Inizia con la modalità privata

Setup and administration

NetApp
April 26, 2024

Sommario

Inizia con la modalità privata

Flusso di lavoro introduttivo (modalità privata)

Inizia a utilizzare BlueXP in modalità privata preparando l'ambiente e implementando il connettore.

La modalità privata viene generalmente utilizzata con ambienti on-premise che non dispongono di connessione a Internet e con aree cloud sicure, tra cui "Cloud segreto AWS", "Cloud AWS top secret", e. "Azure IL6"

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.
3. Per le implementazioni cloud, imposta le autorizzazioni nel tuo cloud provider in modo da poter associare tali autorizzazioni al connettore dopo l'installazione del software.

2 **"Implementare il connettore"**

1. Installare il software del connettore sul proprio host Linux.
2. Configurare BlueXP aprendo un browser Web e immettendo l'indirizzo IP dell'host Linux.
3. Per le implementazioni cloud, fornire a BlueXP le autorizzazioni precedentemente impostate.

Prepararsi per l'implementazione in modalità privata

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

> Se si desidera utilizzare BlueXP in "Cloud segreto AWS" o il "Cloud AWS top secret", quindi seguire le istruzioni separate per iniziare a utilizzare questi ambienti. "Scopri come iniziare a utilizzare Cloud Volumes ONTAP nel cloud segreto AWS o nel cloud top secret"

Passaggio 1: Comprendere il funzionamento della modalità privata

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

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 privata".

Passaggio 2: Esaminare le opzioni di installazione

In modalità privata, è possibile installare il connettore on-premise o nel cloud installando manualmente il connettore sul proprio host Linux.

Il punto in cui viene installato il connettore determina quali servizi e funzionalità di BlueXP sono disponibili quando si utilizza la modalità privata. Ad esempio, per implementare e gestire Cloud Volumes ONTAP, il connettore deve essere installato nel cloud. "Ulteriori informazioni sulla modalità privata".

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.

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 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. 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.

Endpoint per le operazioni quotidiane

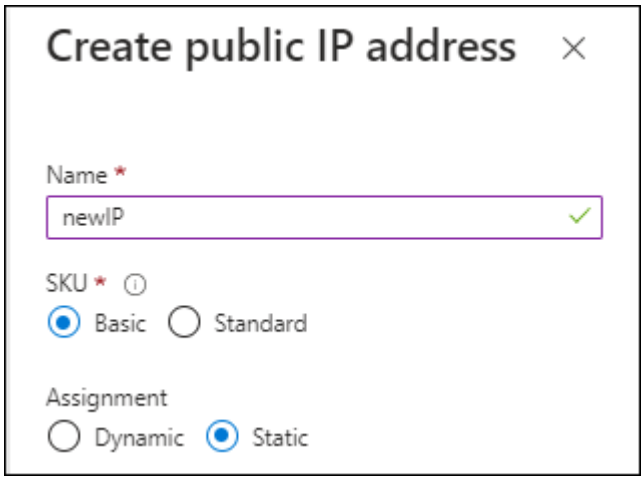
Il connettore contatta i seguenti endpoint per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

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"

Endpoint	Scopo
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Per gestire le risorse nelle aree pubbliche di Azure.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Per gestire le risorse nell'area Azure IL6.
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.

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.

+
Con la modalità privata, l'unica volta in cui BlueXP invia il traffico in uscita è al provider cloud per creare un sistema Cloud Volumes ONTAP.

Porte

Non c'è traffico in entrata verso il connettore, a meno che non venga avviato.

HTTP (80) e HTTPS (443) forniscono l'accesso alla console BlueXP. SSH (22) è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.

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"

Passaggio 5: Preparare le autorizzazioni del cloud

Se il connettore è installato nel cloud e intendi creare sistemi Cloud Volumes ONTAP, BlueXP richiede le autorizzazioni del tuo cloud provider. È necessario impostare le autorizzazioni nel provider cloud e associarle all'istanza di Connector dopo l'installazione.

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. Sarà necessario associare manualmente il ruolo all'istanza EC2 per il connettore.

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. Abilitare un'identità gestita assegnata dal sistema sulla macchina virtuale in cui si intende installare il connettore in modo da poter fornire le autorizzazioni necessarie per Azure 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.

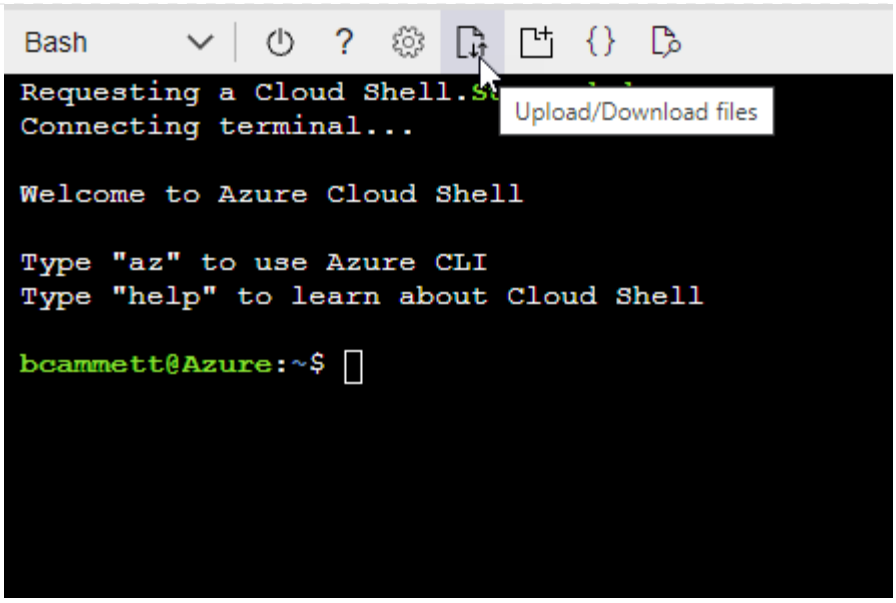
   Esempio

   ```
   "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

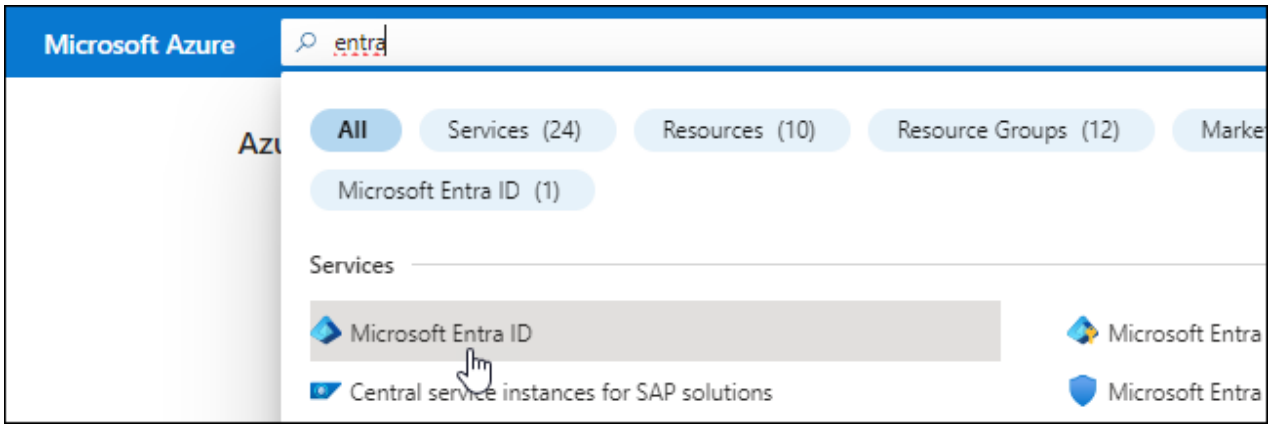
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP. È necessario fornire queste credenziali a BlueXP dopo aver installato il connettore e configurato BlueXP.

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.

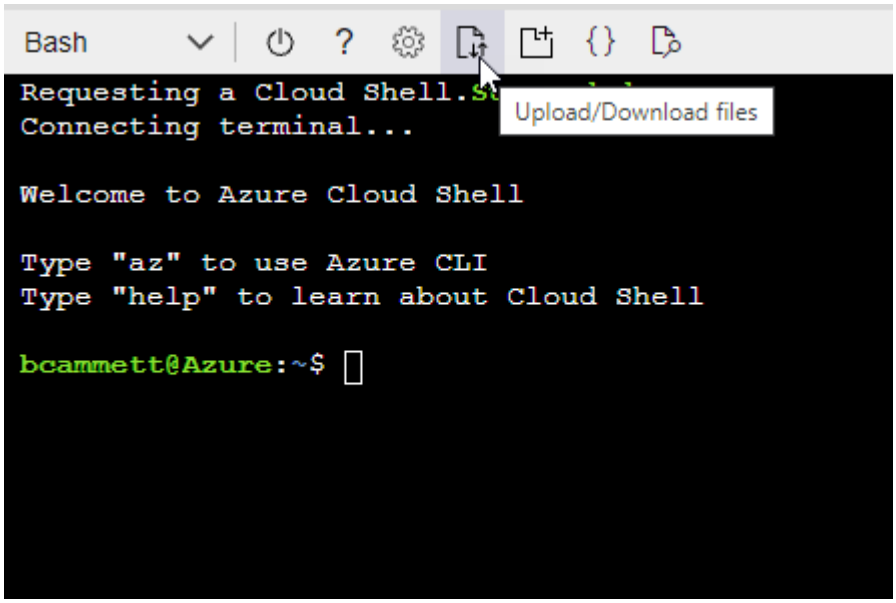
      Esempio

      ```
      "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:

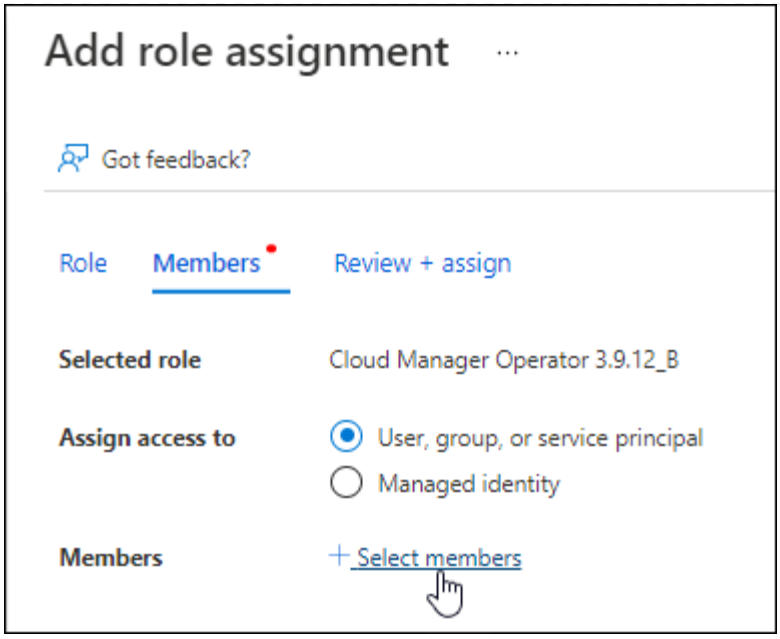
```
az role definition create --role-definition
Connector_Policy.json
```

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:

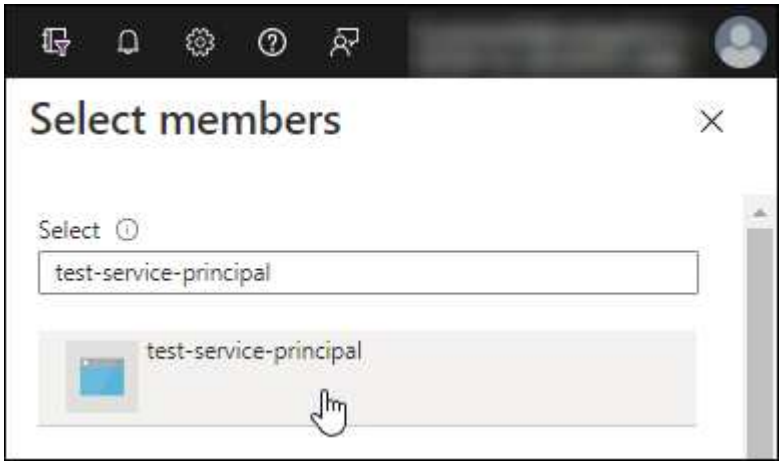
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

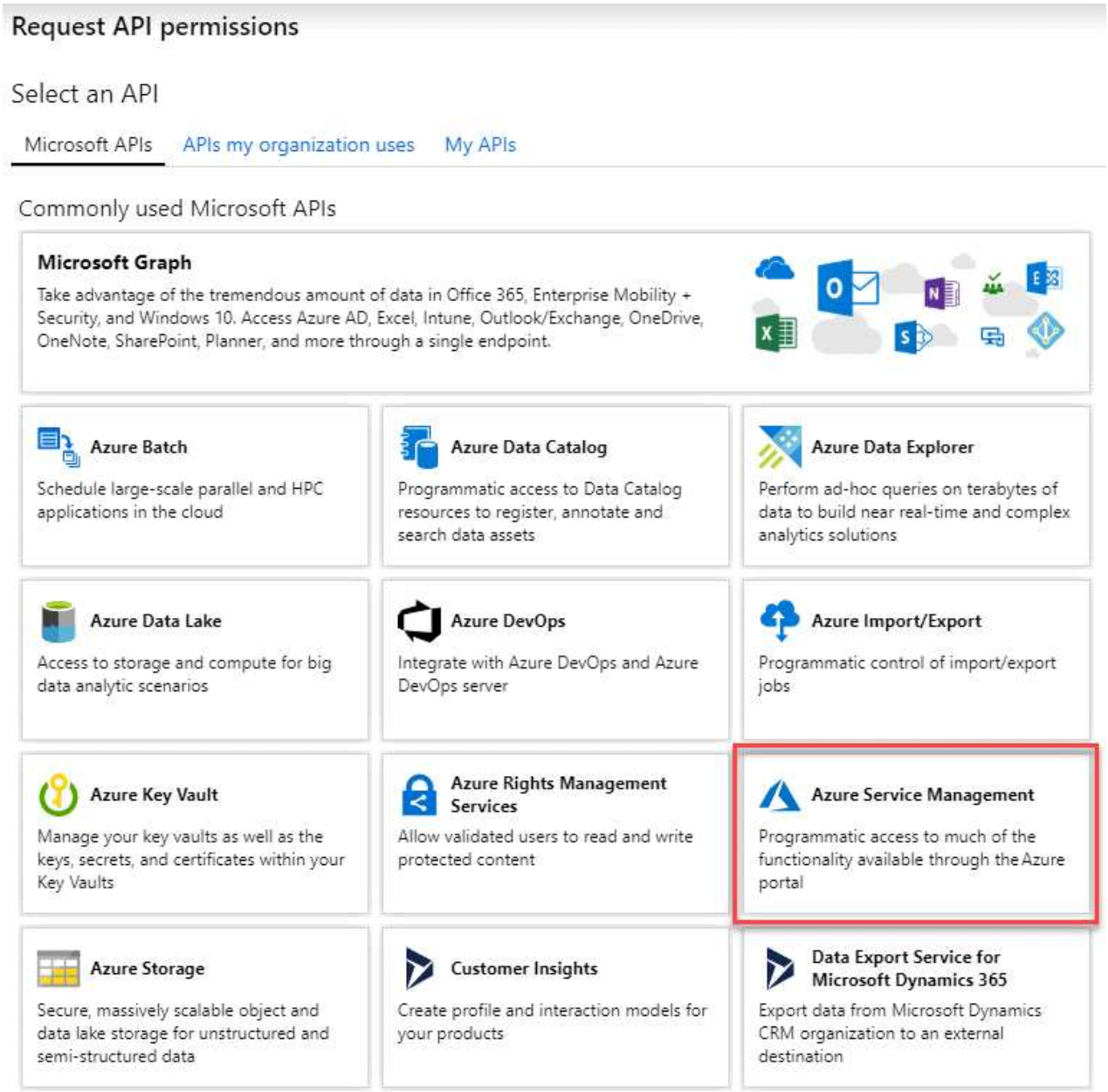
   L'entità del servizio dispone ora delle autorizzazioni Azure necessarie per implementare il connettore.

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.

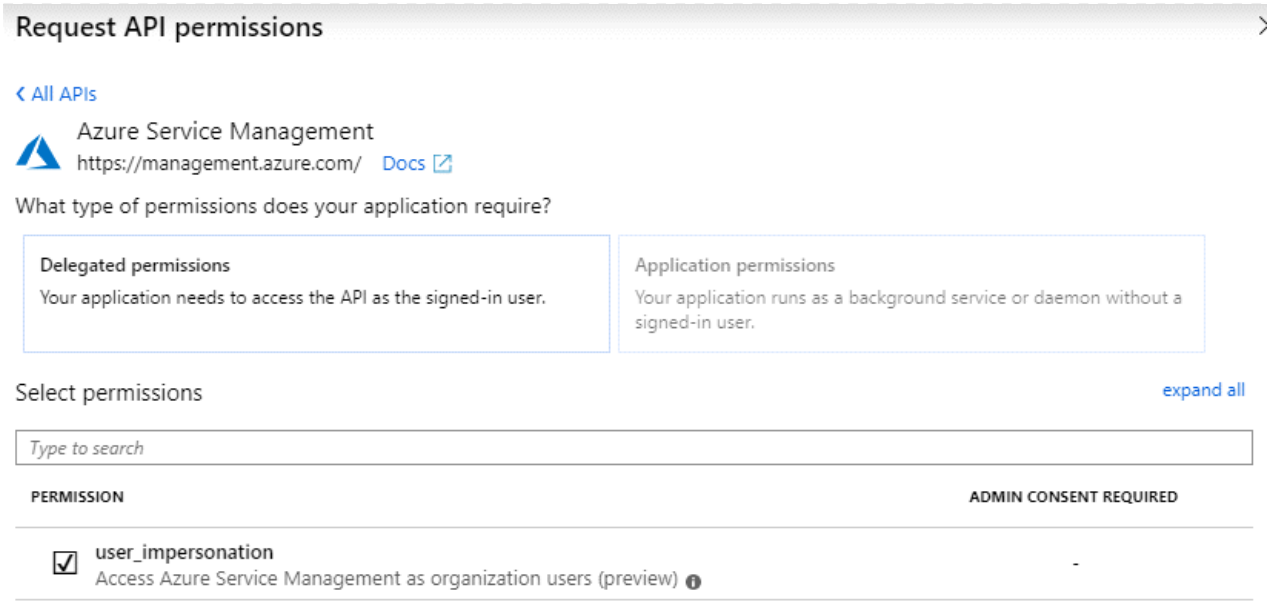
Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

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**.

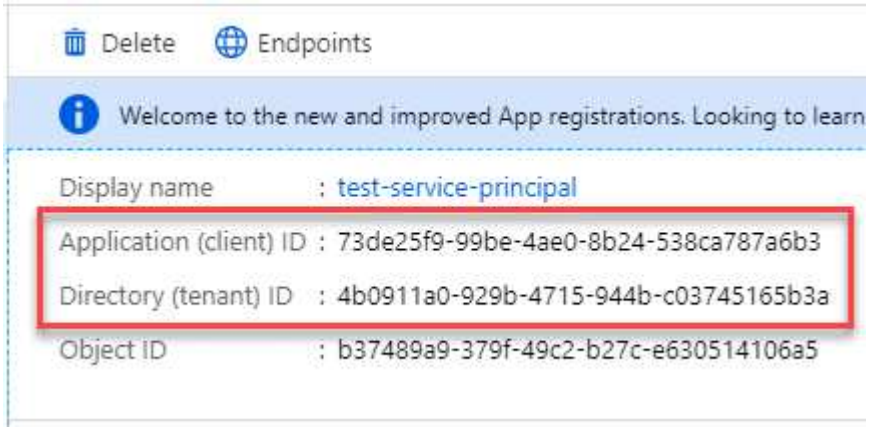


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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 privata

Implementare il connettore in modalità privata in modo da poter utilizzare BlueXP senza connettività in uscita 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

Scaricare il programma di installazione del prodotto dal NetApp Support Site e installare manualmente il connettore sul proprio host Linux.

Se si desidera utilizzare BlueXP in "Cloud segreto AWS" o il "Cloud AWS top secret", quindi seguire le istruzioni separate per iniziare a utilizzare questi ambienti. "Scopri come iniziare a utilizzare Cloud Volumes ONTAP nel cloud segreto AWS o nel cloud top secret"

Prima di iniziare

Per installare il connettore sono necessari i privilegi di root.

Fasi

1. Verificare che docker sia attivato e in esecuzione.

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

2. Scaricare il software del connettore da "Sito di supporto NetApp"

   Assicurarsi di scaricare il programma di installazione offline per le reti private senza accesso a Internet.

3. Copiare il programma di installazione sull'host Linux.
4. Assegnare le autorizzazioni per eseguire lo script.

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

   Dove <version> è la versione del connettore scaricato.

5. Eseguire lo script di installazione:

```
sudo /path/BlueXP-Connector-offline-<version>
```

   Dove <version> è la versione del connettore scaricato.

Risultato

Il software del connettore è installato. Ora puoi configurare BlueXP.

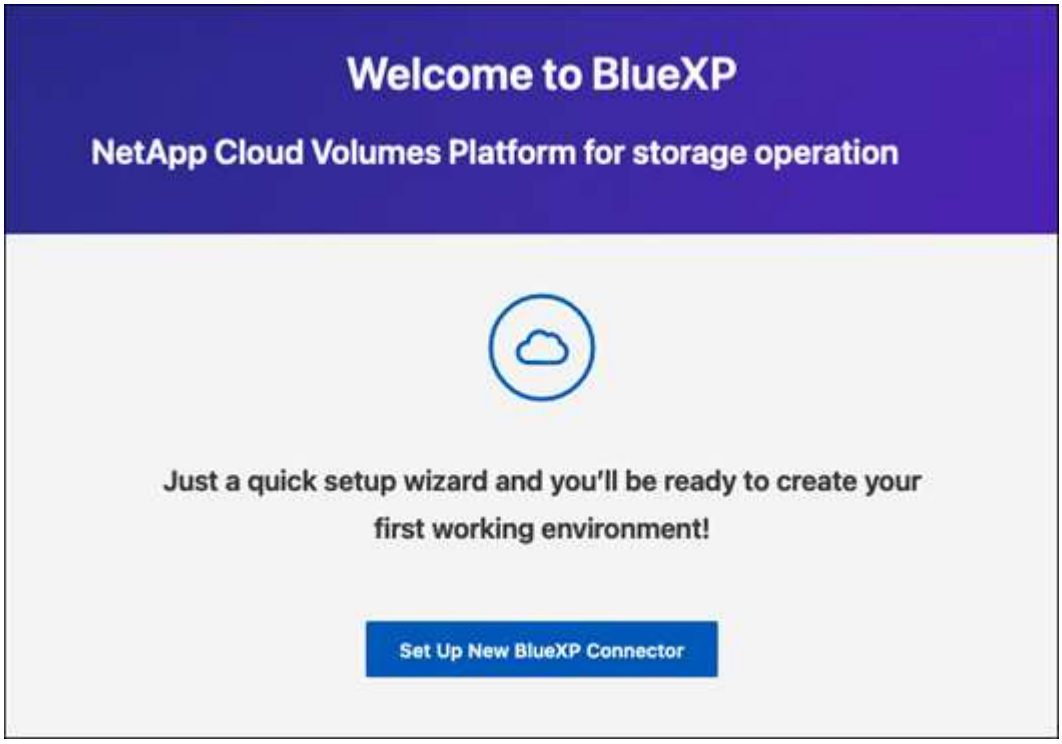
Fase 2: Configurare BlueXP

Quando si accede alla console BlueXP per la prima volta, viene richiesto di configurare BlueXP.

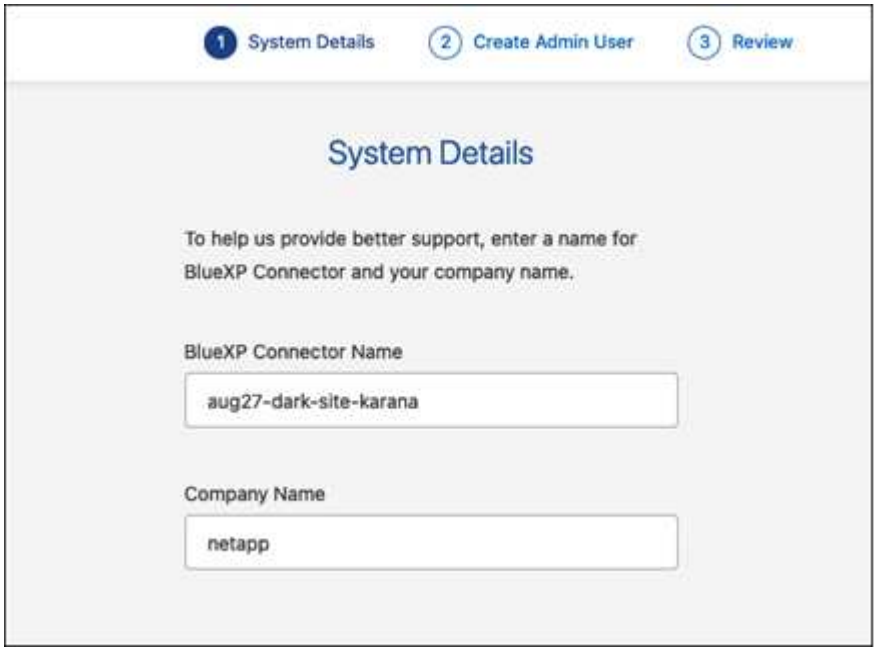
Fasi

1. Aprire un browser Web e immettere https://ipaddress Dove ipaddress è l’indirizzo IP dell’host Linux in cui è stato installato il connettore.

   Viene visualizzata la seguente schermata.



2. Selezionare **Configura nuovo connettore BlueXP** e seguire le istruzioni a schermo per configurare il sistema.
    - **Dettagli sistema**: Inserire un nome per il connettore e il nome della società.



    - **Creare un utente amministratore**: Creare l'utente amministratore per il sistema.

      Questo account utente viene eseguito localmente sul sistema. Non esiste alcuna connessione al servizio auth0 disponibile tramite BlueXP.

    - **Revisione**: Esaminare i dettagli, accettare il contratto di licenza, quindi selezionare **Configurazione**.
3. Accedere a BlueXP utilizzando l'utente amministratore appena creato.

Risultato

Il connettore è stato installato e configurato.

Quando saranno disponibili nuove versioni del software del connettore, verranno pubblicate sul sito di supporto NetApp. "Scopri come aggiornare il connettore".

Quali sono le prossime novità?

Fornire a BlueXP le autorizzazioni precedentemente impostate.

Fase 3: Fornire le autorizzazioni ad BlueXP

Se si desidera creare ambienti di lavoro Cloud Volumes ONTAP, è necessario fornire a BlueXP le autorizzazioni cloud precedentemente configurate.

"Scopri come preparare le autorizzazioni cloud".

Ruolo AWS IAM

Collegare il ruolo IAM precedentemente creato all'istanza di Connector EC2.

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.

Operazioni successive (modalità privata)

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

Per assistenza, consultare la seguente documentazione:

- "Creare sistemi Cloud Volumes ONTAP"
- "Scopri i cluster ONTAP on-premise"
- "Replicare i dati"
- "Eseguire la scansione on-premise dei dati del volume ONTAP utilizzando la classificazione BlueXP"
- "Eseguire il backup on-premise dei dati dei volumi ONTAP su StorageGRID utilizzando il backup e ripristino BlueXP"

Link correlato

"Modalità di implementazione di BlueXP"