# Configurare un connettore

## Cloud Manager 3.8

NetApp
March 25, 2024

# Sommario

# Configurare un connettore

## Scopri di più sui connettori

Nella maggior parte dei casi, un account Admin dovrà implementare un *connettore* nel cloud o nella rete on-premise. Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

### Quando è necessario un connettore

È necessario un connettore per utilizzare una delle seguenti funzionalità in Cloud Manager:

- Cloud Volumes ONTAP
- Cluster ONTAP on-premise
- Conformità al cloud
- Kubernetes
- Backup su cloud
- Monitoraggio
- Tiering on-premise
- Global file cache
- Discovery bucket Amazon S3

Un connettore è ***not*** necessario per Azure NetApp Files, Cloud Volumes Service o Cloud Sync.

Sebbene non sia necessario un connettore per configurare e gestire Azure NetApp Files, è necessario un connettore per utilizzare la conformità cloud per eseguire la scansione dei dati Azure NetApp Files.

### Posizioni supportate

Un connettore è supportato nelle seguenti posizioni:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- On-premise

Se si desidera creare un sistema Cloud Volumes ONTAP in Google Cloud, è necessario disporre di un connettore in esecuzione anche in Google Cloud. Non è possibile utilizzare un connettore in esecuzione in un'altra posizione.

### I connettori devono rimanere in funzione

Un connettore deve rimanere sempre in funzione. È importante per la salute e il funzionamento continui dei servizi che si abilitano.

Ad esempio, un connettore è un componente chiave per lo stato e il funzionamento dei sistemi PAYGO di Cloud Volumes ONTAP. Se un connettore viene spento, i sistemi PAYGO di Cloud Volumes ONTAP si spegneranno dopo aver perso la comunicazione con un connettore per più di 14 giorni.

## Come creare un connettore

Un amministratore dell'account deve creare un connettore prima che un amministratore dell'area di lavoro possa creare un ambiente di lavoro Cloud Volumes ONTAP e utilizzare una qualsiasi delle altre funzionalità sopra elencate.

Un account Admin può creare un connettore in diversi modi:

- Direttamente da Cloud Manager (consigliato)
  - "Creare in AWS"
  - "Crea in Azure"
  - "Creare in GCP"
- "Da AWS Marketplace"
- "Da Azure Marketplace"
- "Scaricando e installando il software su un host Linux esistente"

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiederà di creare un connettore se non ne hai ancora uno.

## Permessi

Sono necessarie autorizzazioni specifiche per creare il connettore e un altro set di autorizzazioni per l'istanza stessa del connettore.

### Autorizzazioni per creare un connettore

L'utente che crea un connettore da Cloud Manager ha bisogno di autorizzazioni specifiche per implementare l'istanza nel provider cloud scelto. Cloud Manager ti ricorderà i requisiti di autorizzazione quando crei un connettore.

"Visualizza le policy per ogni cloud provider".

### Permessi per l'istanza del connettore

Il connettore necessita di autorizzazioni specifiche per il cloud provider per eseguire le operazioni per conto dell'utente. Ad esempio, per implementare e gestire Cloud Volumes ONTAP.

Quando crei un connettore direttamente da Cloud Manager, Cloud Manager crea il connettore con le autorizzazioni necessarie. Non c'è niente da fare.

Se si crea il connettore da AWS Marketplace, Azure Marketplace o installando manualmente il software, è necessario assicurarsi di disporre delle autorizzazioni corrette.

"Visualizza le policy per ogni cloud provider".

### Quando utilizzare connettori multipli

In alcuni casi, potrebbe essere necessario un solo connettore, ma potrebbero essere necessari due o più connettori.

Ecco alcuni esempi:

- Stai utilizzando un ambiente multi-cloud (AWS e Azure), quindi hai un connettore in AWS e un altro in Azure. Ciascuno di essi gestisce i sistemi Cloud Volumes ONTAP in esecuzione in tali ambienti.
- Un provider di servizi potrebbe utilizzare un account Cloud Central per fornire servizi ai propri clienti, mentre utilizza un altro account per fornire il disaster recovery per una delle proprie business unit. Ciascun account dispone di connettori separati.

### Quando passare da un connettore all'altro

Quando crei il primo connettore, Cloud Manager utilizza automaticamente tale connettore per ogni ambiente di lavoro aggiuntivo creato. Una volta creato un connettore aggiuntivo, è necessario passare da un connettore all'altro per visualizzare gli ambienti di lavoro specifici di ciascun connettore.

"Scopri come passare da un connettore all'altro".

### L'interfaccia utente locale

Mentre è necessario eseguire quasi tutte le attività di "Interfaccia utente SaaS", Un'interfaccia utente locale è ancora disponibile sul connettore. Questa interfaccia è necessaria per alcune attività che devono essere eseguite dal connettore stesso:

- "Impostazione di un server proxy"
- Installazione di una patch (in genere collaborerete con il personale NetApp per installare una patch)
- Download dei messaggi AutoSupport (solitamente indirizzati dal personale NetApp in caso di problemi)

"Scopri come accedere all'interfaccia utente locale".

### Aggiornamenti del connettore

Il connettore aggiorna automaticamente il software alla versione più recente, a patto che sia disponibile "accesso a internet in uscita" per ottenere l'aggiornamento software.

# Requisiti di rete per il connettore

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Il passaggio più importante è garantire l'accesso a Internet in uscita a vari endpoint.

Se la rete utilizza un server proxy per tutte le comunicazioni a Internet, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a. "Configurazione del connettore per l'utilizzo di un server proxy".

## Connessione alle reti di destinazione

Un connettore richiede una connessione di rete al tipo di ambiente di lavoro che si sta creando e ai servizi che si intende abilitare.

Ad esempio, se si installa un connettore nella rete aziendale, è necessario impostare una connessione VPN a VPC o VNET in cui si avvia Cloud Volumes ONTAP.

## Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. L'accesso a Internet in uscita è necessario anche se si desidera installare manualmente il connettore su un host Linux o accedere all'interfaccia utente locale in esecuzione sul connettore.

Le sezioni seguenti identificano gli endpoint specifici.

### Endpoint per gestire le risorse in AWS

Un connettore contatta i seguenti endpoint durante la gestione delle risorse in AWS:

| Endpoint | Scopo |
|---|---|
| Servizi AWS (amazonaws.com):<br>• CloudFormation<br>• Elastic Compute Cloud (EC2)<br>• Servizio di gestione delle chiavi (KMS)<br>• Servizio token di sicurezza (STS)<br>• S3 (Simple Storage Service)<br>L'endpoint esatto dipende dalla regione in cui viene implementato Cloud Volumes ONTAP. "Per ulteriori informazioni, fare riferimento alla documentazione AWS." | Consente al connettore di implementare e gestire Cloud Volumes ONTAP in AWS. |
| https://api.services.cloud.netapp.com:443 | Richieste API a NetApp Cloud Central. |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Fornisce l'accesso a immagini, manifesti e modelli software. |
| https://repo.cloud.support.netapp.com | Utilizzato per scaricare le dipendenze di Cloud Manager. |
| http://repo.mysql.com/ | Utilizzato per scaricare MySQL. |
| https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com | Consente al connettore di accedere e scaricare manifesti, modelli e immagini di aggiornamento Cloud Volumes ONTAP. |
| https://cloudmanagerinfraprod.azurecr.io | Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager. |

| Endpoint | Scopo |
| --- | --- |
| https://kinesis.us-east-1.amazonaws.com | Consente a NetApp di eseguire lo streaming dei dati dai record di audit. |
| https://cloudmanager.cloud.netapp.com | Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central. |
| https://netapp-cloud-account.auth0.com | Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata. |
| https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist | Consente di aggiungere l'ID account AWS all'elenco degli utenti autorizzati per Backup in S3. |
| https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup | Comunicazione con NetApp AutoSupport. |
| https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com | Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema. |
| https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com | Consente a NetApp di raccogliere le informazioni necessarie per risolvere i problemi di supporto. |
| https://ipa-signer.cloudmanager.netapp.com | Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ | Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident. |
| Varie sedi di terze parti, ad esempio:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.com<br>Le sedi di terze parti sono soggette a modifiche. | Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti. |

### Endpoint per la gestione delle risorse in Azure

Un connettore contatta i seguenti endpoint durante la gestione delle risorse in Azure:

| Endpoint | Scopo |
| --- | --- |
| https://management.azure.com https://login.microsoftonline.com | Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nella maggior parte delle regioni Azure. |

| Endpoint | Scopo |
| --- | --- |
| https://management.microsoftazure.de https://login.microsoftonline.de | Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure Germania. |
| https://management.usgovcloudapi.net https://login.microsoftonline.com | Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure US Gov. |
| https://api.services.cloud.netapp.com:443 | Richieste API a NetApp Cloud Central. |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Fornisce l'accesso a immagini, manifesti e modelli software. |
| https://repo.cloud.support.netapp.com | Utilizzato per scaricare le dipendenze di Cloud Manager. |
| http://repo.mysql.com/ | Utilizzato per scaricare MySQL. |
| https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com | Consente al connettore di accedere e scaricare manifesti, modelli e immagini di aggiornamento Cloud Volumes ONTAP. |
| https://cloudmanagerinfraprod.azurecr.io | Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager. |
| https://kinesis.us-east-1.amazonaws.com | Consente a NetApp di eseguire lo streaming dei dati dai record di audit. |
| https://cloudmanager.cloud.netapp.com | Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central. |
| https://netapp-cloud-account.auth0.com | Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata. |
| https://mysupport.netapp.com | Comunicazione con NetApp AutoSupport. |
| https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com | Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema. |
| https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com | Consente a NetApp di raccogliere le informazioni necessarie per risolvere i problemi di supporto. |
| https://ipa-signer.cloudmanager.netapp.com | Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ | Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident. |
| *.blob.core.windows.net | Richiesto per coppie ha quando si utilizza un proxy. |

| Endpoint | Scopo |
| --- | --- |
| Varie sedi di terze parti, ad esempio:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.com<br>Le sedi di terze parti sono soggette a modifiche. | Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti. |

### Endpoint per la gestione delle risorse in GCP

Un connettore contatta i seguenti endpoint durante la gestione delle risorse in GCP:

| Endpoint | Scopo |
| --- | --- |
| https://www.googleapis.com | Consente al connettore di contattare le API Google per l'implementazione e la gestione di Cloud Volumes ONTAP in GCP. |
| https://api.services.cloud.netapp.com:443 | Richieste API a NetApp Cloud Central. |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Fornisce l'accesso a immagini, manifesti e modelli software. |
| https://repo.cloud.support.netapp.com | Utilizzato per scaricare le dipendenze di Cloud Manager. |
| http://repo.mysql.com/ | Utilizzato per scaricare MySQL. |
| https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com | Consente al connettore di accedere e scaricare manifesti, modelli e immagini di aggiornamento Cloud Volumes ONTAP. |
| https://cloudmanagerinfraprod.azurecr.io | Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager. |
| https://kinesis.us-east-1.amazonaws.com | Consente a NetApp di eseguire lo streaming dei dati dai record di audit. |
| https://cloudmanager.cloud.netapp.com | Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central. |
| https://netapp-cloud-account.auth0.com | Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata. |
| https://mysupport.netapp.com | Comunicazione con NetApp AutoSupport. |

| Endpoint | Scopo |
| --- | --- |
| https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com | Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema. |
| https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com | Consente a NetApp di raccogliere le informazioni necessarie per risolvere i problemi di supporto. |
| https://ipa-signer.cloudmanager.netapp.com | Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP) |
| https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/ | Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident. |
| Varie sedi di terze parti, ad esempio:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.com<br>Le sedi di terze parti sono soggette a modifiche. | Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti. |

### Endpoint per installare il connettore su un host Linux

È possibile installare manualmente il software del connettore sul proprio host Linux. In tal caso, il programma di installazione del connettore deve accedere ai seguenti URL durante il processo di installazione:

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

L'host potrebbe tentare di aggiornare i pacchetti del sistema operativo durante l'installazione. L'host può contattare diversi siti di mirroring per questi pacchetti di sistemi operativi.

### Endpoint a cui si accede dal browser Web quando si utilizza l'interfaccia utente locale

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

| Endpoint | Scopo |
| --- | --- |
| L'host del connettore | Per caricare la console di Cloud Manager, è necessario inserire l'indirizzo IP dell'host da un browser Web.<br><br>A seconda della connettività con il cloud provider, è possibile utilizzare l'IP privato o un IP pubblico assegnato all'host:<br><br>• Un IP privato funziona se si dispone di una VPN e di un accesso diretto alla rete virtuale<br>• Un IP pubblico funziona in qualsiasi scenario di rete<br><br>In ogni caso, è necessario proteggere l'accesso alla rete assicurandosi che le regole del gruppo di protezione consentano l'accesso solo da IP o subnet autorizzati. |
| https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com | Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite NetApp Cloud Central. |
| https://widget.intercom.io | Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp. |

## Porte e gruppi di sicurezza

Non c'è traffico in entrata verso il connettore, a meno che non venga avviato. HTTP e HTTPS forniscono l'accesso a "UI locale", che utilizzerai in rare circostanze. SSH è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.

### Regole per il connettore in AWS

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

#### Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

| Protocollo | Porta | Scopo |
| --- | --- | --- |
| SSH | 22 | Fornisce l'accesso SSH all'host del connettore |
| HTTP | 80 | Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale e alle connessioni da Cloud Compliance |
| HTTPS | 443 | Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale |
| TCP | 3128 | Fornisce all'istanza Cloud Compliance l'accesso a Internet, se la rete AWS non utilizza un NAT o un proxy |

#### Regole in uscita

Il gruppo di protezione predefinito per il connettore apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

### Regole di base in uscita

Il gruppo di protezione predefinito per il connettore include le seguenti regole in uscita.

| Protocollo | Porta | Scopo |
|---|---|---|
| Tutti i TCP | Tutto | Tutto il traffico in uscita |
| Tutti gli UDP | Tutto | Tutto il traffico in uscita |

### Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

| Servizio | Protocollo | Porta | Destinazione | Scopo |
|---|---|---|---|---|
| Active Directory | TCP | 88 | Insieme di strutture di Active Directory | Autenticazione Kerberos V. |
| | TCP | 139 | Insieme di strutture di Active Directory | Sessione del servizio NetBIOS |
| | TCP | 389 | Insieme di strutture di Active Directory | LDAP |
| | TCP | 445 | Insieme di strutture di Active Directory | Microsoft SMB/CIFS su TCP con frame NetBIOS |
| | TCP | 464 | Insieme di strutture di Active Directory | Kerberos V change & set password (SET_CHANGE) |
| | TCP | 749 | Insieme di strutture di Active Directory | Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS) |
| | UDP | 137 | Insieme di strutture di Active Directory | Servizio nomi NetBIOS |
| | UDP | 138 | Insieme di strutture di Active Directory | Servizio datagramma NetBIOS |
| | UDP | 464 | Insieme di strutture di Active Directory | Amministrazione delle chiavi Kerberos |
| Chiamate API e AutoSupport | HTTPS | 443 | LIF gestione cluster ONTAP e Internet in uscita | Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp |

| Servizio | Protocollo | Porta | Destinazione | Scopo |
|---|---|---|---|---|
| Chiamate API | TCP | 3000 | LIF gestione cluster ONTAP | Chiamate API a ONTAP |
| | TCP | 8088 | Backup su S3 | API chiama il backup in S3 |
| DNS | UDP | 53 | DNS | Utilizzato per la risoluzione DNS da parte di Cloud Manager |
| Conformità al cloud | HTTP | 80 | Istanza di Cloud Compliance | Conformità del cloud per Cloud Volumes ONTAP |

### Regole per il connettore in Azure

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

#### Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

| Porta | Protocollo | Scopo |
|---|---|---|
| 22 | SSH | Fornisce l'accesso SSH all'host del connettore |
| 80 | HTTP | Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale |
| 443 | HTTPS | Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale |

#### Regole in uscita

Il gruppo di protezione predefinito per il connettore apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

### Regole di base in uscita

Il gruppo di protezione predefinito per il connettore include le seguenti regole in uscita.

| Porta | Protocollo | Scopo |
|---|---|---|
| Tutto | Tutti i TCP | Tutto il traffico in uscita |
| Tutto | Tutti gli UDP | Tutto il traffico in uscita |

### Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

| Servizio | Porta | Protocollo | Destinazione | Scopo |
|---|---|---|---|---|
| Active Directory | 88 | TCP | Insieme di strutture di Active Directory | Autenticazione Kerberos V. |
| | 139 | TCP | Insieme di strutture di Active Directory | Sessione del servizio NetBIOS |
| | 389 | TCP | Insieme di strutture di Active Directory | LDAP |
| | 445 | TCP | Insieme di strutture di Active Directory | Microsoft SMB/CIFS su TCP con frame NetBIOS |
| | 464 | TCP | Insieme di strutture di Active Directory | Kerberos V change & set password (SET_CHANGE) |
| | 749 | TCP | Insieme di strutture di Active Directory | Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS) |
| | 137 | UDP | Insieme di strutture di Active Directory | Servizio nomi NetBIOS |
| | 138 | UDP | Insieme di strutture di Active Directory | Servizio datagramma NetBIOS |
| | 464 | UDP | Insieme di strutture di Active Directory | Amministrazione delle chiavi Kerberos |
| Chiamate API e AutoSupport | 443 | HTTPS | LIF gestione cluster ONTAP e Internet in uscita | Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp |
| Chiamate API | 3000 | TCP | LIF gestione cluster ONTAP | Chiamate API a ONTAP |
| DNS | 53 | UDP | DNS | Utilizzato per la risoluzione DNS da parte di Cloud Manager |

### Regole per il connettore in GCP

Le regole firewall per il connettore richiedono regole sia in entrata che in uscita.

#### Regole in entrata

L'origine delle regole in entrata nelle regole firewall predefinite è 0.0.0.0/0.

| Protocollo | Porta | Scopo |
|---|---|---|
| SSH | 22 | Fornisce l'accesso SSH all'host del connettore |
| HTTP | 80 | Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale |
| HTTPS | 443 | Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale |

#### Regole in uscita

Le regole firewall predefinite per il connettore aprono tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

### Regole di base in uscita

Le regole firewall predefinite per il connettore includono le seguenti regole in uscita.

| Protocollo | Porta | Scopo |
|---|---|---|
| Tutti i TCP | Tutto | Tutto il traffico in uscita |
| Tutti gli UDP | Tutto | Tutto il traffico in uscita |

### Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

| Servizio | Protocollo | Porta | Destinazione | Scopo |
|---|---|---|---|---|
| Active Directory | TCP | 88 | Insieme di strutture di Active Directory | Autenticazione Kerberos V. |
| | TCP | 139 | Insieme di strutture di Active Directory | Sessione del servizio NetBIOS |
| | TCP | 389 | Insieme di strutture di Active Directory | LDAP |
| | TCP | 445 | Insieme di strutture di Active Directory | Microsoft SMB/CIFS su TCP con frame NetBIOS |
| | TCP | 464 | Insieme di strutture di Active Directory | Kerberos V change & set password (SET_CHANGE) |
| | TCP | 749 | Insieme di strutture di Active Directory | Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS) |
| | UDP | 137 | Insieme di strutture di Active Directory | Servizio nomi NetBIOS |
| | UDP | 138 | Insieme di strutture di Active Directory | Servizio datagramma NetBIOS |
| | UDP | 464 | Insieme di strutture di Active Directory | Amministrazione delle chiavi Kerberos |
| Chiamate API e AutoSupport | HTTPS | 443 | LIF gestione cluster ONTAP e Internet in uscita | Chiamate API a GCP e ONTAP e invio di messaggi AutoSupport a NetApp |
| Chiamate API | TCP | 3000 | LIF gestione cluster ONTAP | Chiamate API a ONTAP |
| DNS | UDP | 53 | DNS | Utilizzato per la risoluzione DNS da parte di Cloud Manager |

# Creazione di un connettore in AWS da Cloud Manager

Un account Admin deve implementare un *connettore* prima di poter utilizzare la maggior parte delle funzionalità di Cloud Manager. "Scopri quando è necessario un connettore". Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Questa pagina descrive come creare un connettore in AWS direttamente da Cloud Manager. È inoltre possibile

scegliere di "Creare il connettore da AWS Marketplace", o a. "scaricare il software e installarlo sul proprio host".

Questi passaggi devono essere completati da un utente che ha il ruolo di amministratore dell'account. Un amministratore dell'area di lavoro non può creare un connettore.

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiederà di creare un connettore se non ne hai ancora uno.

## Impostazione delle autorizzazioni AWS per creare un connettore

Prima di poter implementare un connettore da Cloud Manager, è necessario assicurarsi che l'account AWS disponga delle autorizzazioni corrette.

**Fasi**

1. Scaricare la policy di Connector IAM dal seguente percorso:

   "NetApp Cloud Manager: Policy AWS, Azure e GCP"

2. Dalla console AWS IAM, creare una policy personalizzata copiando e incollando il testo dal criterio IAM del connettore.
3. Collegare il criterio creato nel passaggio precedente all'utente IAM che creerà il connettore da Cloud Manager.

**Risultato**

L'utente AWS dispone ora delle autorizzazioni necessarie per creare il connettore da Cloud Manager. Quando richiesto da Cloud Manager, devi specificare le chiavi di accesso AWS per questo utente.

## Creazione di un connettore in AWS

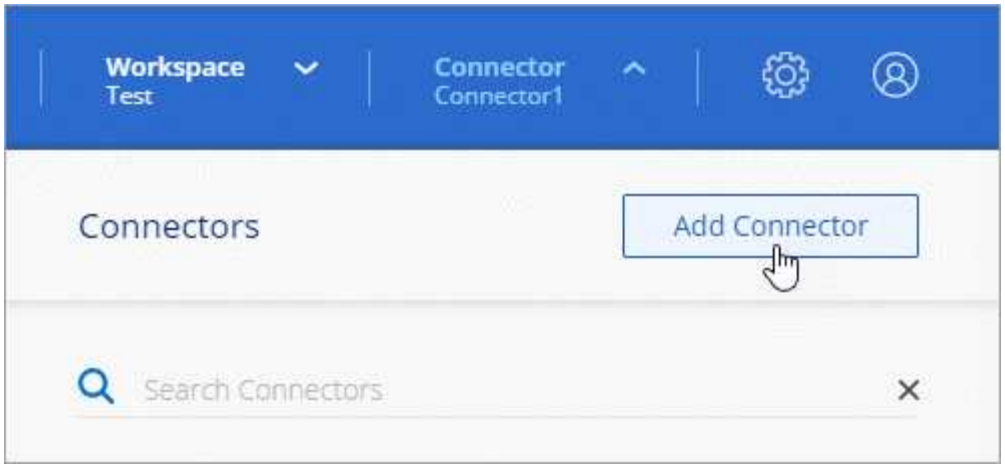
Cloud Manager consente di creare un connettore in AWS direttamente dalla relativa interfaccia utente.

**Di cosa hai bisogno**

- Una chiave di accesso AWS e una chiave segreta per un utente IAM che dispone di "autorizzazioni richieste".
- VPC, subnet e coppia di chiavi nella regione AWS desiderata.

**Fasi**

1. Se si sta creando il primo ambiente di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni. In caso contrario, fare clic sull'elenco a discesa **Connector** e selezionare **Add Connector** (Aggiungi connettore).




2. Fare clic su **Let's Start**.
3. Scegli **Amazon Web Services** come tuo cloud provider.

   Tenere presente che il connettore deve disporre di una connessione di rete con il tipo di ambiente di lavoro che si sta creando e con i servizi che si intende abilitare.

   "Scopri di più sui requisiti di rete per il connettore".

4. Consulta le informazioni necessarie e fai clic su **continua**.
5. Fornire le informazioni richieste:
   - **AWS Credentials**: Immettere un nome per l'istanza e specificare la chiave di accesso AWS e la chiave segreta che soddisfano i requisiti di autorizzazione.
   - **Location**: Specificare una regione AWS, un VPC e una subnet per l'istanza.
   - **Rete**: Selezionare la coppia di chiavi da utilizzare con l'istanza, se attivare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.
   - **Security Group**: Scegliere se creare un nuovo gruppo di sicurezza o se selezionare un gruppo di sicurezza esistente che consenta l'accesso HTTP, HTTPS e SSH in entrata.

     Non c'è traffico in entrata verso il connettore, a meno che non venga avviato. HTTP e HTTPS forniscono l'accesso a "UI locale", che utilizzerai in rare circostanze. SSH è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.

6. Fare clic su **Create** (Crea).

   L'istanza dovrebbe essere pronta in circa 7 minuti. Si consiglia di rimanere sulla pagina fino al completamento del processo.

**Al termine**

È necessario associare un connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano utilizzare tali connettori per creare sistemi Cloud Volumes ONTAP. Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in Cloud Manager per impostazione predefinita. "Scopri di più".

# Creazione di un connettore in Azure da Cloud Manager

Un account Admin deve implementare un *connettore* prima di poter utilizzare la maggior parte delle funzionalità di Cloud Manager. "Scopri quando è necessario un connettore". Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Questa pagina descrive come creare un connettore in Azure direttamente da Cloud Manager. È inoltre possibile scegliere di "Creare il connettore da Azure Marketplace", o a. "scaricare il software e installarlo sul proprio host".

Questi passaggi devono essere completati da un utente che ha il ruolo di amministratore dell'account. Un amministratore dell'area di lavoro non può creare un connettore.

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiederà di creare un connettore se non ne hai ancora uno.

## Impostazione delle autorizzazioni Azure per creare un connettore

Prima di poter implementare un connettore da Cloud Manager, devi assicurarti che il tuo account Azure disponga delle autorizzazioni corrette.

**Fasi**

1. Creare un ruolo personalizzato utilizzando il criterio Azure per il connettore:

   a. Scaricare il "Policy di Azure per il connettore".

      Fare clic con il pulsante destro del mouse sul collegamento e fare clic su **Save link as…** (Salva collegamento con nome…) per scaricare il file.

   b. Modificare il file JSON aggiungendo l'ID di abbonamento Azure all'ambito assegnabile.

      **Esempio**

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

   c. Utilizzare il file JSON per creare un ruolo personalizzato in Azure.

      Nell'esempio seguente viene illustrato come creare un ruolo personalizzato utilizzando Azure CLI 2.0:

      ```
      az role definition create --role-definition
      C:\Policy_for_Setup_As_Service_Azure.json
      ```

   Ora dovresti avere un ruolo personalizzato chiamato *Azure SetupAsService*.

2. Assegnare il ruolo all'utente che implementerà il connettore da Cloud Manager:

   a. Aprire il servizio **Subscriptions** e selezionare l'abbonamento dell'utente.

b. Fare clic su **controllo di accesso (IAM)**.

c. Fare clic su **Aggiungi** > **Aggiungi assegnazione ruolo** e aggiungere le autorizzazioni:

- Selezionare il ruolo **Azure SetupAsService**.

> Azure SetupAsService è il nome predefinito fornito in "Policy di implementazione del connettore per Azure". Se si sceglie un nome diverso per il ruolo, selezionare il nome desiderato.

- Assegnare l'accesso a un utente, un gruppo o un'applicazione * di Azure ad.
- Selezionare l'account utente.
- Fare clic su **Save** (Salva).

**Risultato**

L'utente Azure dispone ora delle autorizzazioni necessarie per implementare il connettore da Cloud Manager.

## Creazione di un connettore in Azure

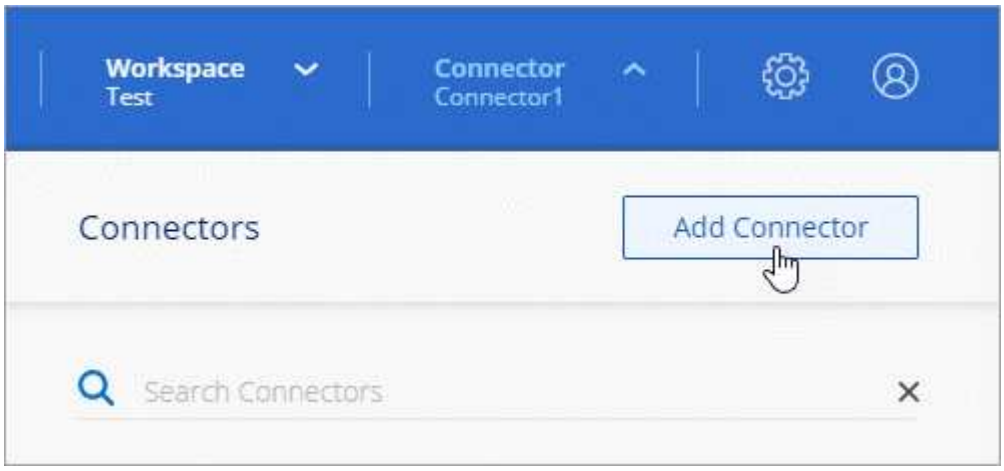
Cloud Manager consente di creare un connettore in Azure direttamente dalla sua interfaccia utente.

**Di cosa hai bisogno**

- Il "autorizzazioni richieste" Per il tuo account Azure.
- Un abbonamento Azure.
- Una VNET e una subnet nella regione Azure desiderata.

**Fasi**

1. Se si sta creando il primo ambiente di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni. In caso contrario, fare clic sull'elenco a discesa **Connector** e selezionare **Add Connector** (Aggiungi connettore).




2. Fare clic su **Let's Start**.
3. Scegli **Microsoft Azure** come tuo cloud provider.

   Tenere presente che il connettore deve disporre di una connessione di rete con il tipo di ambiente di lavoro che si sta creando e con i servizi che si intende abilitare.

   "Scopri di più sui requisiti di rete per il connettore".

4. Consulta le informazioni necessarie e fai clic su **continua**.
5. Se richiesto, accedere all'account Microsoft, che dovrebbe disporre delle autorizzazioni necessarie per creare la macchina virtuale.

   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, Cloud Manager utilizzerà automaticamente tale account. Se disponi di più account, potrebbe essere necessario prima disconnettersi per assicurarsi di utilizzare l'account corretto.

6. Fornire le informazioni richieste:
   - **VM Authentication**: Immettere un nome per la macchina virtuale e un nome utente e una password o una chiave pubblica.
   - **Basic Settings** (Impostazioni di base): Scegliere un abbonamento Azure, un'area Azure e se creare un nuovo gruppo di risorse o utilizzare un gruppo di risorse esistente.
   - **Rete**: Scegliere un VNET e una subnet, se attivare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.
   - **Security Group**: Scegliere se creare un nuovo gruppo di sicurezza o se selezionare un gruppo di sicurezza esistente che consenta l'accesso HTTP, HTTPS e SSH in entrata.

     Non c'è traffico in entrata verso il connettore, a meno che non venga avviato. HTTP e HTTPS forniscono l'accesso a "UI locale", che utilizzerai in rare circostanze. SSH è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.

7. Fare clic su **Create** (Crea).

   La macchina virtuale dovrebbe essere pronta in circa 7 minuti. Si consiglia di rimanere sulla pagina fino al completamento del processo.

**Al termine**

È necessario associare un connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano utilizzare tali connettori per creare sistemi Cloud Volumes ONTAP. Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in Cloud Manager per impostazione predefinita. "Scopri di più".

# Creazione di un connettore in GCP da Cloud Manager

Un account Admin deve implementare un *connettore* prima di poter utilizzare la maggior parte delle funzionalità di Cloud Manager. "Scopri quando è necessario un connettore". Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Questa pagina descrive come creare un connettore in GCP direttamente da Cloud Manager. È inoltre possibile scegliere di "scaricare il software e installarlo sul proprio host".

Questi passaggi devono essere completati da un utente che ha il ruolo di amministratore dell'account. Un amministratore dell'area di lavoro non può creare un connettore.

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiederà di creare un connettore se non ne hai ancora uno.

## Impostazione delle autorizzazioni GCP per creare un connettore

Prima di poter implementare un connettore da Cloud Manager, è necessario assicurarsi che l'account GCP disponga delle autorizzazioni corrette e che sia impostato un account di servizio per la macchina virtuale del connettore.

**Fasi**

1. Assicurarsi che l'utente GCP che implementa Cloud Manager da NetApp Cloud Central disponga delle autorizzazioni in "Policy di implementazione del connettore per GCP".

   "È possibile creare un ruolo personalizzato utilizzando il file YAML" quindi allegarlo all'utente. Per creare il ruolo, dovrai utilizzare la riga di comando di gcloud.

2. Impostare un account di servizio che disponga delle autorizzazioni necessarie per creare e gestire i sistemi Cloud Volumes ONTAP nei progetti.

   Questo account del servizio verrà associato alla macchina virtuale del connettore quando lo si crea da Cloud Manager.

   a. "Creare un ruolo in GCP" che include le autorizzazioni definite in "Policy di Cloud Manager per GCP". Anche in questo caso, è necessario utilizzare la riga di comando di gcloud.

      Le autorizzazioni contenute in questo file YAML sono diverse da quelle del passaggio 2a.

   b. "Creare un account di servizio GCP e applicare il ruolo personalizzato appena creato".

   c. Se si desidera implementare Cloud Volumes ONTAP in altri progetti, "Concedere l'accesso aggiungendo l'account di servizio con il ruolo Cloud Manager a quel progetto". Dovrai ripetere questo passaggio per ogni progetto.

**Risultato**

L'utente GCP dispone ora delle autorizzazioni necessarie per creare il connettore da Cloud Manager e l'account del servizio per la macchina virtuale del connettore è impostato.

## Abilitazione delle API di Google Cloud

Per implementare il connettore e Cloud Volumes ONTAP sono necessarie diverse API.

**Fase**

1. "Abilita le seguenti API di Google Cloud nel tuo progetto".
   - API di Cloud Deployment Manager V2
   - API Cloud Logging
   - API Cloud Resource Manager
   - API di Compute Engine
   - API IAM (Identity and Access Management)

## Creazione di un connettore in GCP

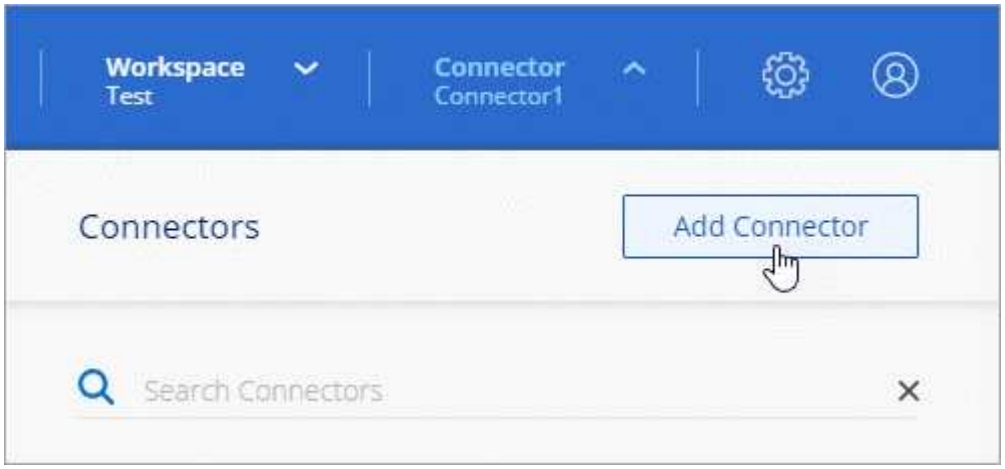
Cloud Manager consente di creare un connettore in GCP direttamente dalla sua interfaccia utente.

**Di cosa hai bisogno**

- Il "autorizzazioni richieste" Per il tuo account Google Cloud.
- Un progetto Google Cloud.
- Account di servizio che dispone delle autorizzazioni necessarie per creare e gestire Cloud Volumes ONTAP.
- Un VPC e una subnet nell'area di Google Cloud desiderata.

**Fasi**

1. Se si sta creando il primo ambiente di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni. In caso contrario, fare clic sull'elenco a discesa **Connector** e selezionare **Add Connector** (Aggiungi connettore).




2. Fare clic su **Let's Start**.
3. Scegli **Google Cloud Platform** come tuo cloud provider.

   Tenere presente che il connettore deve disporre di una connessione di rete con il tipo di ambiente di lavoro che si sta creando e con i servizi che si intende abilitare.

   "Scopri di più sui requisiti di rete per il connettore".

4. Consulta le informazioni necessarie e fai clic su **continua**.
5. Se richiesto, accedere all'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.

6. Fornire le informazioni richieste:
   - **Basic Settings** (Impostazioni di base): Immettere un nome per l'istanza della macchina virtuale e specificare un account di progetto e servizio con le autorizzazioni richieste.
   - **Location**: Specificare una regione, una zona, un VPC e una subnet per l'istanza.
   - **Network** (rete): Scegliere se attivare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.

- **Firewall Policy**: Scegliere se creare una nuova policy firewall o se selezionare una policy firewall esistente che consenta l'accesso HTTP, HTTPS e SSH in entrata.

  Non c'è traffico in entrata verso il connettore, a meno che non venga avviato. HTTP e HTTPS forniscono l'accesso a "UI locale", che utilizzerai in rare circostanze. SSH è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.

7. Fare clic su **Create** (Crea).

   L'istanza dovrebbe essere pronta in circa 7 minuti. Si consiglia di rimanere sulla pagina fino al completamento del processo.

**Al termine**

È necessario associare un connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano utilizzare tali connettori per creare sistemi Cloud Volumes ONTAP. Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in Cloud Manager per impostazione predefinita. "Scopri di più".