



Account di cloud provider

Cloud Manager 3.7

NetApp
March 25, 2024

Sommario

- Account di cloud provider 1
 - Account e autorizzazioni AWS 1
 - Account e autorizzazioni Azure 3
 - Progetti, autorizzazioni e account Google Cloud 5

Account di cloud provider

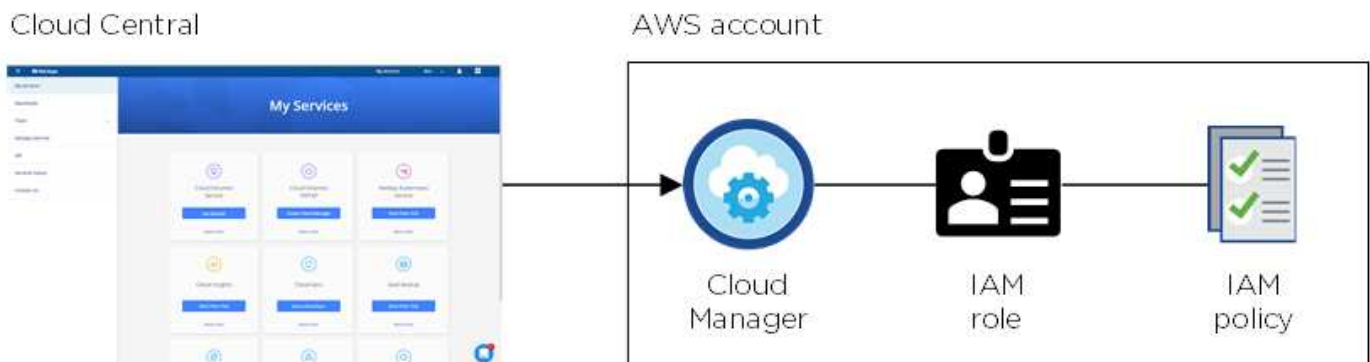
Account e autorizzazioni AWS

Cloud Manager consente di scegliere l'account AWS in cui si desidera implementare un sistema Cloud Volumes ONTAP. È possibile implementare tutti i sistemi Cloud Volumes ONTAP nell'account AWS iniziale oppure impostare account aggiuntivi.

L'account AWS iniziale

Quando si implementa Cloud Manager da NetApp Cloud Central, è necessario utilizzare un account AWS che disponga delle autorizzazioni per avviare l'istanza di Cloud Manager. Le autorizzazioni richieste sono elencate nella ["Policy NetApp Cloud Central per AWS"](#).

Quando Cloud Central avvia l'istanza di Cloud Manager in AWS, crea un ruolo IAM e un profilo di istanza per l'istanza. Allega inoltre una policy che fornisce a Cloud Manager le autorizzazioni per implementare e gestire Cloud Volumes ONTAP in quell'account AWS. ["Analisi dell'utilizzo delle autorizzazioni da parte di Cloud Manager"](#).



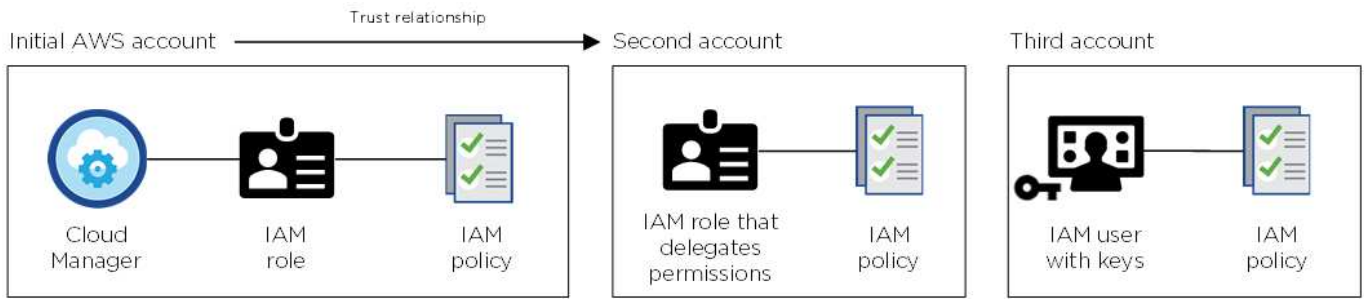
Cloud Manager seleziona questo account cloud provider per impostazione predefinita quando crei un nuovo ambiente di lavoro:

Details & Credentials

This working environment will be created in Cloud Provider Account: Instance Profile | Account ID: [REDACTED] | [Switch Account](#)

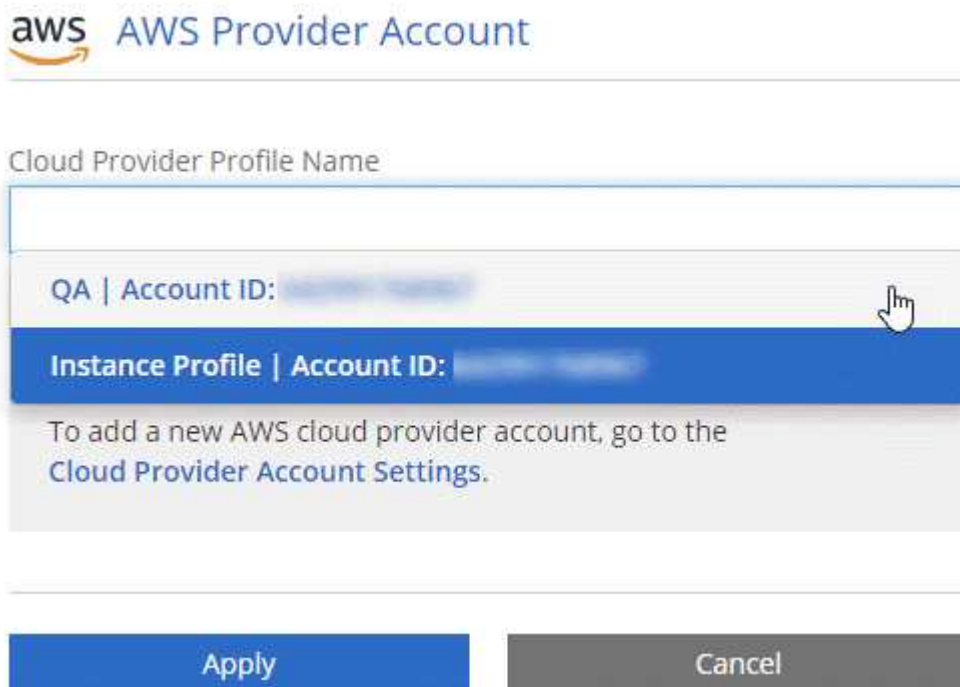
Account AWS aggiuntivi

Se si desidera avviare Cloud Volumes ONTAP in diversi account AWS, è possibile farlo ["Fornire le chiavi AWS per un utente IAM o l'ARN di un ruolo in un account attendibile"](#). L'immagine seguente mostra due account aggiuntivi, uno che fornisce le autorizzazioni tramite un ruolo IAM in un account attendibile e l'altro tramite le chiavi AWS di un utente IAM:



Allora "Aggiungi gli account del provider cloud a Cloud Manager" Specificando il nome risorsa Amazon (ARN) del ruolo IAM o le chiavi AWS per l'utente IAM.

Dopo aver aggiunto un altro account, è possibile passare a tale account durante la creazione di un nuovo ambiente di lavoro:



E le implementazioni di Marketplace e on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato da NetApp Cloud Central. È inoltre possibile implementare Cloud Manager in AWS da "Mercato AWS" e puoi farlo "Installazione di Cloud Manager on-premise".

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

Per le implementazioni on-premise, non è possibile impostare un ruolo IAM per il sistema Cloud Manager, ma è possibile fornire le autorizzazioni esattamente come si farebbe per altri account AWS.

Account e autorizzazioni Azure

Cloud Manager consente di scegliere l'account Azure in cui si desidera implementare un sistema Cloud Volumes ONTAP. Puoi implementare tutti i tuoi sistemi Cloud Volumes ONTAP nell'account Azure iniziale oppure puoi impostare altri account.

L'account Azure iniziale

Quando si implementa Cloud Manager da NetApp Cloud Central, è necessario utilizzare un account Azure che disponga delle autorizzazioni necessarie per implementare la macchina virtuale Cloud Manager. Le autorizzazioni richieste sono elencate nella ["Policy di NetApp Cloud Central per Azure"](#).

Quando Cloud Central implementa la macchina virtuale Cloud Manager in Azure, abilita una ["identità gestita assegnata dal sistema"](#) Sulla macchina virtuale Cloud Manager, crea un ruolo personalizzato e lo assegna alla macchina virtuale. Il ruolo fornisce a Cloud Manager le autorizzazioni per implementare e gestire Cloud Volumes ONTAP in quell'abbonamento Azure. ["Analisi dell'utilizzo delle autorizzazioni da parte di Cloud Manager"](#).



Cloud Manager seleziona questo account cloud provider per impostazione predefinita quando crei un nuovo ambiente di lavoro:

Details & Credentials

This working environment will be created in Cloud Provider Account: Managed Service Identity | Azure Subscription: OCCM QA1 | [Switch Account](#)

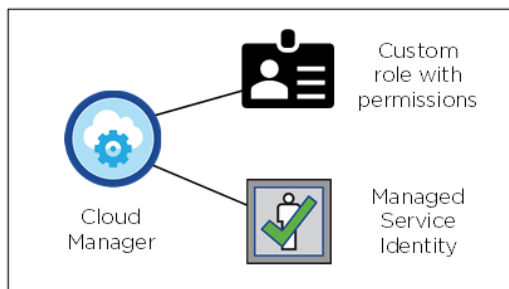
Abbonamenti Azure aggiuntivi per l'account iniziale

L'identità gestita è associata all'abbonamento con cui hai lanciato Cloud Manager. Se si desidera selezionare un abbonamento Azure diverso, è necessario ["associare l'identità gestita a tali sottoscrizioni"](#).

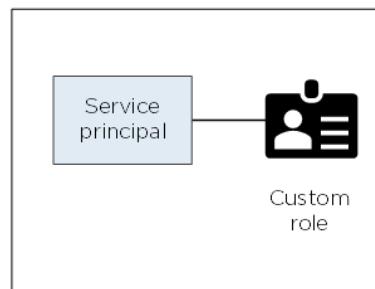
Altri account Azure

Se si desidera implementare Cloud Volumes ONTAP in diversi account Azure, è necessario concedere le autorizzazioni richieste da ["Creazione e configurazione di un'entità di servizio in Azure Active Directory"](#) Per ciascun account Azure. L'immagine seguente mostra due account aggiuntivi, ciascuno configurato con un'entità del servizio e un ruolo personalizzato che fornisce le autorizzazioni:

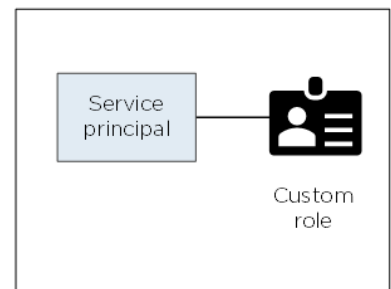
Initial Azure account



Second account



Third account



Allora "Aggiungi gli account del provider cloud a Cloud Manager" Fornendo dettagli sull'identità del servizio ad.

Dopo aver aggiunto un altro account, è possibile passare a tale account durante la creazione di un nuovo ambiente di lavoro:

Microsoft Azure Provider Account

Cloud Provider Profile Name

Azure Keys | Application ID: [redacted] ...

Dev Keys | Application ID: [redacted] ...

Managed Service Identity

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply

Cancel

E le implementazioni di Marketplace e on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato da NetApp Cloud Central. È inoltre possibile implementare Cloud Manager in Azure da ["Azure Marketplace"](#) e puoi farlo ["Installazione di Cloud Manager on-premise"](#).

Se si utilizza Marketplace, le autorizzazioni vengono fornite nello stesso modo. Devi solo creare e configurare manualmente l'identità gestita per Cloud Manager, quindi fornire le autorizzazioni per eventuali account aggiuntivi.

Per le implementazioni on-premise, non è possibile impostare un'identità gestita per il sistema Cloud Manager, ma è possibile fornire autorizzazioni come faresti per altri account.

Progetti, autorizzazioni e account Google Cloud

Un account di servizio fornisce a Cloud Manager le autorizzazioni per implementare e gestire i sistemi Cloud Volumes ONTAP nello stesso progetto di Cloud Manager o in progetti diversi. Gli account Google Cloud aggiunti a Cloud Manager vengono utilizzati per abilitare il tiering dei dati.

Progetto e permessi per Cloud Manager

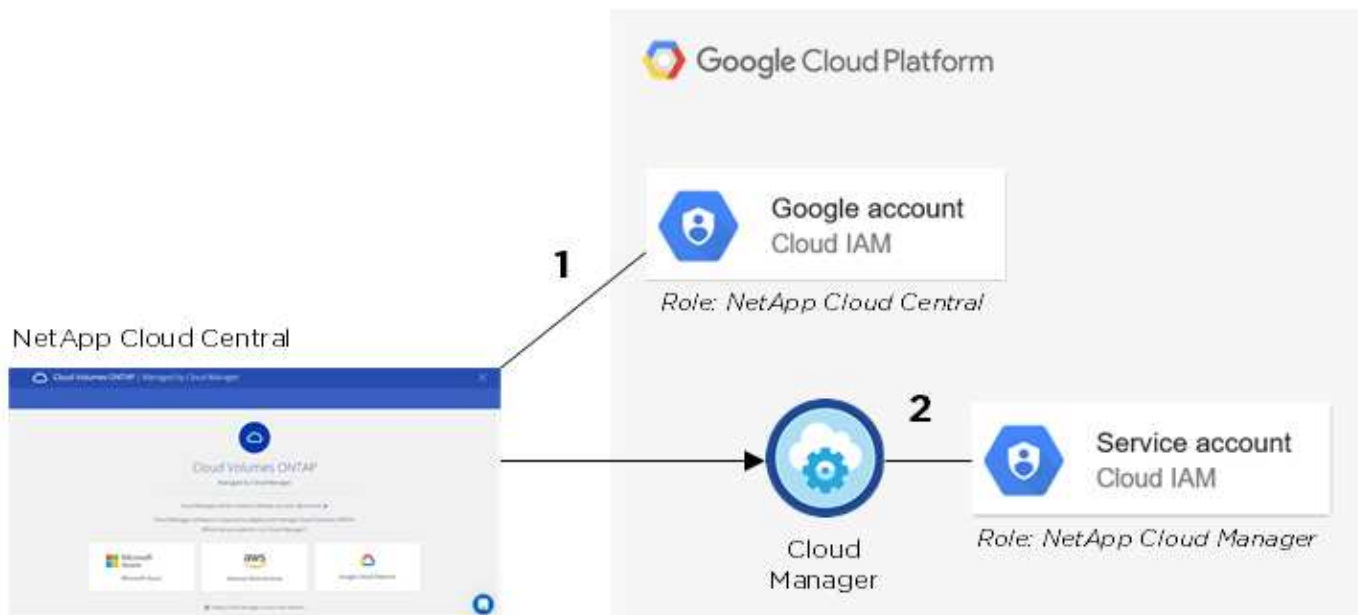
Prima di poter implementare Cloud Volumes ONTAP in Google Cloud, devi prima implementare Cloud Manager in un progetto Google Cloud. Cloud Manager non può essere eseguito in sede o in un altro cloud provider.

Prima di implementare Cloud Manager da, è necessario disporre di due set di autorizzazioni ["NetApp Cloud Central"](#):

1. È necessario implementare Cloud Manager utilizzando un account Google che disponga delle autorizzazioni per avviare l'istanza della macchina virtuale di Cloud Manager da Cloud Central.
2. Durante l'implementazione di Cloud Manager, viene richiesto di selezionare un ["account di servizio"](#) Per l'istanza della macchina virtuale. Cloud Manager ottiene le autorizzazioni dall'account del servizio per creare e gestire i sistemi Cloud Volumes ONTAP per conto dell'utente. Le autorizzazioni vengono fornite allegando un ruolo personalizzato all'account del servizio.

Abbiamo impostato due file YAML che includono le autorizzazioni richieste per l'utente e l'account del servizio. ["Scopri come utilizzare i file YAML per impostare le autorizzazioni"](#).

La seguente immagine mostra i requisiti di autorizzazione descritti nei numeri 1 e 2 precedenti:



Progetto per Cloud Volumes ONTAP

Cloud Volumes ONTAP può risiedere nello stesso progetto di Cloud Manager o in un progetto diverso. Per implementare Cloud Volumes ONTAP in un progetto diverso, devi prima aggiungere l'account del servizio e il ruolo di Cloud Manager a quel progetto.

- ["Scopri come configurare l'account di servizio Cloud Manager \(vedi punto 4\)"](#).
- ["Scopri come implementare Cloud Volumes ONTAP in GCP e selezionare un progetto"](#).

Account per il tiering dei dati

Per abilitare il tiering dei dati su un sistema Cloud Volumes ONTAP, è necessario aggiungere un account Google Cloud a Cloud Manager. Il tiering dei dati esegue automaticamente il tiering dei dati cold in uno storage a oggetti a basso costo, consentendoti di recuperare spazio sullo storage primario e ridurre lo storage secondario.

Quando si aggiunge l'account, è necessario fornire a Cloud Manager una chiave di accesso allo storage per un account di servizio che dispone delle autorizzazioni Storage Admin. Cloud Manager utilizza le chiavi di accesso per configurare e gestire un bucket di cloud storage per il tiering dei dati.

Dopo aver aggiunto un account Google Cloud, è possibile attivare il tiering dei dati sui singoli volumi quando vengono creati, modificati o replicati.

- ["Scopri come configurare e aggiungere account GCP a Cloud Manager"](#).
- ["Scopri come eseguire il tiering dei dati inattivi verso uno storage a oggetti a basso costo"](#).

Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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 CONSEQUENZIALE (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.