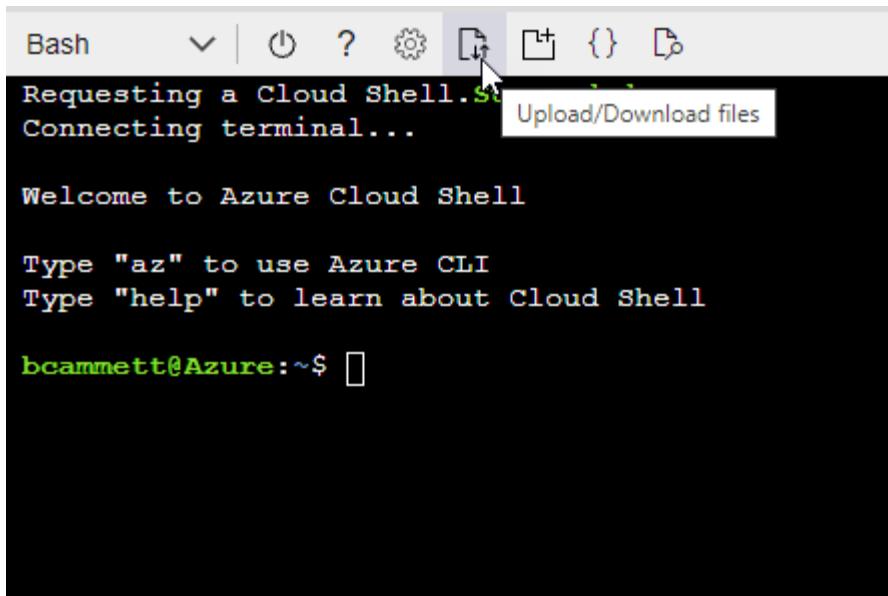
    "AssignableScopes": [
        "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz"
    ]

```

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.

- Inizia ["Azure Cloud Shell"](#) e scegli l'ambiente Bash.
- 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.

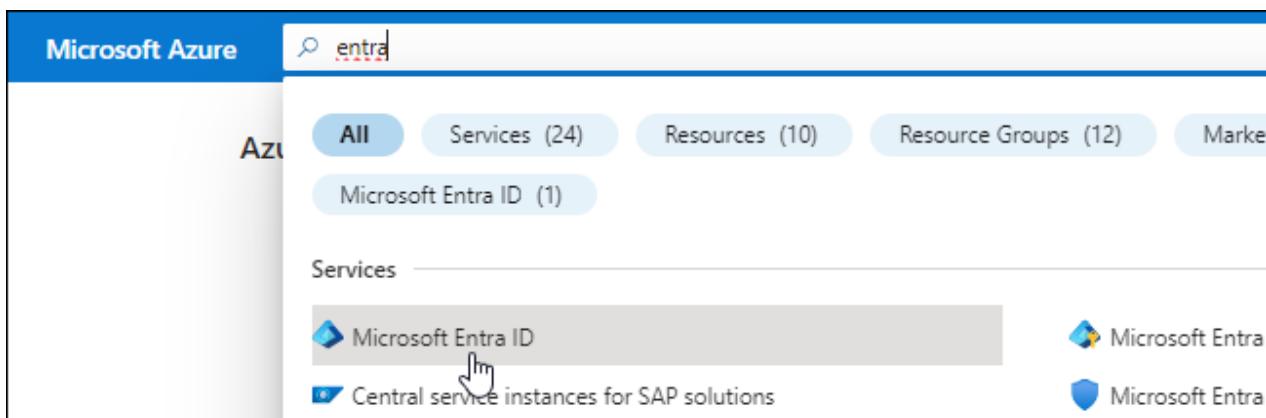
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie alla console.

### 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:

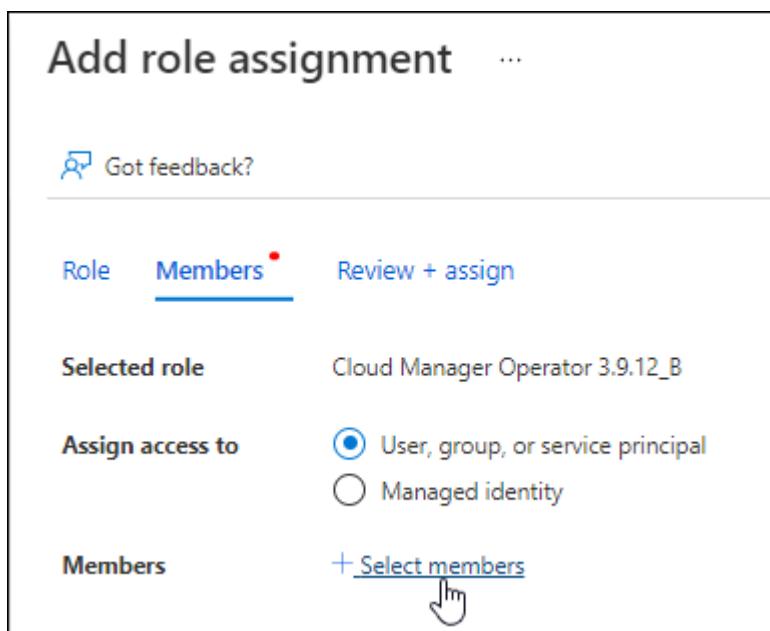
- **Nome:** inserisci un nome per l'applicazione.
- **Tipo di account:** seleziona un tipo di account (qualsiasi funzionerà con la NetApp Console).
- **URI di reindirizzamento:** puoi lasciare vuoto questo campo.

6. Seleziona **Registrati**.

Hai creato l'applicazione AD e il servizio principale.

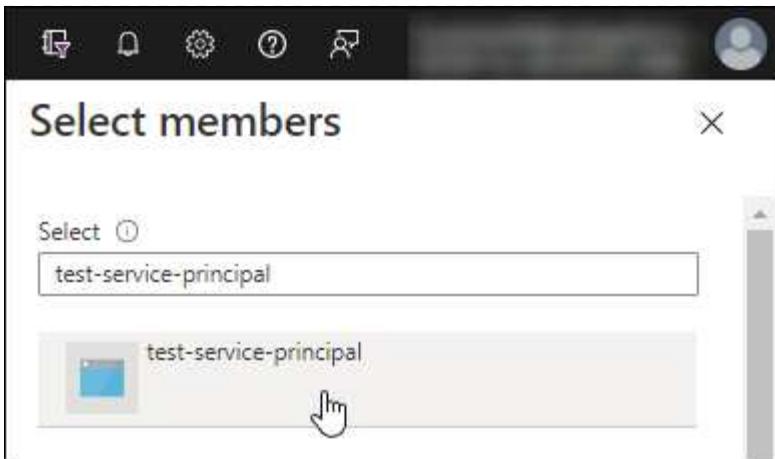
#### Assegna il ruolo personalizzato all'applicazione

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**.

## Request API permissions

### Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

#### Commonly used Microsoft APIs

##### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



##### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

##### Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

##### Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

##### Azure Data Lake

Access to storage and compute for big data analytic scenarios

##### Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

##### Azure Import/Export

Programmatic control of import/export jobs

##### Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

##### Azure Rights Management Services

Allow validated users to read and write protected content

##### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

##### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

##### Customer Insights

Create profile and interaction models for your products

##### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

## Request API permissions

[All APIs](#)

 Azure Service Management  
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

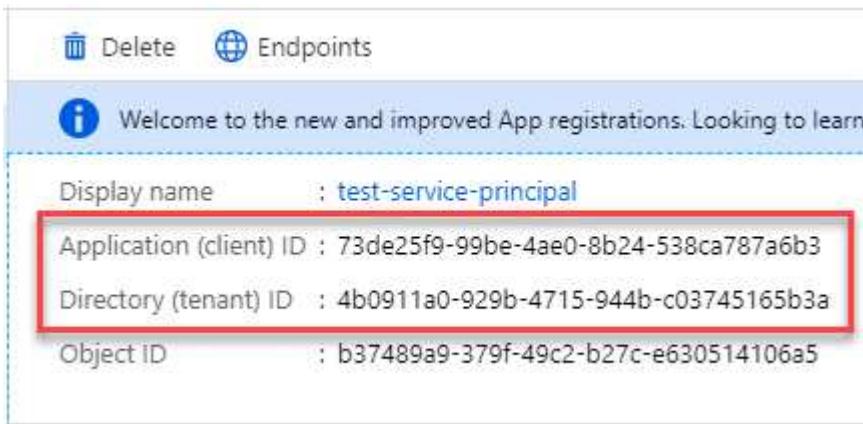
Select permissions

[expand all](#)

<input type="text"/> Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) <small> ⓘ</small>	

### 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)**.



The screenshot shows the Microsoft Entra ID App registrations page. It displays a registration for an application named "test-service-principal". The "Display name" is "test-service-principal". The "Application (client) ID" is "73de25f9-99be-4ae0-8b24-538ca787a6b3", and the "Directory (tenant) ID" is "4b0911a0-929b-4715-944b-c03745165b3a". These two IDs are highlighted with a red box. The "Object ID" is "b37489a9-379f-49c2-b27c-e630514106a5".

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.

>

## Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA

Copy to clipboard

## Risultato

Il tuo service principal è ora configurato e dovrà 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, deselectare 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
\ <a href="https://management.azure.com">https://management.azure.com</a> \ <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> \ <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> \ <a href="https://core.windows.net">https://core.windows.net</a>	Per gestire le risorse nelle aree pubbliche di Azure.
\ <a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> \ <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> \ <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> \ <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	Per gestire le risorse nelle regioni di Azure Cina.
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.

Punti finali	Scopo
<ul style="list-style-type: none"> <li>\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \</li> <li><a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a></li> </ul>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>• Quando si distribuisce un nuovo agente, il controllo di convalida verifica la connettività agli endpoint correnti. Se usi "<a href="#">punti finali precedenti</a>" , il controllo di convalida fallisce. Per evitare questo errore, saltare il controllo di convalida.</li> </ul> <p>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a> .</p> <ul style="list-style-type: none"> <li>• Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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.

## Abilità 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.

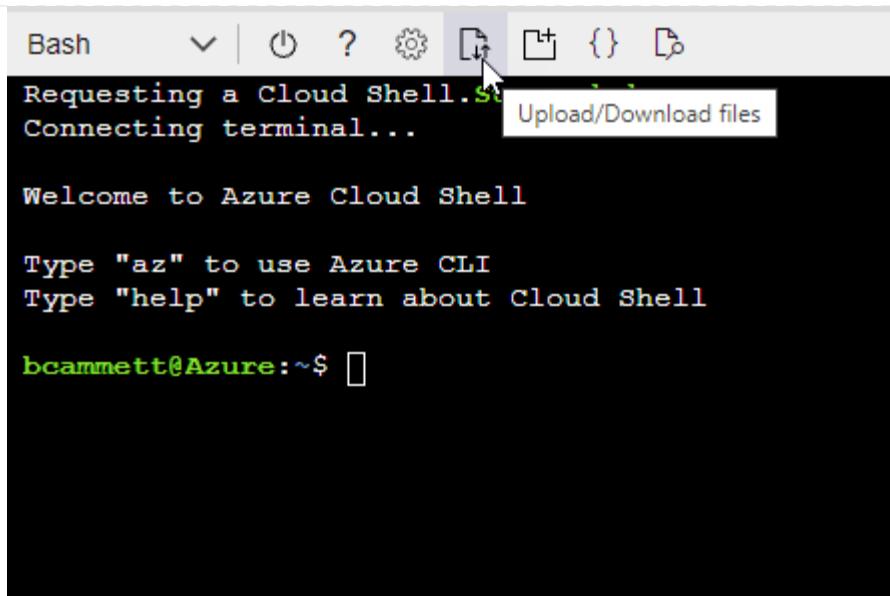
### Esempio

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"  
]
```

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. Inizia ["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

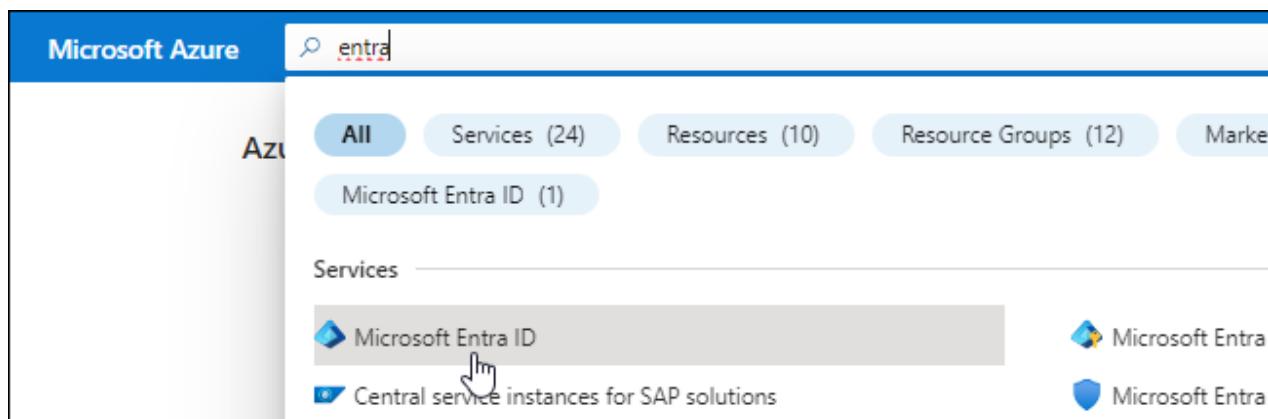
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie alla console.

#### 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"](#)

- Copia il contenuto del ["autorizzazioni di ruolo personalizzate per l'agente della console"](#) e salvarli in un file JSON.
- 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 .

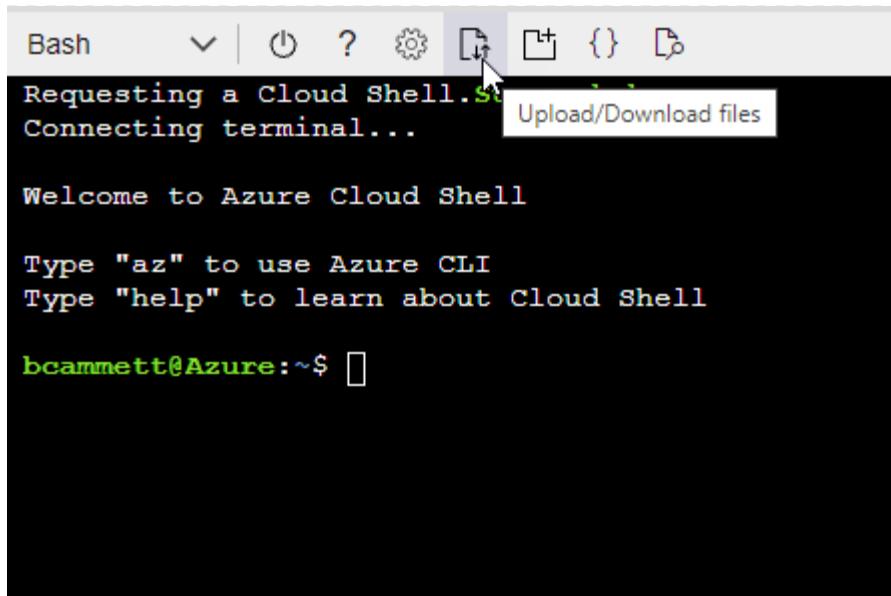
#### Esempio

```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"
]
```

- 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.

- Inizia ["Azure Cloud Shell"](#) e scegli l'ambiente Bash.
- Carica il file JSON.



```
Bash      |  ?  |  ⚙  |  ↻  |  { }  |  ⌂  |  ↻  |  { }  |  ⌂
Requesting a Cloud Shell...
Connecting terminal...
Upload/Download files

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

- 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:

- Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
- Seleziona l'abbonamento.
- Selezionare **Controllo accessi (IAM)** > **Aggiungi** > **Aggiungi assegnazione ruolo**.
- Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.
- Nella scheda **Membri**, completa i seguenti passaggi:
  - Mantieni selezionato **Utente, gruppo o entità servizio**.
  - Seleziona **Seleziona membri**.

## Add role assignment

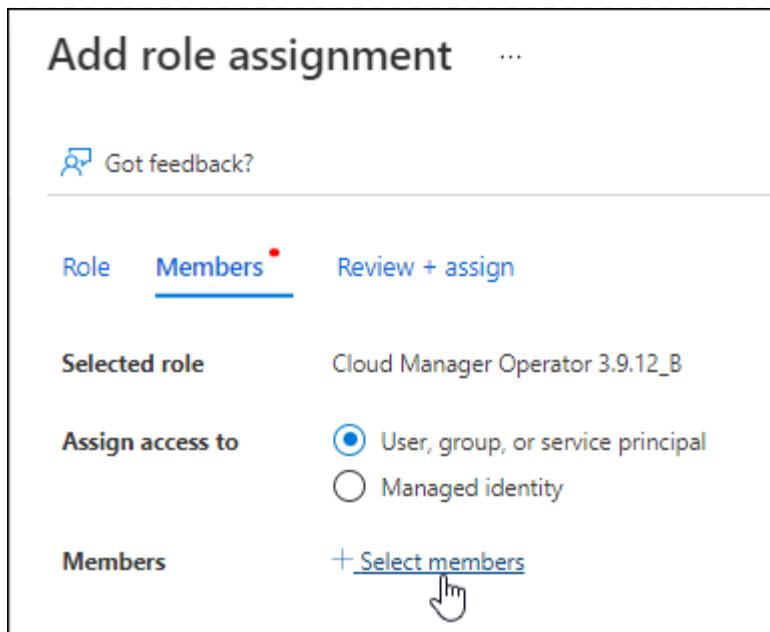
Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12\_B

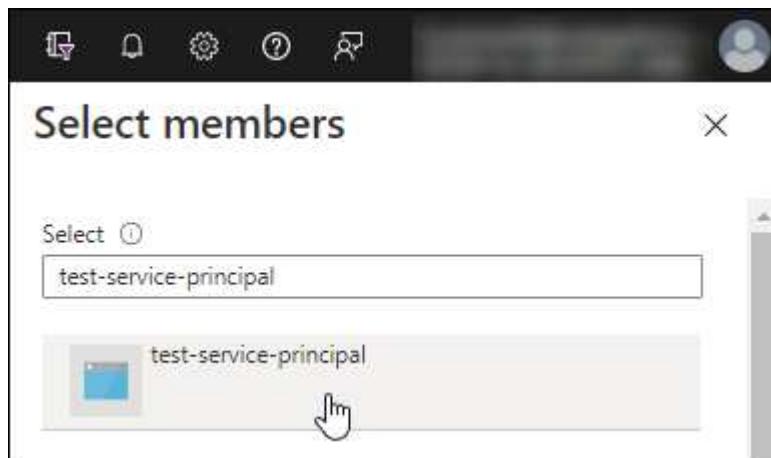
Assign access to  User, group, or service principal  Managed identity

Members [Select members](#) 



- Cerca il nome dell'applicazione.

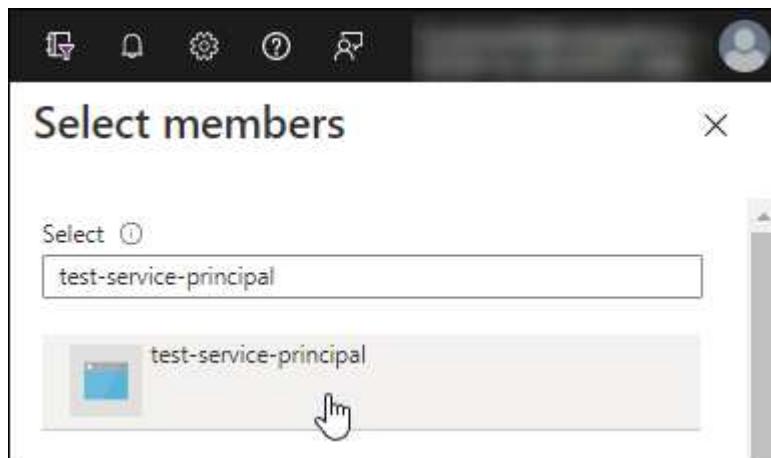
Ecco un esempio:



Select members

Select  test-service-principal

test-service-principal 



- 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.

### Request API permissions

#### Select an API

Microsoft APIs   APIs my organization uses   My APIs

#### Commonly used Microsoft APIs

##### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



##### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

##### Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

##### Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

##### Azure Data Lake

Access to storage and compute for big data analytic scenarios

##### Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

##### Azure Import/Export

Programmatic control of import/export jobs

##### Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

##### Azure Rights Management Services

Allow validated users to read and write protected content

##### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

##### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

##### Customer Insights

Create profile and interaction models for your products

##### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

## Request API permissions

[All APIs](#)

 Azure Service Management  
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

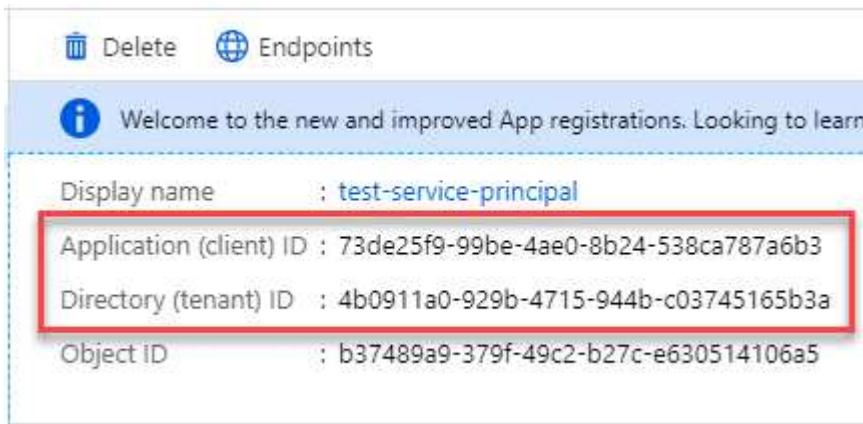
Select permissions

[expand all](#)

Type to search		PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation	Access Azure Service Management as organization users (preview)	<a href="#">Details</a>	

### 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)**.



The screenshot shows the Microsoft Entra ID App registrations page. It displays a registration for an application named 'test-service-principal'. The 'Display name' is 'test-service-principal'. The 'Application (client) ID' is '73de25f9-99be-4ae0-8b24-538ca787a6b3', and the 'Directory (tenant) ID' is '4b0911a0-929b-4715-944b-c03745165b3a'. These two IDs are highlighted with a red box. The 'Object ID' is 'b37489a9-379f-49c2-b27c-e630514106a5'.

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.

## Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	<a href="#">Copy to clipboard</a>
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA	

## 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:

<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

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

- Specificare l'organizzazione della console da associare all'agente della console.
- Inserisci un nome per il sistema.
- 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" .

- Selezione **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		<p>9,6</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	<p>4.0.0 o versione successiva con la console in modalità standard o modalità limitata</p>	<p>Podman versione 5.4.0 con podman-compose 1.5.0.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>
Supportato in modalità di applicazione o modalità permissiva		<p>da 9,1 a 9,4</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	<p>3.9.50 o versione successiva con la Console in modalità standard o modalità limitata</p>	<p>Podman versione 4.9.4 con podman-compose 1.5.0.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>

Sistema operativo	Versioni del sistema operativo supportate	Versioni dell'agente supportate	Strumento contenitore richiesto	SELinux
Supportato in modalità di applicazione o modalità permissiva		<p>da 8,6 a 8,10</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	3.9.50 o versione successiva con la Console in modalità standard o modalità limitata	<p>Podman versione 4.6.1 o 4.9.4 con podman-compose 1.0.6.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>
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, dovrà cambiare 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
\ <a href="https://management.azure.com">https://management.azure.com</a> \ <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> \ <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> \ <a href="https://core.windows.net">https://core.windows.net</a>	Per gestire le risorse nelle aree pubbliche di Azure.
\ <a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> \ <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> \ <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> \ <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	Per gestire le risorse nelle regioni di Azure Cina.
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.

Punti finali	Scopo
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \ <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>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.</li> <li>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a> .</li> <li>Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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.

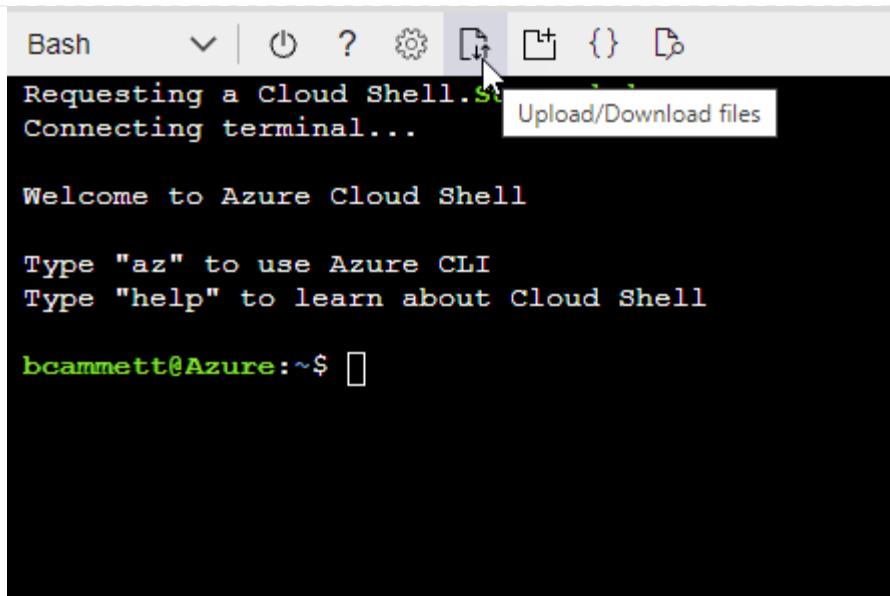
### Esempio

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"  
]
```

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. Inizia ["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

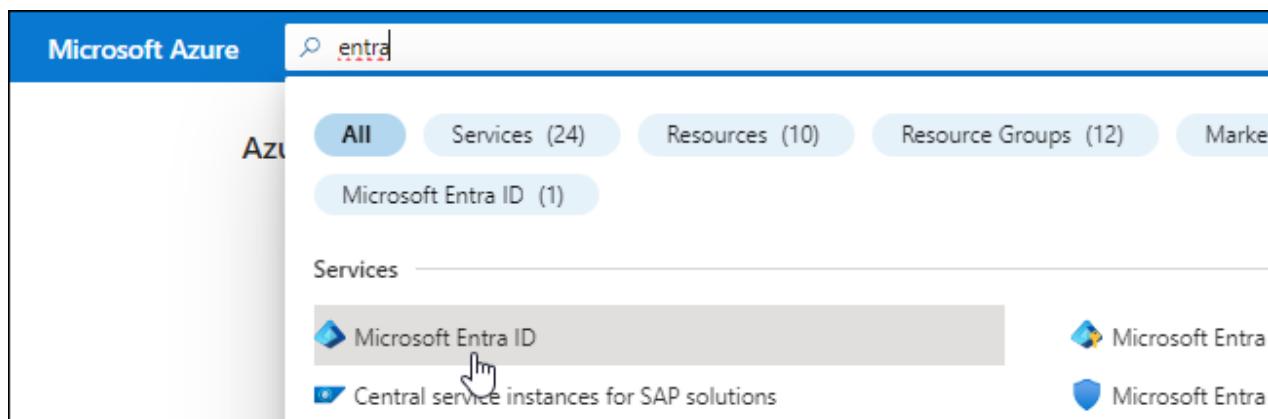
Creare e configurare un'entità servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie all'agente della console.

#### 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"](#)

- Copia il contenuto del ["autorizzazioni di ruolo personalizzate per l'agente della console"](#) e salvarli in un file JSON.
- 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 .

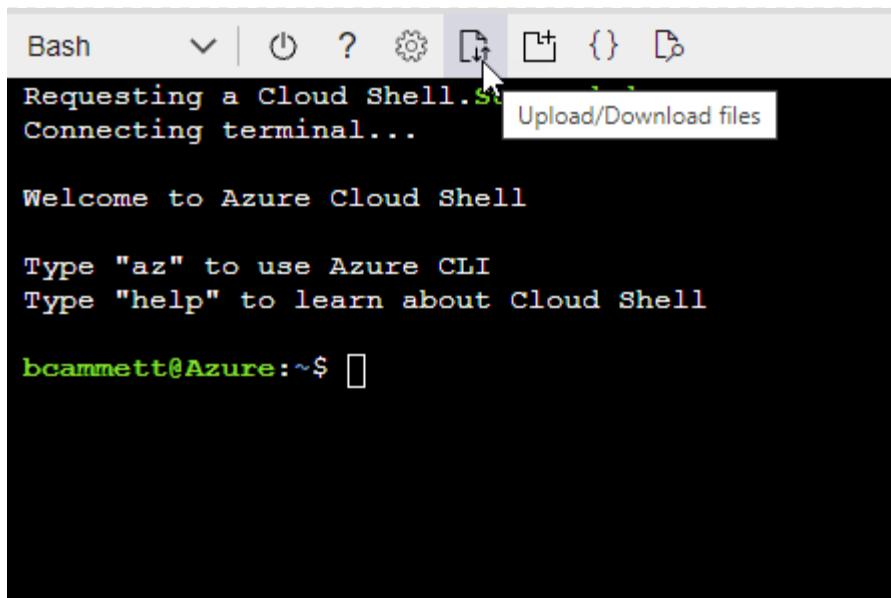
#### Esempio

```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"
]
```

- 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.

- Inizia ["Azure Cloud Shell"](#) e scegli l'ambiente Bash.
- Carica il file JSON.



Bash | ⌂ ? ⚙️ ⌂ { } ⌂

Requesting a Cloud Shell... Connecting terminal... Upload/Download files

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI  
Type "help" to learn about Cloud Shell

bcammett@Azure:~\$

- 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:

- Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
- Seleziona l'abbonamento.
- Selezionare **Controllo accessi (IAM)** > **Aggiungi** > **Aggiungi assegnazione ruolo**.
- Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.
- Nella scheda **Membri**, completa i seguenti passaggi:
  - Mantieni selezionato **Utente, gruppo o entità servizio**.
  - Seleziona **Seleziona membri**.

## Add role assignment

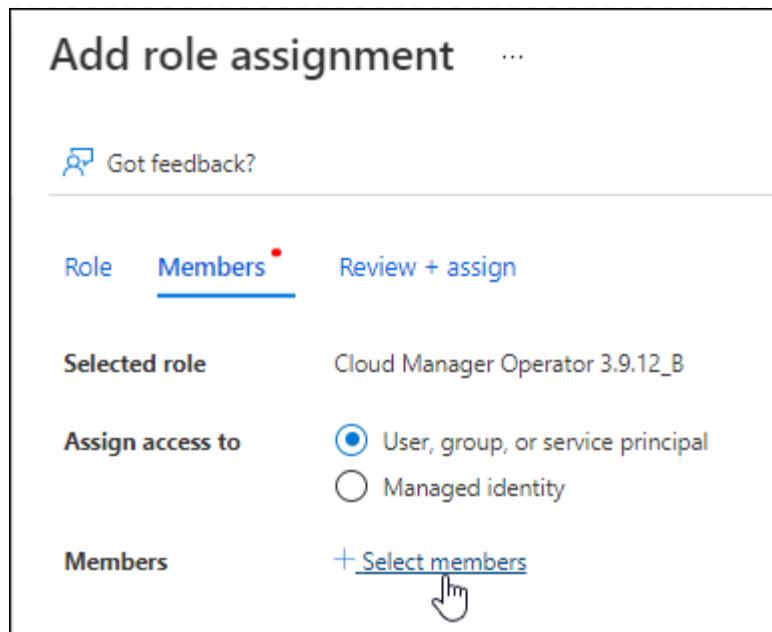
Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12\_B

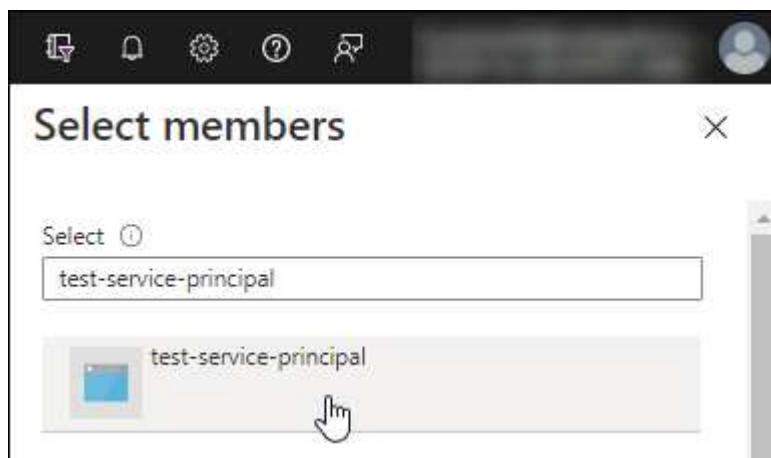
Assign access to  User, group, or service principal  Managed identity

Members [Select members](#) 



- Cerca il nome dell'applicazione.

Ecco un esempio:



Select members

Select  test-service-principal

test-service-principal 

- 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.

### Request API permissions

#### Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

#### Commonly used Microsoft APIs

##### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



##### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

##### Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

##### Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

##### Azure Data Lake

Access to storage and compute for big data analytic scenarios

##### Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

##### Azure Import/Export

Programmatic control of import/export jobs

##### Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

##### Azure Rights Management Services

Allow validated users to read and write protected content

##### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

##### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

##### Customer Insights

Create profile and interaction models for your products

##### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

## Request API permissions

[All APIs](#)

 Azure Service Management  
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

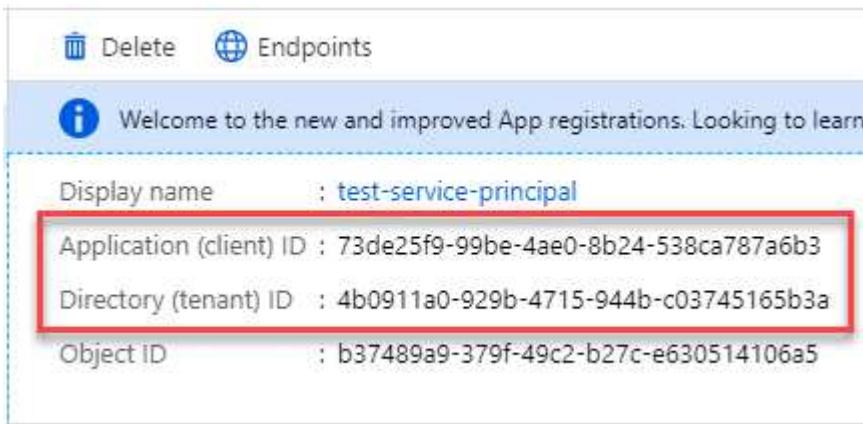
Select permissions

[expand all](#)

Type to search		PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation	Access Azure Service Management as organization users (preview)	<a href="#">Details</a>	

### 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)**.



The screenshot shows the Microsoft Entra ID App registrations page. It displays a registration for an application named 'test-service-principal'. The 'Display name' is 'test-service-principal'. The 'Application (client) ID' is '73de25f9-99be-4ae0-8b24-538ca787a6b3', and the 'Directory (tenant) ID' is '4b0911a0-929b-4715-944b-c03745165b3a'. These two IDs are highlighted with a red box. The 'Object ID' is 'b37489a9-379f-49c2-b27c-e630514106a5'.

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.

>

## Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	<a href="#">Copy to clipboard</a>
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA	

## Risultato

Il tuo service principal è ora configurato e dovrassi 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:

`<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>`

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["comprendere 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
\ <a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> \ <a href="https://compute.googleapis.com/compute/v1">https://compute.googleapis.com/compute/v1</a> \ <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> \ <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> \ <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> \ <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> \ <a href="https://iam.googleapis.com/">https://iam.googleapis.com/</a> \ <a href="https://v1">https://v1</a> \ <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> \ <a href="https://config.googleapis.com/v1/projects">https://config.googleapis.com/v1/projects</a>	Per gestire le risorse in Google Cloud.
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.

Punti finali	Scopo
<ul style="list-style-type: none"> <li>\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \</li> <li><a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a></li> </ul>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>Quando si distribuisce un nuovo agente, il controllo di convalida verifica la connettività agli endpoint correnti. Se usi "<a href="#">punti finali precedenti</a>" , il controllo di convalida fallisce. Per evitare questo errore, saltare il controllo di convalida.</li> <li>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. "<a href="#">Scopri come aggiornare l'elenco degli endpoint</a>" .</li> <li>Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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.

## Abilità 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	<a href="#">"Politica di distribuzione degli agenti"</a>	compute.network User	Distribuzione dell'agente nel progetto di servizio
account di servizio agente	Costume	Progetto di servizio	<a href="#">"Politica dell'account del servizio agente"</a>	compute.network User 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.network User	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.network User	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 Infrastructure Manager
- API di Cloud Deployment Manager V2
- API di registrazione cloud
- API di Cloud Resource Manager
- API di Compute Engine
- API di gestione dell'identità e dell'accesso (IAM)
- API del servizio di gestione delle chiavi cloud (KMS)

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

["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
\ <a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> \ <a href="https://compute.googleapis.com/compute/v1/">https://compute.googleapis.com/compute/v1/</a> \ <a href="https://cloudresourcemanager.googleapis.com/v1/projects/">https://cloudresourcemanager.googleapis.com/v1/projects/</a> \ <a href="https://www.googleapis.com/compute/beta/">https://www.googleapis.com/compute/beta/</a> \ <a href="https://storage.googleapis.com/storage/v1/">https://storage.googleapis.com/storage/v1/</a> \ <a href="https://www.googleapis.com/storage/v1/">https://www.googleapis.com/storage/v1/</a> \ <a href="https://iam.googleapis.com/">https://iam.googleapis.com/</a> \ v1 \ <a href="https://cloudkms.googleapis.com/v1/">https://cloudkms.googleapis.com/v1/</a> \ <a href="https://config.googleapis.com/v1/projects">https://config.googleapis.com/v1/projects</a>	Per gestire le risorse in Google Cloud.
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .

Punti finali	Scopo
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \ <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>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.</li> <li>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a> .</li> <li>Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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:

- Crea un file YAML che includa il contenuto del ["autorizzazioni dell'account di servizio per l'agente della console"](#).
- Da Google Cloud, attiva Cloud Shell.
- Carica il file YAML che include le autorizzazioni richieste.
- 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:

- Dal servizio IAM e amministrazione, seleziona **Account di servizio > Crea account di servizio**.
- Inserisci i dettagli dell'account di servizio e seleziona **Crea e continua**.
- Seleziona il ruolo che hai appena creato.
- 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.

- 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	<a href="#">"Politica di distribuzione degli agenti"</a>	compute.network User	Distribuzione dell'agente nel progetto di servizio
account di servizio agente	Costume	Progetto di servizio	<a href="#">"Politica dell'account del servizio agente"</a>	compute.network User 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.network User	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.network User	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 Infrastructure Manager
- API di Cloud Deployment Manager V2
- API di registrazione cloud
- API di Cloud Resource Manager
- API di Compute Engine
- API di gestione dell'identità e dell'accesso (IAM)
- API del servizio di gestione delle chiavi cloud (KMS)

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

["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		<p>9,6</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	<p>4.0.0 o versione successiva con la console in modalità standard o modalità limitata</p>	<p>Podman versione 5.4.0 con podman-compose 1.5.0.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>
Supportato in modalità di applicazione o modalità permissiva		<p>da 9,1 a 9,4</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	<p>3.9.50 o versione successiva con la Console in modalità standard o modalità limitata</p>	<p>Podman versione 4.9.4 con podman-compose 1.5.0.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>

Sistema operativo	Versioni del sistema operativo supportate	Versioni dell'agente supportate	Strumento contenitore richiesto	SELinux
Supportato in modalità di applicazione o modalità permissiva		<p>da 8,6 a 8,10</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	3.9.50 o versione successiva con la Console in modalità standard o modalità limitata	<p>Podman versione 4.6.1 o 4.9.4 con podman-compose 1.0.6.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a></p>
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, dovrà cambiare 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
\ <a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> \ <a href="https://compute.googleapis.com/compute/v1">https://compute.googleapis.com/compute/v1</a> \ <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> \ <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> \ <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> \ <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> \ <a href="https://iam.googleapis.com">https://iam.googleapis.com</a> / v1 \ <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> \ <a href="https://config.googleapis.com/v1/projects">https://config.googleapis.com/v1/projects</a>	Per gestire le risorse in Google Cloud.
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.

Punti finali	Scopo
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \ <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>Quando si distribuisce un nuovo agente, il controllo di convalida verifica la connettività agli endpoint correnti. Se usi "<a href="#">punti finali precedenti</a>" , il controllo di convalida fallisce. Per evitare questo errore, saltare il controllo di convalida.</li> </ul> <p>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. "<a href="#">Scopri come aggiornare l'elenco degli endpoint</a>".</p> <ul style="list-style-type: none"> <li>Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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.

## Abilità 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:

- Crea un file YAML che include il contenuto del ["autorizzazioni dell'account di servizio per l'agente della console"](#).
- Da Google Cloud, attiva Cloud Shell.
- Carica il file YAML che include le autorizzazioni richieste.
- 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:

- Dal servizio IAM e amministrazione, seleziona **Account di servizio > Crea account di servizio**.
- Inserisci i dettagli dell'account di servizio e seleziona **Crea e continua**.
- Seleziona il ruolo che hai appena creato.
- 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	<a href="#">"Politica di distribuzione degli agenti"</a>	compute.network User	Distribuzione dell'agente nel progetto di servizio
account di servizio agente	Costume	Progetto di servizio	<a href="#">"Politica dell'account del servizio agente"</a>	compute.network User 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.network User	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.network User	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 Infrastructure Manager
- API di Cloud Deployment Manager V2
- API di registrazione cloud
- API di Cloud Resource Manager
- API di Compute Engine
- API di gestione dell'identità e dell'accesso (IAM)
- API del servizio di gestione delle chiavi cloud (KMS)

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

["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, dovrà 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:

<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

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.

## Install a local agent

### Installare manualmente un agente Console in locale

Install a local agent Console, then log in and configure it to work with your organization Console.



If you are a VMWare user, you can use an OVA to install the Console agent in your VCenter. ["Scopri di più sull'installazione di un agente in un VCenter."](#)

Before proceeding with the installation, it is necessary to ensure that the host (VM or host Linux) satisfies the requirements.

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		<p>9,6</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	<p>4.0.0 o versione successiva con la console in modalità standard o modalità limitata</p>	<p>Podman versione 5.4.0 con podman-compose 1.5.0.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>
Supportato in modalità di applicazione o modalità permissiva		<p>da 9,1 a 9,4</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	<p>3.9.50 o versione successiva con la Console in modalità standard o modalità limitata</p>	<p>Podman versione 4.9.4 con podman-compose 1.5.0.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>

Sistema operativo	Versioni del sistema operativo supportate	Versioni dell'agente supportate	Strumento contenitore richiesto	SELinux
Supportato in modalità di applicazione o modalità permissiva		<p>da 8,6 a 8,10</p> <ul style="list-style-type: none"> <li>• Solo versioni in lingua inglese.</li> <li>• 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.</li> </ul>	3.9.50 o versione successiva con la Console in modalità standard o modalità limitata	<p>Podman versione 4.6.1 o 4.9.4 con podman-compose 1.0.6.</p> <p><a href="#">Visualizza i requisiti di configurazione di Podman</a>.</p>
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): <ul style="list-style-type: none"><li>• Formazione delle nuvole</li><li>• Elastic Compute Cloud (EC2)</li><li>• Gestione dell'identità e degli accessi (IAM)</li><li>• Servizio di gestione delle chiavi (KMS)</li><li>• Servizio token di sicurezza (STS)</li><li>• Servizio di archiviazione semplice (S3)</li></ul>	Per gestire le risorse AWS. L'endpoint dipende dalla tua regione AWS. <a href="#">"Per i dettagli, fare riferimento alla documentazione AWS"</a>
Amazon FsX per NetApp ONTAP: <ul style="list-style-type: none"><li>• api.workloads.netapp.com</li></ul>	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 .
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	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	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a>.</p> <ul style="list-style-type: none"> <li>• Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \ <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a> .</p> <ul style="list-style-type: none"> <li>• Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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 .

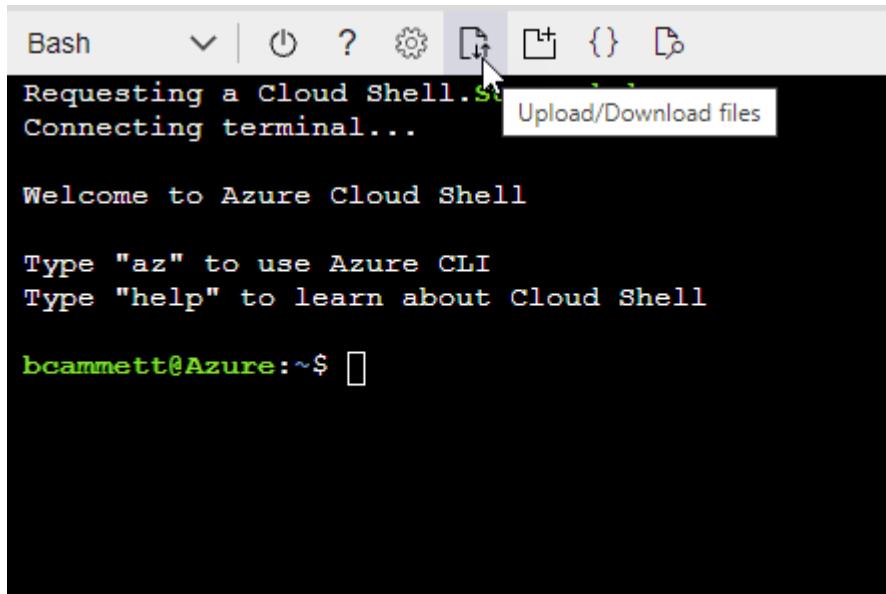
### Esempio

```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"
]
```

- 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**.

## Add role assignment

Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12\_B

Assign access to  User, group, or service principal  Managed identity

Members [Select members](#) 

- 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.

### Request API permissions

#### Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

#### Commonly used Microsoft APIs

##### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



##### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

##### Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

##### Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

##### Azure Data Lake

Access to storage and compute for big data analytic scenarios

##### Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

##### Azure Import/Export

Programmatic control of import/export jobs

##### Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

##### Azure Rights Management Services

Allow validated users to read and write protected content

##### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

##### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

##### Customer Insights

Create profile and interaction models for your products

##### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

## Request API permissions

[All APIs](#)

 Azure Service Management  
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

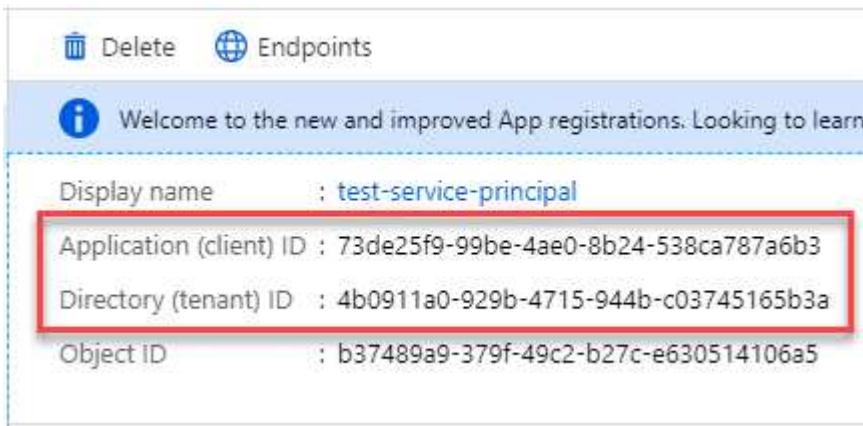
Select permissions

[expand all](#)

<input type="text"/> Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) <small> ⓘ</small>	

### 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)**.



The screenshot shows the Microsoft Entra ID App registrations page. It displays a list of registered applications. One application is highlighted, showing its details: Display name: test-service-principal. The Application (client) ID is 73de25f9-99be-4ae0-8b24-538ca787a6b3. The Directory (tenant) ID is 4b0911a0-929b-4715-944b-c03745165b3a. The Object ID is b37489a9-379f-49c2-b27c-e630514106a5. The Application (client) ID and Directory (tenant) ID are highlighted with a red box.

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.

## Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA	

## 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 dovrà installare Podman o Docker, a seconda del tuo sistema operativo Linux.

### Install 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, dovrà cambiare 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.

- Eseguire l'SSH sulla macchina virtuale dell'agente Console.
- 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): <ul style="list-style-type: none"><li>• Formazione delle nuvole</li><li>• Elastic Compute Cloud (EC2)</li><li>• Gestione dell'identità e degli accessi (IAM)</li><li>• Servizio di gestione delle chiavi (KMS)</li><li>• Servizio token di sicurezza (STS)</li><li>• Servizio di archiviazione semplice (S3)</li></ul>	Per gestire le risorse AWS. L'endpoint dipende dalla tua regione AWS. <a href="#">"Per i dettagli, fare riferimento alla documentazione AWS"</a>
Amazon FsX per NetApp ONTAP: <ul style="list-style-type: none"><li>• api.workloads.netapp.com</li></ul>	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 .
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.

Punti finali	Scopo
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \ <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a>.</p> <ul style="list-style-type: none"> <li>• Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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
\ <a href="https://management.azure.com">https://management.azure.com</a> \ <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> \ <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> \ <a href="https://core.windows.net">https://core.windows.net</a>	Per gestire le risorse nelle aree pubbliche di Azure.
\ <a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> \ <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> \ <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> \ <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	Per gestire le risorse nelle regioni di Azure Cina.

Punti finali	Scopo
\ <a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp .
\ <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	Per aggiornare le credenziali del sito di supporto NetApp (NSS) o per aggiungere nuove credenziali NSS alla NetApp Console.
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp , nonché per ricevere aggiornamenti software per Cloud Volumes ONTAP.
\ <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> \ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> \ <a href="https://console.netapp.com">https://console.netapp.com</a> \ <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> \ <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	Per fornire funzionalità e servizi all'interno della NetApp Console.
\ <a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> \ <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>Per ottenere immagini per gli aggiornamenti dell'agente della console.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p>Sebbene gli endpoint precedenti siano ancora supportati, NetApp consiglia di aggiornare le regole del firewall agli endpoint correnti il prima possibile. <a href="#">"Scopri come aggiornare l'elenco degli endpoint"</a> .</p> <ul style="list-style-type: none"> <li>• Quando esegui l'aggiornamento agli endpoint correnti nel firewall, gli agenti esistenti continueranno a funzionare.</li> </ul>

## 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 .

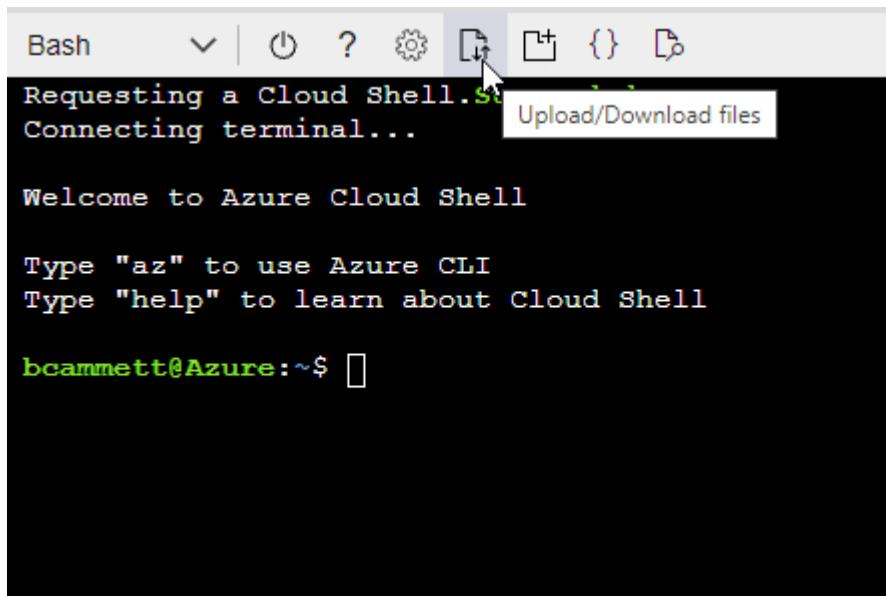
### Esempio

```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"
]
```

- 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**.

## Add role assignment

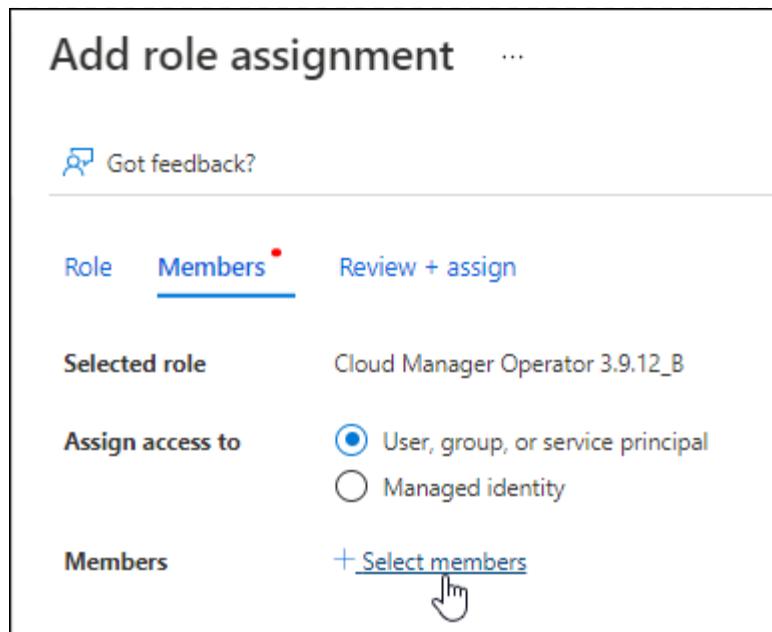
Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12\_B

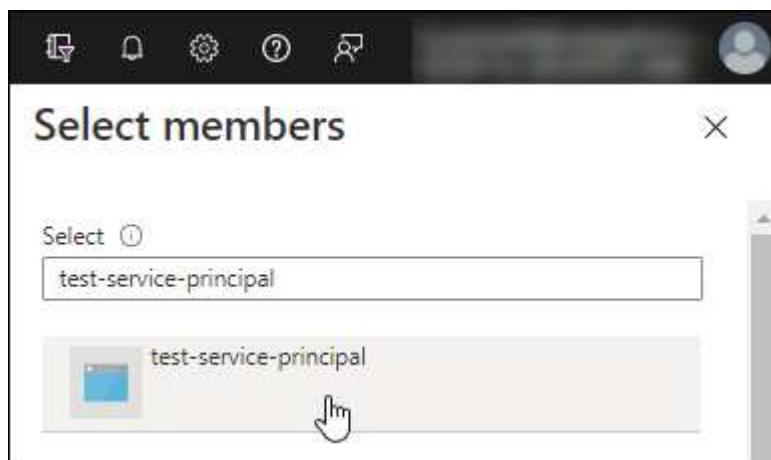
Assign access to  User, group, or service principal  Managed identity

Members [Select members](#)



- 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.

### Request API permissions

#### Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

#### Commonly used Microsoft APIs

##### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



##### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

##### Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

##### Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

##### Azure Data Lake

Access to storage and compute for big data analytic scenarios

##### Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

##### Azure Import/Export

Programmatic control of import/export jobs

##### Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

##### Azure Rights Management Services

Allow validated users to read and write protected content

##### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

##### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

##### Customer Insights

Create profile and interaction models for your products

##### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

## Request API permissions

[All APIs](#)

 Azure Service Management  
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

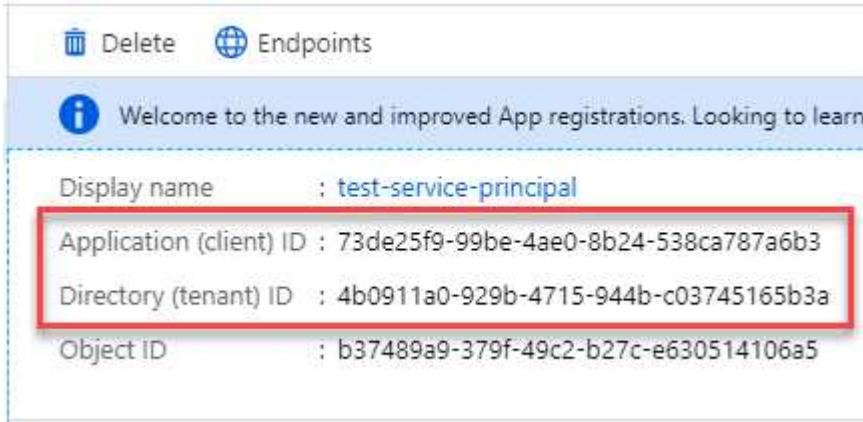
Select permissions

[expand all](#)

<input type="text"/> Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) <small> ⓘ</small>	

### 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)**.



The screenshot shows the Microsoft Entra ID App registrations page. It displays a list of registered applications. One application is highlighted, showing its details: Display name: test-service-principal. The Application (client) ID is 73de25f9-99be-4ae0-8b24-538ca787a6b3. The Directory (tenant) ID is 4b0911a0-929b-4715-944b-c03745165b3a. These two IDs are highlighted with a red box. The Object ID is b37489a9-379f-49c2-b27c-e630514106a5.

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.

## Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	<a href="#">Copy to clipboard</a>
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA	

## 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 <b>Distribuisci modello OVF</b> .... b. Scegliere il file OVA dall'URL o andare alla sua posizione, quindi selezionare <b>Avanti</b> .	a. Vai alla tua libreria di contenuti e seleziona l'OVA dell'agente Console. b. Seleziona <b>Azioni &gt; Nuova VM da questo modello</b>

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	<ul style="list-style-type: none"><li>• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale</li><li>• Utilizzato durante il processo di aggiornamento Cloud Volumes ONTAP</li></ul>
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale

## Mantieni gli agenti della console

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

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

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

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

### Limitazioni

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

### Accedi alla console di manutenzione della VM

È possibile accedere alla console di manutenzione dal client VSphere.

#### Passi

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

### Cambia la password dell'utente principale

Puoi cambiare la password per `maint` utente.

#### Passi

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

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

#### **Aumentare la CPU o la RAM dell'istanza della VM**

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

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

#### **Passaggi nel client VSphere**

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

#### **Passaggi nella console di manutenzione**

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

#### **Visualizza le impostazioni di rete per la VM dell'agente**

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

#### **Passi**

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

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

#### Aggiornare le route statiche per la VM dell'agente

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

#### Passi

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

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

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

#### Passi

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

#### Accedi agli strumenti diagnostici dell'agente

Accedi agli strumenti diagnostici per risolvere i problemi con l'agente Console. L'assistenza NetApp potrebbe chiederti di farlo durante la risoluzione dei problemi.

## Passi

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

## Accedi agli strumenti diagnostici dell'agente da remoto

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

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

## Passi

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

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

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

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

## Installa un certificato HTTPS

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

### Informazioni su questo compito

È possibile installare il certificato utilizzando una delle seguenti opzioni:

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

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

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

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

### Passi

- Selezionare **Amministrazione > Agenti**.
  - Nella pagina **Panoramica**, seleziona il menu azioni per un agente Console e seleziona **Configurazione HTTPS**.
- Per modificarlo, è necessario che l'agente della console sia connesso.
- Nella pagina Configurazione HTTPS, installa un certificato generando una richiesta di firma del certificato (CSR) o installando il tuo certificato firmato da una CA:

Opzione	Descrizione
Generare una CSR	<ol style="list-style-type: none"><li>Immettere il nome host o il DNS dell'host dell'agente della console (il suo nome comune), quindi selezionare <b>Genera CSR</b>. La console visualizza una richiesta di firma del certificato.</li><li>Utilizzare il CSR per inviare una richiesta di certificato SSL a una CA. Il certificato deve utilizzare il formato X.509 codificato Base-64 Privacy Enhanced Mail (PEM).</li><li>Carica il file del certificato e seleziona <b>Installa</b>.</li></ol>
Installa il tuo certificato firmato da CA	<ol style="list-style-type: none"><li>Selezionare <b>Installa certificato firmato da CA</b>.</li><li>Caricare sia il file del certificato che la chiave privata, quindi selezionare <b>Installa</b>. Il certificato deve utilizzare il formato X.509 codificato Base-64 Privacy Enhanced Mail (PEM).</li></ol>

## Risultato

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

## Rinnova il certificato HTTPS della console

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

### Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona il menu azioni per un agente Console e seleziona **Configurazione HTTPS**.  
Vengono visualizzati i dettagli relativi al certificato, inclusa la data di scadenza.
3. Selezionare **Cambia certificato** e seguire i passaggi per generare una CSR o installare il proprio certificato firmato da una CA.

## Configurare un agente Console per utilizzare un server proxy

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

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

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

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

## Configurazioni supportate

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



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

## Abilita un proxy esplicito su un agente della console

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

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

### Passi

1. Selezionare **Amministrazione > Agenti**.
  2. Nella pagina **Panoramica**, seleziona il menu azioni per un agente della console e seleziona **Modifica agente**.
- Per modificarlo, l'agente della console deve essere attivo.
3. Selezionare **Configurazione proxy HTTP**.
  4. Selezionare **Proxy esplicito** nel campo **Tipo di configurazione**.
  5. Seleziona **Abilita proxy**.
  6. Specificare il server utilizzando la sintassi `<a href="http://<em>address:port</em>" class="bare">http://<em>address:port</em></a>` O `<a href="https://<em>address:port</em>" class="bare">https://<em>address:port</em></a>`
  7. Specificare un nome utente e una password se è richiesta l'autenticazione di base per il server.

Notare quanto segue:

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

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

Ad esempio: netapp%92proxy

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

## 8. Seleziona **Salva**.

### Abilita un proxy trasparente per un agente della console

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

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

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

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

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

#### Passi

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

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

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

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

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

## Modificare il proxy trasparente per l'agente della console

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



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

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

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

## Abilita il traffico API diretto

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

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

["Scopri di più sull'utilizzo di un collegamento privato di Azure o di endpoint di servizio con Cloud Volumes ONTAP"](#)

### Passi

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

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

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

## Risolvere i problemi dell'agente della console

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

Se si dispone di un account del sito di supporto NetApp , è anche possibile visualizzare "[Base di conoscenza NetApp](#) ."

## Messaggi di errore comuni e risoluzioni

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

Messaggio di errore	Spiegazione	Cosa fare
Impossibile caricare l'interfaccia utente dell'agente della console	L'installazione dell'agente non è riuscita	<ul style="list-style-type: none"> <li>• Verificare che il servizio Service Manager sia attivo.</li> <li>• Verificare che tutti i contenitori siano in esecuzione.</li> <li>• Assicurati che il tuo firewall consenta l'accesso al servizio sulla porta 8888.</li> <li>• Se i problemi persistono, contatta l'assistenza.</li> </ul>
Impossibile accedere all'interfaccia utente dell'agente NetApp	Questo messaggio viene visualizzato quando si tenta di accedere all'indirizzo IP di un agente. L'agente potrebbe non riuscire a inizializzarsi se non dispone dell'accesso di rete corretto o se è instabile.	<ul style="list-style-type: none"> <li>• Connetersi all'agente della console.</li> <li>• Verificare che il servizio Service Manager</li> <li>• Verificare che l'agente disponga dell'accesso alla rete di cui ha bisogno. <a href="#">"Scopri di più sugli endpoint di accesso alla rete richiesti."</a></li> </ul>
Impossibile caricare le impostazioni dell'agente	La Console visualizza questo messaggio quando si tenta di accedere alla pagina delle impostazioni dell'agente.	<ul style="list-style-type: none"> <li>• Verificare se il contenitore OCCM è in esecuzione e funzionante.</li> <li>• Se il problema persiste, contattare l'assistenza.</li> </ul>
Impossibile caricare le informazioni di supporto per l'agente.	Questo messaggio viene visualizzato se l'agente non riesce ad accedere al tuo account di supporto.	<ul style="list-style-type: none"> <li>• Verificare che l'agente abbia accesso in uscita agli endpoint richiesti. <a href="#">"Scopri di più sugli endpoint di accesso alla rete richiesti."</a></li> </ul>

## Controllare lo stato dell'agente della console

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

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

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

## Docker (per distribuzioni Ubuntu e VCenter)

```
docker ps -a
```

## Podman (per distribuzioni RedHat Enterprise Linux)

```
podman ps -a
```

## Visualizza la versione dell'agente della console

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

### Passi

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

La Console visualizza la versione nella parte superiore della pagina.

## Verifica l'accesso alla rete

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

## Eseguire controlli di configurazione sull'agente Console

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

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



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

### Passi dalla console

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

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

## Problemi di installazione dell'agente della console

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

È inoltre possibile accedere al report di convalida in formato JSON e ai log di configurazione direttamente dall'host dell'agente della console nelle seguenti directory:

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

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

#### Disabilitare i controlli di configurazione per le installazioni manuali

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

#### Passi

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

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

#### Passi

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

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

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

```
"skipConfigCheck": true
```

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

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

## Lavora con il supporto NetApp

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

### Trova l'ID dell'agente della console

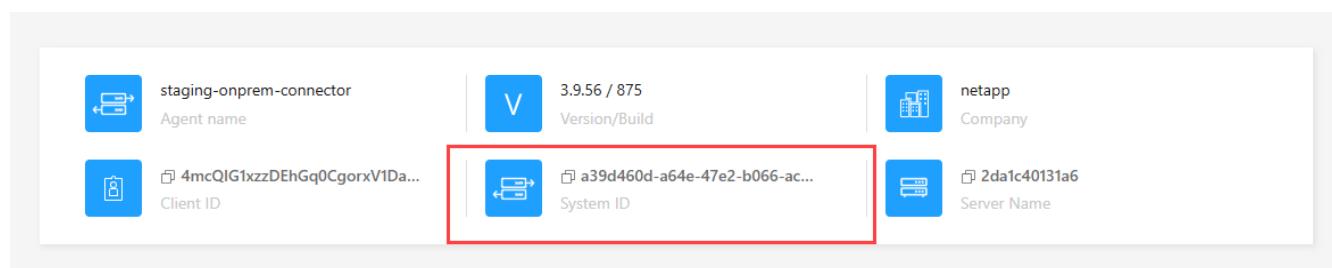
Per iniziare, potrebbe essere necessario l'ID di sistema del tuo agente Console. L'ID viene solitamente utilizzato per scopi di licenza e risoluzione dei problemi.

#### Passi

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

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

#### Esempio



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

### Scarica o invia un messaggio AutoSupport

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



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

#### Passi

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

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

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

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

## Fare un passo

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

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

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

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

["Scopri di più sulla chiamata API /occm/config"](#)

## Ottieni assistenza dalla Knowledge Base NetApp

["Visualizza le informazioni sulla risoluzione dei problemi create dal team di supporto NetApp" .](#)

## Disinstallare e rimuovere un agente Console

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

["Scopri di più sulle modalità di distribuzione NetApp Console" .](#)

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

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

### Passi

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

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

*silent* esegue lo script senza chiedere conferma.

## Rimuovere gli agenti della console dalla console

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

Tenere presente quanto segue sulla rimozione di un agente Console:

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

## Passi

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

## Gestisci le credenziali del provider cloud

### AWS

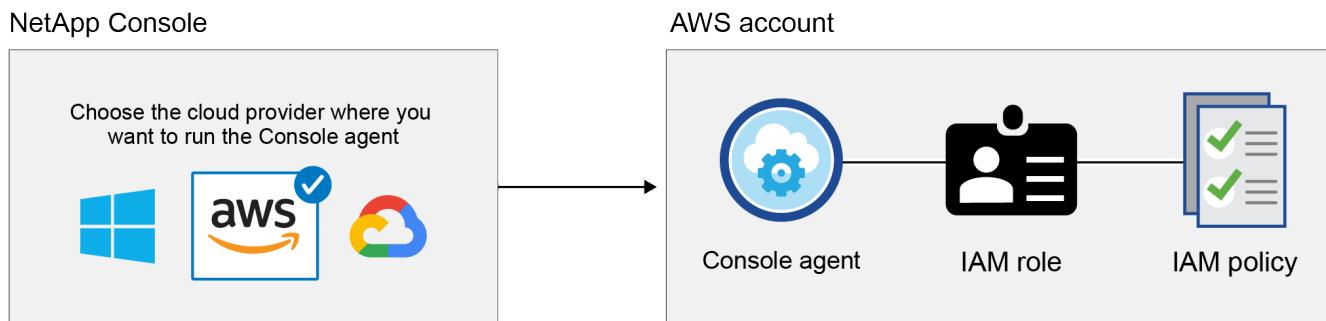
#### Scopri di più sulle credenziali e le autorizzazioni AWS nella NetApp Console

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

#### Credenziali AWS iniziali

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

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



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

Details & Credentials			
Instance Profile	██████████	QA Subscription	
Credentials	Account ID	Marketplace Subscription	
			<a href="#">Edit Credentials</a>

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

#### Credenziali AWS aggiuntive

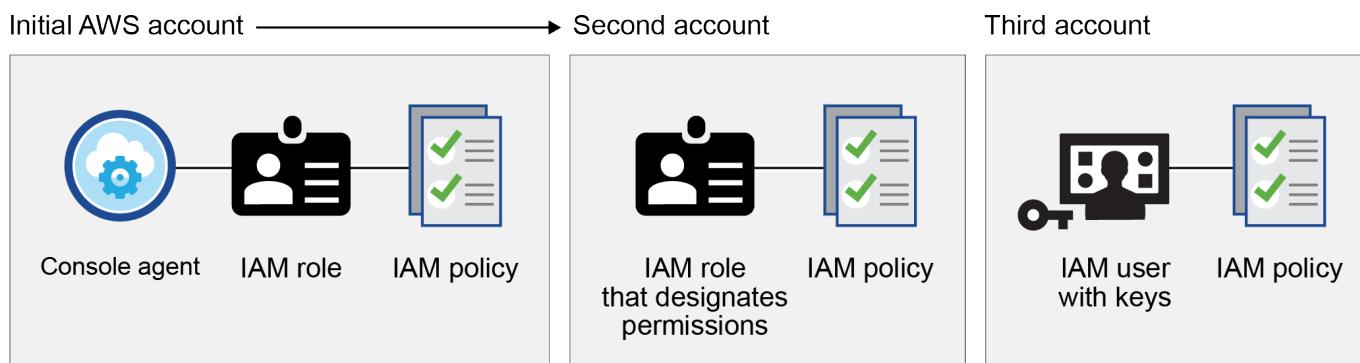
È possibile aggiungere ulteriori credenziali AWS alla Console nei seguenti casi:

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

Per maggiori dettagli, consultare le sezioni seguenti.

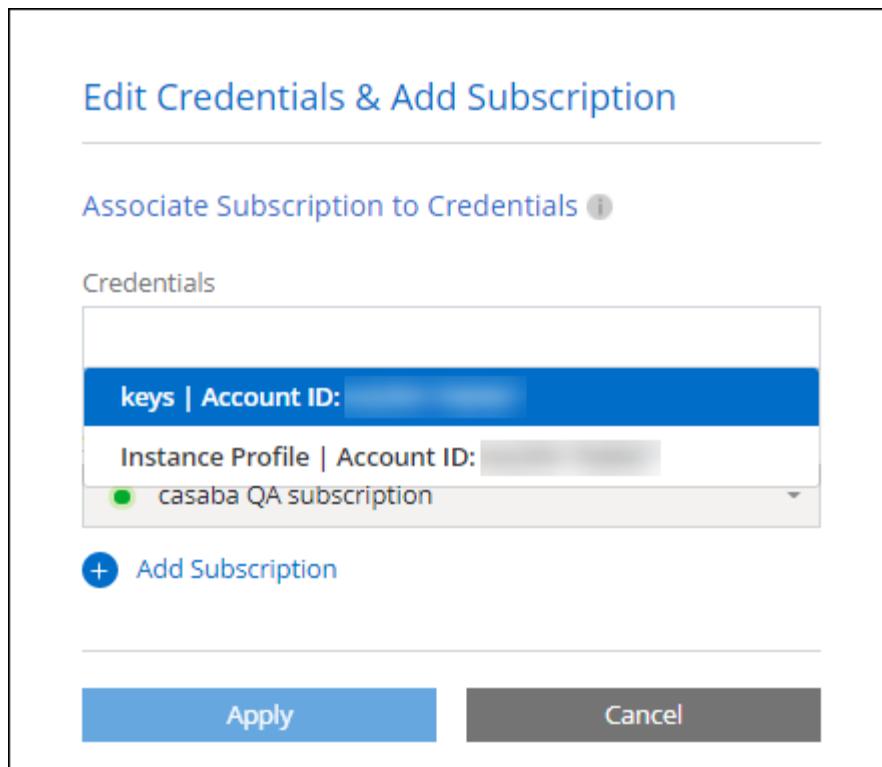
#### Aggiungi le credenziali AWS per utilizzare un agente della console con un altro account AWS

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



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

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



["Scopri come aggiungere le credenziali AWS a un agente esistente."](#)

### **Aggiungi le credenziali AWS per creare un agente della console**

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

["Scopri come aggiungere le credenziali AWS alla Console per creare un agente della Console"](#)

### **Aggiungi le credenziali AWS per FSx per ONTAP**

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

["Scopri come aggiungere le credenziali AWS alla console per Amazon FSx per ONTAP"](#)

### **Credenziali e abbonamenti al marketplace**

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

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

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

### **Domande frequenti**

Le seguenti domande riguardano credenziali e abbonamenti.

## **Come posso ruotare in modo sicuro le mie credenziali AWS?**

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

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

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

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

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

["Scopri come associare un abbonamento AWS"](#) .

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

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

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

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

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

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

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

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

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

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

- Modalità standard
  - ["Impostare le autorizzazioni per una distribuzione AWS Marketplace"](#)
  - ["Impostare le autorizzazioni per le distribuzioni in locale"](#)
- Modalità limitata
  - ["Imposta le autorizzazioni per la modalità limitata"](#)

## Gestisci le credenziali AWS e gli abbonamenti al marketplace per NetApp Console

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

### Panoramica

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

- Aggiungi ulteriori credenziali AWS a un agente esistente

Aggiungi le credenziali AWS a un agente della console per gestire le risorse cloud. [Scopri come aggiungere le credenziali AWS a un agente della console](#) .

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

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

- Aggiungere le credenziali AWS alla console per FSx per ONTAP

Aggiungi nuove credenziali AWS alla Console per creare e gestire FSx per ONTAP. ["Scopri come impostare le autorizzazioni per FSx per ONTAP"](#)

### Come ruotare le credenziali

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

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

Ruota manualmente le chiavi di accesso AWS aggiornandole nella Console.

### Aggiungere credenziali aggiuntive a un agente della console

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

["Scopri come la NetApp Console utilizza le credenziali e le autorizzazioni AWS".](#)

### Concedi permessi

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



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

## Scelte

- [Concedi autorizzazioni assumendo un ruolo IAM in un altro account](#)
- [Concedi le autorizzazioni fornendo le chiavi AWS](#)

### Concedi autorizzazioni assumendo un ruolo IAM in un altro account

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

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

#### Passi

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

Assicurati di fare quanto segue:

- In **Tipo di entità attendibile**, seleziona **Account AWS**.
- Seleziona **Un altro account AWS** e inserisci l'ID dell'account in cui risiede un'istanza dell'agente della console.
- Creare le policy richieste copiando e incollando il contenuto di "[le policy IAM per un agente Console](#)".

3. Copia l'ARN del ruolo IAM in modo da poterlo incollare nella Console in un secondo momento.

#### Risultato

L'account dispone delle autorizzazioni richieste. [Ora puoi aggiungere le credenziali a un agente della console](#) .

### Concedi le autorizzazioni fornendo le chiavi AWS

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

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

#### Passi

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

["Documentazione AWS: creazione di policy IAM"](#)

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

## Aggiungi le credenziali a un agente esistente

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



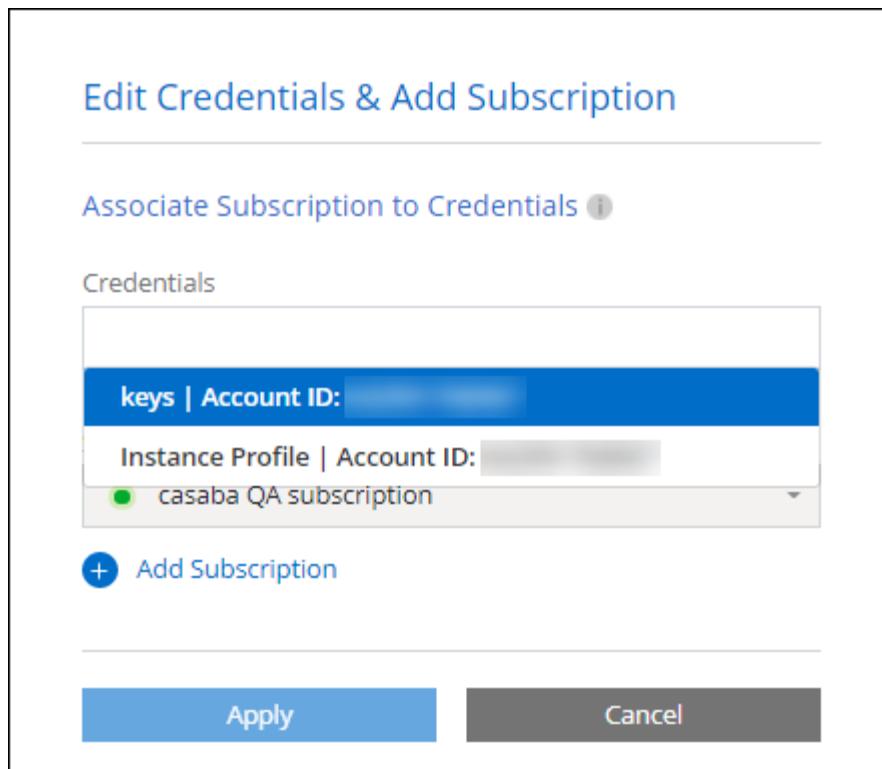
Potrebbero volerci alcuni minuti prima che le nuove credenziali del tuo provider cloud diventino disponibili.

### Passi

1. Utilizzare la barra di navigazione superiore per selezionare un agente della console a cui si desidera aggiungere le credenziali.
2. Nella barra di navigazione a sinistra, seleziona **Amministrazione > Credenziali**.
3. Nella pagina **Credenziali dell'organizzazione**, seleziona **Aggiungi credenziali** e segui i passaggi della procedura guidata.
  - a. **Posizione delle credenziali**: seleziona **Amazon Web Services > Agente**.
  - b. **Definisci credenziali**: fornisci l'ARN (Amazon Resource Name) di un ruolo IAM attendibile oppure inserisci una chiave di accesso AWS e una chiave segreta.
  - c. **Abbonamento Marketplace**: associa un abbonamento Marketplace a queste credenziali abbonandoti ora o selezionando un abbonamento esistente.
- d. **Revisione**: conferma i dettagli sulle nuove credenziali e seleziona **Aggiungi**.

### Risultato

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



#### Aggiungere le credenziali alla Console per creare un agente Console

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

#### Impostare il ruolo IAM

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

#### Passi

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

Assicurati di fare quanto segue:

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

Ad esempio, la policy dovrebbe apparire così:

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

+

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

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

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

## Risultato

Il ruolo IAM ora dispone delle autorizzazioni necessarie. [Ora puoi aggiungerlo alla Console.](#)

## Aggiungi le credenziali

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

### Prima di iniziare

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

### Passi

1. Selezionare **Amministrazione > Credenziali**.



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

## Aggiungere le credenziali alla console per Amazon FSx per ONTAP

Per i dettagli, fare riferimento al "["la documentazione della console per Amazon FSx per ONTAP"](#)"

### Configurare un abbonamento AWS

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

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

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

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

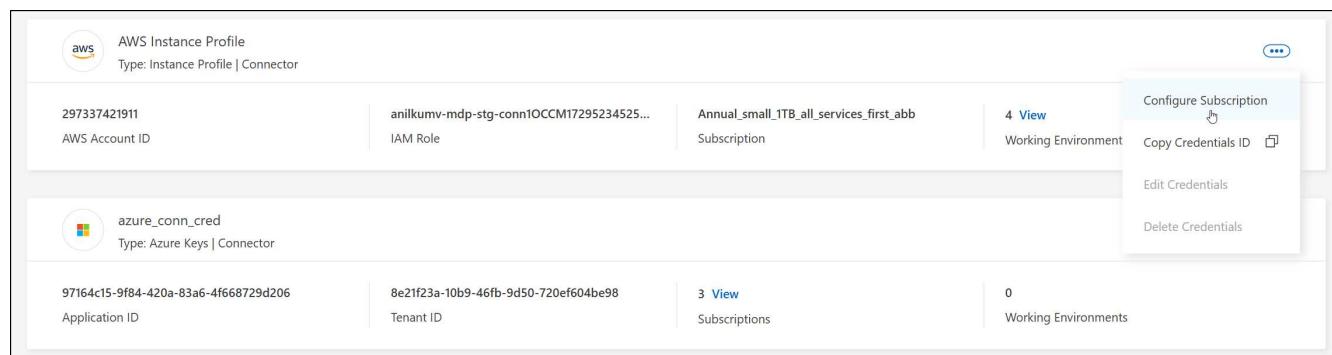
### Prima di iniziare

Prima di poter configurare un abbonamento, è necessario creare un agente Console. "["Scopri come creare un agente Console"](#)" .

### Passi

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

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



4. Per associare le credenziali a un abbonamento esistente, seleziona l'abbonamento dall'elenco a discesa e seleziona **Configura**.
5. Per associare le credenziali a un nuovo abbonamento, seleziona **Aggiungi abbonamento > Continua** e segui i passaggi indicati in AWS Marketplace:
  - a. Seleziona **Visualizza opzioni di acquisto**.
  - b. Seleziona **Iscriviti**.
  - c. Seleziona **Configura il tuo account**.

Verrai reindirizzato alla NetApp Console.

d. Dalla pagina **Assegnazione abbonamento**:

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

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

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

- Seleziona **Salva**.

#### **Associa un abbonamento esistente alla tua organizzazione**

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

- "[Scopri di più sulle modalità di distribuzione della console](#)"
- "[Scopri di più sulla gestione dell'identità e dell'accesso alla console](#)"

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

#### **Passi**

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

Vedrai solo gli abbonamenti associati all'organizzazione o all'account che stai visualizzando. Se non vedi il tuo abbonamento, procedi come segue.

2. Accedi alla console AWS e vai su **Abbonamenti AWS Marketplace**.
3. Trova l'abbonamento.

The screenshot shows the AWS Marketplace interface. On the left, a sidebar menu includes 'Manage subscriptions', 'Private offers', 'Discover products', 'Vendor Insights', 'Private Marketplace', and 'Settings'. The main content area displays a product card for 'NetApp BlueXP' by NetApp, Inc. The card shows the following details: 'Delivery method' (SaaS), 'Service start' (Feb 15, 2022), and 'Access level' (Agreement). At the bottom of the card are 'Set up product' and 'Manage' buttons. The top right of the main area has 'Launch new instance' and 'Manage' buttons.

4. Seleziona **Configura prodotto**.

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

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

The screenshot shows the NetApp BlueXP subscription page. The top navigation bar includes 'place', 'Search', and 'Hello, assumed-role/AWSRes...'. The main content area has a 'Set up your account' button with a cursor hovering over it. Below the button, the text reads: 'up your account and complete your registration. If you are unable to complete your registration, return through the [Your Software](#) page on e'. The page also shows 'NetApp BlueXP > Subscribe' and 'Subscribe to NetApp BlueXP' buttons. A 'Offers' section is visible at the bottom.

La pagina **Assegnazione abbonamento** su [netapp.com](http://netapp.com) dovrebbe caricarsi in una nuova scheda o finestra del browser.

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

6. Dalla pagina **Assegnazione abbonamento**:

- Seleziona le organizzazioni o gli account della Console a cui desideri associare questo abbonamento.

- Nel campo **Sostituisci abbonamento esistente**, scegli se desideri sostituire automaticamente l'abbonamento esistente per un'organizzazione o un account con questo nuovo abbonamento.

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

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

### Subscription Assignment

Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name i  
PayAsYouGo

Select the NetApp accounts that you'd like to associate this subscription with. i  
You can automatically replace the existing subscription for one account with this new subscription.

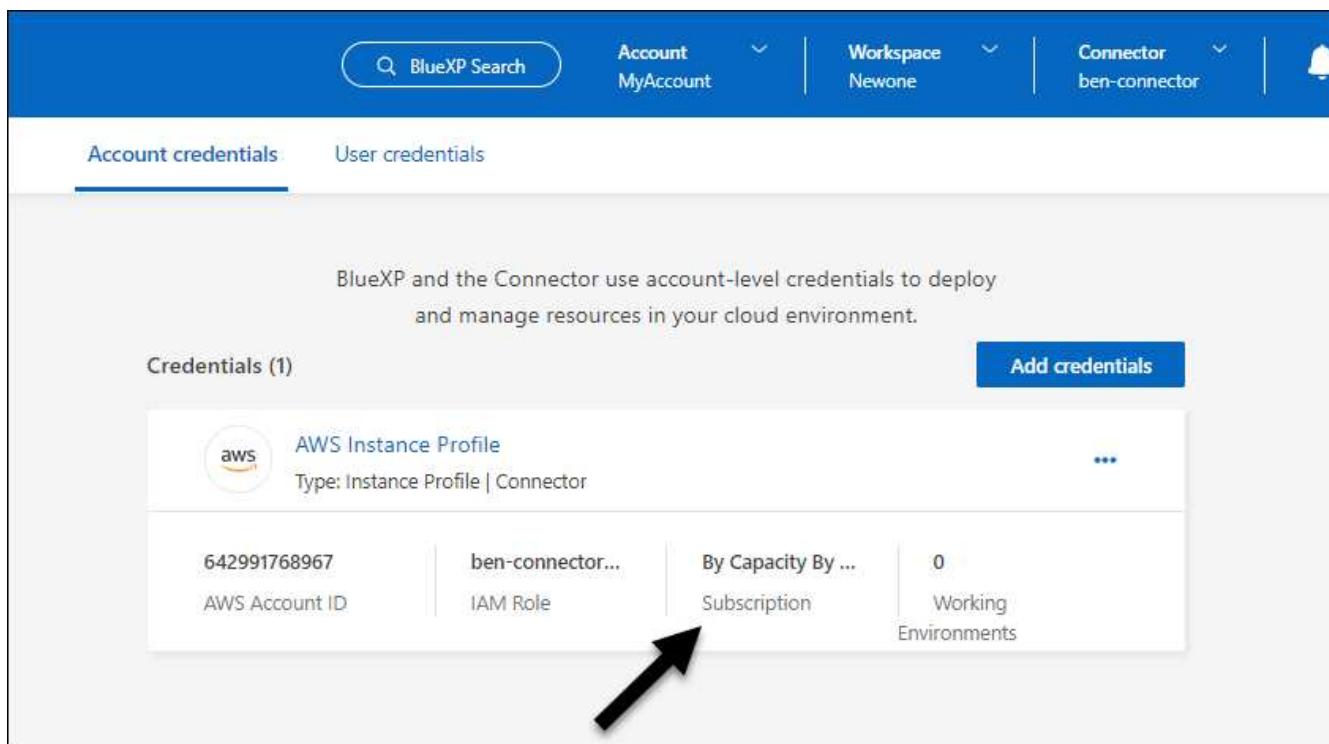
NetApp account	Replace existing subscription
<input checked="" type="checkbox"/> cloudTiering_undefined	<input type="checkbox"/>
<input checked="" type="checkbox"/> CS-HhewH	<input type="checkbox"/>
<input checked="" type="checkbox"/> benAccount	<input checked="" type="checkbox"/>

Save

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

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

Ecco un esempio.



BlueXP and the Connector use account-level credentials to deploy and manage resources in your cloud environment.

Credentials (1)

**AWS Instance Profile**  
Type: Instance Profile | Connector

642991768967	ben-connector...	By Capacity By ...	0
AWS Account ID	IAM Role	Subscription	Working Environments

### Modifica credenziali

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

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

### Passi

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

### Elimina le credenziali

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

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

### Passi

1. Selezionare **Amministrazione > Credenziali**.

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

## Azzurro

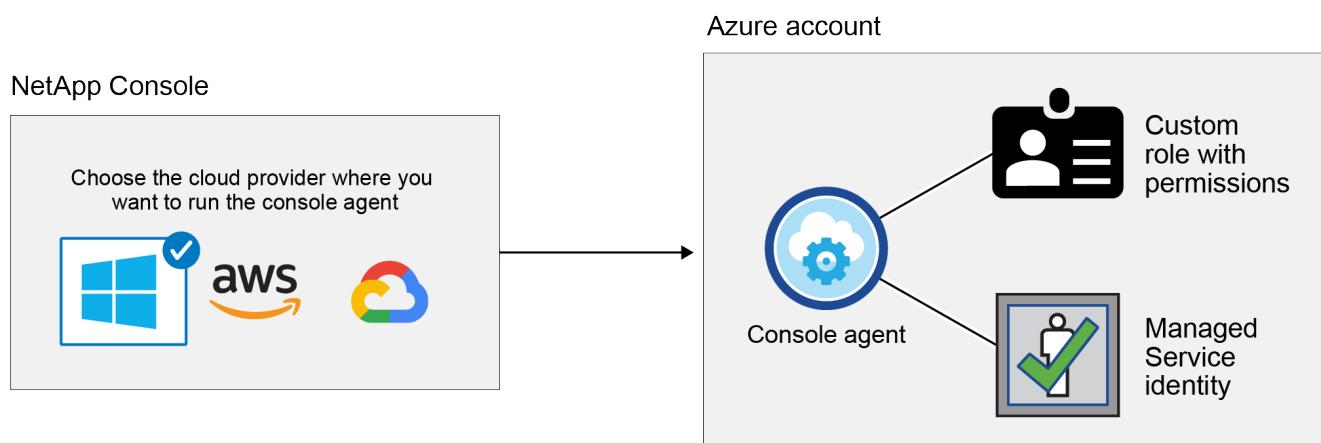
### Scopri di più sulle credenziali e le autorizzazioni di Azure nella NetApp Console

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

#### Credenziali iniziali di Azure

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

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



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

Details & Credentials			
Managed Service Ide...	OCCM QA1	<span> ⓘ No subscription is associated</span>	<a href="#">Edit Credentials</a>

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

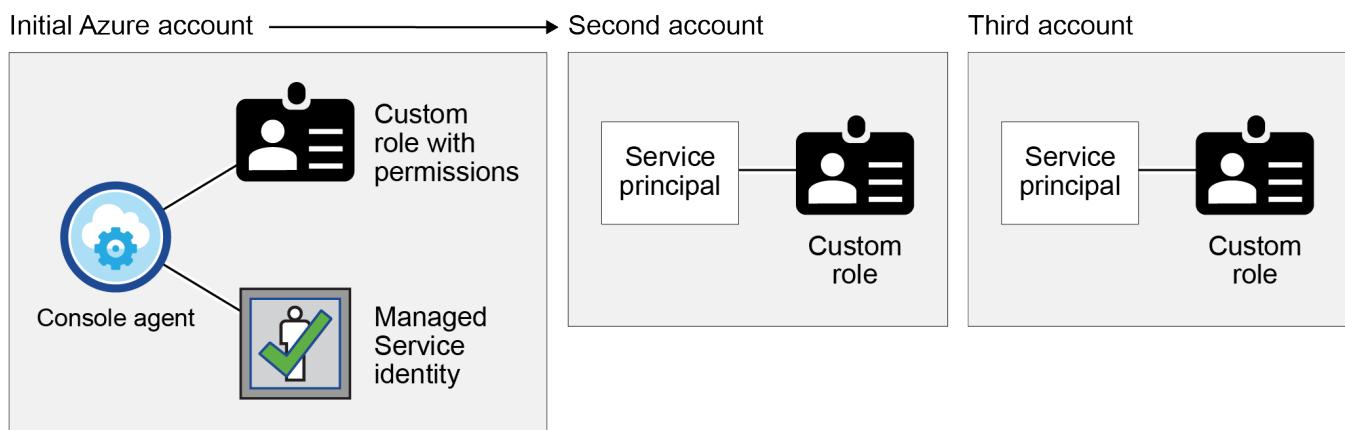
possibile aggiungere credenziali aggiuntive.

#### Abbonamenti Azure aggiuntivi per un'identità gestita

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

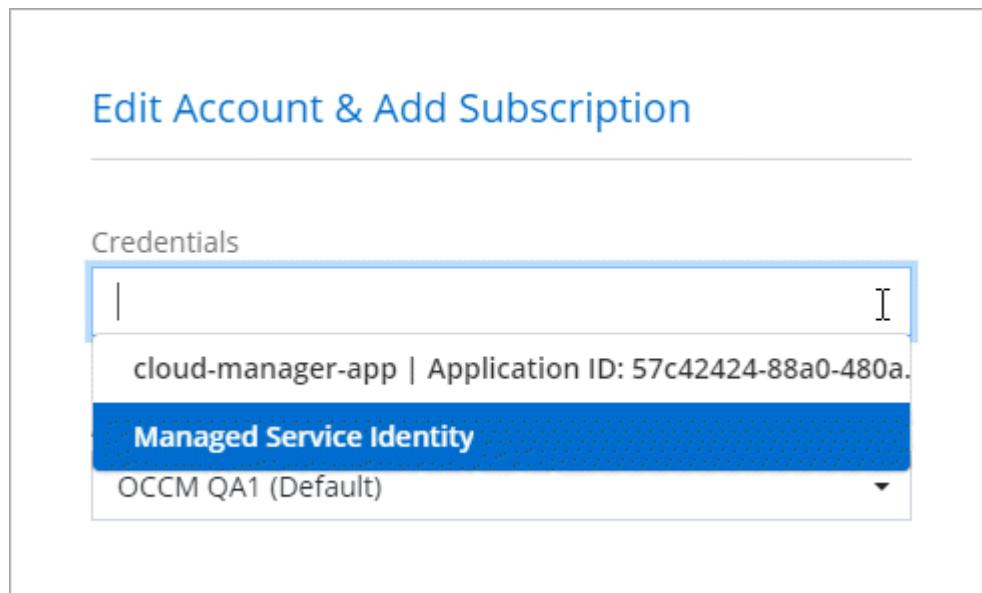
#### Credenziali Azure aggiuntive

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



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

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



## Credenziali e abbonamenti al marketplace

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

["Scopri come associare una sottoscrizione Azure"](#) .

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

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

## Domande frequenti

La seguente domanda riguarda le credenziali e gli abbonamenti.

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

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

["Scopri come associare una sottoscrizione Azure"](#) .

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

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

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

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

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

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

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

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

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

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

- Modalità standard
  - ["Impostare le autorizzazioni per una distribuzione di Azure Marketplace"](#)

- "Impostare le autorizzazioni per le distribuzioni in locale"
- Modalità limitata
  - "Imposta le autorizzazioni per la modalità limitata"

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

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

### Panoramica

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

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

### Associare ulteriori sottoscrizioni di Azure a un'identità gestita

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

### Informazioni su questo compito

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

### Passi

1. Accedi al portale di Azure.
2. Aprire il servizio **Abbonamenti** e quindi selezionare l'abbonamento in cui si desidera distribuire Cloud Volumes ONTAP.
3. Selezionare **Controllo accessi (IAM)**.

a. Selezionare **Aggiungi > Aggiungi assegnazione ruolo** e quindi aggiungere le autorizzazioni:

- Selezionare il ruolo **Operatore console**.



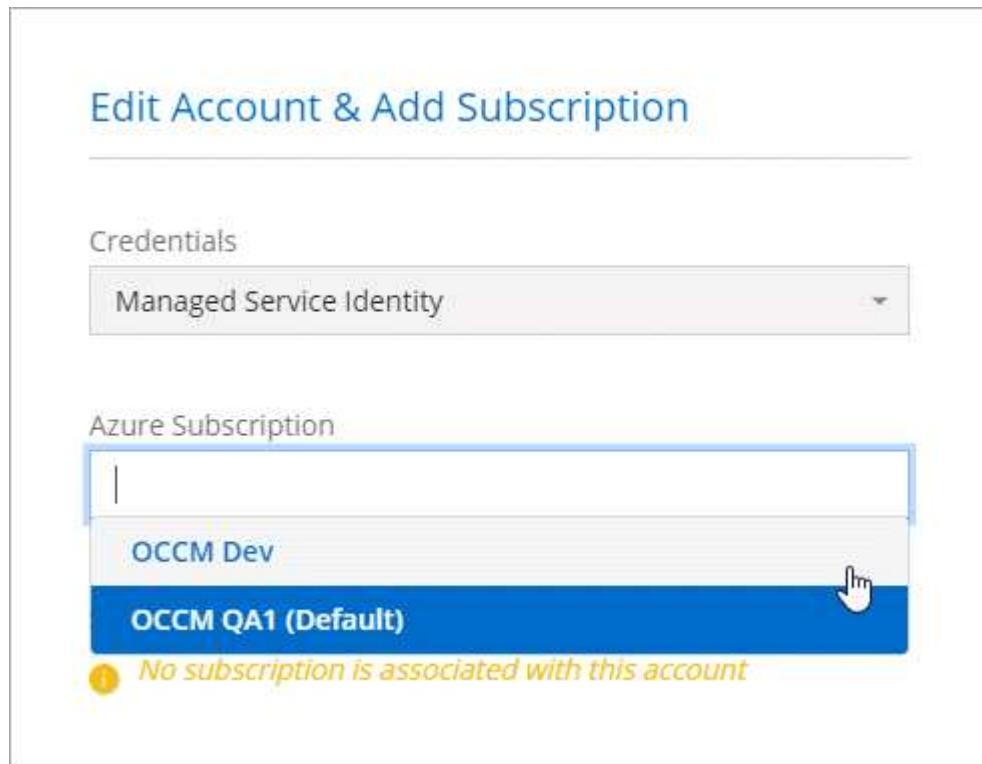
Console Operator è il nome predefinito fornito in un criterio dell'agente Console. Se hai scelto un nome diverso per il ruolo, seleziona quel nome.

- Assegna l'accesso a una **Macchina Virtuale**.
- Selezionare la sottoscrizione in cui è stata creata una macchina virtuale dell'agente Console.
- Selezionare una macchina virtuale agente Console.
- Seleziona **Salva**.

4. Ripetere questi passaggi per ulteriori abbonamenti.

### Risultato

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



#### Aggiungi ulteriori credenziali di Azure alla NetApp Console

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



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

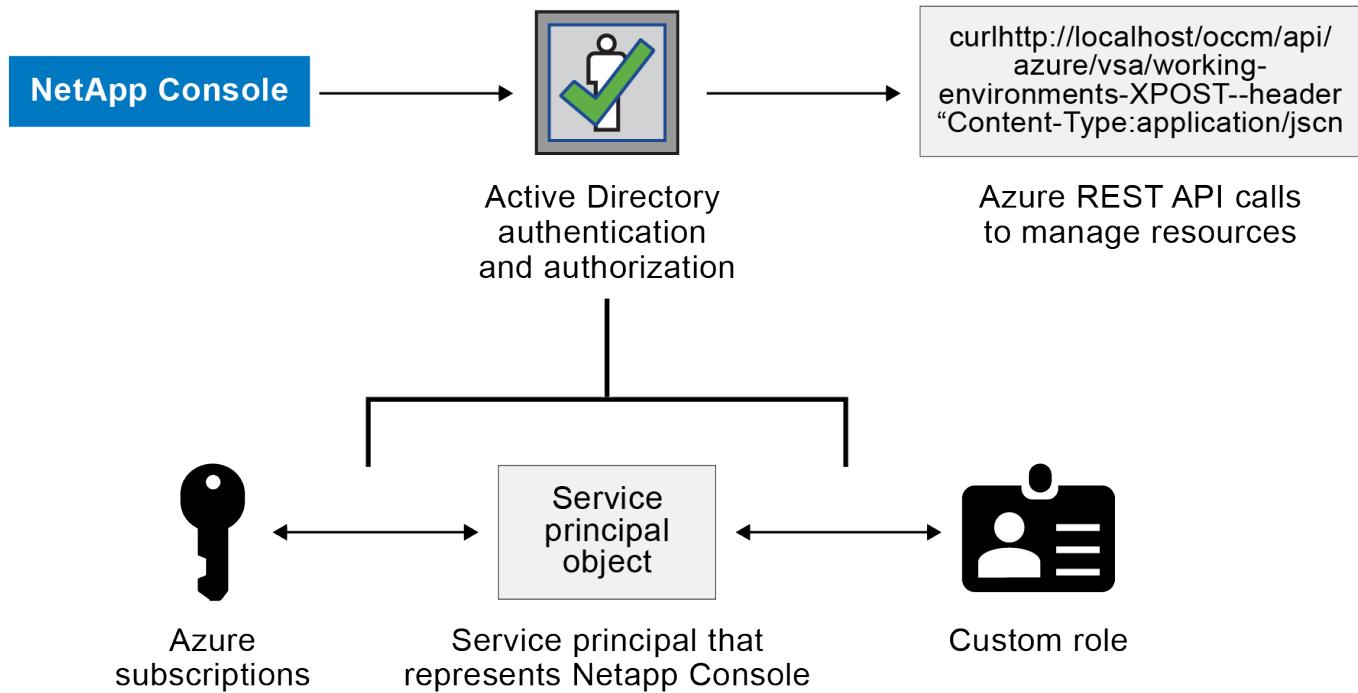
Se si desidera distribuire Cloud Volumes ONTAP utilizzando credenziali Azure *diverse*, è necessario concedere le autorizzazioni richieste creando e configurando un'entità servizio in Microsoft Entra ID per ciascun account Azure. È quindi possibile aggiungere le nuove credenziali alla Console.

#### Concedi le autorizzazioni di Azure utilizzando un'entità servizio

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

#### Informazioni su questo compito

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



## Passi

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

## Creare un'applicazione Microsoft Entra

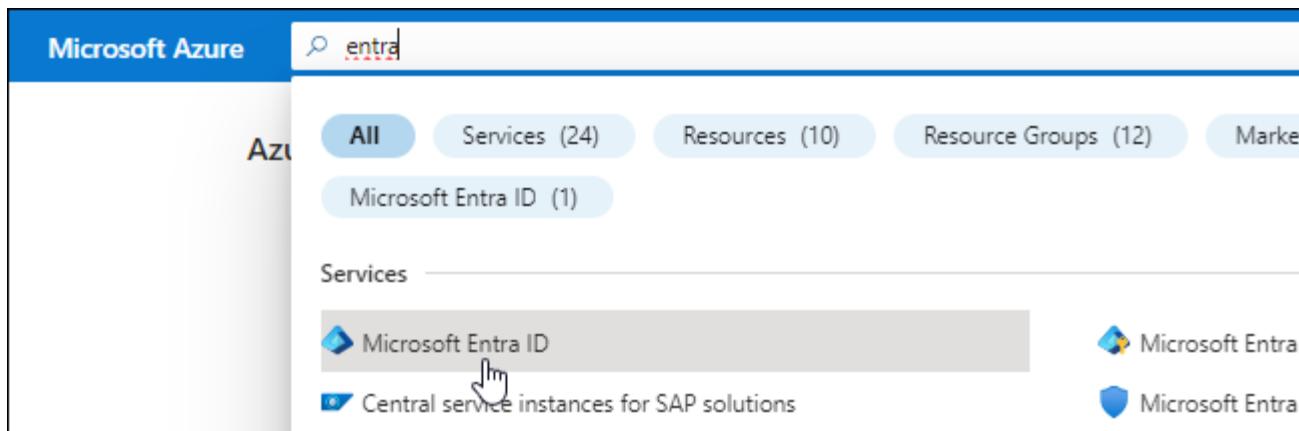
Creare un'applicazione Microsoft Entra e un'entità servizio che la console può utilizzare per il controllo degli accessi basato sui ruoli.

## Passi

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

Per i dettagli, fare riferimento a ["Documentazione di Microsoft Azure: autorizzazioni richieste"](#)

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



3. Nel menu, seleziona **Registrazioni app**.

4. Selezionare **Nuova registrazione**.

5. Specificare i dettagli sull'applicazione:

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

6. Seleziona **Registrati**.

Hai creato l'applicazione AD e il servizio principale.

### Assegnare l'applicazione a un ruolo

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

#### Passi

1. Crea un ruolo personalizzato:

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

- Copia il contenuto del ["autorizzazioni di ruolo personalizzate per l'agente della console"](#) e salvarli in un file JSON.
- 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 .

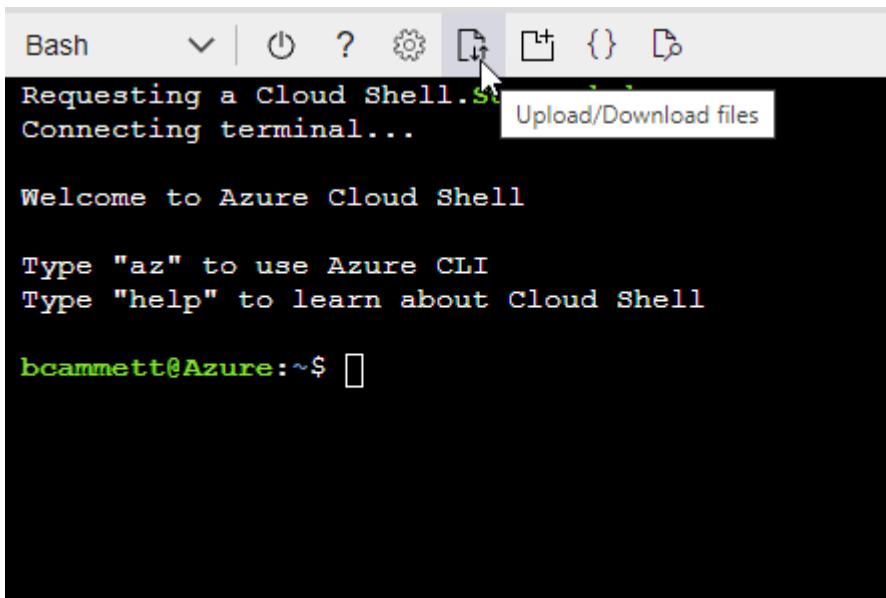
#### Esempio

```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"
]
```

- 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:

- Dal portale di Azure, aprire il servizio **Sottoscrizioni**.
- Seleziona l'abbonamento.
- Selezionare **Controllo accessi (IAM)** > **Aggiungi** > **Aggiungi assegnazione ruolo**.
- Nella scheda **Ruolo**, seleziona il ruolo **Operatore console** e seleziona **Avanti**.
- Nella scheda **Membri**, completa i seguenti passaggi:
  - Mantieni selezionato **Utente, gruppo o entità servizio**.

- Seleziona **Seleziona membri**.

Add role assignment ...

Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12\_B

Assign access to  User, group, or service principal  Managed identity

Members [Select members](#)

- Cerca il nome dell'applicazione.

Ecco un esempio:

Select members

Select  test-service-principal

test-service-principal

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

f. Seleziona **Revisiona + assegna**.

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

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

## Aggiungere autorizzazioni API di gestione dei servizi Windows Azure

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

### Passi

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

### Request API permissions

#### Select an API

[Microsoft APIs](#) [APIs my organization uses](#) [My APIs](#)

#### Commonly used Microsoft APIs

##### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



##### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

##### Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

##### Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

##### Azure Data Lake

Access to storage and compute for big data analytic scenarios

##### Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

##### Azure Import/Export

Programmatic control of import/export jobs

##### Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

##### Azure Rights Management Services

Allow validated users to read and write protected content

##### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

##### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

##### Customer Insights

Create profile and interaction models for your products

##### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

## Request API permissions

[All APIs](#)

 Azure Service Management  
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

**user\_impersonation**

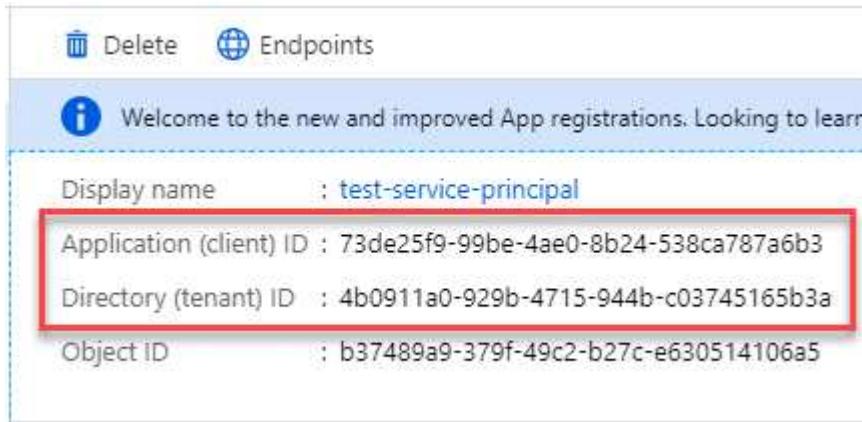
Access Azure Service Management as organization users (preview) [?](#)

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

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

### Passi

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



The screenshot shows the Microsoft Entra ID App registrations page. At the top, there are 'Delete' and 'Endpoints' buttons. A message box says 'Welcome to the new and improved App registrations. Looking to learn'. Below, there is a table with the following data:

Display name	: test-service-principal
Application (client) ID	: 73de25f9-99be-4ae0-8b24-538ca787a6b3
Directory (tenant) ID	: 4b0911a0-929b-4715-944b-c03745165b3a
Object ID	: b37489a9-379f-49c2-b27c-e630514106a5

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

## Crea un segreto client

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

### Passi

1. Aprire il servizio **Microsoft Entra ID**.

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

#### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Client secrets			<a href="#">New client secret</a>
DESCRIPTION	EXPIRES	VALUE	<a href="#">Copy to clipboard</a>
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA	

#### Risultato

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

#### Aggiungere le credenziali alla Console

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

#### Prima di iniziare

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

#### Prima di iniziare

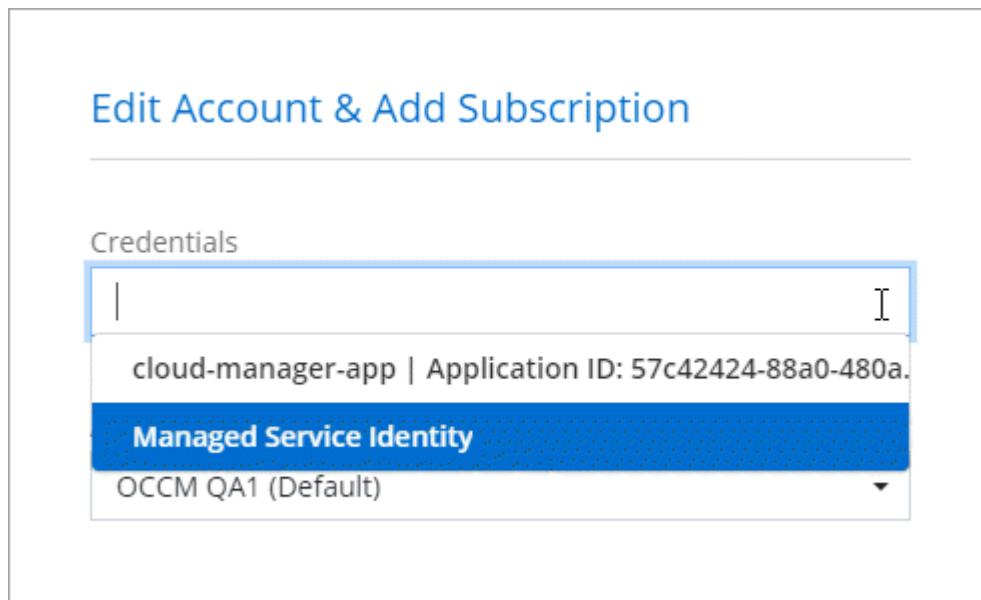
Prima di poter modificare le impostazioni della console, è necessario creare un agente della console. ["Scopri come creare un agente Console"](#) .

#### Passi

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

## Risultato

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



The screenshot shows a user interface for managing account credentials. At the top, the title 'Edit Account & Add Subscription' is visible. Below it, the section 'Credentials' is labeled. A dropdown menu is open, showing the text 'cloud-manager-app | Application ID: 57c42424-88a0-480a.' and the option 'Managed Service Identity' which is highlighted with a blue bar. Below this, the option 'OCCM QA1 (Default)' is listed. The interface has a clean, modern design with a white background and blue accents.

### Gestisci le credenziali esistenti

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

### Associare una sottoscrizione di Azure Marketplace alle credenziali

Dopo aver aggiunto le credenziali di Azure alla console, è possibile associare a tali credenziali un abbonamento ad Azure Marketplace. È possibile utilizzare l'abbonamento per creare un sistema Cloud Volumes ONTAP con pagamento in base al consumo e accedere ai servizi dati NetApp .

Esistono due scenari in cui potresti associare una sottoscrizione ad Azure Marketplace dopo aver già aggiunto le credenziali alla Console:

- Non hai associato un abbonamento quando hai aggiunto inizialmente le credenziali alla Console.
- Si desidera modificare la sottoscrizione di Azure Marketplace associata alle credenziali di Azure.

La sostituzione dell'attuale abbonamento al marketplace lo aggiorna per i sistemi Cloud Volumes ONTAP esistenti e nuovi.

### Passi

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

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

4. Per associare le credenziali a un abbonamento esistente, seleziona l'abbonamento dall'elenco a discesa e

seleziona **Configura**.

5. Per associare le credenziali a un nuovo abbonamento, seleziona **Aggiungi abbonamento > Continua** e segui i passaggi in Azure Marketplace:

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

Verrai reindirizzato alla NetApp Console.

e. Dalla pagina **Assegnazione abbonamento**:

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

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

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

- Seleziona **Salva**.

## Modifica credenziali

Modifica le tue credenziali di Azure nella Console. Ad esempio, è possibile aggiornare il segreto client se è stato creato un nuovo segreto per l'applicazione del servizio principale.

### Passi

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

## Elimina le credenziali

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

### Passi

1. Selezionare **Amministrazione > Credenziali**.
2. Selezionare **Credenziali dell'organizzazione**.
3. Nella pagina **Credenziali dell'organizzazione**, seleziona il menu azioni per un set di credenziali, quindi seleziona **Elimina credenziali**.
4. Selezionare **Elimina** per confermare.

## Google Cloud

### Scopri di più sui progetti e sulle autorizzazioni di Google Cloud

Scopri come la NetApp Console utilizza le credenziali di Google Cloud per eseguire azioni per tuo conto e come tali credenziali sono associate agli abbonamenti al marketplace. Comprendere questi dettagli può essere utile quando si gestiscono le credenziali per uno o più progetti Google Cloud. Ad esempio, potresti voler ottenere informazioni sull'account di servizio associato alla VM dell'agente Console.

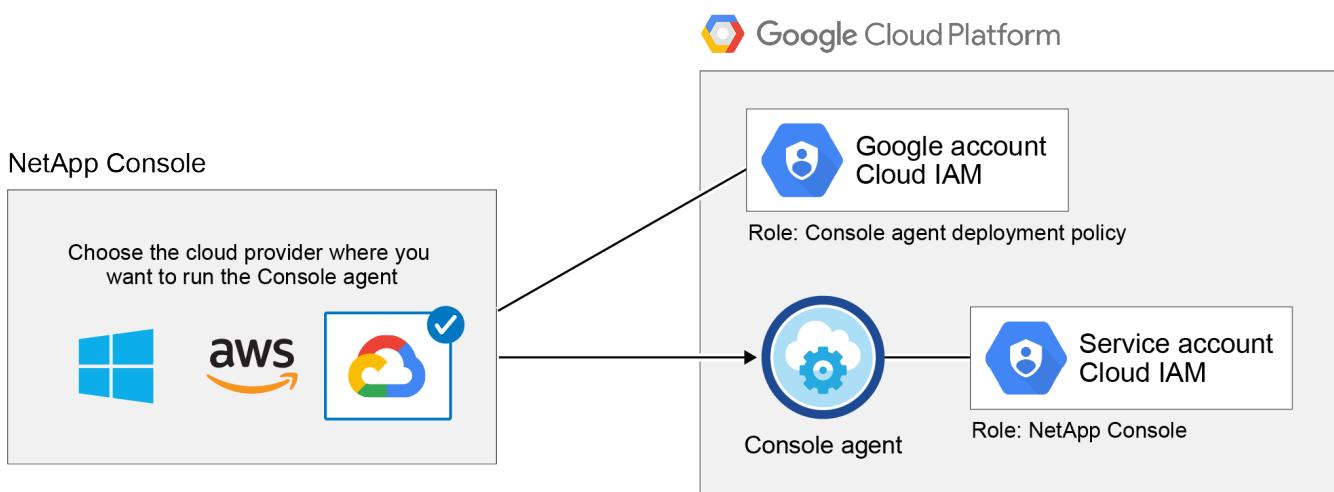
#### Progetto e autorizzazioni per NetApp Console

Prima di poter utilizzare la Console per gestire le risorse nel tuo progetto Google Cloud, devi prima distribuire un agente Console. L'agente non può essere in esecuzione presso la tua sede o presso un altro provider cloud.

Prima di distribuire un agente Console direttamente dalla Console, è necessario disporre di due set di autorizzazioni:

1. È necessario distribuire un agente Console utilizzando un account Google che disponga delle autorizzazioni per avviare l'agente Console dalla Console.
2. Quando si distribuisce l'agente Console, viene richiesto di selezionare un ["account di servizio"](#) per l'agente. La console ottiene le autorizzazioni dall'account di servizio per creare e gestire i sistemi Cloud Volumes ONTAP, per gestire i backup utilizzando il backup e il ripristino NetApp e altro ancora. Le autorizzazioni vengono fornite associando un ruolo personalizzato all'account di servizio.

L'immagine seguente illustra i requisiti di autorizzazione descritti nei numeri 1 e 2 sopra:



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

- ["Imposta le autorizzazioni di Google Cloud per la modalità standard"](#)
- ["Imposta le autorizzazioni per la modalità limitata"](#)

#### Credenziali e abbonamenti al marketplace

Quando distribuisci un agente Console in Google Cloud, la Console crea un set predefinito di credenziali per l'account del servizio Google Cloud nel progetto in cui risiede l'agente Console. Per poter pagare i servizi dati

Cloud Volumes ONTAP e NetApp , queste credenziali devono essere associate a un abbonamento a Google Cloud Marketplace.

["Scopri come associare un abbonamento a Google Cloud Marketplace"](#) .

Tieni presente quanto segue in merito alle credenziali di Google Cloud e agli abbonamenti al marketplace:

- È possibile associare un solo set di credenziali Google Cloud a un agente Console
- È possibile associare solo un abbonamento a Google Cloud Marketplace alle credenziali
- Puoi sostituire un abbonamento esistente al marketplace con un nuovo abbonamento

#### **Progetto per Cloud Volumes ONTAP**

Cloud Volumes ONTAP può risiedere nello stesso progetto dell'agente Console oppure in un progetto diverso. Per distribuire Cloud Volumes ONTAP in un progetto diverso, è necessario prima aggiungere l'account del servizio agente Console e il ruolo a quel progetto.

- ["Scopri come configurare l'account di servizio"](#)
- ["Scopri come distribuire Cloud Volumes ONTAP in Google Cloud e selezionare un progetto"](#)

#### **Gestisci le autorizzazioni dell'agente della console per le distribuzioni di Google Cloud**

Occasionalmente, NetApp aggiorna le autorizzazioni richieste per l'account di servizio utilizzato per l'agente della console quando viene distribuito in Google Cloud.

["Verificare l'elenco delle autorizzazioni Google richieste"](#) .

Utilizza Google Cloud Console per aggiornare il ruolo IAM assegnato all'account di servizio in modo che corrisponda al nuovo set di autorizzazioni.

["Documentazione di Google Cloud: modifica un ruolo personalizzato"](#)

## Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.