AWS

Cloud Manager 3.8

NetApp
March 25, 2024

Sommario

AWS

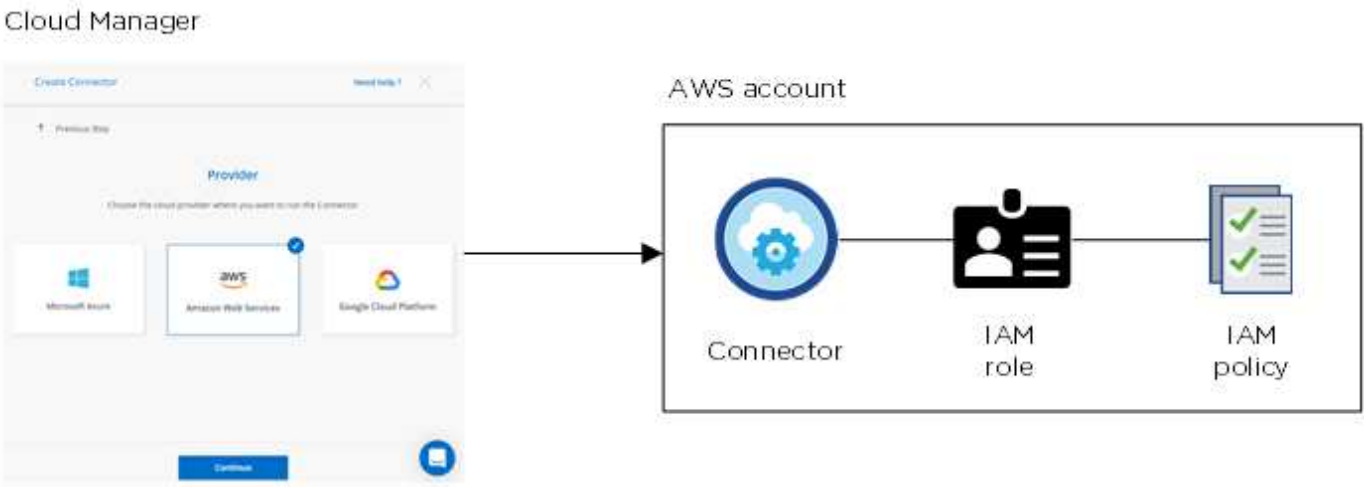
Credenziali e autorizzazioni AWS

Cloud Manager consente di scegliere le credenziali AWS da utilizzare durante l'implementazione di Cloud Volumes ONTAP. È possibile implementare tutti i sistemi Cloud Volumes ONTAP utilizzando le credenziali AWS iniziali oppure aggiungere credenziali aggiuntive.

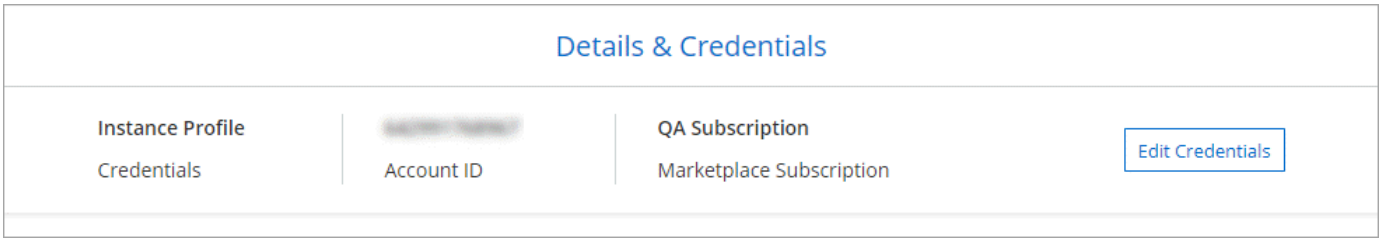
Credenziali AWS iniziali

Quando si implementa un connettore da Cloud Manager, è necessario utilizzare un account AWS che disponga delle autorizzazioni per avviare l'istanza di Connector. Le autorizzazioni richieste sono elencate nella "Policy di implementazione del connettore per AWS".

Quando Cloud Manager avvia l'istanza del connettore 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 gestire risorse e processi all'interno di tale account AWS. "Analisi dell'utilizzo delle autorizzazioni da parte di Cloud Manager".

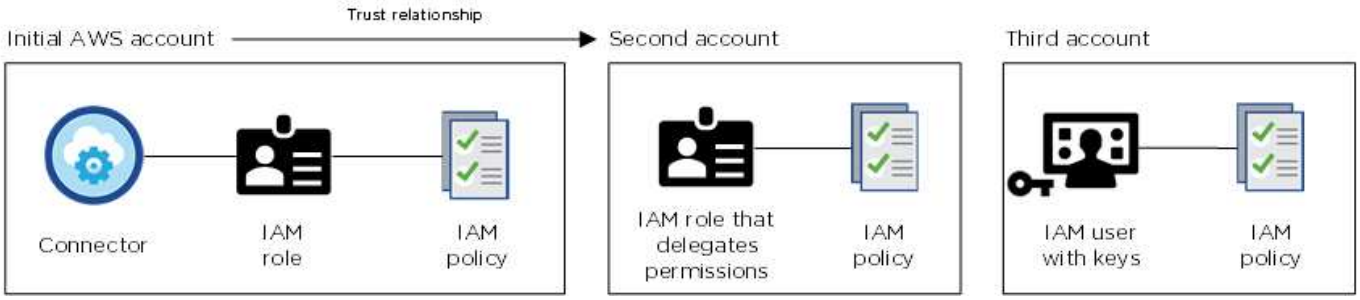


Cloud Manager seleziona queste credenziali AWS per impostazione predefinita quando crei un nuovo ambiente di lavoro per Cloud Volumes ONTAP:



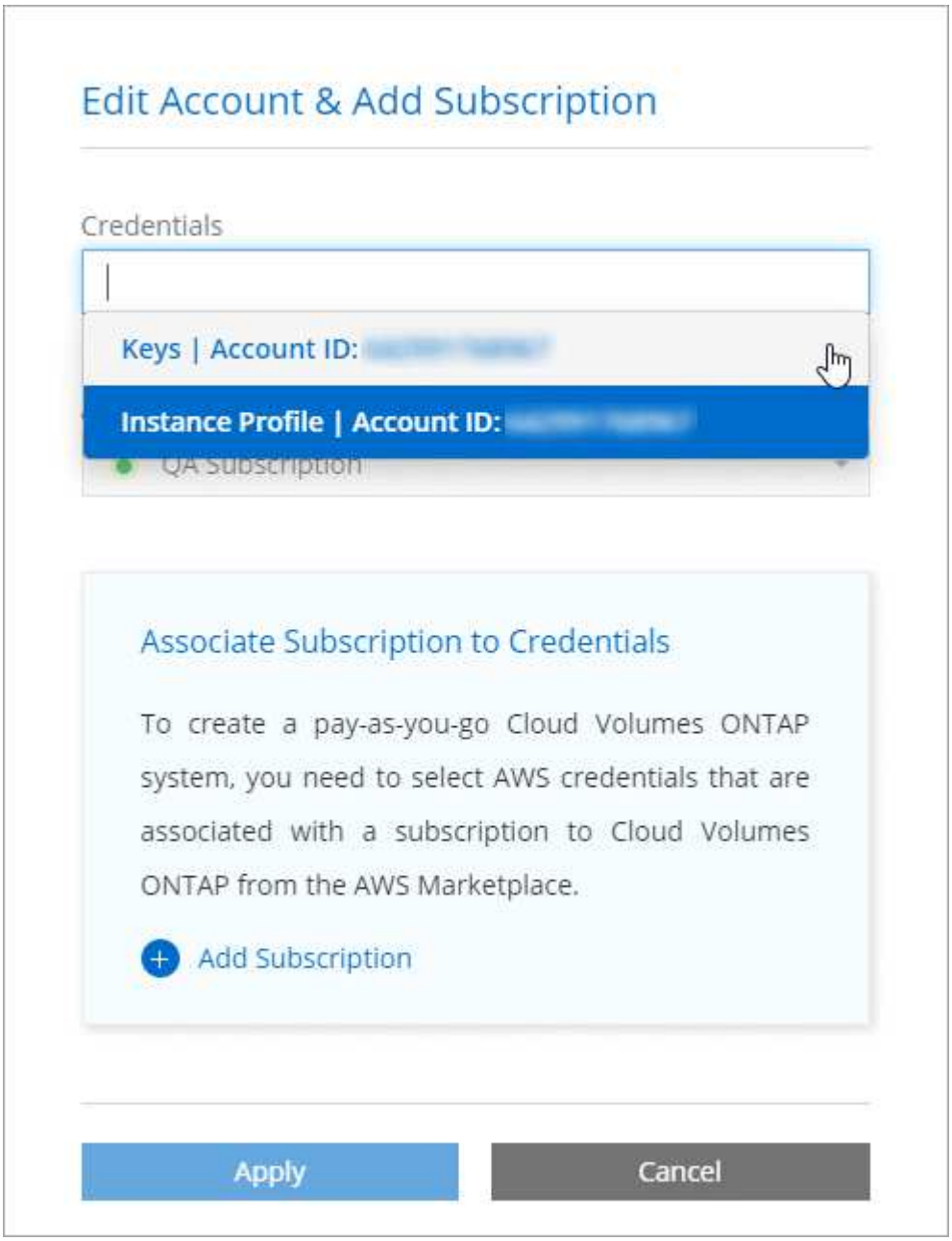
Credenziali AWS aggiuntive

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 "Aggiungere le credenziali dell'account 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 set di credenziali, è possibile passare a queste quando si crea un nuovo ambiente di lavoro:



E le implementazioni di Marketplace e on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato per il connettore, che proviene da Cloud Manager. È inoltre possibile implementare un connettore in AWS da "Mercato AWS" e puoi farlo "Installare il connettore 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.

Come si possono ruotare in modo sicuro le credenziali AWS?

Come descritto in precedenza, Cloud Manager consente di fornire le credenziali AWS in diversi modi: Un ruolo IAM associato all'istanza del connettore, assumendo un ruolo IAM in un account attendibile o fornendo le chiavi di accesso AWS.

Con le prime due opzioni, Cloud Manager utilizza AWS Security Token Service per ottenere credenziali temporanee che ruotano costantemente. Questo processo è la Best practice: È automatico e sicuro.

Se si forniscono a Cloud Manager le chiavi di accesso AWS, è necessario ruotarle aggiornandole in Cloud Manager a intervalli regolari. Si tratta di un processo completamente manuale.

Gestione delle credenziali AWS e delle sottoscrizioni per Cloud Manager

Quando si crea un sistema Cloud Volumes ONTAP, è necessario selezionare le credenziali e l'abbonamento AWS da utilizzare con tale sistema. Se si gestiscono più sottoscrizioni AWS, è possibile assegnarle a diverse credenziali AWS dalla pagina credenziali.

Prima di aggiungere le credenziali AWS a Cloud Manager, è necessario fornire le autorizzazioni necessarie per tale account. Le autorizzazioni consentono a Cloud Manager di gestire risorse e processi all'interno di tale account AWS. La modalità di fornitura delle autorizzazioni dipende dal fatto che si desideri fornire a Cloud Manager le chiavi AWS o l'ARN di un ruolo in un account attendibile.

Quando hai implementato un connettore da Cloud Manager, Cloud Manager ha aggiunto automaticamente le credenziali AWS per l'account in cui hai implementato il connettore. Questo account iniziale non viene aggiunto se il software Connector è stato installato manualmente su un sistema esistente. "Scopri le credenziali e le autorizzazioni AWS".

Scelte

- Concessione delle autorizzazioni fornendo le chiavi AWS
- Concessione delle autorizzazioni assumendo ruoli IAM in altri account

Come si possono ruotare in modo sicuro le credenziali AWS?

Cloud Manager consente di fornire le credenziali AWS in diversi modi: Un ruolo IAM associato all'istanza del connettore, 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, Cloud Manager utilizza AWS Security Token Service per ottenere credenziali temporanee che ruotano costantemente. Questo processo è la Best practice, è automatico e sicuro.

Se si forniscono a Cloud Manager le chiavi di accesso AWS, è necessario ruotarle aggiornandole in Cloud Manager a intervalli regolari. Si tratta di un processo completamente manuale.

Concessione delle autorizzazioni fornendo le chiavi AWS

Se si desidera fornire a Cloud Manager le chiavi AWS per un utente IAM, è necessario concedere le autorizzazioni necessarie a tale utente. La policy IAM di Cloud Manager definisce le azioni e le risorse AWS che Cloud Manager può utilizzare.

Fasi

1. Scarica la policy IAM di Cloud Manager da "Pagina delle policy di Cloud Manager".
2. Dalla console IAM, creare la propria policy copiando e incollando il testo dalla policy IAM di Cloud Manager.

   "Documentazione AWS: Creazione di policy IAM"

3. Allegare il criterio a un ruolo IAM o a un utente IAM.
   - "Documentazione AWS: Creazione dei ruoli IAM"
   - "Documentazione di AWS: Aggiunta e rimozione dei criteri IAM"

Risultato

L'account dispone ora delle autorizzazioni necessarie. Ora puoi aggiungerlo a Cloud Manager.

Concessione delle autorizzazioni assumendo ruoli IAM in altri account

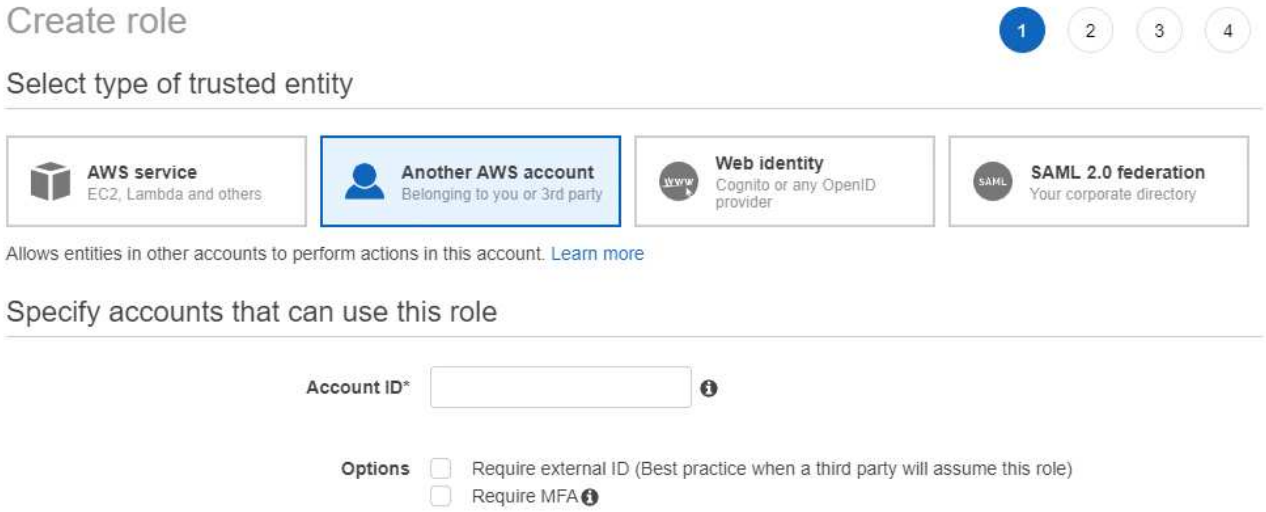
È possibile impostare una relazione di trust tra l'account AWS di origine in cui è stata implementata l'istanza di Connector e altri account AWS utilizzando i ruoli IAM. In seguito, fornirai a Cloud Manager l'ARN dei ruoli IAM degli account attendibili.

Fasi

1. Accedere all'account di destinazione in cui si desidera implementare Cloud Volumes ONTAP e creare un ruolo IAM selezionando **un altro account AWS**.

   Assicurarsi di effettuare le seguenti operazioni:

   - Inserire l'ID dell'account in cui risiede l'istanza di Connector.
   - Allegare la policy IAM di Cloud Manager, disponibile in "Pagina delle policy di Cloud Manager".



2. Accedere all'account di origine in cui risiede l'istanza di Connector e selezionare il ruolo IAM associato all'istanza.

   a. Fare clic su **Allega policy**, quindi su **Crea policy**.

   b. Creare una policy che includa l'azione "sts:AssumeRole" e l'ARN del ruolo creato nell'account di destinazione.

   Esempio

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Risultato

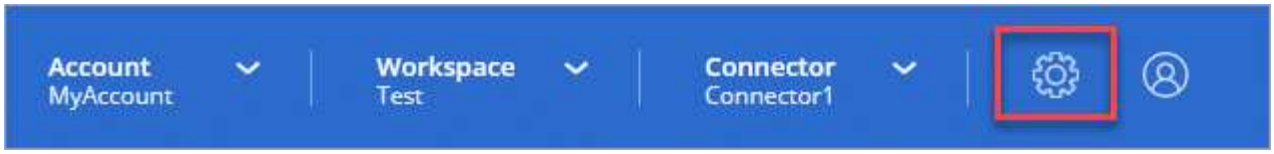
L'account dispone ora delle autorizzazioni necessarie. Ora puoi aggiungerlo a Cloud Manager.

Aggiunta di credenziali AWS a Cloud Manager

Dopo aver fornito un account AWS con le autorizzazioni richieste, è possibile aggiungere le credenziali per tale account a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.



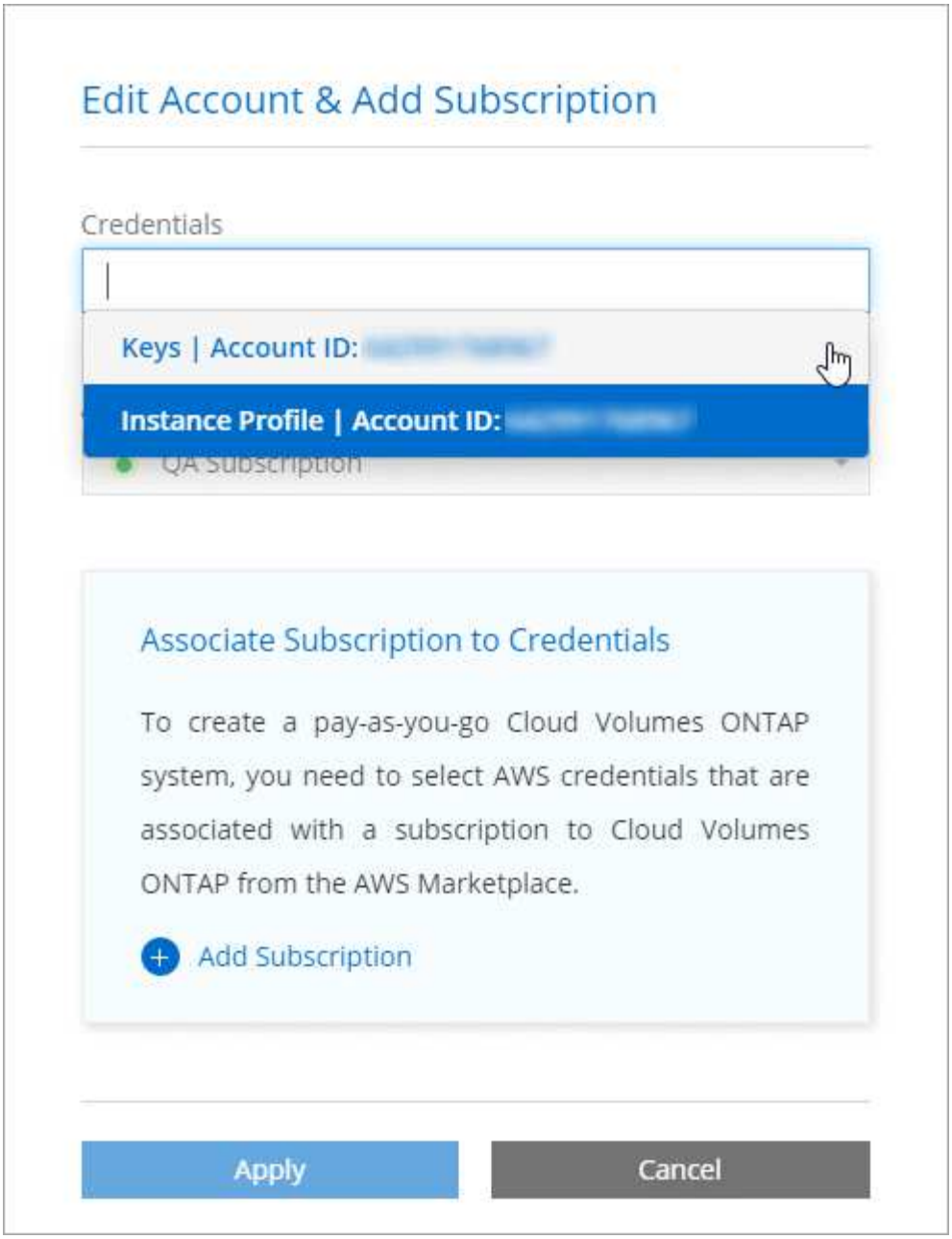
2. Fare clic su **Add Credentials** (Aggiungi credenziali) e selezionare **AWS**.
3. Fornire le chiavi AWS o l'ARN di un ruolo IAM attendibile.
4. Confermare che i requisiti della policy sono stati soddisfatti e fare clic su **continua**.
5. Scegli l'abbonamento pay-as-you-go che desideri associare alle credenziali o fai clic su **Aggiungi abbonamento** se non ne hai ancora uno.

   Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, le credenziali AWS devono essere associate a un abbonamento a Cloud Volumes ONTAP da AWS Marketplace.

6. Fare clic su **Aggiungi**.

Risultato

È ora possibile passare a un set di credenziali diverso dalla pagina Dettagli e credenziali quando si crea un nuovo ambiente di lavoro:



Associazione di un abbonamento AWS alle credenziali

Dopo aver aggiunto le credenziali AWS a Cloud Manager, è possibile associare un abbonamento AWS Marketplace a tali credenziali. L'abbonamento consente di creare un sistema Cloud Volumes ONTAP pay-as-you-go e di utilizzare altri servizi cloud NetApp.

Esistono due scenari in cui è possibile associare un abbonamento AWS Marketplace dopo aver aggiunto le credenziali a Cloud Manager:

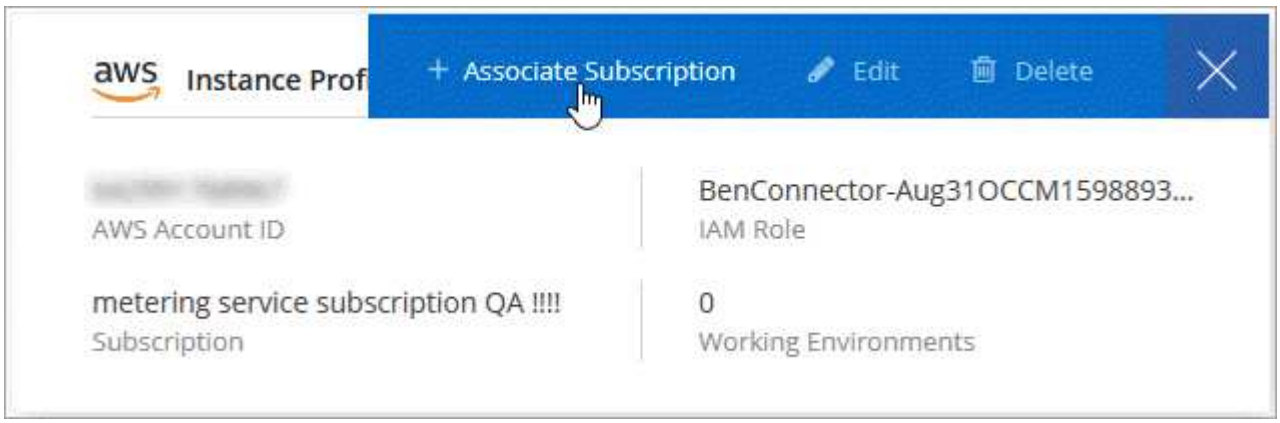
- Non hai associato un abbonamento quando inizialmente hai aggiunto le credenziali a Cloud Manager.
- Si desidera sostituire un abbonamento AWS Marketplace esistente con un nuovo abbonamento.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.
2. Passare il mouse su un set di credenziali e fare clic sul menu delle azioni.
3. Dal menu, fare clic su **Associa abbonamento**.



4. Selezionare un abbonamento dall'elenco a discesa oppure fare clic su **Aggiungi abbonamento** e seguire la procedura per creare un nuovo abbonamento.

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_aws.mp4 *(video)*