Inizia con la modalità limitata

Setup and administration

NetApp
April 26, 2024

Sommario

Inizia con la modalità limitata

Flusso di lavoro introduttivo (modalità limitata)

Inizia a utilizzare BlueXP in modalità limitata preparando il tuo ambiente, implementando il connettore e iscrivendoti a BlueXP.

La modalità limitata viene generalmente utilizzata dai governi locali e statali e da società regolamentate, comprese le implementazioni nelle aree pubbliche di AWS GovCloud e Azure. Prima di iniziare, dovresti avere una conoscenza di "BlueXP", "Connettori", e. "modalità di distribuzione".

1 **"Prepararsi per l'implementazione"**

1. Prepara un host Linux dedicato che soddisfi i requisiti di CPU, RAM, spazio su disco, motore Docker e altro ancora.
2. Configurare una rete che fornisca accesso alle reti di destinazione, accesso a Internet in uscita per installazioni manuali e accesso a Internet in uscita per l'accesso quotidiano.
3. Imposta le autorizzazioni nel tuo cloud provider in modo da poter associare tali autorizzazioni all'istanza di Connector dopo averla implementata.

2 **"Implementare il connettore"**

1. Installare il connettore dal mercato del provider di servizi cloud o installando manualmente il software sul proprio host Linux.
2. Configurare BlueXP aprendo un browser Web e immettendo l'indirizzo IP dell'host Linux.
3. Fornire a BlueXP le autorizzazioni precedentemente impostate.

3 **"Iscriviti a BlueXP"**

Iscriviti a BlueXP dal mercato del tuo cloud provider per pagare i servizi BlueXP a una tariffa oraria (PAYGO) o attraverso un contratto annuale.

Prepararsi per l'implementazione in modalità limitata

Preparare l'ambiente prima di implementare BlueXP in modalità limitata. Ad esempio, è necessario rivedere i requisiti degli host, preparare il networking, impostare le autorizzazioni e molto altro ancora.

Fase 1: Comprendere il funzionamento della modalità limitata

Prima di iniziare, è necessario conoscere il funzionamento di BlueXP in modalità limitata.

Ad esempio, è necessario comprendere la necessità di utilizzare l'interfaccia basata su browser disponibile localmente dal connettore BlueXP che si desidera installare. Non è possibile accedere a BlueXP dalla console basata sul Web fornita tramite il layer SaaS.

Inoltre, non tutti i servizi BlueXP sono disponibili.

"Scopri come funziona la modalità limitata".

Passaggio 2: Esaminare le opzioni di installazione

In modalità limitata, è possibile installare solo il connettore nel cloud. Sono disponibili le seguenti opzioni di installazione:

- Da AWS Marketplace
- Da Azure Marketplace
- Installazione manuale del connettore sul proprio host Linux in esecuzione in AWS, Azure o Google Cloud

Fase 3: Esaminare i requisiti dell'host

Il software del connettore deve essere eseguito su un host che soddisfi i requisiti specifici del sistema operativo, della RAM, dei requisiti delle porte e così via.

Quando si implementa il connettore da AWS o Azure Marketplace, l'immagine include il sistema operativo e i componenti software richiesti. È sufficiente scegliere un tipo di istanza che soddisfi i requisiti di CPU e RAM.

Host dedicato

Il connettore non è supportato su un host condiviso con altre applicazioni. L'host deve essere un host dedicato.

Sistemi operativi supportati

- Ubuntu 22,04 LTS
- CentOS 7.6, 7.7, 7.8 e 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 e 7.9

  L'host deve essere registrato con 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 del connettore.

  Il connettore è supportato dalle versioni in lingua inglese di questi sistemi operativi.

Hypervisor

È richiesto un hypervisor bare metal o in hosting certificato per l'esecuzione di Ubuntu, CentOS o Red Hat Enterprise Linux.

"Soluzione Red Hat: Quali hypervisor sono certificati per eseguire Red Hat Enterprise Linux?"

CPU

4 core o 4 vCPU

RAM

14 GB

Tipo di istanza AWS EC2

Un tipo di istanza che soddisfa i requisiti di CPU e RAM indicati in precedenza. Si consiglia di utilizzare t3.xlarge.

Dimensione delle macchine virtuali Azure

Un tipo di istanza che soddisfa i requisiti di CPU e RAM indicati in precedenza. Si consiglia DS3 v2.

Tipo di macchina Google Cloud

Un tipo di istanza che soddisfa i requisiti di CPU e RAM indicati in precedenza. Consigliamo n2-standard-4.

Il connettore è supportato in Google Cloud su un'istanza di macchina virtuale con un sistema operativo che supporta "Funzioni di VM schermate"

Spazio su disco in /opz

100 GiB di spazio deve essere disponibile

Spazio su disco in /var

20 GiB di spazio deve essere disponibile

Motore Docker

Prima di installare il connettore, è necessario disporre di Docker Engine sull'host.

- La versione minima supportata è 19,3.1.
- La versione massima supportata è 25,0.5.

"Visualizzare le istruzioni di installazione"

Fase 4: Preparare il collegamento in rete

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Oltre a disporre di una rete virtuale e di una subnet per il connettore, è necessario assicurarsi che siano soddisfatti i seguenti requisiti.

Connessioni alle reti di destinazione

Il connettore deve disporre di una connessione di rete alla posizione in cui si intende gestire lo storage. Ad esempio, il VPC o VNET in cui si intende implementare Cloud Volumes ONTAP o il data center in cui risiedono i cluster ONTAP on-premise.

Preparare la rete per l'accesso dell'utente alla console BlueXP

In modalità limitata, l'interfaccia utente di BlueXP è accessibile dal connettore. Quando si utilizza l'interfaccia utente di BlueXP, si contatta alcuni endpoint per completare le attività di gestione dei dati. Questi endpoint vengono contattati dal computer di un utente quando si completano azioni specifiche dalla console BlueXP.

Endpoint	Scopo
https://signin.b2c.netapp.com	Necessario per aggiornare le credenziali NetApp Support Site (NSS) o per aggiungere nuove credenziali NSS a BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite BlueXP.

Endpoint	Scopo
https://widget.intercom.io	Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp.

Endpoint contattati durante l'installazione manuale

Quando si installa manualmente il connettore sul proprio host Linux, il programma di installazione del connettore richiede l'accesso ai seguenti URL durante il processo di installazione:

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  Questo endpoint non è richiesto nelle regioni governative di Azure.

- https://occmclientinfragov.azurecr.us

  Questo endpoint è richiesto solo nelle regioni governative di Azure.

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.

Accesso a Internet in uscita per le operazioni quotidiane

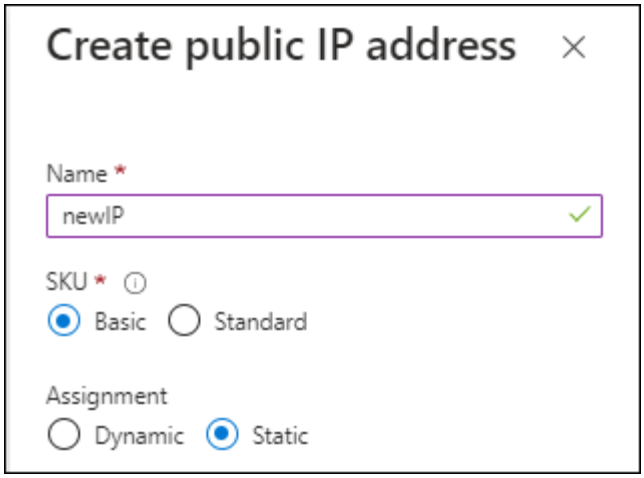
La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita. Il connettore richiede l'accesso a Internet in uscita per contattare i seguenti endpoint al fine di gestire risorse e processi all'interno dell'ambiente di cloud pubblico.

Endpoint	Scopo
Servizi AWS (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Gestione delle identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • S3 (Simple Storage Service)	Per gestire le risorse in AWS. L'endpoint esatto dipende dall'area AWS che stai utilizzando. "Per ulteriori informazioni, fare riferimento alla documentazione AWS"
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.

Endpoint	Scopo
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Per gestire le risorse nelle regioni governative 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 Azure China.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Per gestire le risorse in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Per ottenere informazioni sulle licenze e inviare messaggi AutoSupport al supporto NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Fornire funzionalità e servizi SaaS all'interno di BlueXP. Tenere presente che il connettore sta contattando "cloudmanager.cloud.netapp.com" , ma inizierà a contattare "api.bluexp.netapp.com" in una versione successiva.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io Questo endpoint non è richiesto nelle regioni governative di Azure. https://occmclientinfragov.azurecr.us Questo endpoint è richiesto solo nelle regioni governative di Azure.	Per aggiornare il connettore e i relativi componenti Docker.

Indirizzo IP pubblico in Azure

Se si desidera utilizzare un indirizzo IP pubblico con la macchina virtuale del connettore in Azure, l'indirizzo IP deve utilizzare una SKU di base per assicurarsi che BlueXP utilizzi questo indirizzo IP pubblico.



Se invece si utilizza un indirizzo IP SKU standard, BlueXP utilizza l'indirizzo *private* IP del connettore, invece dell'indirizzo IP pubblico. Se il computer utilizzato per accedere a BlueXP Console non dispone dell'accesso a tale indirizzo IP privato, le azioni da BlueXP Console non avranno esito positivo.

"Documentazione di Azure: SKU IP pubblico"

Server proxy

Se l'organizzazione richiede la distribuzione di un server proxy per tutto il traffico Internet in uscita, ottenere le seguenti informazioni sul proxy HTTP o HTTPS. Queste informazioni devono essere fornite durante l'installazione.

- Indirizzo IP
- Credenziali
- Certificato HTTPS

BlueXP non supporta i server proxy trasparenti.

Porte

Non c'è traffico in entrata verso il connettore, a meno che non venga avviato o se il connettore viene 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 verrà utilizzata in rare circostanze.
- SSH (22) è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.
- Le connessioni in entrata sulla porta 3128 sono necessarie se si implementano 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 a Internet in uscita per inviare messaggi AutoSupport, BlueXP configura automaticamente tali sistemi in modo che utilizzino un server proxy incluso nel connettore. L'unico requisito è garantire che il gruppo di sicurezza del connettore consenta le connessioni in entrata sulla porta 3128. Dopo aver implementato il connettore, aprire questa porta.

Enable NTP (attiva NTP)

Se stai pensando di utilizzare la classificazione BlueXP per analizzare le origini dati aziendali, dovresti attivare un servizio NTP (Network Time Protocol) sia sul sistema del connettore BlueXP che sul sistema di classificazione BlueXP in modo che l'ora venga sincronizzata tra i sistemi. "Scopri di più sulla

classificazione BlueXP"

Se si prevede di creare il connettore dal mercato del provider di servizi cloud, sarà necessario implementare questo requisito di rete dopo aver creato il connettore.

Passaggio: 5 preparare le autorizzazioni del cloud

BlueXP richiede le autorizzazioni del provider cloud per implementare Cloud Volumes ONTAP in una rete virtuale e utilizzare i servizi dati BlueXP. È necessario impostare le autorizzazioni nel provider cloud e associarle al connettore.

Per visualizzare i passaggi richiesti, selezionare l'opzione di autenticazione che si desidera utilizzare per il provider di servizi cloud.

Ruolo AWS IAM

Utilizzare un ruolo IAM per fornire al connettore le autorizzazioni.

Se si crea il connettore da AWS Marketplace, viene richiesto di selezionare il ruolo IAM quando si avvia l'istanza EC2.

Se si installa manualmente il connettore sul proprio host Linux, è necessario associare il ruolo all'istanza EC2.

Fasi

1. Accedere alla console AWS e accedere al servizio IAM.
2. Creare una policy:
   a. Selezionare **Criteri > Crea policy**.
   b. Selezionare **JSON** e copiare e incollare il contenuto di "Policy IAM per il connettore".
   c. Completare i passaggi rimanenti per creare il criterio.
3. Creare un ruolo IAM:
   a. Selezionare **ruoli > Crea ruolo**.
   b. Selezionare **servizio AWS > EC2**.
   c. Aggiungere le autorizzazioni allegando il criterio appena creato.
   d. Completare i passaggi rimanenti per creare il ruolo.

Risultato

Ora hai un ruolo IAM per l'istanza di Connector EC2.

Chiave di accesso AWS

Impostare le autorizzazioni e una chiave di accesso per un utente IAM. Dopo aver installato il connettore e configurato BlueXP, è necessario fornire a BlueXP la chiave di accesso AWS.

Fasi

1. Accedere alla console AWS e accedere al servizio IAM.
2. Creare una policy:

   a. Selezionare **Criteri > Crea policy**.
   b. Selezionare **JSON** e copiare e incollare il contenuto di "Policy IAM per il connettore".
   c. Completare i passaggi rimanenti per creare il criterio.

      A seconda dei servizi BlueXP che si intende utilizzare, potrebbe essere necessario creare una seconda policy.

   Per le regioni standard, le autorizzazioni sono distribuite in due policy. Sono necessarie due policy a causa di un limite massimo di dimensioni dei caratteri per le policy gestite in AWS. "Scopri di più sulle policy IAM per il connettore".

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

4. Assicurarsi che l'utente disponga di una chiave di accesso che è possibile aggiungere a BlueXP dopo aver installato il connettore.

Risultato

L'account dispone ora delle autorizzazioni necessarie.

Ruolo di Azure

Creare un ruolo personalizzato Azure con le autorizzazioni richieste. Assegnerai questo ruolo alla macchina virtuale del connettore.

Si noti che è possibile creare un ruolo personalizzato di Azure utilizzando il portale Azure, Azure PowerShell, Azure CLI o REST API. I passaggi seguenti mostrano come creare il ruolo utilizzando la CLI di Azure. Se si preferisce utilizzare un metodo diverso, fare riferimento a. "Documentazione di Azure"

Fasi

1. Se si prevede di installare manualmente il software sul proprio host, abilitare un'identità gestita assegnata dal sistema sulla macchina virtuale in modo da poter fornire le autorizzazioni Azure richieste attraverso un ruolo personalizzato.

   "Documentazione di Microsoft Azure: Configurare le identità gestite per le risorse Azure su una macchina virtuale utilizzando il portale Azure"

2. Copiare il contenuto di "Autorizzazioni di ruolo personalizzate per il connettore" E salvarli in un file JSON.
3. Modificare il file JSON aggiungendo gli ID di abbonamento Azure all'ambito assegnabile.

   Aggiungere l'ID per ogni abbonamento Azure che si desidera utilizzare con BlueXP.

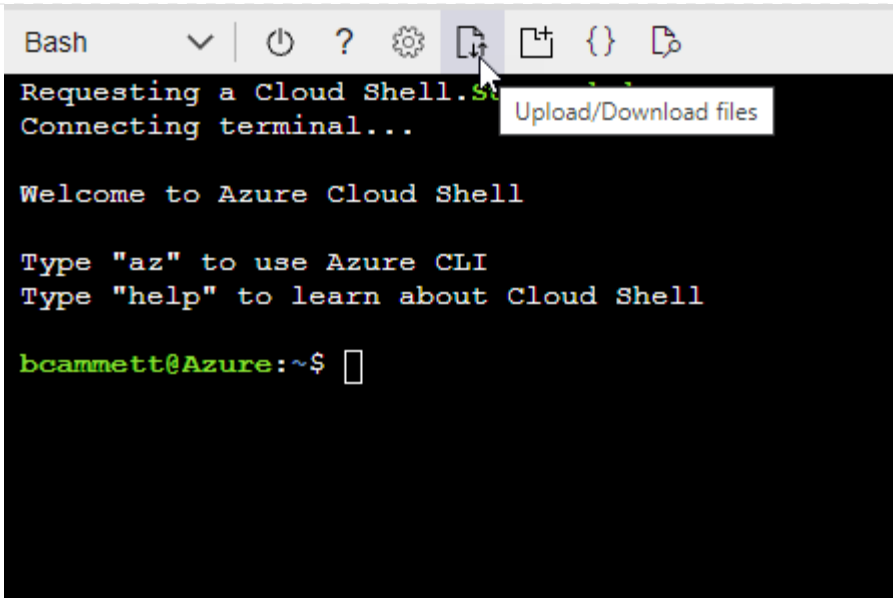
   Esempio

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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

   I passaggi seguenti descrivono come creare il ruolo utilizzando Bash in Azure Cloud Shell.

   a. Inizio "Azure Cloud Shell" E scegliere l'ambiente Bash.
   b. Caricare il file JSON.



c. Utilizzare la CLI di Azure per creare il ruolo personalizzato:

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

Risultato

A questo punto, dovrebbe essere disponibile un ruolo personalizzato denominato BlueXP Operator che è possibile assegnare alla macchina virtuale Connector.

Entità del servizio Azure

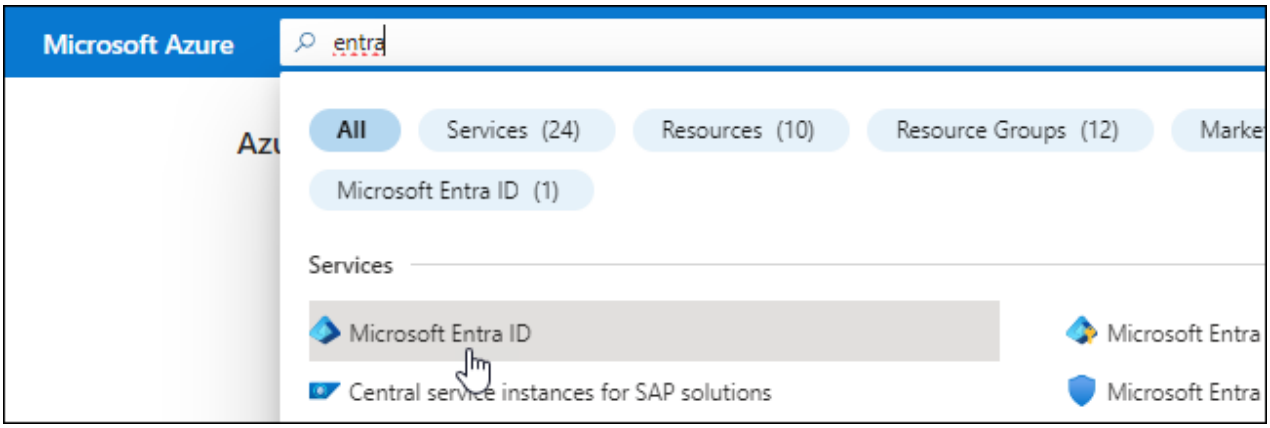
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP. È necessario fornire queste credenziali a BlueXP dopo aver installato il connettore e configurato BlueXP.

Creare un'applicazione Microsoft Entra per il controllo degli accessi basato sui ruoli

1. Assicurarsi di disporre delle autorizzazioni in Azure per creare un'applicazione Active Directory e assegnarla a un ruolo.

   Per ulteriori informazioni, fare riferimento a. "Documentazione di Microsoft Azure: Autorizzazioni richieste"

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



3. Nel menu, selezionare **App Registrations**.
4. Selezionare **Nuova registrazione**.
5. Specificare i dettagli dell'applicazione:
   - **Nome**: Immettere un nome per l'applicazione.
   - **Tipo di account**: Selezionare un tipo di account (qualsiasi sarà compatibile con BlueXP).
   - **Reindirizza URI**: Questo campo può essere lasciato vuoto.
6. Selezionare **Registra**.

   Hai creato l'applicazione ad e il service principal.

Assegnare l'applicazione a un ruolo

1. Creare un ruolo personalizzato:

   Si noti che è possibile creare un ruolo personalizzato di Azure utilizzando il portale Azure, Azure PowerShell, Azure CLI o REST API. I passaggi seguenti mostrano come creare il ruolo utilizzando la CLI di Azure. Se si preferisce utilizzare un metodo diverso, fare riferimento a. "Documentazione di Azure"

   a. Copiare il contenuto di "Autorizzazioni di ruolo personalizzate per il connettore" E salvarli in un file JSON.

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

      È necessario aggiungere l'ID per ogni abbonamento Azure da cui gli utenti creeranno i sistemi Cloud Volumes ONTAP.

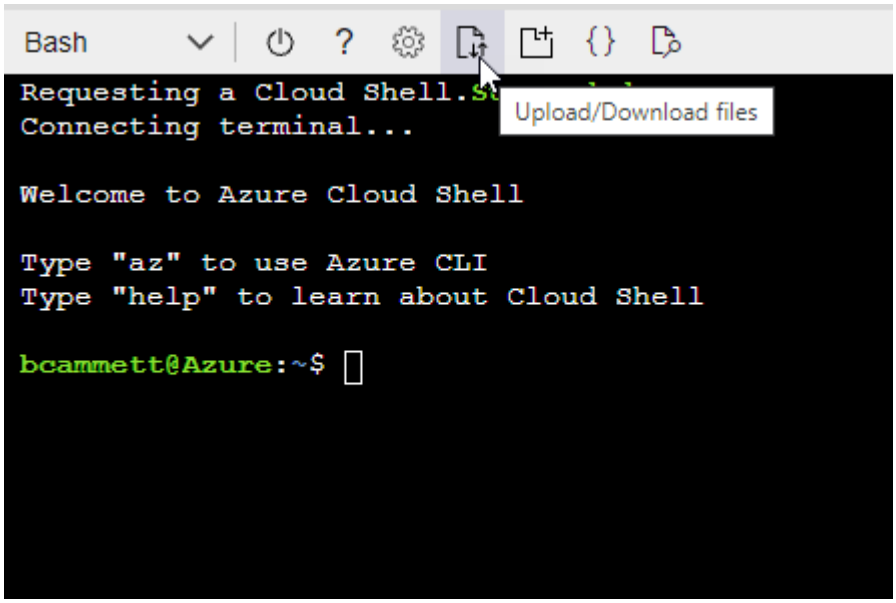
      Esempio

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

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

      I passaggi seguenti descrivono come creare il ruolo utilizzando Bash in Azure Cloud Shell.

- Inizio "Azure Cloud Shell" E scegliere l'ambiente Bash.
- Caricare il file JSON.



- Utilizzare la CLI di Azure per creare il ruolo personalizzato:

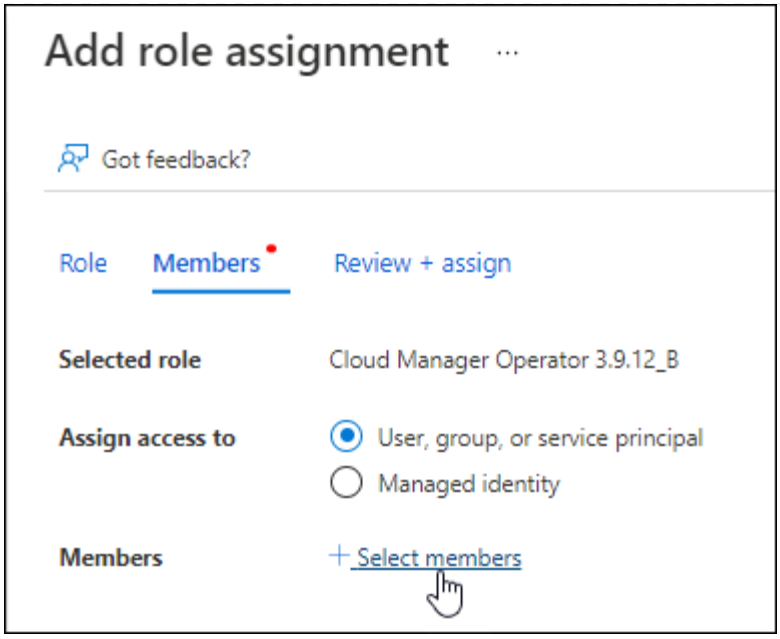
```
az role definition create --role-definition
Connector_Policy.json
```

A questo punto, dovrebbe essere disponibile un ruolo personalizzato denominato BlueXP Operator che è possibile assegnare alla macchina virtuale Connector.

2. Assegnare l'applicazione al ruolo:

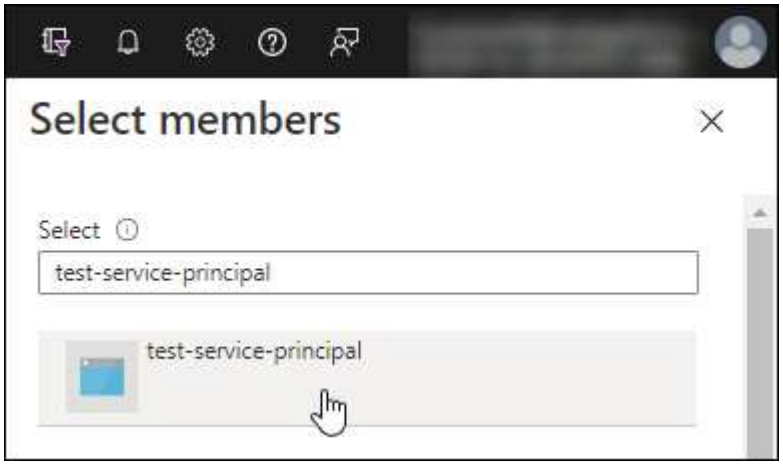
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda **membri**, completare la seguente procedura:

      - Mantieni selezionata l'opzione **User, group o service principal**.
      - Seleziona **Seleziona membri**.



- Cercare il nome dell'applicazione.

  Ecco un esempio:



- Selezionare l'applicazione e selezionare **Seleziona**.
- Selezionare **Avanti**.

f. Selezionare **Rivedi + assegna**.

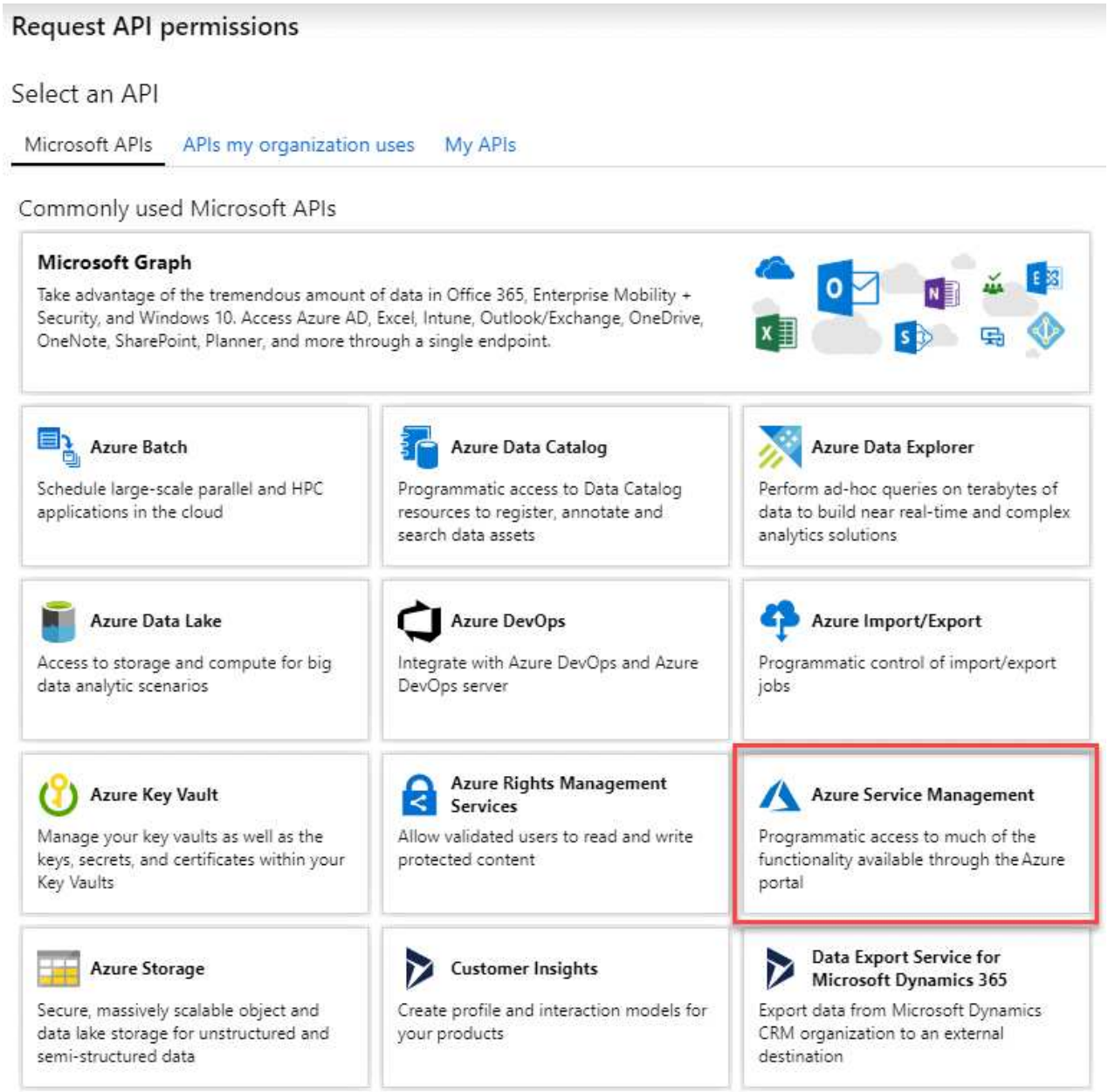
   L'entità del servizio dispone ora delle autorizzazioni Azure necessarie per implementare il connettore.

Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

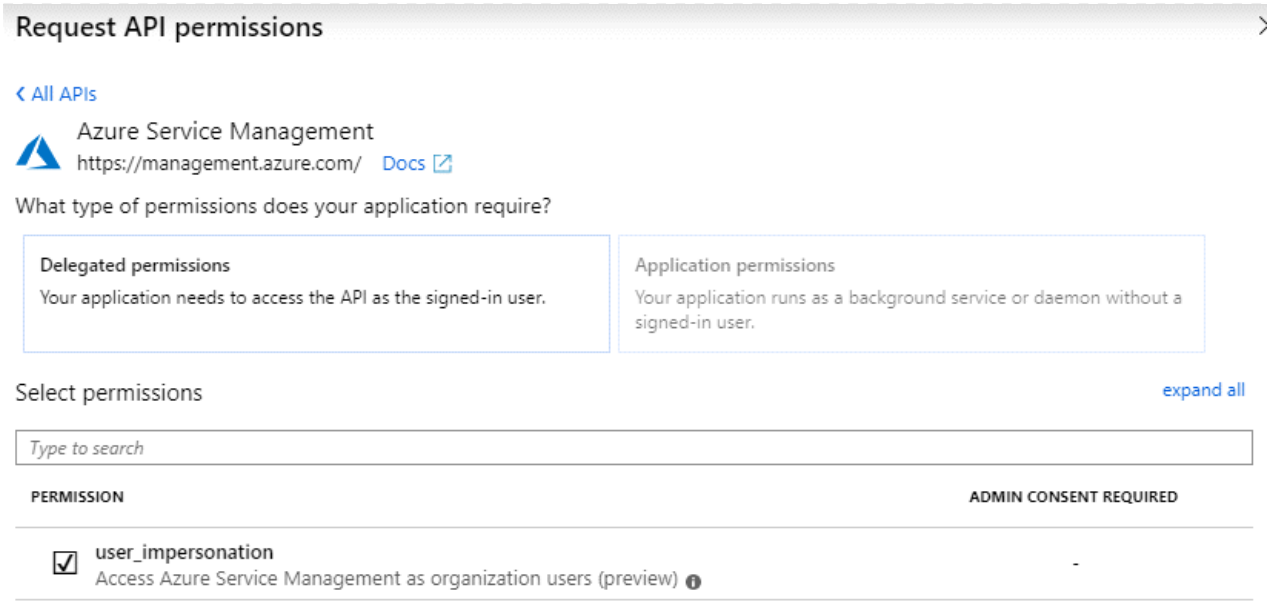
Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

1. Nel servizio **Microsoft Entra ID**, selezionare **registrazioni app** e selezionare l'applicazione.
2. Selezionare **API permissions > Add a permission** (autorizzazioni API > Aggiungi autorizzazione).

3. In **Microsoft API**, selezionare **Azure Service Management**.

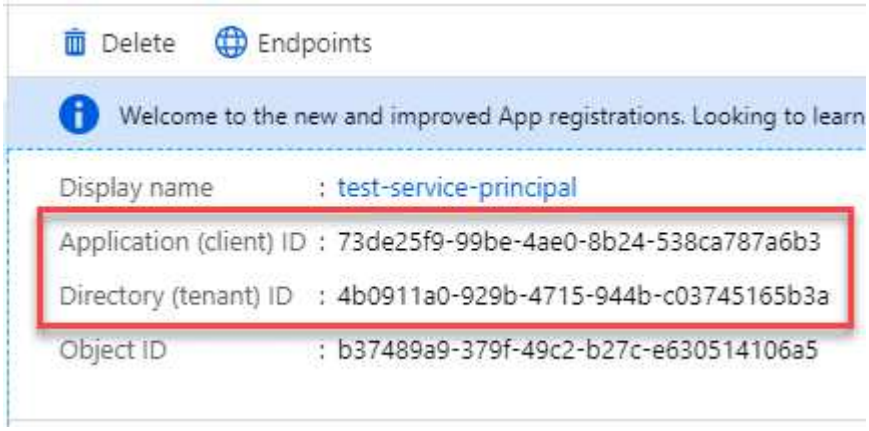


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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

1. Nel servizio **Microsoft Entra ID**, selezionare **registrazioni app** e selezionare l'applicazione.
2. Copiare **Application (client) ID** e **Directory (tenant) ID**.



Quando si aggiunge l'account Azure a BlueXP, è necessario fornire l'ID dell'applicazione (client) e l'ID della directory (tenant) per l'applicazione. BlueXP utilizza gli ID per effettuare l'accesso a livello di programmazione.

Creare un client segreto

1. Aprire il servizio **Microsoft Entra ID**.
2. Selezionare **App Registrations** e selezionare l'applicazione.
3. Selezionare **certificati e segreti > nuovo segreto client**.
4. Fornire una descrizione del segreto e una durata.
5. Selezionare **Aggiungi**.
6. Copiare il valore del client secret.

A questo punto, si dispone di una chiave segreta del client che BlueXP può utilizzare per eseguire l'autenticazione con Microsoft Entra ID.

Risultato

L'entità del servizio è ora impostata e l'ID dell'applicazione (client), l'ID della directory (tenant) e il valore del client secret dovrebbero essere stati copiati. Quando si aggiunge un account Azure, è necessario inserire queste informazioni in BlueXP.

Account del servizio Google Cloud

Creare un ruolo e applicarlo a un account di servizio da utilizzare per l'istanza della macchina virtuale del connettore.

Fasi

1. Creare un ruolo personalizzato in Google Cloud:

   a. Creare un file YAML che includa le autorizzazioni definite in "Policy di Connector per Google Cloud".

   b. Da Google Cloud, attiva la shell cloud.

   c. Caricare il file YAML che include le autorizzazioni richieste per il connettore.

   d. Creare un ruolo personalizzato utilizzando `gcloud iam roles create` comando.

      Nell'esempio seguente viene creato un ruolo denominato "Connector" a livello di progetto:

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Documenti Google Cloud: Creazione e gestione di ruoli personalizzati"

2. Creare un account di servizio in Google Cloud:

   a. Dal servizio IAM & Admin, selezionare **account di servizio > Crea account di servizio**.

   b. Inserire i dettagli dell'account del servizio e selezionare **Crea e continua**.

   c. Selezionare il ruolo appena creato.

   d. Completare i passaggi rimanenti per creare il ruolo.

      "Documenti Google Cloud: Creazione di un account di servizio"

Risultato

A questo punto si dispone di un account di servizio che è possibile assegnare all'istanza della macchina virtuale di Connector.

Passaggio 6: Abilitare le API di Google Cloud

Per implementare Cloud Volumes ONTAP in Google Cloud 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)
    - API di Cloud Key Management Service (KMS)

      (Necessario solo se si intende utilizzare il backup e ripristino BlueXP con le chiavi di crittografia gestite dal cliente (CMEK))

Implementare il connettore in modalità limitata

Implementare il connettore in modalità limitata in modo da poter utilizzare BlueXP con connettività in uscita limitata al livello BlueXP SaaS. Per iniziare, installare il connettore, configurare BlueXP accedendo all'interfaccia utente in esecuzione sul connettore, quindi fornire le autorizzazioni cloud precedentemente impostate.

Fase 1: Installare il connettore

Installare il connettore dal mercato del provider di servizi cloud o installando manualmente il software sul proprio host Linux.

Mercato commerciale AWS

Prima di iniziare

Dovresti disporre di quanto segue:

- VPC e subnet che soddisfano i requisiti di rete.

  "Scopri i requisiti di rete"

- Un ruolo IAM con un criterio allegato che include le autorizzazioni richieste per il connettore.

  "Scopri come impostare le autorizzazioni AWS"

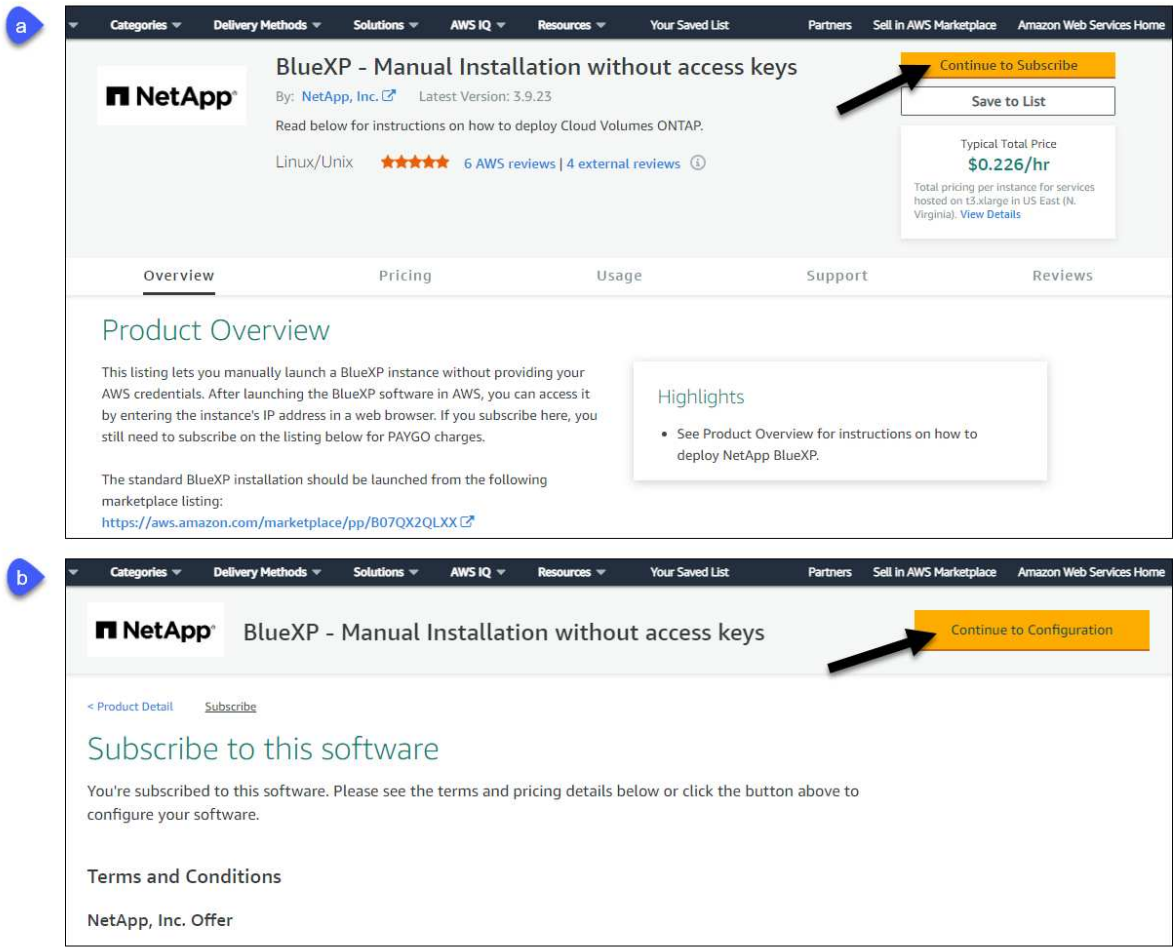
- Autorizzazioni per iscriversi e annullare l'iscrizione da AWS Marketplace per l'utente IAM.
- Comprensione dei requisiti di CPU e RAM per l'istanza.

  "Esaminare i requisiti dell'istanza".

- Coppia di chiavi per l'istanza EC2.

Fasi

1. Accedere alla "Pagina BlueXP su AWS Marketplace"
2. Nella pagina Marketplace, selezionare **Continue to Subscribe**, quindi selezionare **Continue to Configuration**.



3. Modificare una delle opzioni predefinite e selezionare **Continue to Launch** (continua fino all'avvio).
4. In **Choose Action** (Scegli azione), selezionare **Launch through EC2** (Avvia tramite EC2*), quindi selezionare **Launch** (Avvia).

   Questi passaggi descrivono come avviare l'istanza dalla console EC2 perché la console consente di associare un ruolo IAM all'istanza del connettore. Ciò non è possibile utilizzando l'azione **Launch from Website** (Avvia dal sito Web).

5. Seguire le istruzioni per configurare e implementare l'istanza:

   - **Nome e tag**: Immettere un nome e tag per l'istanza.
   - **Immagine dell'applicazione e del sistema operativo**: Saltare questa sezione. Il connettore AMI è già selezionato.
   - **Tipo di istanza**: A seconda della disponibilità della regione, scegliere un tipo di istanza che soddisfi i requisiti di RAM e CPU (si consiglia t3.xlarge).
   - **Coppia di chiavi (login)**: Selezionare la coppia di chiavi che si desidera utilizzare per connettersi in modo sicuro all'istanza.
   - **Impostazioni di rete**: Modificare le impostazioni di rete in base alle esigenze:
     - Scegliere il VPC e la subnet desiderati.
     - Specificare se l'istanza deve avere un indirizzo IP pubblico.
     - Specificare le impostazioni del firewall che abilitano i metodi di connessione richiesti per l'istanza del connettore: SSH, HTTP e HTTPS.

       Sono necessarie altre regole per configurazioni specifiche.

   "Visualizzare le regole del gruppo di sicurezza per AWS".

   - **Configura archiviazione**: Mantenere 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**, quindi scegliere una chiave KMS.

   - **Dettagli avanzati**: In **Profilo istanza IAM**, scegliere il ruolo IAM che include le autorizzazioni richieste per il connettore.
   - **Riepilogo**: Esaminare il riepilogo e selezionare **Avvia istanza**.

Risultato

AWS avvia il software con le impostazioni specificate. L'istanza di Connector e il software dovrebbero essere in esecuzione in circa cinque minuti.

Quali sono le prossime novità?

Configurare BlueXP.

Mercato AWS Gov

Prima di iniziare

Dovresti disporre di quanto segue:

- VPC e subnet che soddisfano i requisiti di rete.

  "Scopri i requisiti di rete"

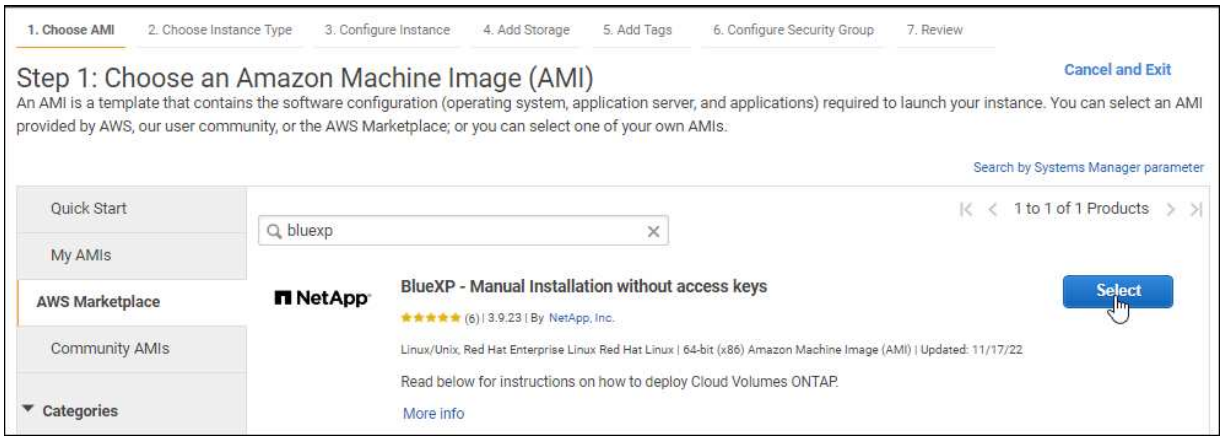
- Un ruolo IAM con un criterio allegato che include le autorizzazioni richieste per il connettore.

  "Scopri come impostare le autorizzazioni AWS"

- Autorizzazioni per iscriversi e annullare l'iscrizione da AWS Marketplace per l'utente IAM.
- Coppia di chiavi per l'istanza EC2.

Fasi

1. Vai all'offerta BlueXP in AWS Marketplace.
   a. Aprire il servizio EC2 e selezionare **Avvia istanza**.
   b. Selezionare **AWS Marketplace**.
   c. Cercare BlueXP e selezionare l'offerta.

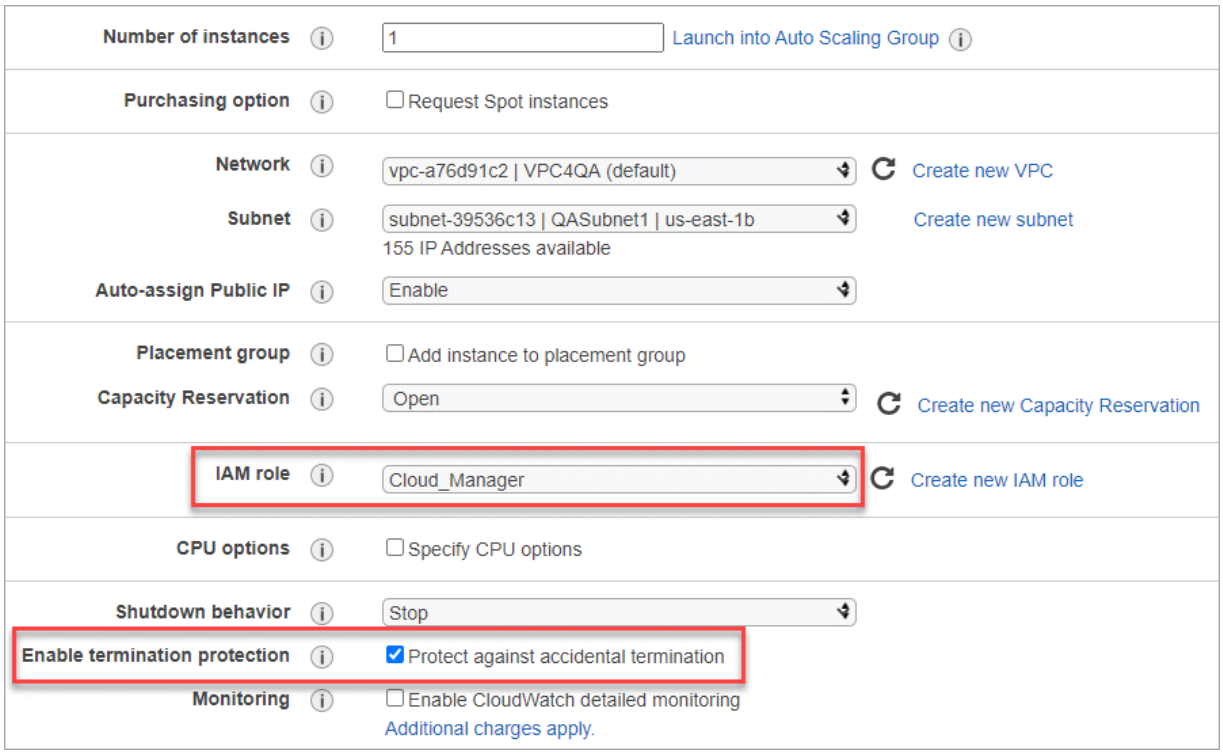


   d. Selezionare **continua**.

2. Seguire le istruzioni per configurare e implementare l'istanza:
   - **Scegliere un tipo di istanza**: A seconda della disponibilità della regione, scegliere uno dei tipi di istanza supportati (si consiglia t3.xlarge).

     "Esaminare i requisiti dell'istanza".

   - **Configure Instance Details** (Configura dettagli istanza): Selezionare un VPC e una subnet, scegliere il ruolo IAM creato nel passaggio 1, abilitare la protezione di terminazione (scelta consigliata) e scegliere qualsiasi altra opzione di configurazione che soddisfi i requisiti.



- **Add Storage** (Aggiungi storage): Mantenere le opzioni di storage predefinite.
- **Add Tags** (Aggiungi tag): Se si desidera, inserire i tag per l'istanza.
- **Configure Security Group** (Configura gruppo di protezione): Specificare i metodi di connessione richiesti per l'istanza del connettore: SSH, HTTP e HTTPS.
- **Revisione**: Rivedere le selezioni e selezionare **Avvio**.

Risultato

AWS avvia il software con le impostazioni specificate. L'istanza di Connector e il software dovrebbero essere in esecuzione in circa cinque minuti.

Quali sono le prossime novità?

Configurare BlueXP.

Azure Marketplace

Prima di iniziare

Dovresti disporre di quanto segue:

- VNET e subnet che soddisfano i requisiti di rete.

  "Scopri i requisiti di rete"

- Un ruolo personalizzato di Azure che include le autorizzazioni richieste per il connettore.

  "Scopri come impostare le autorizzazioni Azure"

Fasi

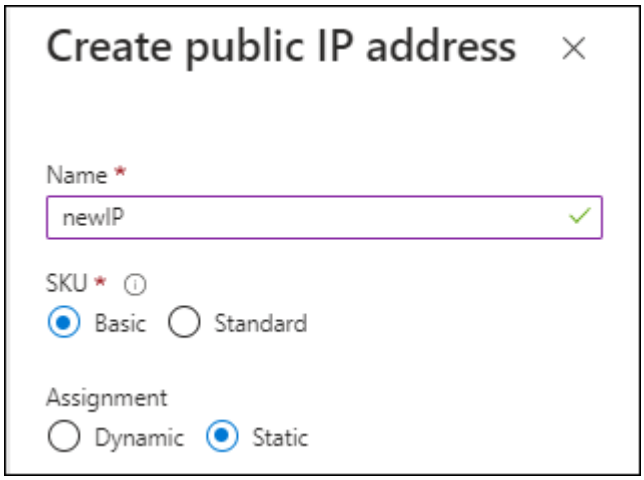
1. Accedere alla pagina NetApp Connector VM in Azure Marketplace.
   - "Pagina di Azure Marketplace per le regioni commerciali"

- "Pagina di Azure Marketplace per le regioni governative di Azure"

2. Selezionare **Get it now** (Ottieni ora), quindi selezionare **Continue** (continua).
3. Dal portale Azure, selezionare **Create** e seguire la procedura per configurare la macchina virtuale.

   Durante la configurazione della macchina virtuale, tenere presente quanto segue:

   - **Dimensione della macchina virtuale**: Scegli una dimensione della macchina virtuale che soddisfi i requisiti di CPU e RAM. Si consiglia DS3 v2.
   - **Dischi**: Il connettore può funzionare in modo ottimale con dischi HDD o SSD.
   - **Public IP**: Se si desidera utilizzare un indirizzo IP pubblico con la macchina virtuale del connettore, l'indirizzo IP deve utilizzare una SKU di base per garantire che BlueXP utilizzi questo indirizzo IP pubblico.



     Se invece si utilizza un indirizzo IP SKU standard, BlueXP utilizza l'indirizzo *private* IP del connettore, invece dell'indirizzo IP pubblico. Se il computer utilizzato per accedere a BlueXP Console non dispone dell'accesso a tale indirizzo IP privato, le azioni da BlueXP Console non avranno esito positivo.

   "Documentazione di Azure: SKU IP pubblico"

   - **Network Security group**: Il connettore richiede connessioni in entrata utilizzando SSH, HTTP e HTTPS.

     "Visualizza le regole del gruppo di sicurezza per Azure".

   - **Identity**: In **Management**, selezionare **Enable system assigned Managed Identity**.

     Questa impostazione è importante perché un'identità gestita consente alla macchina virtuale Connector di identificarsi in Microsoft Entra ID senza fornire credenziali. "Scopri di più sulle identità gestite per le risorse Azure".

4. Nella pagina **Review + create**, esaminare le selezioni e selezionare **Create** per avviare l'implementazione.

Risultato

Azure implementa la macchina virtuale con le impostazioni specificate. La macchina virtuale e il software del connettore dovrebbero essere in esecuzione in circa cinque minuti.

Quali sono le prossime novità?

Configurare BlueXP.

Installazione manuale

Prima di iniziare

Dovresti disporre di quanto segue:

- Privilegi root per installare il connettore.
- Dettagli su un server proxy, se è richiesto un proxy per l'accesso a Internet dal connettore.

  È possibile configurare un server proxy dopo l'installazione, ma per farlo è necessario riavviare il connettore.

  BlueXP non supporta i server proxy trasparenti.

- Un certificato firmato dalla CA, se il server proxy utilizza HTTPS o se il proxy è un proxy di intercettazione.

A proposito di questa attività

Il programma di installazione disponibile sul NetApp Support Site potrebbe essere una versione precedente. Dopo l'installazione, il connettore si aggiorna automaticamente se è disponibile una nuova versione.

Fasi

1. Verificare che docker sia attivato e in esecuzione.

   ```
   sudo systemctl enable docker && sudo systemctl start docker
   ```

2. 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 avrà esito negativo.

3. Scaricare il software del connettore da "Sito di supporto NetApp", Quindi copiarlo sull'host Linux.

   È necessario scaricare il programma di installazione del connettore "online" da utilizzare nella rete o nel cloud. Un programma di installazione "offline" separato è disponibile per il connettore, ma è supportato solo con le implementazioni in modalità privata.

4. Assegnare le autorizzazioni per eseguire lo script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

   Dove <version> è la versione del connettore scaricato.

5. Eseguire lo script di installazione.

```
./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

I parametri --proxy e --cakert sono facoltativi. Se si dispone di un server proxy, è necessario immettere i parametri come mostrato. Il programma di installazione non richiede di fornire informazioni su un proxy.

Ecco un esempio del comando che utilizza entrambi i parametri facoltativi:

```
./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxy configura il connettore per l'utilizzo di un server proxy HTTP o HTTPS 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

  Tenere presente 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 \ come illustrato sopra.
  - BlueXP non supporta password che includono il carattere @.

--cakert specifica un certificato firmato da CA da utilizzare per l'accesso HTTPS tra il connettore e il server proxy. Questo parametro è necessario solo se si specifica un server proxy HTTPS o se il proxy è un proxy di intercettazione.

Risultato

Il connettore è ora installato. Al termine dell'installazione, il servizio di connessione (occm) viene riavviato due volte se si specifica un server proxy.

Quali sono le prossime novità?

Configurare BlueXP.

Fase 2: Configurare BlueXP

Quando si accede alla console BlueXP per la prima volta, viene richiesto di scegliere un account a cui associare il connettore ed è necessario attivare la modalità limitata.

Se si dispone già di un account e si desidera crearne un altro, è necessario utilizzare l'API tenancy. "Scopri come creare un account BlueXP aggiuntivo".

Fasi

1. Aprire un browser Web da un host connesso all'istanza del connettore e immettere il seguente URL:

   https://ipaddress

2. Iscriviti o accedi a BlueXP.
3. Una volta effettuato l'accesso, configurare BlueXP:

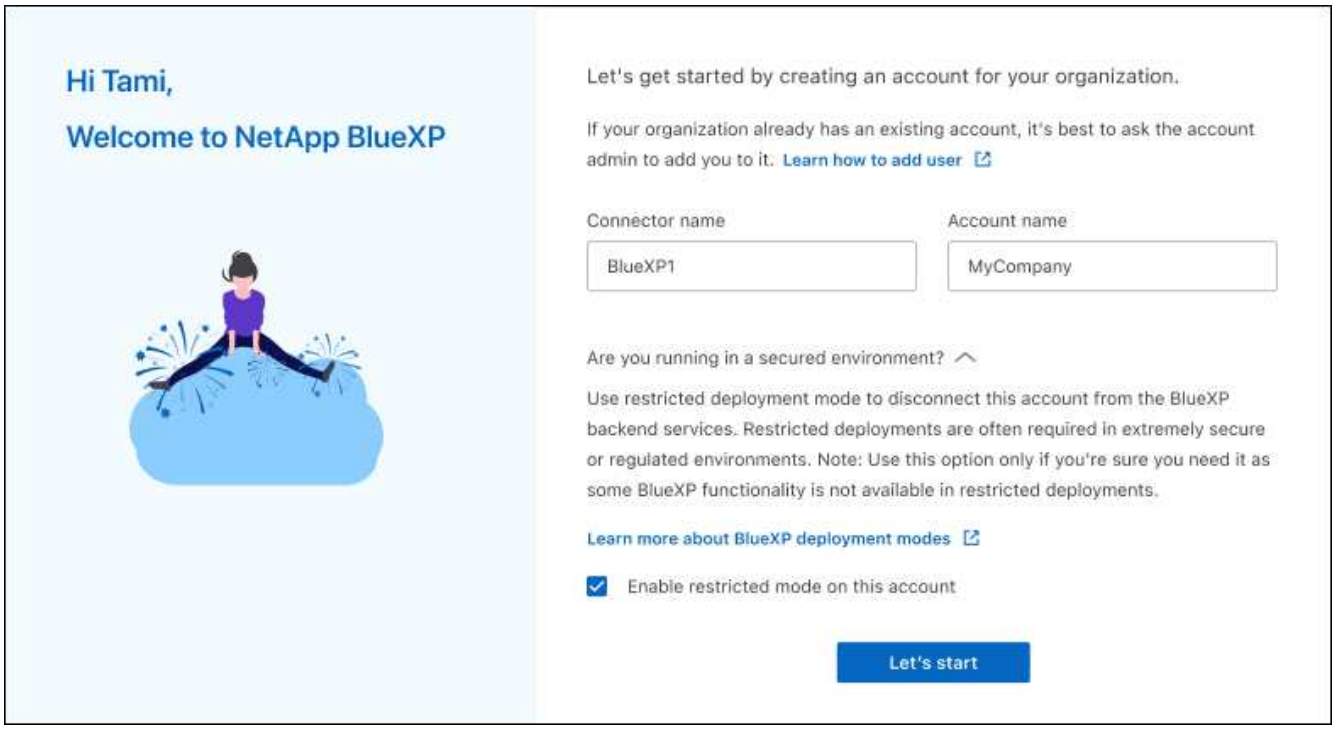
   a. Inserire un nome per il connettore.
   b. Immettere un nome per un nuovo account BlueXP o selezionare un account esistente.

      È possibile selezionare un account esistente se l'accesso è già associato a un account BlueXP.

   c. Selezionare **l'esecuzione in un ambiente protetto?**
   d. Selezionare **Enable restricted mode on this account** (attiva modalità limitata su questo account).

      Tenere presente che non è possibile modificare questa impostazione dopo che BlueXP ha creato l'account. Non puoi attivare la modalità limitata in un secondo momento e non puoi disattivarla in un secondo momento.

      Se il connettore è stato implementato in un'area governativa, la casella di controllo è già attivata e non può essere modificata. Questo perché la modalità limitata è l'unica modalità supportata nelle regioni governative.



   a. Selezionare **Let's start**.

Risultato

Il connettore è ora installato e configurato con l'account BlueXP. Tutti gli utenti devono accedere a BlueXP utilizzando l'indirizzo IP dell'istanza del connettore.

Quali sono le prossime novità?

Fornire a BlueXP le autorizzazioni precedentemente impostate.

Fase 3: Fornire le autorizzazioni ad BlueXP

Se il connettore è stato distribuito da Azure Marketplace o se il software del connettore è stato installato manualmente, è necessario fornire le autorizzazioni precedentemente impostate per poter utilizzare i servizi BlueXP.

Questi passaggi non si applicano se il connettore è stato implementato da AWS Marketplace perché è stato scelto il ruolo IAM richiesto durante l'implementazione.

"Scopri come preparare le autorizzazioni cloud".

Ruolo AWS IAM

Collegare il ruolo IAM precedentemente creato all'istanza EC2 in cui è stato installato il connettore.

Questa procedura si applica solo se il connettore è stato installato manualmente in AWS. Per le implementazioni di AWS Marketplace, l'istanza di Connector è già stata associata a un ruolo IAM che include le autorizzazioni richieste.

Fasi

1. Accedere alla console Amazon EC2.
2. Selezionare **istanze**.
3. Selezionare l'istanza del connettore.
4. Selezionare **azioni > sicurezza > Modifica ruolo IAM**.
5. Selezionare il ruolo IAM e selezionare **Aggiorna ruolo IAM**.

Risultato

BlueXP dispone ora delle autorizzazioni necessarie per eseguire azioni in AWS per conto dell'utente.

Chiave di accesso AWS

Fornire a BlueXP la chiave di accesso AWS per un utente IAM che dispone delle autorizzazioni necessarie.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

2. Selezionare **Aggiungi credenziali** e seguire la procedura guidata.
   a. **Credentials Location**: Selezionare **Amazon Web Services > Connector**.
   b. **Definisci credenziali**: Inserire una chiave di accesso AWS e una chiave segreta.
   c. **Marketplace Subscription**: Consente di associare un abbonamento Marketplace a queste credenziali sottoscrivendo ora o selezionando un abbonamento esistente.
   d. **Revisione**: Confermare i dettagli relativi alle nuove credenziali e selezionare **Aggiungi**.

Risultato

BlueXP dispone ora delle autorizzazioni necessarie per eseguire azioni in AWS per conto dell'utente.

Ruolo di Azure

Accedere al portale Azure e assegnare il ruolo personalizzato Azure alla macchina virtuale Connector per una o più sottoscrizioni.

Fasi

1. Dal portale Azure, aprire il servizio **Subscriptions** e selezionare l'abbonamento.

   È importante assegnare il ruolo dal servizio **Sottoscrizioni** perché questo specifica l'ambito

dell'assegnazione del ruolo al livello di sottoscrizione. L'oggetto *scope* definisce l'insieme di risorse a cui si applica l'accesso. Se specifichi un ambito a un livello diverso (ad esempio, a livello di macchina virtuale), la tua capacità di completare azioni da BlueXP sarà interessata.

"Documentazione Microsoft Azure: Comprensione dell'ambito per i role-based access control Azure"

2. Selezionare **Access Control (IAM)** > **Add** > **Add role assignment**.
3. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.

> BlueXP Operator è il nome predefinito fornito nel criterio BlueXP. Se si sceglie un nome diverso per il ruolo, selezionare il nome desiderato.

4. Nella scheda **membri**, completare la seguente procedura:
   a. Assegnare l'accesso a un'identità * gestita.
   b. Selezionare **Seleziona membri**, selezionare l'abbonamento in cui è stata creata la macchina virtuale del connettore, in **identità gestita**, scegliere **macchina virtuale**, quindi selezionare la macchina virtuale del connettore.
   c. Selezionare **Seleziona**.
   d. Selezionare **Avanti**.
   e. Selezionare **Rivedi + assegna**.
   f. Se si desidera gestire le risorse in abbonamenti Azure aggiuntivi, passare a tale abbonamento e ripetere la procedura.

Risultato

BlueXP dispone ora delle autorizzazioni necessarie per eseguire azioni in Azure per conto dell'utente.

Entità del servizio Azure

Fornire a BlueXP le credenziali per l'entità del servizio Azure precedentemente configurata.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

2. Selezionare **Aggiungi credenziali** e seguire la procedura guidata.
   a. **Credentials Location**: Selezionare **Microsoft Azure > Connector**.
   b. **Definisci credenziali**: Immettere le informazioni sull'entità del servizio Microsoft Entra che concede le autorizzazioni richieste:
      - ID dell'applicazione (client)
      - ID directory (tenant)
      - Segreto del client
   c. **Marketplace Subscription**: Consente di associare un abbonamento Marketplace a queste credenziali sottoscrivendo ora o selezionando un abbonamento esistente.

d. **Revisione**: Confermare i dettagli relativi alle nuove credenziali e selezionare **Aggiungi**.

Risultato

BlueXP dispone ora delle autorizzazioni necessarie per eseguire azioni in Azure per conto dell'utente.

Account del servizio Google Cloud

Associare l'account del servizio alla macchina virtuale del connettore.

Fasi

1. Accedere al portale Google Cloud e assegnare l'account del servizio all'istanza della macchina virtuale del connettore.

   "Documentazione di Google Cloud: Modifica dell'account del servizio e degli ambiti di accesso per un'istanza"

2. Se si desidera gestire le risorse in altri progetti, concedere l'accesso aggiungendo l'account di servizio con il ruolo BlueXP a tale progetto. Dovrai ripetere questo passaggio per ogni progetto.

Risultato

BlueXP dispone ora delle autorizzazioni necessarie per eseguire azioni in Google Cloud per tuo conto.

Iscriviti a BlueXP (modalità limitata)

Iscriviti a BlueXP dal mercato del tuo cloud provider per pagare i servizi BlueXP a una tariffa oraria (PAYGO) o attraverso un contratto annuale. Se hai acquistato una licenza da NetApp (BYOL), devi anche iscriverti all'offerta Marketplace. La licenza viene sempre addebitata per prima, ma l'utente verrà addebitato alla tariffa oraria se supera la capacità concessa in licenza o se scade il termine della licenza.

Un abbonamento al marketplace consente di addebitare i seguenti servizi BlueXP in modalità limitata:

- Backup e recovery
- Classificazione
- Cloud Volumes ONTAP

Prima di iniziare

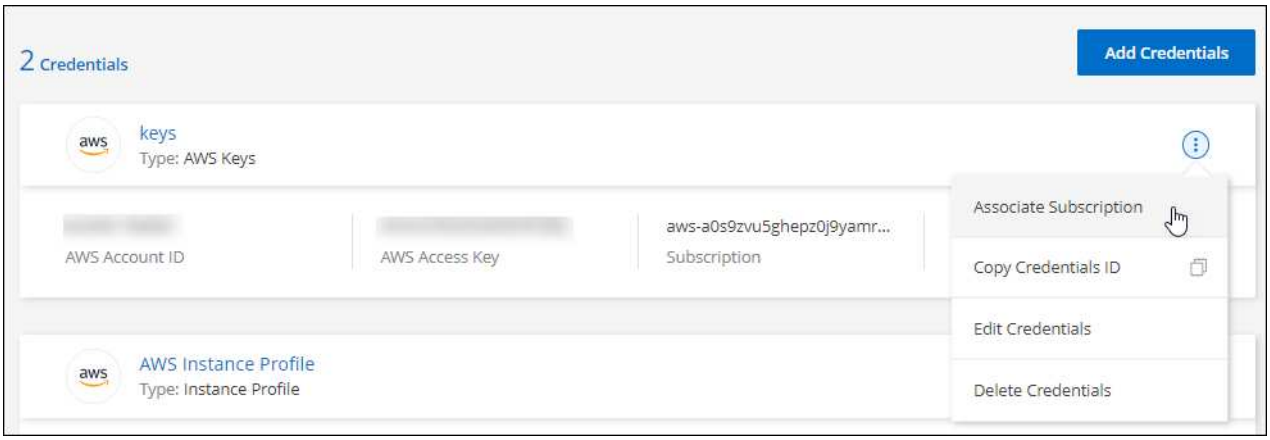
L'iscrizione a BlueXP implica l'associazione di un abbonamento Marketplace alle credenziali cloud associate a un connettore. Se hai seguito il flusso di lavoro "Get Started with Restricted mode" (inizia con la modalità limitata), dovresti già disporre di un connettore. Per ulteriori informazioni, consulta la "Avvio rapido per BlueXP in modalità limitata".

AWS

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.
2. Selezionare il menu delle azioni per una serie di credenziali, quindi selezionare **Associa abbonamento**.

   Selezionare le credenziali associate a un connettore. Non puoi associare un abbonamento al marketplace alle credenziali associate a BlueXP.



3. Per associare le credenziali a un abbonamento esistente, selezionare l'abbonamento dall'elenco a discesa e selezionare **Associa**.
4. Per associare le credenziali a un nuovo abbonamento, selezionare **Aggiungi abbonamento > continua** e seguire la procedura descritta in AWS Marketplace:

   a. Selezionare **Visualizza opzioni di acquisto**.

   b. Selezionare **Iscriviti**.

   c. Selezionare **Configura account**.

      Verrai reindirizzato al sito Web di BlueXP.

   d. Dalla pagina **Subscription Assignment**:

      - Seleziona gli account BlueXP a cui desideri associare questo abbonamento.
      - Nel campo **Sostituisci abbonamento esistente**, scegli se desideri sostituire automaticamente l'abbonamento esistente per un account con questo nuovo abbonamento.

        BlueXP sostituisce l'abbonamento esistente per tutte le credenziali dell'account con questo nuovo abbonamento. Se un insieme di credenziali non è mai stato associato a un abbonamento, questo nuovo abbonamento non sarà associato a tali credenziali.

      Per tutti gli altri account, è necessario associare manualmente l'abbonamento ripetendo questa procedura.

      - Selezionare **Salva**.

        Il seguente video mostra i passaggi per iscriversi a AWS Marketplace:

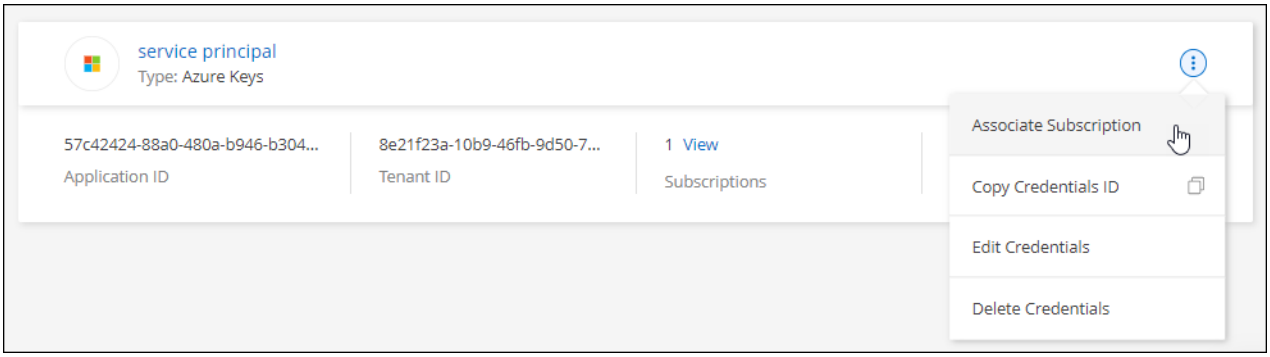
Iscriviti a BlueXP dal marketplace AWS

Azure

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.
2. Selezionare il menu delle azioni per una serie di credenziali, quindi selezionare **Associa abbonamento**.

   Selezionare le credenziali associate a un connettore. Non puoi associare un abbonamento al marketplace alle credenziali associate a BlueXP.



3. Per associare le credenziali a un abbonamento esistente, selezionare l'abbonamento dall'elenco a discesa e selezionare **Associa**.
4. Per associare le credenziali a un nuovo abbonamento, selezionare **Aggiungi abbonamento > continua** e seguire la procedura in Azure Marketplace:

   a. Se richiesto, accedere all'account Azure.

   b. Selezionare **Iscriviti**.

   c. Compila il modulo e seleziona **Iscriviti**.

   d. Una volta completato il processo di iscrizione, selezionare **Configura account**.

      Verrai reindirizzato al sito Web di BlueXP.

   e. Dalla pagina **Subscription Assignment**:

      - Seleziona gli account BlueXP a cui desideri associare questo abbonamento.
      - Nel campo **Sostituisci abbonamento esistente**, scegli se desideri sostituire automaticamente l'abbonamento esistente per un account con questo nuovo abbonamento.

        BlueXP sostituisce l'abbonamento esistente per tutte le credenziali dell'account con questo nuovo abbonamento. Se un insieme di credenziali non è mai stato associato a un abbonamento, questo nuovo abbonamento non sarà associato a tali credenziali.

      Per tutti gli altri account, è necessario associare manualmente l'abbonamento ripetendo questa procedura.

      - Selezionare **Salva**.

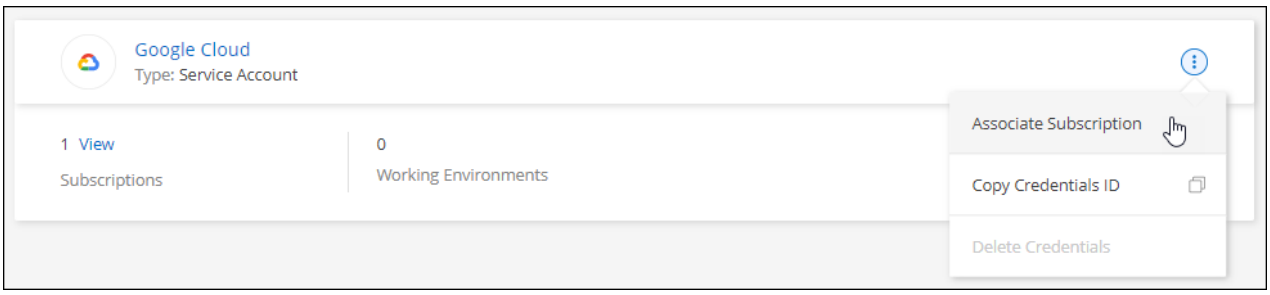
        Il seguente video mostra i passaggi per iscriversi a Azure Marketplace:

Iscriviti a BlueXP da Azure Marketplace

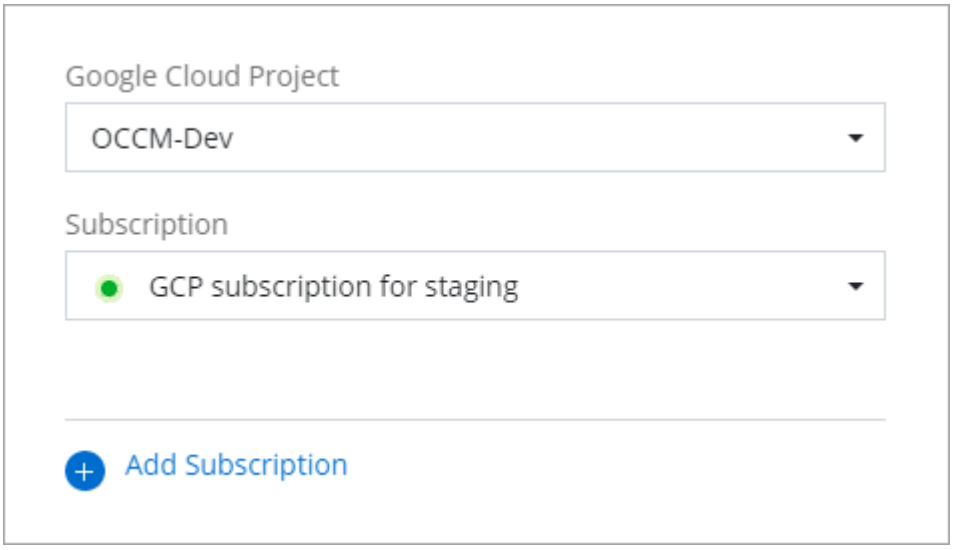
Google Cloud

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.
2. Selezionare il menu delle azioni per una serie di credenziali, quindi selezionare **Associa abbonamento**.



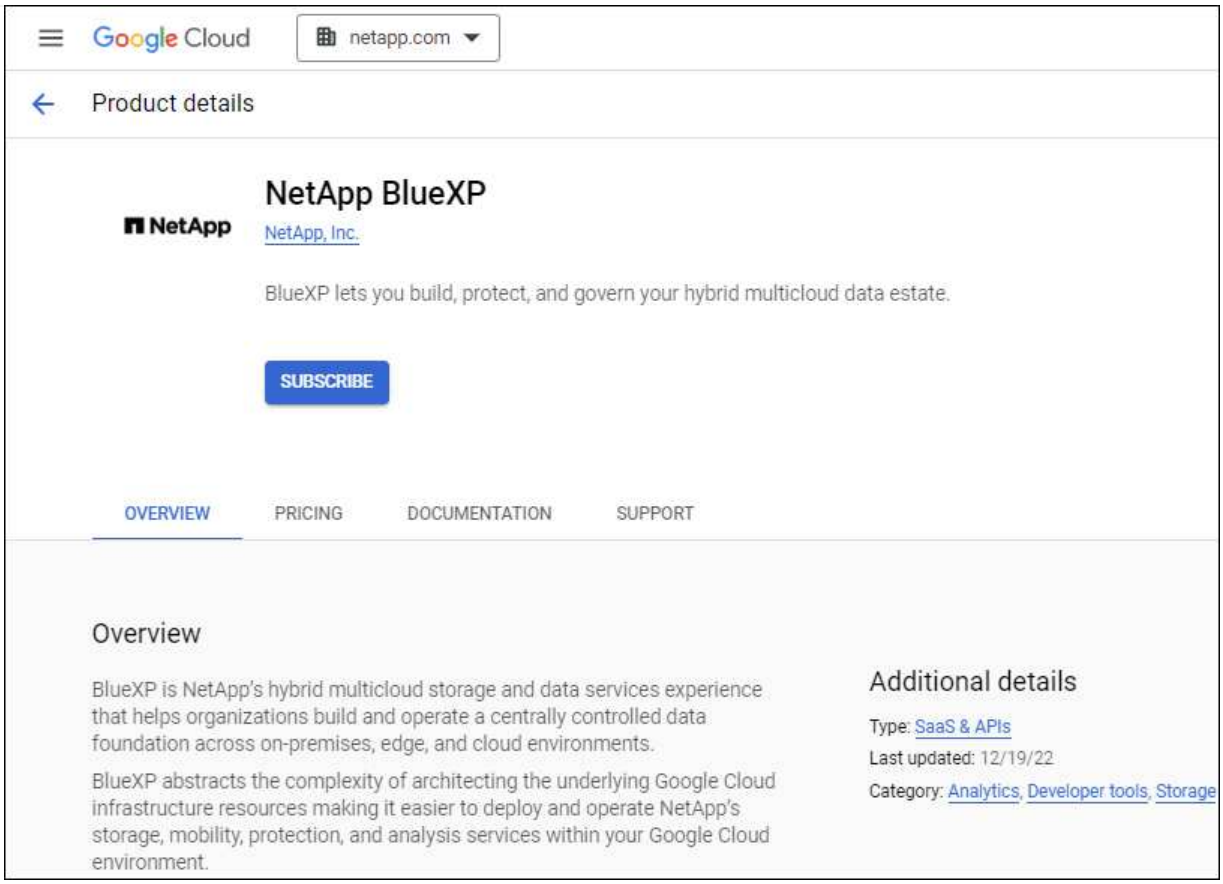
3. Per associare le credenziali a un abbonamento esistente, selezionare un progetto e un abbonamento Google Cloud dall'elenco a discesa, quindi selezionare **Associa**.



4. Se non disponi già di un abbonamento, seleziona **Aggiungi abbonamento > continua** e segui la procedura in Google Cloud Marketplace.

> Prima di completare i seguenti passaggi, assicurarsi di disporre dei privilegi di Billing Admin nell'account Google Cloud e di un account di accesso BlueXP.

   a. Dopo essere stati reindirizzati a "Pagina NetApp BlueXP su Google Cloud Marketplace", assicurarsi che il progetto corretto sia selezionato nel menu di navigazione superiore.



b. Selezionare **Iscriviti**.

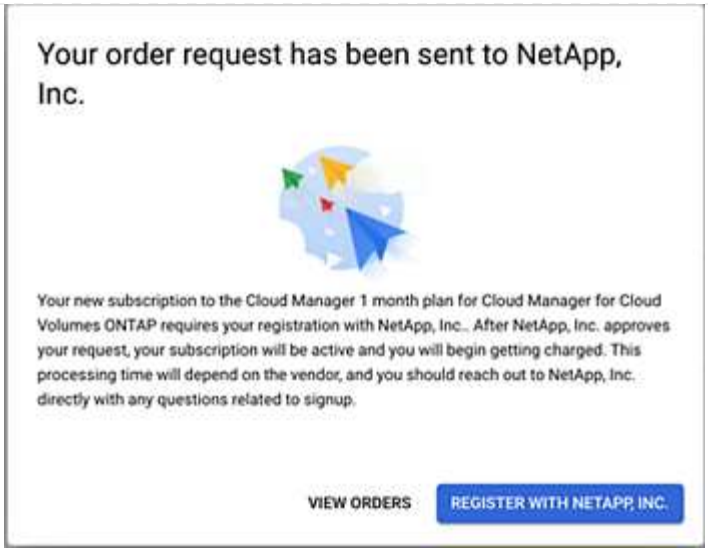
c. Selezionare l'account di fatturazione appropriato e accettare i termini e le condizioni.

d. Selezionare **Iscriviti**.

   Questa fase invia la richiesta di trasferimento a NetApp.

e. Nella finestra di dialogo a comparsa, selezionare **Registra con NetApp, Inc.**

   Questa fase deve essere completata per collegare l'abbonamento a Google Cloud al tuo account BlueXP. Il processo di collegamento di un abbonamento non viene completato fino a quando non si viene reindirizzati da questa pagina e si accede a BlueXP.



f. Completare la procedura riportata nella pagina **Subscription Assignment**:

> Se qualcuno della tua organizzazione ha già sottoscritto l'abbonamento a NetApp BlueXP dal tuo account di fatturazione, verrai reindirizzato a. "La pagina Cloud Volumes ONTAP sul sito Web di BlueXP" invece. In caso di imprevisti, contatta il tuo team di vendita NetApp. Google abilita un solo abbonamento per account di fatturazione Google.

- Seleziona gli account BlueXP a cui desideri associare questo abbonamento.
- Nel campo **Sostituisci abbonamento esistente**, scegli se desideri sostituire automaticamente l'abbonamento esistente per un account con questo nuovo abbonamento.

  BlueXP sostituisce l'abbonamento esistente per tutte le credenziali dell'account con questo nuovo abbonamento. Se un insieme di credenziali non è mai stato associato a un abbonamento, questo nuovo abbonamento non sarà associato a tali credenziali.

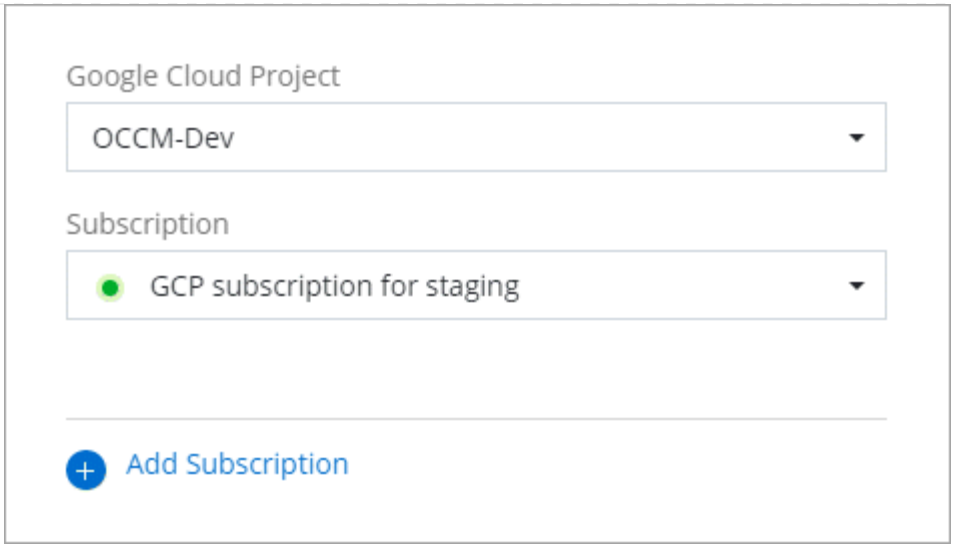
Per tutti gli altri account, è necessario associare manualmente l'abbonamento ripetendo questa procedura.

- Selezionare **Salva**.

  Il seguente video mostra i passaggi per iscriversi a Google Cloud Marketplace:

Iscriviti a BlueXP da Google Cloud Marketplace

a. Una volta completata questa procedura, tornare alla pagina credenziali in BlueXP e selezionare questo nuovo abbonamento.



Link correlati

- "Gestire le licenze BYOL basate sulla capacità per Cloud Volumes ONTAP"
- "Gestire le licenze BYOL per i servizi dati BlueXP"
- "Gestire le credenziali AWS e le sottoscrizioni per BlueXP"
- "Gestire le credenziali e le sottoscrizioni di Azure per BlueXP"
- "Gestire le credenziali e le sottoscrizioni di Google Cloud per BlueXP"

Operazioni successive (modalità limitata)

Dopo aver eseguito BlueXP in modalità limitata, è possibile iniziare a utilizzare i servizi BlueXP supportati in modalità limitata.

Per assistenza, consultare la documentazione relativa a questi servizi:

- "Documentazione di Amazon FSX per ONTAP"
- "Documenti Azure NetApp Files"
- "Documenti di backup e recovery"
- "Documenti di classificazione"
- "Documenti Cloud Volumes ONTAP"
- "Documentazione sul cluster ONTAP on-premise"
- "Documenti di replica"

Link correlato

"Modalità di implementazione di BlueXP"