Creare un connettore

Setup and administration

NetApp
April 26, 2024

Sommario

Creare un connettore

AWS

Opzioni di installazione del connettore in AWS

Esistono diversi modi per creare un connettore in AWS. Direttamente da BlueXP è il modo più comune.

Sono disponibili le seguenti opzioni di installazione:

- "Creare il connettore direttamente da BlueXP" (questa è l'opzione standard)

  Questa azione avvia un'istanza EC2 che esegue Linux e il software Connector in un VPC a scelta.

- "Creare un connettore da AWS Marketplace"

  Questa azione avvia anche un'istanza EC2 che esegue Linux e il software Connector, ma l'implementazione viene avviata direttamente dal marketplace di AWS e non da BlueXP.

- "Scaricare e installare manualmente il software sul proprio host Linux"

L'opzione di installazione scelta influisce sul modo in cui si prepara l'installazione. Ciò include il modo in cui si forniscono a BlueXP le autorizzazioni necessarie per autenticare e gestire le risorse in AWS.

Crea un connettore in AWS da BlueXP

Per creare un connettore in AWS da BlueXP, devi configurare il tuo networking, preparare le autorizzazioni AWS e quindi creare il connettore.

Prima di iniziare

Dovresti rivedere "Limitazioni del connettore".

Fase 1: Configurare la rete

Assicurarsi che la posizione di rete in cui si intende installare il connettore supporti i seguenti requisiti. Il connettore, che soddisfa questi requisiti, consente di gestire le risorse e i processi all'interno del tuo ambiente di cloud ibrido.

VPC e subnet

Quando si crea il connettore, è necessario specificare il VPC e la subnet in cui deve risiedere il connettore.

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete alla posizione in cui si intende creare e gestire gli ambienti di lavoro. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema storage nel tuo ambiente on-premise.

Accesso a Internet in uscita

La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

Endpoint contattati dal connettore

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 per le operazioni quotidiane.

Si noti che gli endpoint elencati di seguito sono tutte le voci CNAME.

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://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	Per aggiornare il connettore e i relativi componenti Docker.

Endpoint contattati dalla console BlueXP

Quando utilizzi la console basata sul web BlueXP fornita attraverso il layer SaaS, contatta diversi endpoint per completare le attività di gestione dei dati. Sono inclusi gli endpoint che vengono contattati per implementare il connettore dalla console BlueXP.

"Visualizzare l'elenco degli endpoint contattati dalla console BlueXP".

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"

Una volta creato il connettore, sarà necessario implementare questo requisito di rete.

Passaggio 2: Impostare le autorizzazioni AWS

BlueXP deve eseguire l'autenticazione con AWS prima di poter implementare l'istanza del connettore nel VPC. È possibile scegliere uno dei seguenti metodi di autenticazione:

- Lasciare che BlueXP assuma un ruolo IAM con le autorizzazioni richieste
- Fornire una chiave di accesso AWS e una chiave segreta per un utente IAM che dispone delle autorizzazioni richieste

Con entrambe le opzioni, il primo passo è creare un criterio IAM. Questo criterio contiene solo le autorizzazioni necessarie per avviare l'istanza di Connector in AWS da BlueXP.

Se necessario, è possibile limitare la policy IAM utilizzando il modulo IAM `Condition` elemento. "Documentazione AWS: Elemento Condition"

> Quando BlueXP crea il connettore, applica un nuovo set di autorizzazioni all'istanza del connettore che consente al connettore di gestire le risorse AWS.

Fasi

1. Accedere alla console AWS IAM.
2. Selezionare **Criteri > Crea policy**.
3. Selezionare **JSON**.

4. Copiare e incollare il seguente criterio:

   Si ricorda che questo criterio contiene solo le autorizzazioni necessarie per avviare l'istanza di Connector in AWS da BlueXP. "Visualizza le autorizzazioni richieste per l'istanza del connettore".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
```

```
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/OCCMInstance": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

5. Selezionare **Avanti** e aggiungere tag, se necessario.
6. Selezionare **Avanti** e immettere un nome e una descrizione.
7. Selezionare **Crea policy**.
8. Allegare il criterio a un ruolo IAM che BlueXP può assumere o a un utente IAM in modo da poter fornire a BlueXP le chiavi di accesso:
   - (Opzione 1) impostare un ruolo IAM che BlueXP può assumere:
     i. Accedere alla console AWS IAM nell'account di destinazione.
     ii. In Gestione accessi, selezionare **ruoli > Crea ruolo** e seguire i passaggi per creare il ruolo.
     iii. In **Trusted entity type**, selezionare **AWS account**.
     iv. Selezionare **un altro account AWS** e inserire l'ID dell'account BlueXP SaaS: 952013314444
     v. Selezionare il criterio creato nella sezione precedente.

vi. Dopo aver creato il ruolo, copiare l'ARN del ruolo in modo da poterlo incollare in BlueXP quando si crea il connettore.

- (Opzione 2) impostare le autorizzazioni per un utente IAM in modo da poter fornire a BlueXP le chiavi di accesso:

  i. Dalla console di AWS IAM, selezionare **Users** (utenti), quindi selezionare il nome utente.

  ii. Selezionare **Aggiungi permessi > Allega direttamente policy esistenti**.

  iii. Selezionare il criterio creato.

  iv. Selezionare **Avanti**, quindi selezionare **Aggiungi permessi**.

  v. Assicurarsi di disporre della chiave di accesso e della chiave segreta per l'utente IAM.

Risultato

Ora dovresti disporre di un ruolo IAM con le autorizzazioni richieste o di un utente IAM con le autorizzazioni richieste. Quando si crea il connettore da BlueXP, è possibile fornire informazioni sul ruolo o sulle chiavi di accesso.

Fase 3: Creare il connettore

Creare il connettore direttamente dalla console BlueXP basata sul Web.

A proposito di questa attività

La creazione del connettore da BlueXP implementa un'istanza EC2 in AWS usando una configurazione predefinita. Dopo aver creato il connettore, non si dovrebbe passare a un tipo di istanza EC2 più piccolo che ha meno CPU o RAM. "Informazioni sulla configurazione predefinita del connettore".

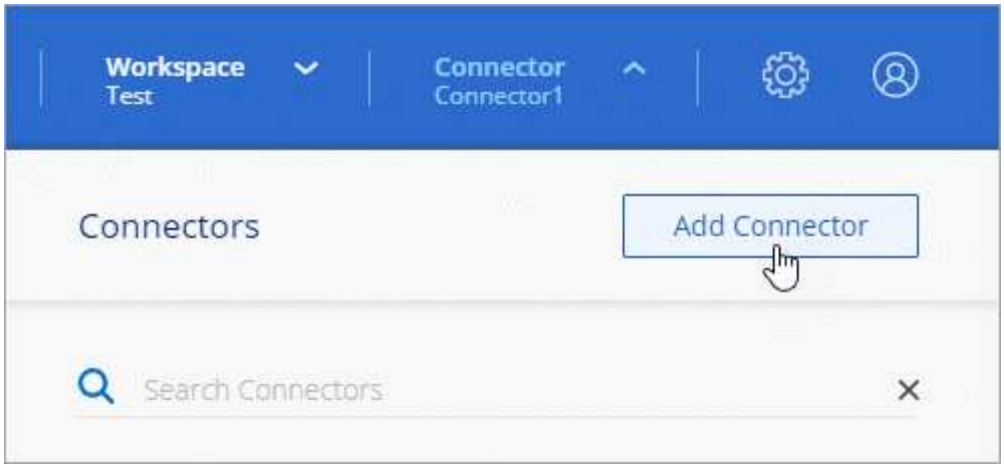
Prima di iniziare

Dovresti disporre di quanto segue:

- Metodo di autenticazione AWS: Un ruolo IAM o chiavi di accesso per un utente IAM con le autorizzazioni richieste.
- VPC e subnet che soddisfano i requisiti di rete.
- Coppia di chiavi per l'istanza EC2.
- Dettagli su un server proxy, se è richiesto un proxy per l'accesso a Internet dal connettore.

Fasi

1. Selezionare l'elenco a discesa **Connector** (connettore) e selezionare **Add Connector** (Aggiungi connettore).



2. Scegli **Amazon Web Services** come cloud provider e seleziona **continua**.
3. Nella pagina **Deploying a Connector** (implementazione di un connettore), consultare i dettagli relativi alle esigenze. Sono disponibili due opzioni:
   a. Selezionare **continua** per prepararsi all'implementazione utilizzando la guida all'interno del prodotto. Ogni fase della guida all'interno del prodotto include le informazioni contenute in questa pagina della documentazione.
   b. Selezionare **Skip to Deployment** (passa alla distribuzione) se si è già pronti seguendo la procedura riportata in questa pagina.
4. Seguire i passaggi della procedura guidata per creare il connettore:
   - **Get Ready**: Consulta le informazioni necessarie.
   - **AWS Credentials**: Specificare la regione AWS e scegliere un metodo di autenticazione, ovvero un ruolo IAM che BlueXP può assumere o una chiave di accesso AWS e una chiave segreta.

     Se si sceglie **assumere ruolo**, è possibile creare il primo set di credenziali dalla distribuzione guidata del connettore. Qualsiasi set di credenziali aggiuntivo deve essere creato dalla pagina credenziali. Saranno quindi disponibili dalla procedura guidata in un elenco a discesa. "Scopri come aggiungere ulteriori credenziali".

   - **Dettagli**: Fornire dettagli sul connettore.
     - Immettere un nome per l'istanza.
     - Aggiungere tag personalizzati (metadati) all'istanza.
     - Scegliere se si desidera che BlueXP crei un nuovo ruolo con le autorizzazioni richieste o se si desidera selezionare un ruolo esistente configurato "le autorizzazioni richieste".
     - Scegliere se si desidera crittografare i dischi EBS del connettore. È possibile utilizzare la chiave di crittografia predefinita o una chiave personalizzata.
   - **Rete**: Specificare un VPC, una subnet e una coppia di chiavi per l'istanza, scegliere se attivare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione del proxy.

     Assicurarsi di disporre della coppia di chiavi corretta da utilizzare con il connettore. Senza una coppia di chiavi, non sarà possibile accedere alla macchina virtuale Connector.

   - **Security Group**: Scegliere se creare un nuovo gruppo di sicurezza o se selezionare un gruppo di sicurezza esistente che consenta le regole in entrata e in uscita richieste.

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

- **Revisione**: Controllare le selezioni per verificare che la configurazione sia corretta.

5. Selezionare **Aggiungi**.

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

Risultato

Una volta completato il processo, il connettore è disponibile per l'utilizzo da parte di BlueXP.

Se hai bucket Amazon S3 nello stesso account AWS in cui hai creato il connettore, vedrai automaticamente un ambiente di lavoro Amazon S3 su BlueXP Canvas. "Scopri come gestire i bucket S3 da BlueXP"

Creare un connettore da AWS Marketplace

Per creare un connettore dal marketplace AWS, devi configurare la tua rete, preparare le autorizzazioni AWS, rivedere i requisiti delle istanze e creare quindi il connettore.

Prima di iniziare

Dovresti rivedere "Limitazioni del connettore".

Fase 1: Configurare la rete

Assicurarsi che la posizione di rete in cui si intende installare il connettore supporti i seguenti requisiti. Il connettore, che soddisfa questi requisiti, consente di gestire le risorse e i processi all'interno del tuo ambiente di cloud ibrido.

VPC e subnet

Quando si crea il connettore, è necessario specificare il VPC e la subnet in cui deve risiedere il connettore.

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete alla posizione in cui si intende creare e gestire gli ambienti di lavoro. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema storage nel tuo ambiente on-premise.

Accesso a Internet in uscita

La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

Endpoint contattati dal connettore

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 per le operazioni quotidiane.

Si noti che gli endpoint elencati di seguito sono tutte le voci CNAME.

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://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	Per aggiornare il connettore e i relativi componenti Docker.

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"

Una volta creato il connettore, sarà necessario implementare questo requisito di rete.

Passaggio 2: Impostare le autorizzazioni AWS

Per prepararsi all'implementazione di un marketplace, creare policy IAM in AWS e allegarle a un ruolo IAM. Quando si crea il connettore da AWS Marketplace, viene richiesto di selezionare il ruolo IAM.

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. 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 si dispone di un ruolo IAM che è possibile associare all'istanza EC2 durante la distribuzione da AWS Marketplace.

Passaggio 3: Esaminare i requisiti dell'istanza

Quando si crea il connettore, è necessario scegliere un tipo di istanza EC2 che soddisfi i seguenti requisiti.

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.

Fase 4: Creare il connettore

Creare il connettore direttamente dall'AWS Marketplace.

A proposito di questa attività

La creazione del connettore da AWS Marketplace implementa un'istanza EC2 in AWS utilizzando una configurazione predefinita. "Informazioni sulla configurazione predefinita del connettore".

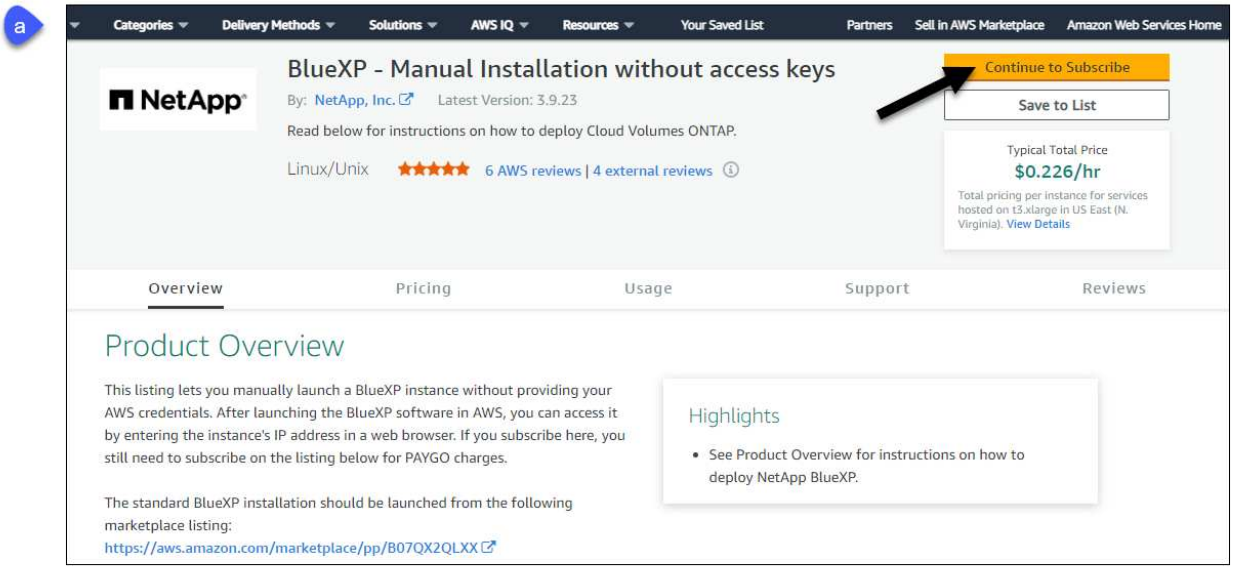
Prima di iniziare

Dovresti disporre di quanto segue:

- VPC e subnet che soddisfano i requisiti di rete.
- Un ruolo IAM con un criterio allegato che include le autorizzazioni richieste per il connettore.
- Autorizzazioni per iscriversi e annullare l'iscrizione da AWS Marketplace per l'utente IAM.
- Comprensione dei requisiti di CPU e RAM per l'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**.

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

6. Aprire un browser Web da un host connesso alla macchina virtuale Connector e immettere il seguente URL:

   https://ipaddress

7. Dopo aver effettuato l'accesso, configurare il connettore:
   a. Specificare l'account BlueXP da associare al connettore.
   b. Immettere un nome per il sistema.
   c. In **stai eseguendo in un ambiente protetto?** Mantieni disattivata la modalità limitata.

      La modalità limitata deve essere disattivata perché questa procedura descrive come utilizzare BlueXP in modalità standard. Attivare la modalità limitata solo se si dispone di un ambiente sicuro e si desidera disconnettere questo account dai servizi di back-end BlueXP. In tal caso, "Segui i passaggi per iniziare a utilizzare BlueXP in modalità limitata".

   d. Selezionare **Let's start**.

Risultato

Il connettore è ora installato e configurato con l'account BlueXP.

Aprire un browser Web e accedere a. "Console BlueXP" Per iniziare a utilizzare il connettore con BlueXP.

Se hai bucket Amazon S3 nello stesso account AWS in cui hai creato il connettore, vedrai automaticamente un ambiente di lavoro Amazon S3 su BlueXP Canvas. "Scopri come gestire i bucket S3 da BlueXP"

Installare manualmente il connettore in AWS

Per installare manualmente il connettore sul proprio host Linux, è necessario rivedere i requisiti dell'host, configurare la rete, preparare le autorizzazioni AWS, installare il connettore e quindi fornire le autorizzazioni preparate.

Prima di iniziare

Dovresti rivedere "Limitazioni del connettore".

Fase 1: 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.

Coppia di chiavi

Quando si crea il connettore, è necessario selezionare una coppia di chiavi EC2 da utilizzare con l'istanza.

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 2: Configurare la rete

Assicurarsi che la posizione di rete in cui si intende installare il connettore supporti i seguenti requisiti. Il connettore, che soddisfa questi requisiti, consente di gestire le risorse e i processi all'interno del tuo ambiente di cloud ibrido.

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete alla posizione in cui si intende creare e gestire gli ambienti di lavoro. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema storage nel tuo ambiente on-premise.

Accesso a Internet in uscita

La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

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

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

Endpoint contattati dal connettore

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 per le operazioni quotidiane.

Si noti che gli endpoint elencati di seguito sono tutte le voci CNAME.

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://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	Per aggiornare il connettore e i relativi componenti Docker.

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"

Passaggio 3: Impostare le autorizzazioni

Devi fornire autorizzazioni AWS ad BlueXP tramite una delle seguenti opzioni:

- Opzione 1: Creazione di criteri IAM e associazione dei criteri a un ruolo IAM che è possibile associare all'istanza EC2.
- Opzione 2: Fornisci a BlueXP la chiave di accesso AWS a un utente IAM che dispone delle autorizzazioni necessarie.

Segui i passaggi per preparare le autorizzazioni per BlueXP.

Ruolo IAM

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. 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 si dispone di un ruolo IAM che è possibile associare all'istanza EC2 dopo aver installato il connettore.

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

Ora si dispone di un utente IAM che dispone delle autorizzazioni necessarie e di una chiave di accesso

che è possibile fornire a BlueXP.

Fase 4: Installare il connettore

Una volta completati i prerequisiti, è possibile installare manualmente il software sul proprio host Linux.

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.

6. Attendere il completamento dell'installazione.

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

7. Aprire un browser Web da un host connesso alla macchina virtuale Connector e immettere il seguente URL:

   https://ipaddress

8. Dopo aver effettuato l'accesso, configurare il connettore:
   a. Specificare l'account BlueXP da associare al connettore.
   b. Immettere un nome per il sistema.

c. In **stai eseguendo in un ambiente protetto?** Mantieni disattivata la modalità limitata.

   La modalità limitata deve essere disattivata perché questa procedura descrive come utilizzare BlueXP in modalità standard. Attivare la modalità limitata solo se si dispone di un ambiente sicuro e si desidera disconnettere questo account dai servizi di back-end BlueXP. In tal caso, "Segui i passaggi per iniziare a utilizzare BlueXP in modalità limitata".

d. Selezionare **Let's start**.

Risultato

Il connettore è ora installato e configurato con l'account BlueXP.

Se hai bucket Amazon S3 nello stesso account AWS in cui hai creato il connettore, vedrai automaticamente un ambiente di lavoro Amazon S3 su BlueXP Canvas. "Scopri come gestire i bucket S3 da BlueXP"

Fase 5: Fornire le autorizzazioni ad BlueXP

Ora che hai installato il connettore, devi fornire ad BlueXP le autorizzazioni AWS precedentemente configurate. La fornitura delle autorizzazioni consente a BlueXP di gestire l'infrastruttura di dati e storage in AWS.

Ruolo 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.

Accedere alla "Console BlueXP" Per iniziare a utilizzare il connettore con BlueXP.

Chiave di accesso AWS

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

Fasi

1. Assicurarsi che il connettore corretto sia attualmente selezionato in BlueXP.
2. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

3. 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.

Accedere alla "Console BlueXP" Per iniziare a utilizzare il connettore con BlueXP.

Azure

Opzioni di installazione del connettore in Azure

Esistono diversi modi per creare un connettore in Azure. Direttamente da BlueXP è il

modo più comune.

Sono disponibili le seguenti opzioni di installazione:

- "Crea un connettore direttamente da BlueXP" (questa è l'opzione standard)

  Questa azione avvia una macchina virtuale che esegue Linux e il software del connettore in un VNET a scelta.

- "Creare un connettore da Azure Marketplace"

  Questa azione avvia anche una macchina virtuale con Linux e il software Connector, ma l'implementazione viene avviata direttamente da Azure Marketplace e non da BlueXP.

- "Scaricare e installare manualmente il software sul proprio host Linux"

L'opzione di installazione scelta influisce sul modo in cui si prepara l'installazione. Ciò include il modo in cui si forniscono a BlueXP le autorizzazioni necessarie per autenticare e gestire le risorse in Azure.

Creare un connettore in Azure da BlueXP

Per creare un connettore in Azure da BlueXP, devi configurare il networking, preparare le autorizzazioni di Azure e quindi creare il connettore.

Prima di iniziare

Dovresti rivedere "Limitazioni del connettore".

Fase 1: Configurare la rete

Assicurarsi che la posizione di rete in cui si intende installare il connettore supporti i seguenti requisiti. Il connettore, che soddisfa questi requisiti, consente di gestire le risorse e i processi all'interno del tuo ambiente di cloud ibrido.

Regione di Azure

Se si utilizza Cloud Volumes ONTAP, il connettore deve essere implementato nella stessa area Azure dei sistemi Cloud Volumes ONTAP gestiti o in "Coppia di regioni Azure" Per i sistemi Cloud Volumes ONTAP. Questo requisito garantisce l'utilizzo di una connessione Azure Private link tra Cloud Volumes ONTAP e i relativi account di storage associati.

"Scopri come Cloud Volumes ONTAP utilizza un collegamento privato Azure"

VNET e subnet

Quando si crea il connettore, è necessario specificare il VNET e la subnet in cui deve risiedere il connettore.

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete alla posizione in cui si intende creare e gestire gli ambienti di lavoro. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema storage nel tuo ambiente on-premise.

Accesso a Internet in uscita

La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

Endpoint contattati dal connettore

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 per le operazioni quotidiane.

Si noti che gli endpoint elencati di seguito sono tutte le voci CNAME.

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.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Per gestire le risorse nelle regioni Azure China.
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	Per aggiornare il connettore e i relativi componenti Docker.

Endpoint contattati dalla console BlueXP

Quando utilizzi la console basata sul web BlueXP fornita attraverso il layer SaaS, contatta diversi endpoint per completare le attività di gestione dei dati. Sono inclusi gli endpoint che vengono contattati per implementare il connettore dalla console BlueXP.

"Visualizzare l'elenco degli endpoint contattati dalla console BlueXP".

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"

Una volta creato il connettore, sarà necessario implementare questo requisito di rete.

Passaggio 2: Creare un ruolo personalizzato

Creare un ruolo personalizzato Azure che è possibile assegnare all'account Azure o a un'entità del servizio Microsoft Entra. BlueXP esegue l'autenticazione con Azure e utilizza queste autorizzazioni per creare l'istanza di Connector per conto dell'utente.

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. Copiare le autorizzazioni richieste per un nuovo ruolo personalizzato in Azure e salvarle in un file JSON.

> Questo ruolo personalizzato contiene solo le autorizzazioni necessarie per avviare la macchina virtuale del connettore in Azure da BlueXP. Non utilizzare questa policy per altre situazioni. Quando BlueXP crea il connettore, applica un nuovo set di autorizzazioni alla macchina virtuale del connettore che consente al connettore di gestire le risorse nell'ambiente di cloud pubblico.

```
{
    "Name": "Azure SetupAsService",
    "Actions": [
        "Microsoft.Compute/disks/delete",
```

```
        "Microsoft.Compute/disks/read",
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/locations/operations/read",
        "Microsoft.Compute/operations/read",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/extensions/write",
        "Microsoft.Compute/virtualMachines/extensions/read",
        "Microsoft.Compute/availabilitySets/read",
        "Microsoft.Network/locations/operationResults/read",
        "Microsoft.Network/locations/operations/read",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
        "Microsoft.Network/networkInterfaces/ipConfigurations/read",
        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "Microsoft.Resources/resources/read",
        "Microsoft.Resources/subscriptions/operationresults/read",
```

```
        "Microsoft.Resources/subscriptions/resourceGroups/delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}
```

2. Modificare il JSON aggiungendo il proprio ID di abbonamento Azure all'ambito assegnabile.

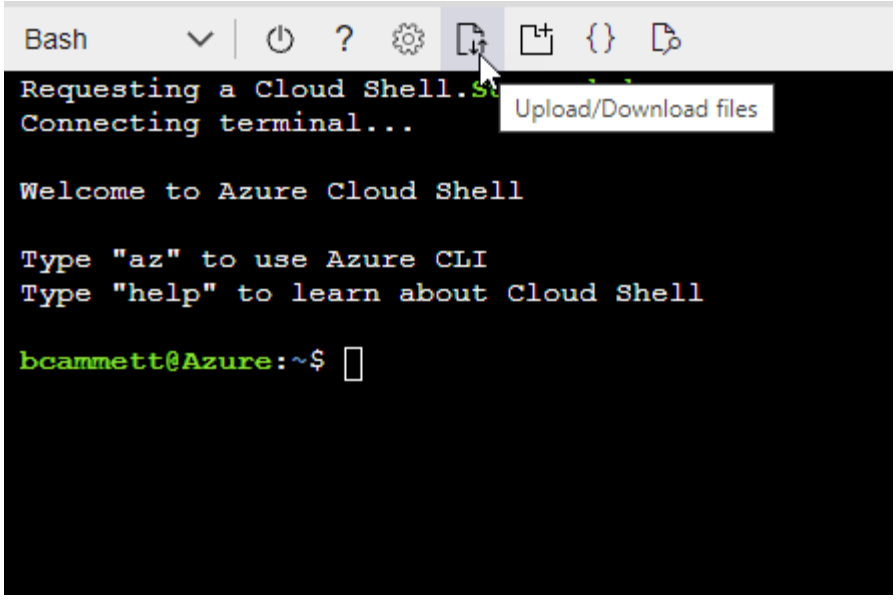
   Esempio

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

3. 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. Immettere il seguente comando Azure CLI:

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

Ora dovresti avere un ruolo personalizzato chiamato *Azure SetupAsService*. È ora possibile applicare questo ruolo personalizzato al proprio account utente o a un service principal.

Fase 3: Configurare l'autenticazione

Quando si crea il connettore da BlueXP, è necessario fornire un login che consenta a BlueXP di autenticarsi con Azure e implementare la macchina virtuale. Sono disponibili due opzioni:

1. Accedi con l'account Azure quando richiesto. Questo account deve disporre di autorizzazioni Azure specifiche. Questa è l'opzione predefinita.
2. Fornire dettagli su un'entità del servizio Microsoft Entra. Questa entità del servizio richiede anche autorizzazioni specifiche.

Seguire la procedura per preparare uno di questi metodi di autenticazione per l'utilizzo con BlueXP.

Account Azure

Assegnare il ruolo personalizzato all'utente che implementerà il connettore da BlueXP.

Fasi

1. Nel portale Azure, aprire il servizio **Subscriptions** e selezionare l'abbonamento dell'utente.
2. Fare clic su **controllo di accesso (IAM)**.
3. Fare clic su **Aggiungi** > **Aggiungi assegnazione ruolo** e aggiungere le autorizzazioni:
   a. Selezionare il ruolo **Azure SetupAsService** e fare clic su **Avanti**.

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

   b. Mantieni selezionata l'opzione **User, group o service principal**.
   c. Fare clic su **Select members** (Seleziona membri), scegliere il proprio account utente e fare clic su **Select** (Seleziona).
   d. Fare clic su **Avanti**.
   e. Fare clic su **Rivedi + assegna**.

Risultato

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

Principale del servizio

Invece di effettuare l'accesso con l'account Azure, è possibile fornire a BlueXP le credenziali per un'entità del servizio Azure che dispone delle autorizzazioni necessarie.

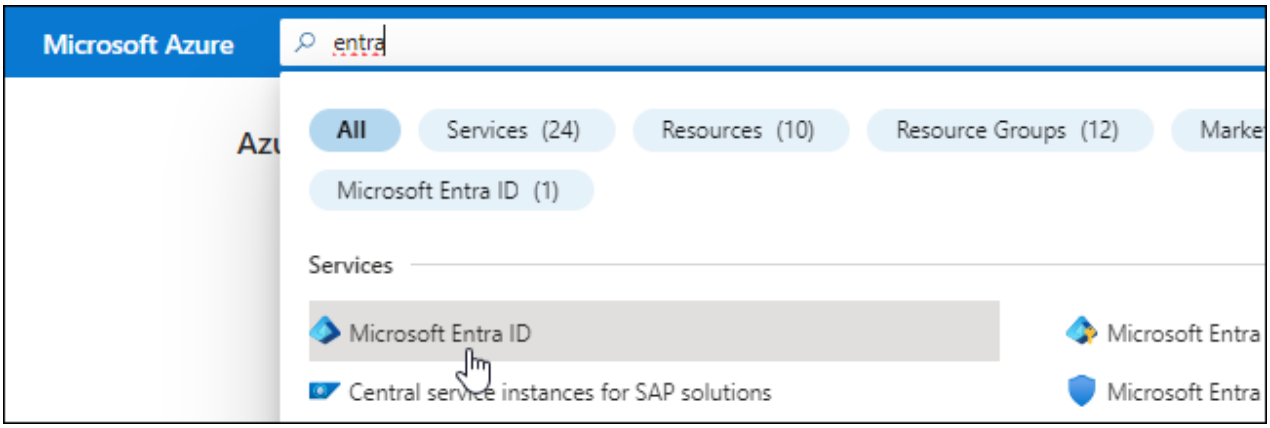
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP.

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**.

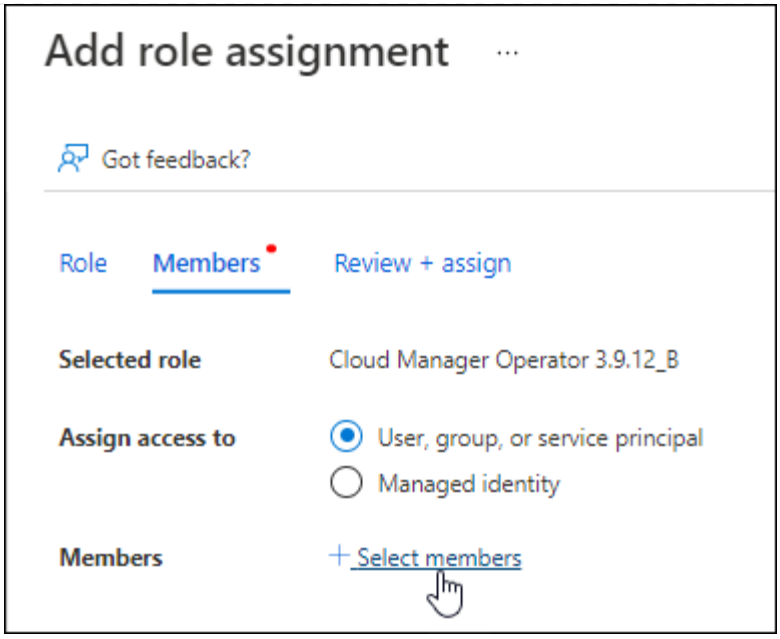
   Hai creato l'applicazione ad e il service principal.

Assegnare il ruolo personalizzato all'applicazione

1. Dal portale Azure, aprire il servizio **Subscriptions**.
2. Selezionare l'abbonamento.
3. Fare clic su **Access control (IAM) > Add > Add role assignment** (controllo accesso (IAM) > Add > Add role assign
4. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e fare clic su **Avanti**.
5. Nella scheda **membri**, completare la seguente procedura:

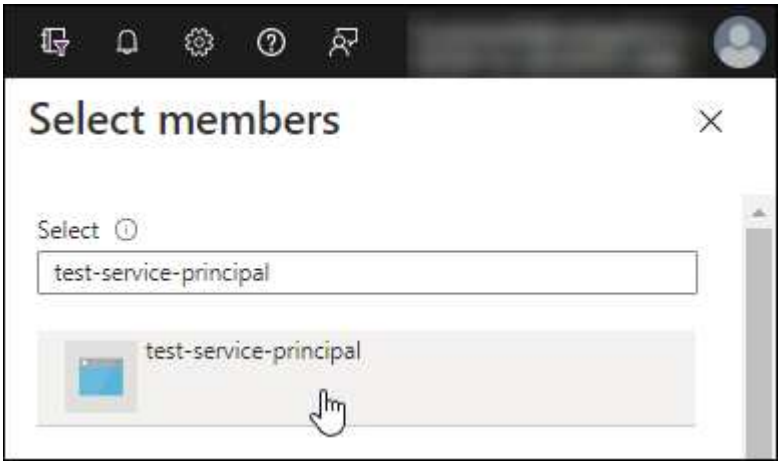
   a. Mantieni selezionata l'opzione **User, group o service principal**.

   b. Fare clic su **Seleziona membri**.



c. Cercare il nome dell'applicazione.

   Ecco un esempio:



a. Selezionare l'applicazione e fare clic su **Select** (Seleziona).
b. Fare clic su **Avanti**.

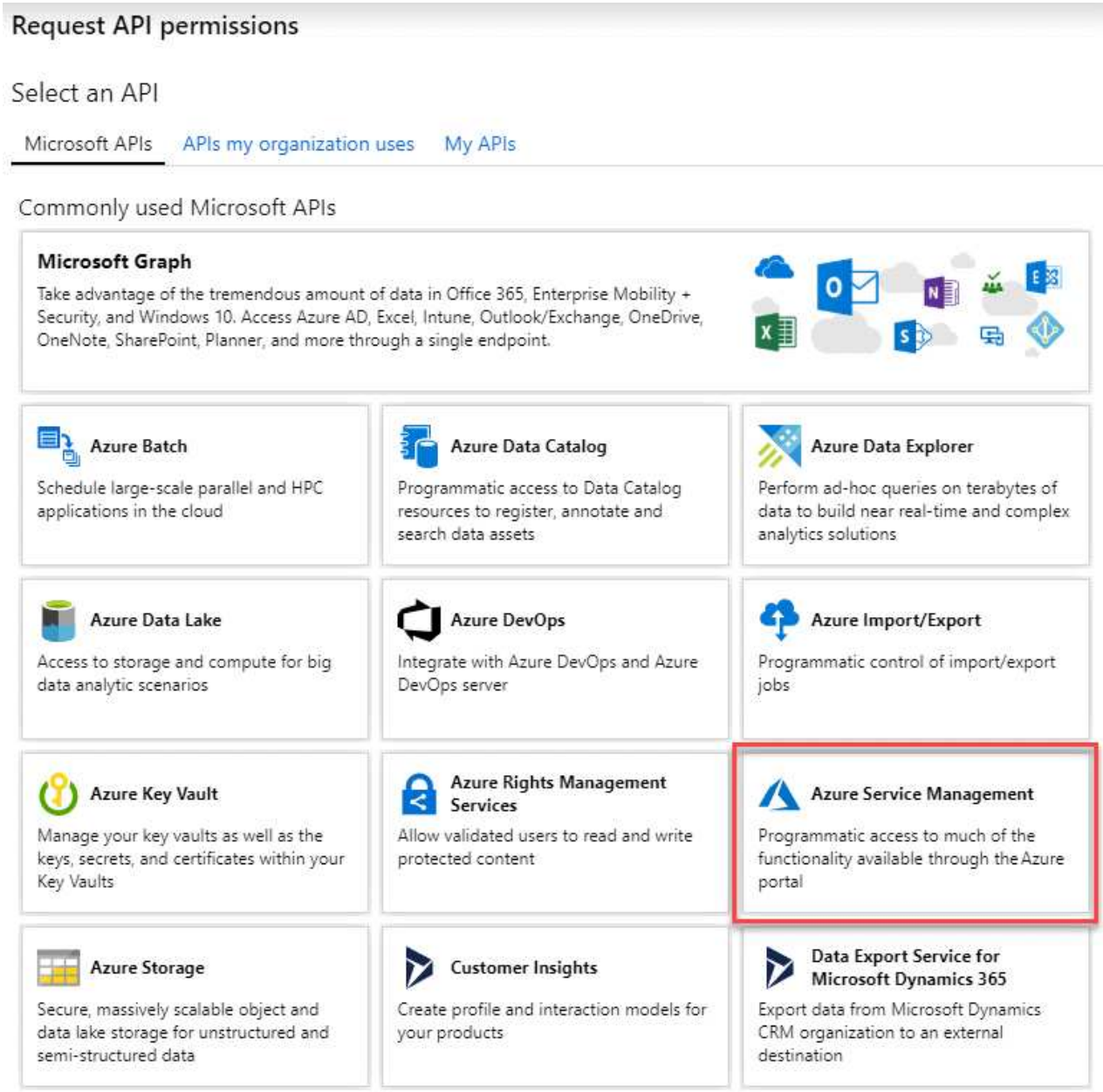
6. Fare clic su **Rivedi + assegna**.

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

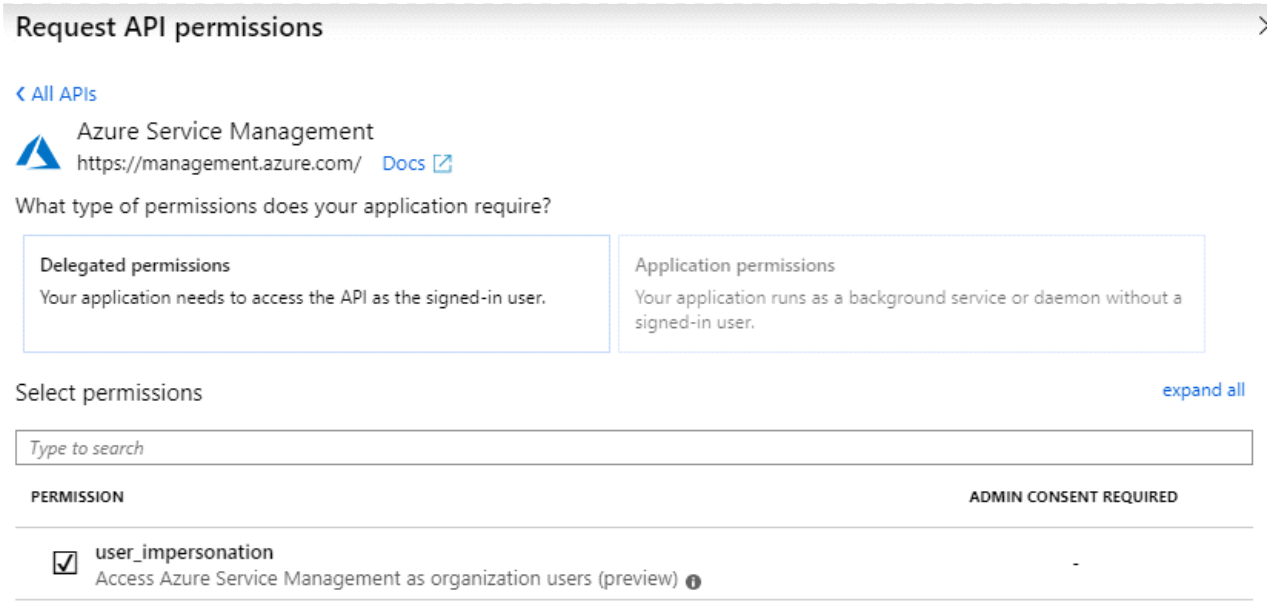
   Se si desidera gestire le risorse in più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. Ad esempio, BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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**.

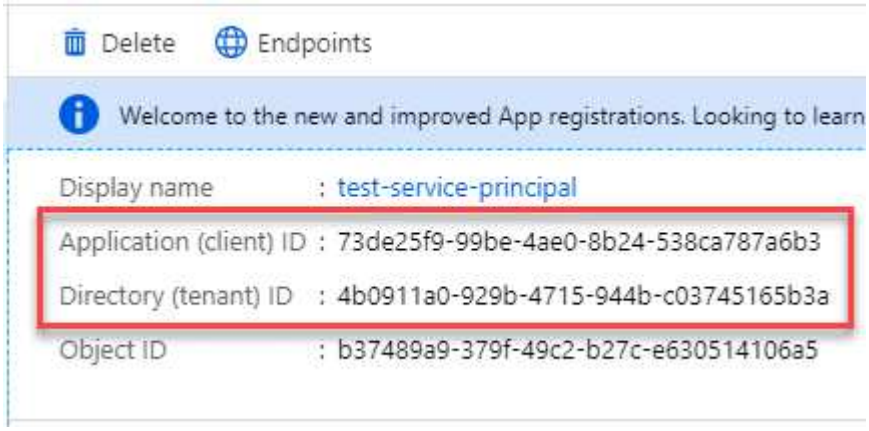


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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. Inserire queste informazioni in BlueXP quando si crea il connettore.

Fase 4: Creare il connettore

Creare il connettore direttamente dalla console BlueXP basata sul Web.

A proposito di questa attività

La creazione del connettore da BlueXP implementa una macchina virtuale in Azure usando una configurazione predefinita. Dopo aver creato il connettore, non si dovrebbe passare a un tipo di VM più piccolo che abbia meno CPU o RAM. "Informazioni sulla configurazione predefinita del connettore".

Prima di iniziare

Dovresti disporre di quanto segue:

- Un abbonamento Azure.
- Una VNET e una subnet nella regione Azure desiderata.
- Dettagli su un server proxy, se l'organizzazione richiede un proxy per tutto il traffico Internet in uscita:
  - Indirizzo IP
  - Credenziali
  - Certificato HTTPS
- Una chiave pubblica SSH, se si desidera utilizzare tale metodo di autenticazione per la macchina virtuale Connector. L'altra opzione per il metodo di autenticazione consiste nell'utilizzare una password.

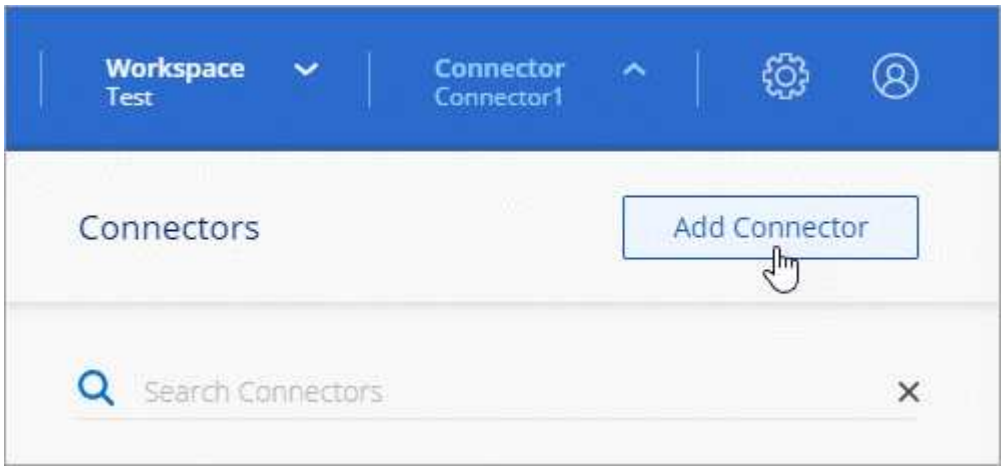
  "Scopri di più sulla connessione a una macchina virtuale Linux in Azure"

- Se non si desidera che BlueXP crei automaticamente un ruolo Azure per il connettore, sarà necessario crearne uno personalizzato "utilizzando il criterio riportato in questa pagina".

  Queste autorizzazioni sono valide per l'istanza del connettore. Si tratta di un set di autorizzazioni diverso da quello precedentemente impostato per l'implementazione della macchina virtuale del connettore.

Fasi

1. Selezionare l'elenco a discesa **Connector** (connettore) e selezionare **Add Connector** (Aggiungi connettore).



2. Scegli **Microsoft Azure** come tuo cloud provider.
3. Nella pagina **implementazione di un connettore**:

   a. In **Authentication** (autenticazione), selezionare l'opzione di autenticazione che corrisponde alla modalità di impostazione delle autorizzazioni Azure:

      - Selezionare **account utente Azure** per accedere all'account Microsoft, che dovrebbe disporre delle autorizzazioni necessarie.

        Il modulo è di proprietà e ospitato da Microsoft. Le tue credenziali non vengono fornite a NetApp.

        > Se hai già effettuato l'accesso a un account Azure, BlueXP utilizzerà automaticamente tale account. Se disponi di più account, potrebbe essere necessario prima disconnettersi per assicurarsi di utilizzare l'account corretto.

      - Selezionare **identità servizio Active Directory** per immettere le informazioni sull'entità del servizio Microsoft Entra che concede le autorizzazioni richieste:
        - ID dell'applicazione (client)
        - ID directory (tenant)
        - Segreto del client

   Scopri come ottenere questi valori per un service principal.

4. Seguire i passaggi della procedura guidata per creare il connettore:

   - **VM Authentication**: Scegliere un abbonamento Azure, una posizione, un nuovo gruppo di risorse o un gruppo di risorse esistente, quindi scegliere un metodo di autenticazione per la macchina virtuale Connector che si sta creando.

     Il metodo di autenticazione per la macchina virtuale può essere una password o una chiave pubblica SSH.

   "Scopri di più sulla connessione a una macchina virtuale Linux in Azure"

   - **Dettagli**: Immettere un nome per l'istanza, specificare i tag e scegliere se si desidera che BlueXP crei un nuovo ruolo con le autorizzazioni richieste o se si desidera selezionare un ruolo esistente impostato "le autorizzazioni richieste".

     Nota: Puoi scegliere le sottoscrizioni Azure associate a questo ruolo. Ogni abbonamento scelto

fornisce le autorizzazioni di connessione per gestire le risorse in tale abbonamento (ad esempio, Cloud Volumes ONTAP).

- **Rete**: Scegliere un VNET e una subnet, se attivare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.
- **Security Group**: Scegliere se creare un nuovo gruppo di sicurezza o se selezionare un gruppo di sicurezza esistente che consenta le regole in entrata e in uscita richieste.

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

- **Revisione**: Controllare le selezioni per verificare che la configurazione sia corretta.

5. Fare clic su **Aggiungi**.

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

Risultato

Una volta completato il processo, il connettore è disponibile per l'utilizzo da parte di BlueXP.

Se disponi di storage Azure Blob nella stessa iscrizione di Azure in cui hai creato il connettore, visualizzerai automaticamente un ambiente di lavoro dello storage di Azure Blob su BlueXP Canvas. "Scopri come gestire lo storage BLOB di Azure da BlueXP"

Creare un connettore da Azure Marketplace

Per creare un connettore da Azure Marketplace, è necessario configurare la rete, preparare le autorizzazioni di Azure, rivedere i requisiti delle istanze e quindi creare il connettore.

Prima di iniziare

Dovresti rivedere "Limitazioni del connettore".

Fase 1: Configurare la rete

Assicurarsi che la posizione di rete in cui si intende installare il connettore supporti i seguenti requisiti. Il connettore, che soddisfa questi requisiti, consente di gestire le risorse e i processi all'interno del tuo ambiente di cloud ibrido.

Regione di Azure

Se si utilizza Cloud Volumes ONTAP, il connettore deve essere implementato nella stessa area Azure dei sistemi Cloud Volumes ONTAP gestiti o in "Coppia di regioni Azure" Per i sistemi Cloud Volumes ONTAP. Questo requisito garantisce l'utilizzo di una connessione Azure Private link tra Cloud Volumes ONTAP e i relativi account di storage associati.

"Scopri come Cloud Volumes ONTAP utilizza un collegamento privato Azure"

VNET e subnet

Quando si crea il connettore, è necessario specificare il VNET e la subnet in cui deve risiedere il connettore.

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete alla posizione in cui si intende creare e gestire gli ambienti di lavoro. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema storage nel tuo ambiente on-premise.

Accesso a Internet in uscita

La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

Endpoint contattati dal connettore

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 per le operazioni quotidiane.

Si noti che gli endpoint elencati di seguito sono tutte le voci CNAME.

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.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Per gestire le risorse nelle regioni Azure China.
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	Per aggiornare il connettore e i relativi componenti Docker.

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"

Una volta creato il connettore, sarà necessario implementare questo requisito di rete.

Fase 2: Esaminare i requisiti della VM

Quando si crea il connettore, è necessario scegliere un tipo di macchina virtuale che soddisfi i seguenti requisiti.

CPU

4 core o 4 vCPU

RAM

14 GB

Dimensione delle macchine virtuali Azure

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

Passaggio 3: Impostare le autorizzazioni

È possibile fornire le autorizzazioni nei seguenti modi:

- Opzione 1: Assegnare un ruolo personalizzato alla macchina virtuale Azure utilizzando un'identità gestita assegnata dal sistema.
- Opzione 2: Fornire a BlueXP le credenziali per un'entità del servizio Azure che dispone delle autorizzazioni necessarie.

Segui questa procedura per configurare le autorizzazioni per BlueXP.

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"

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.

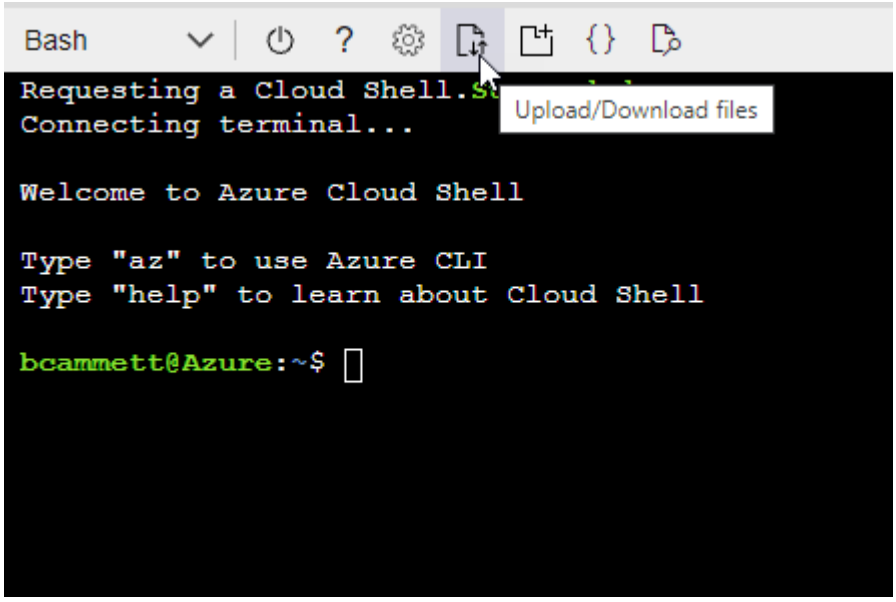
   Esempio

   ```
   "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.

Principale del servizio

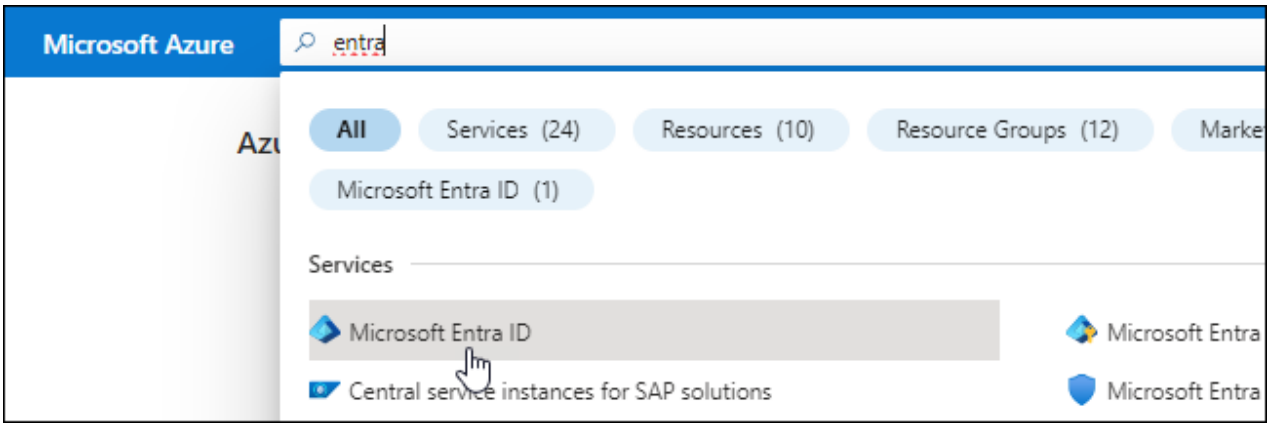
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP.

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.

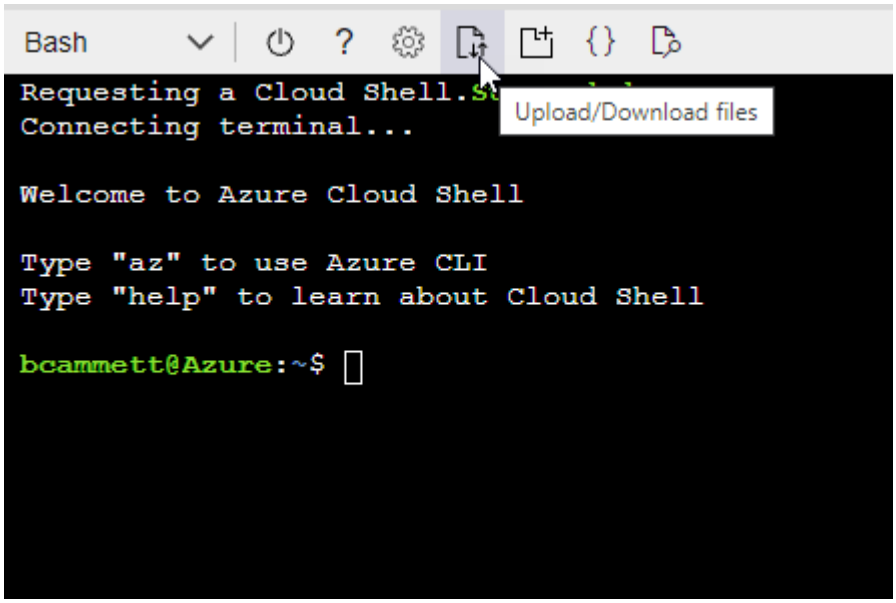
   Esempio

```
"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
```

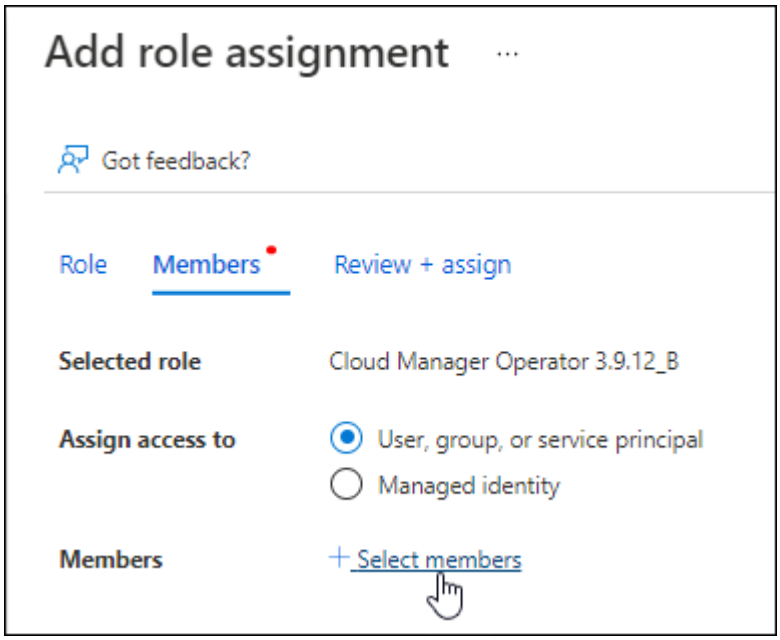
   A questo punto, dovrebbe essere disponibile un ruolo personalizzato denominato BlueXP

Operator che è possibile assegnare alla macchina virtuale Connector.

2. Assegnare l'applicazione al ruolo:

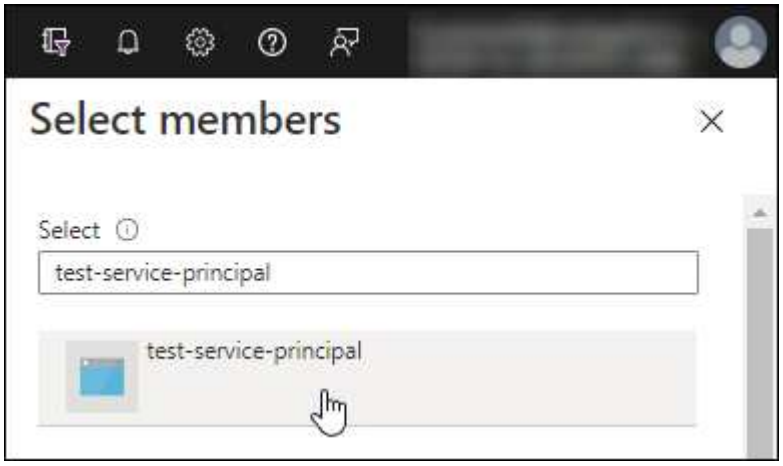
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

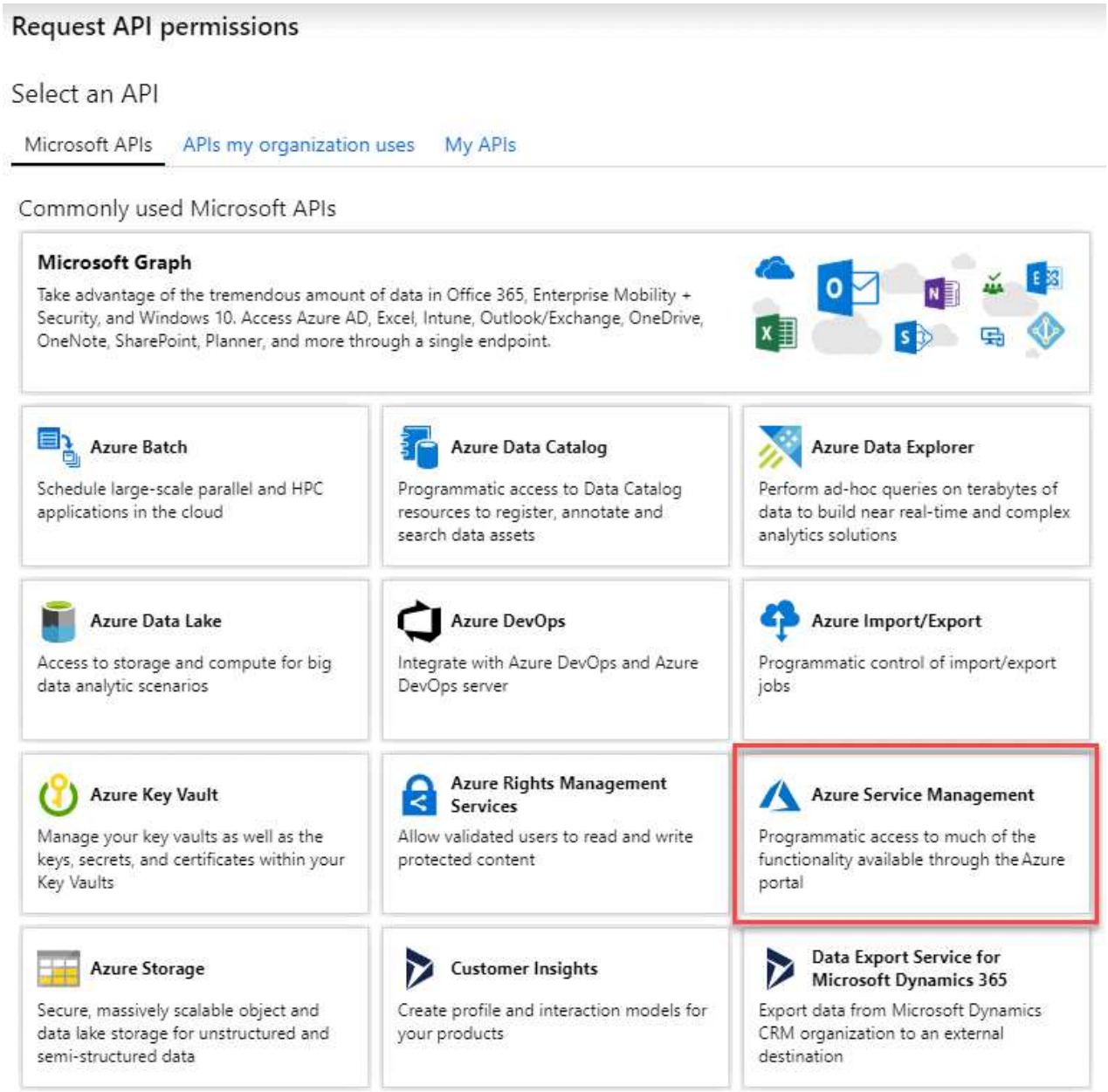
f. Selezionare **Rivedi + assegna**.

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

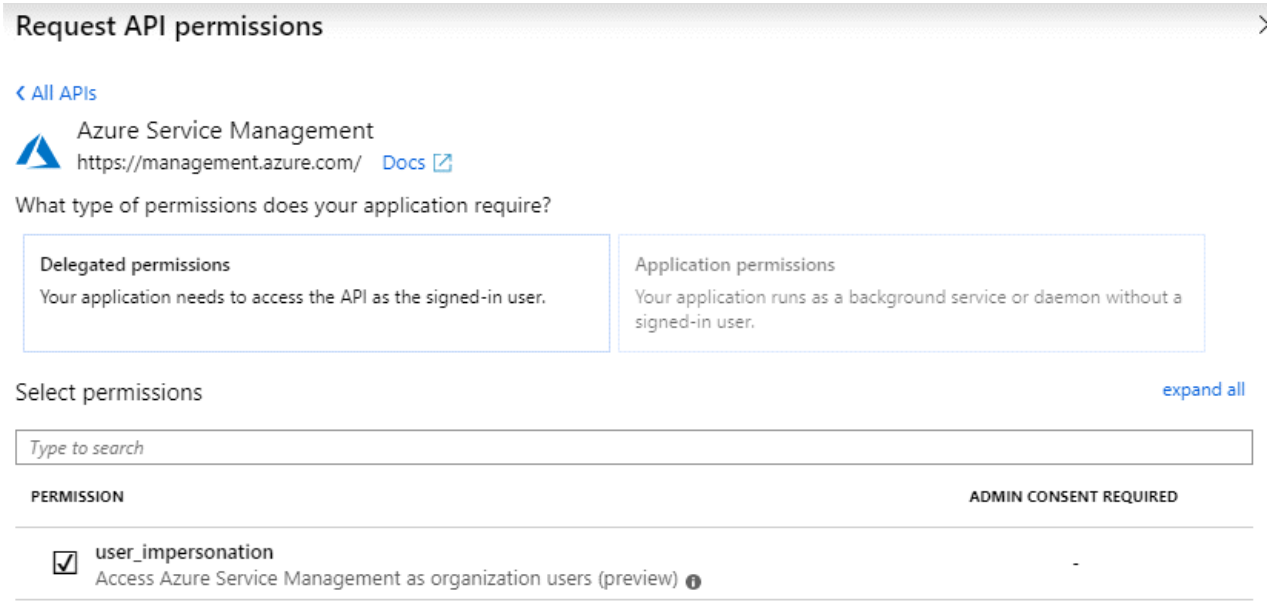
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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**.

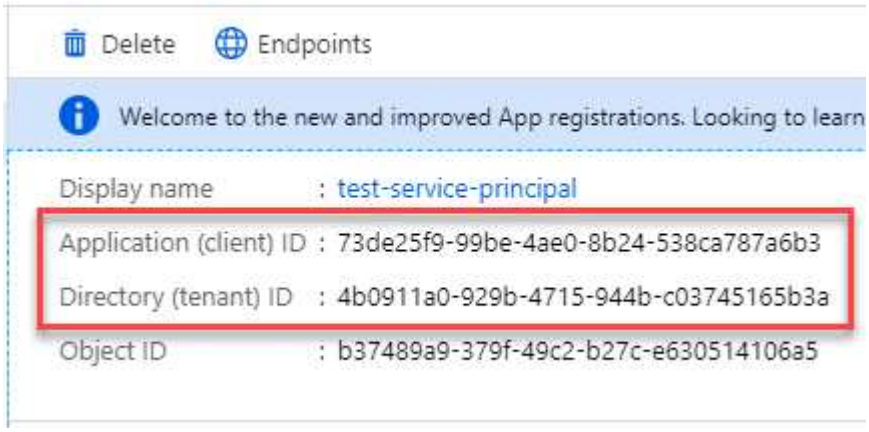


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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.

Fase 4: Creare il connettore

Avviare il connettore direttamente da Azure Marketplace.

A proposito di questa attività

La creazione del connettore da Azure Marketplace implementa una macchina virtuale in Azure utilizzando una configurazione predefinita. "Informazioni sulla configurazione predefinita del connettore".

Prima di iniziare

Dovresti disporre di quanto segue:

- Un abbonamento Azure.
- Una VNET e una subnet nella regione Azure desiderata.
- Dettagli su un server proxy, se l'organizzazione richiede un proxy per tutto il traffico Internet in uscita:
  - Indirizzo IP
  - Credenziali
  - Certificato HTTPS
- Una chiave pubblica SSH, se si desidera utilizzare tale metodo di autenticazione per la macchina virtuale Connector. L'altra opzione per il metodo di autenticazione consiste nell'utilizzare una password.

  "Scopri di più sulla connessione a una macchina virtuale Linux in Azure"

- Se non si desidera che BlueXP crei automaticamente un ruolo Azure per il connettore, sarà necessario crearne uno personalizzato "utilizzando il criterio riportato in questa pagina".

  Queste autorizzazioni sono valide per l'istanza del connettore. Si tratta di un set di autorizzazioni diverso da quello precedentemente impostato per l'implementazione della macchina virtuale del connettore.

Fasi

1. Accedere alla pagina NetApp Connector VM in Azure Marketplace.

"Pagina di Azure Marketplace per le regioni commerciali"

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.
   - **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.

   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.

5. Aprire un browser Web da un host connesso alla macchina virtuale Connector e immettere il seguente URL:

   https://ipaddress

6. Dopo aver effettuato l'accesso, configurare il connettore:
   a. Specificare l'account BlueXP da associare al connettore.
   b. Immettere un nome per il sistema.
   c. In **stai eseguendo in un ambiente protetto?** Mantieni disattivata la modalità limitata.

      La modalità limitata deve essere disattivata perché questa procedura descrive come utilizzare BlueXP in modalità standard. Attivare la modalità limitata solo se si dispone di un ambiente sicuro e si desidera disconnettere questo account dai servizi di back-end BlueXP. In tal caso, "Segui i passaggi per iniziare a utilizzare BlueXP in modalità limitata".

   d. Selezionare **Let's start**.

Risultato

Il connettore è ora installato e configurato con l'account BlueXP.

Se disponi di storage Azure Blob nella stessa iscrizione di Azure in cui hai creato il connettore, visualizzerai automaticamente un ambiente di lavoro dello storage di Azure Blob su BlueXP Canvas. "Scopri come gestire lo storage BLOB di Azure da BlueXP"

Fase 5: Fornire le autorizzazioni ad BlueXP

Una volta creato il connettore, devi fornire ad BlueXP le autorizzazioni impostate in precedenza. La fornitura delle autorizzazioni consente a BlueXP di gestire l'infrastruttura di dati e storage in Azure.

Ruolo personalizzato

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.

Quali sono le prossime novità?

Accedere alla "Console BlueXP" Per iniziare a utilizzare il connettore con BlueXP.

Principale del servizio

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.

Installare manualmente il connettore in Azure

Per installare manualmente il connettore sul proprio host Linux, è necessario rivedere i requisiti dell'host, configurare la rete, preparare le autorizzazioni di Azure, installare il connettore e quindi fornire le autorizzazioni preparate.

Prima di iniziare

Dovresti rivedere "Limitazioni del connettore".

Fase 1: 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

Dimensione delle macchine virtuali Azure

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

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 2: Configurare la rete

Assicurarsi che la posizione di rete in cui si intende installare il connettore supporti i seguenti requisiti. Il connettore, che soddisfa questi requisiti, consente di gestire le risorse e i processi all'interno del tuo ambiente di cloud ibrido.

Regione di Azure

Se si utilizza Cloud Volumes ONTAP, il connettore deve essere implementato nella stessa area Azure dei sistemi Cloud Volumes ONTAP gestiti o in "Coppia di regioni Azure" Per i sistemi Cloud Volumes ONTAP. Questo requisito garantisce l'utilizzo di una connessione Azure Private link tra Cloud Volumes ONTAP e i relativi account di storage associati.

"Scopri come Cloud Volumes ONTAP utilizza un collegamento privato Azure"

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete alla posizione in cui si intende creare e gestire gli ambienti di lavoro. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema storage nel tuo ambiente on-premise.

Accesso a Internet in uscita

La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

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

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

Endpoint contattati dal connettore

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 per le operazioni quotidiane.

Si noti che gli endpoint elencati di seguito sono tutte le voci CNAME.

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.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Per gestire le risorse nelle regioni Azure China.
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	Per aggiornare il connettore e i relativi componenti Docker.

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"

Passaggio 3: Impostare le autorizzazioni

Devi fornire le autorizzazioni di Azure a BlueXP tramite una delle seguenti opzioni:

- Opzione 1: Assegnare un ruolo personalizzato alla macchina virtuale Azure utilizzando un'identità gestita assegnata dal sistema.
- Opzione 2: Fornire a BlueXP le credenziali per un'entità del servizio Azure che dispone delle autorizzazioni necessarie.

Segui i passaggi per preparare le autorizzazioni per BlueXP.

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"

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.

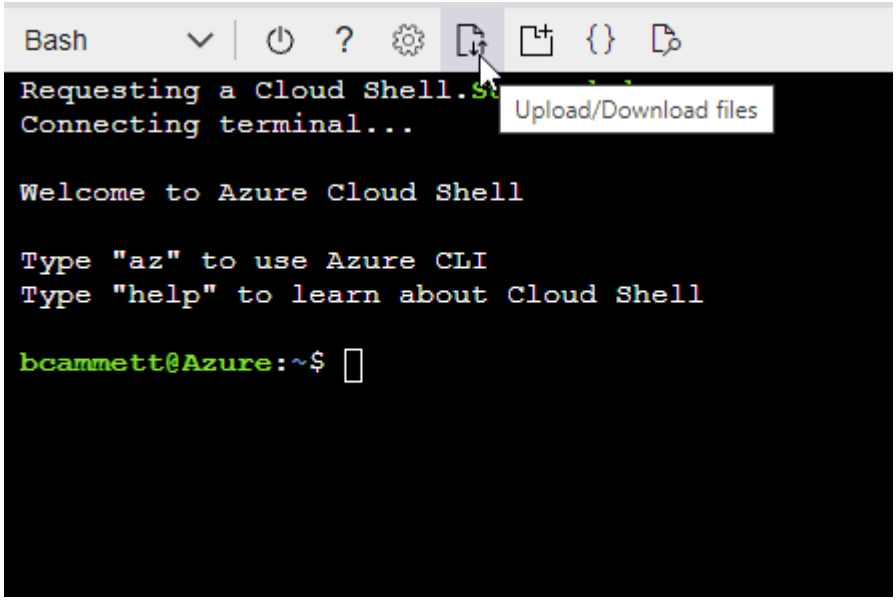
   Esempio

   ```
   "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.

Principale del servizio

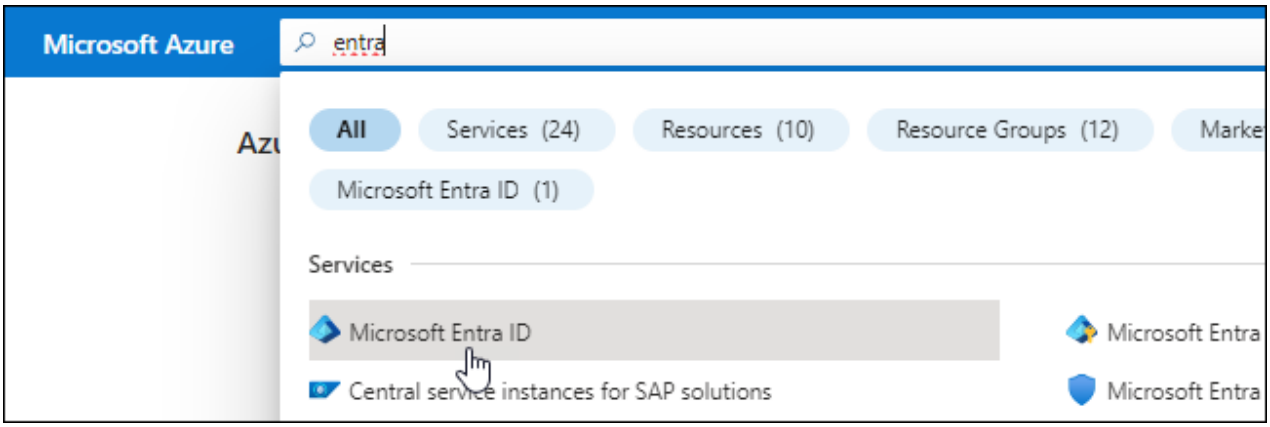
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP.

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.

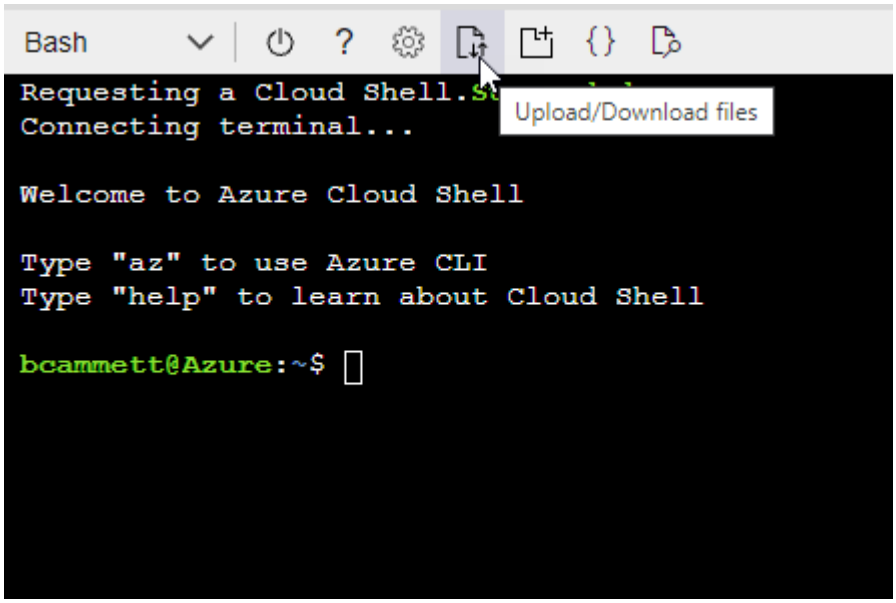
   Esempio

```
"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
```

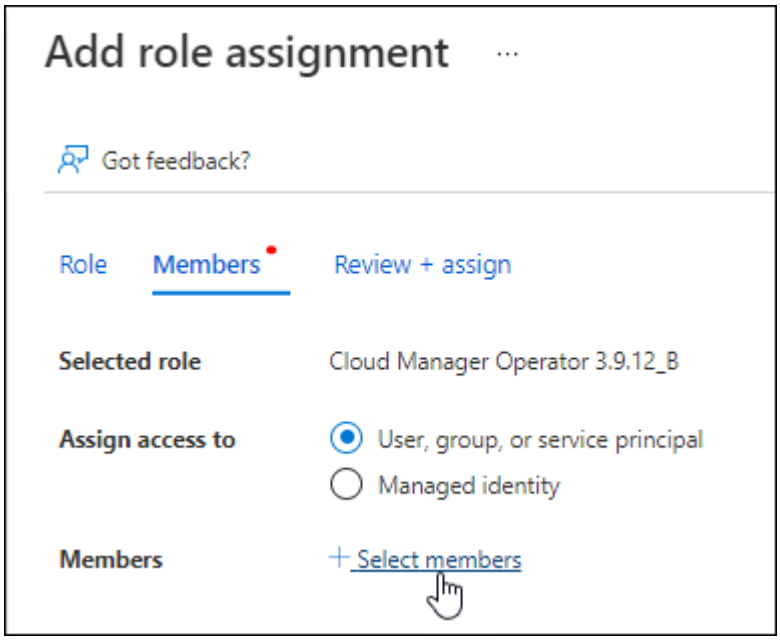
   A questo punto, dovrebbe essere disponibile un ruolo personalizzato denominato BlueXP

Operator che è possibile assegnare alla macchina virtuale Connector.

2. Assegnare l'applicazione al ruolo:

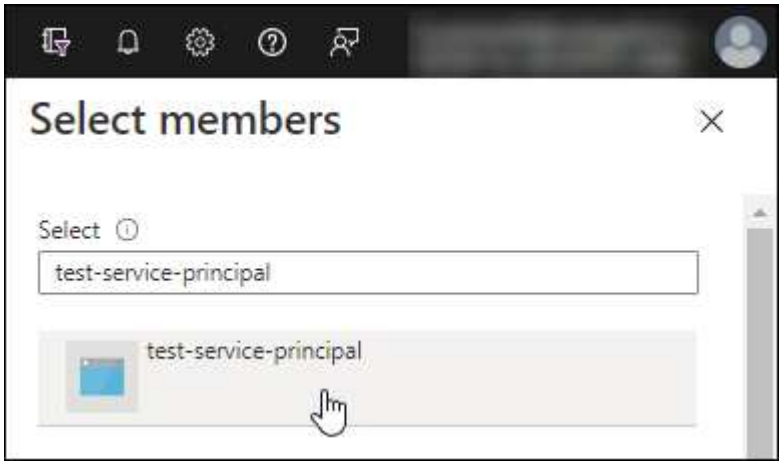
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

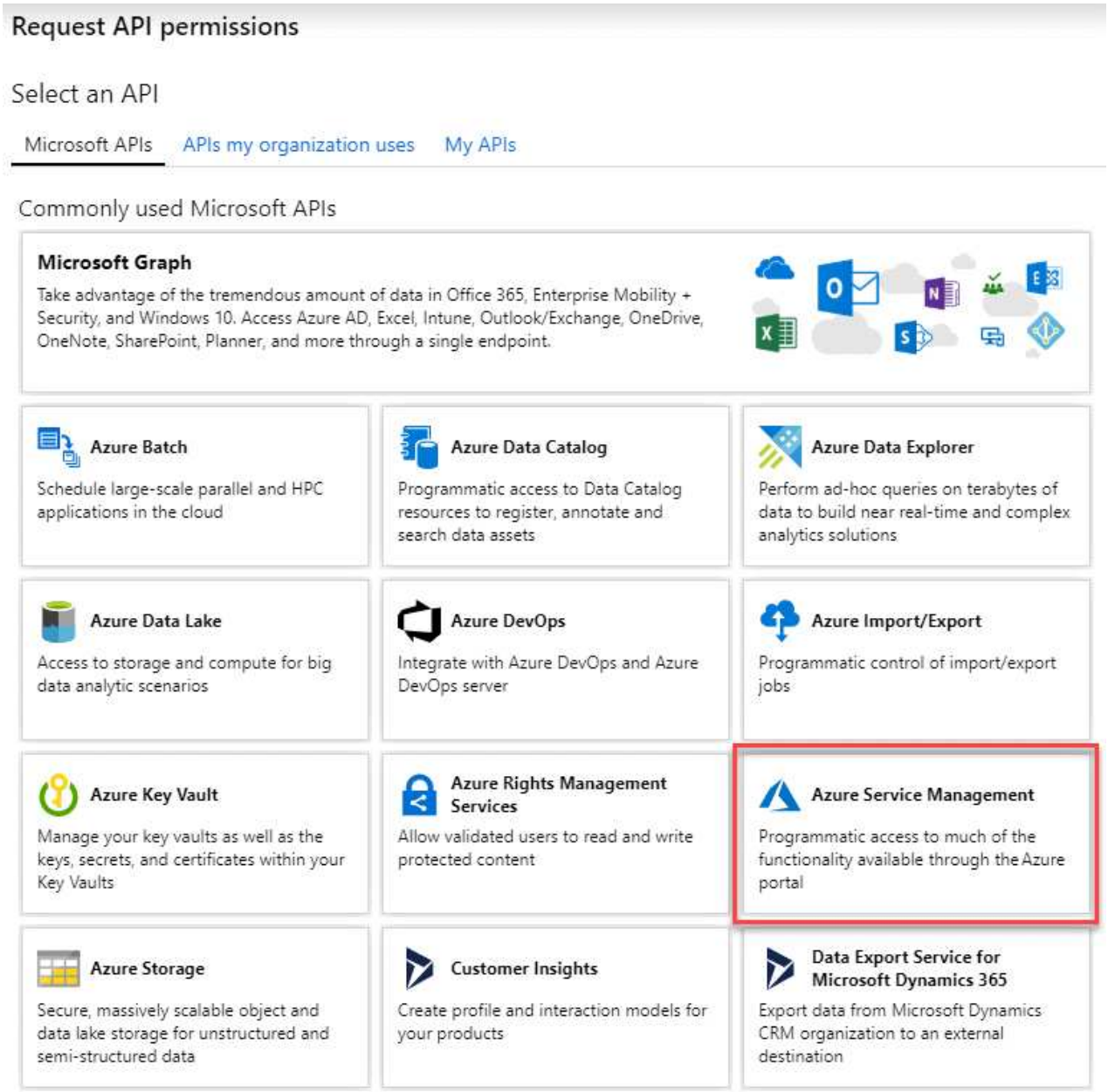
f. Selezionare **Rivedi + assegna**.

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

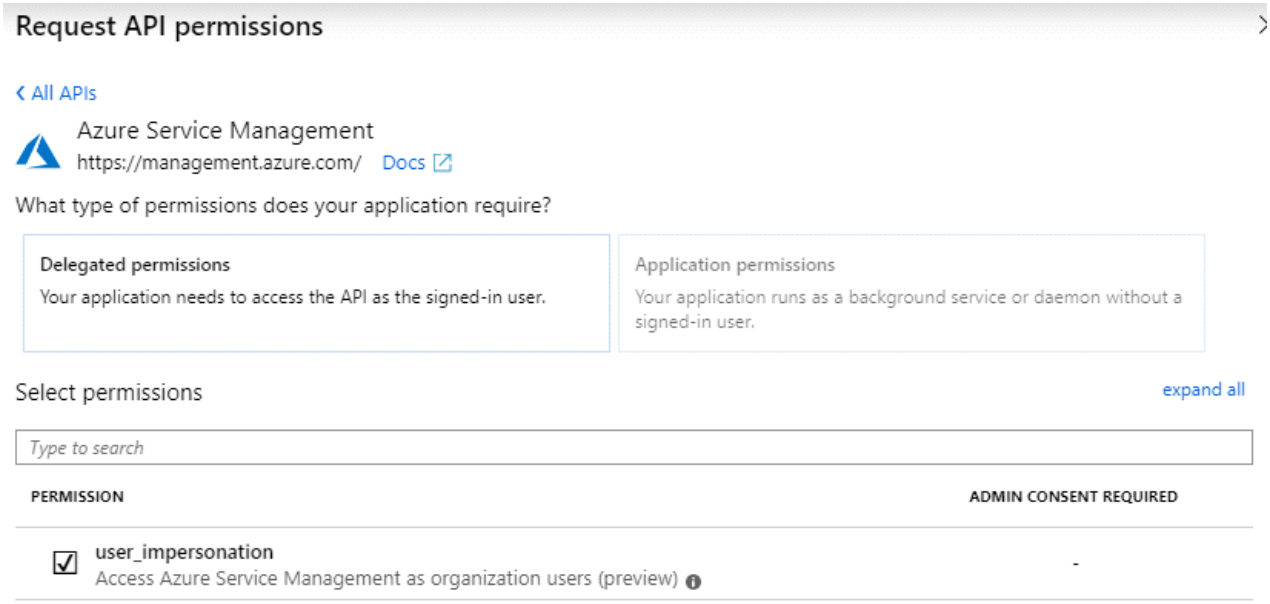
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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**.

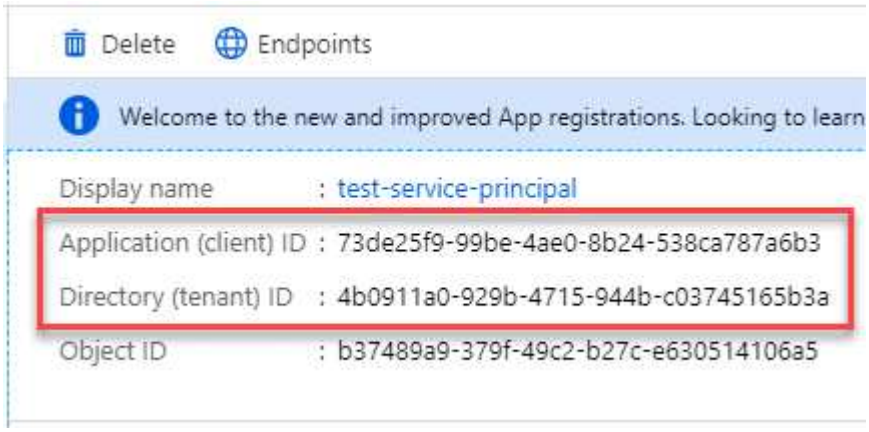


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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.

Fase 4: Installare il connettore

Una volta completati i prerequisiti, è possibile installare manualmente il software sul proprio host Linux.

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.
- Un'identità gestita abilitata sulla macchina virtuale in Azure 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"

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.

6. Attendere il completamento dell’installazione.

   Al termine dell’installazione, il servizio di connessione (occm) viene riavviato due volte se si specifica un server proxy.

7. Aprire un browser Web da un host connesso alla macchina virtuale Connector e immettere il seguente URL:

   https://ipaddress

8. Dopo aver effettuato l’accesso, configurare il connettore:
   a. Specificare l’account BlueXP da associare al connettore.
   b. Immettere un nome per il sistema.
   c. In **stai eseguendo in un ambiente protetto?** Mantieni disattivata la modalità limitata.

      La modalità limitata deve essere disattivata perché questa procedura descrive come utilizzare BlueXP in modalità standard. Attivare la modalità limitata solo se si dispone di un ambiente sicuro e si desidera disconnettere questo account dai servizi di back-end BlueXP. In tal caso, "Segui i passaggi per iniziare a utilizzare BlueXP in modalità limitata".

   d. Selezionare **Let’s start**.

Risultato

Il connettore è ora installato e configurato con l’account BlueXP.

Se disponi di storage Azure Blob nella stessa iscrizione di Azure in cui hai creato il connettore, visualizzerai automaticamente un ambiente di lavoro dello storage di Azure Blob su BlueXP Canvas. "Scopri come gestire lo storage BLOB di Azure da BlueXP"

Fase 5: Fornire le autorizzazioni ad BlueXP

Una volta installato il connettore, devi fornire ad BlueXP le autorizzazioni di Azure precedentemente configurate. La fornitura delle autorizzazioni consente a BlueXP di gestire l’infrastruttura di dati e storage in Azure.

Ruolo personalizzato

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.

Quali sono le prossime novità?

Accedere alla "Console BlueXP" Per iniziare a utilizzare il connettore con BlueXP.

Principale del servizio

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.

Google Cloud

Opzioni di installazione del connettore in Google Cloud

Esistono diversi modi per creare un connettore in Google Cloud. Direttamente da BlueXP è il modo più comune.

Sono disponibili le seguenti opzioni di installazione:

- "Creare il connettore direttamente da BlueXP" (questa è l'opzione standard)

  Questa azione avvia un'istanza della macchina virtuale che esegue Linux e il software del connettore in un VPC a scelta.

- "Creare il connettore utilizzando gcloud"

  Questa azione avvia anche un'istanza di macchina virtuale che esegue Linux e il software Connector, ma l'implementazione viene avviata direttamente da Google Cloud e non da BlueXP.

- "Scaricare e installare manualmente il software sul proprio host Linux"

L'opzione di installazione scelta influisce sul modo in cui si prepara l'installazione. Ciò include il modo in cui si forniscono a BlueXP le autorizzazioni necessarie per autenticare e gestire le risorse in Google Cloud.

Crea un connettore in Google Cloud da BlueXP o gcloud

Per creare un connettore in Google Cloud da BlueXP o usando gcloud, devi configurare la rete, preparare le autorizzazioni di Google Cloud, abilitare le API di Google Cloud e quindi creare il connettore.

Prima di iniziare

Dovresti rivedere "Limitazioni del connettore".

Fase 1: Configurare la rete

Configura il tuo networking in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud ibrido. Ad esempio, è necessario assicurarsi che le connessioni siano disponibili per le reti di destinazione e che sia disponibile l'accesso a Internet in uscita.

VPC e subnet

Quando si crea il connettore, è necessario specificare il VPC e la subnet in cui deve risiedere il connettore.

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete alla posizione in cui si intende creare e gestire gli ambienti di lavoro. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema storage nel tuo ambiente on-premise.

Accesso a Internet in uscita

La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

Endpoint contattati dal connettore

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 per le operazioni quotidiane.

Si noti che gli endpoint elencati di seguito sono tutte le voci CNAME.

Endpoint	Scopo
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.

Endpoint	Scopo
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Per aggiornare il connettore e i relativi componenti Docker.

Endpoint contattati dalla console BlueXP

Quando utilizzi la console basata sul web BlueXP fornita attraverso il layer SaaS, contatta diversi endpoint per completare le attività di gestione dei dati. Sono inclusi gli endpoint che vengono contattati per implementare il connettore dalla console BlueXP.

"Visualizzare l'elenco degli endpoint contattati dalla console BlueXP".

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"

Una volta creato il connettore, sarà necessario implementare questo requisito di rete.

Passaggio 2: Impostare le autorizzazioni per creare il connettore

Prima di poter implementare un connettore da BlueXP o utilizzando gcloud, devi impostare le autorizzazioni per l'utente Google Cloud che implementerà la macchina virtuale del connettore.

Fasi

1. Creare un ruolo personalizzato in Google Cloud:

    a. Creare un file YAML che includa le seguenti autorizzazioni:

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
```

```
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. Da Google Cloud, attiva la shell cloud.

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

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

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

   I ruoli iam di gcloud creano connectorDeployment --project=myproject --file=Connector -deployment.yaml

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

2. Assegnare questo ruolo personalizzato all'utente che implementerà il connettore da BlueXP o utilizzando gcloud.

   "Documenti di Google Cloud: Assegnare un singolo ruolo"

Risultato

L'utente di Google Cloud dispone ora delle autorizzazioni necessarie per creare il connettore.

Passaggio 3: Impostare le autorizzazioni per il connettore

Un account di servizio Google Cloud è necessario per fornire a Connector le autorizzazioni necessarie per gestire le risorse in Google Cloud. Quando si crea il connettore, è necessario associare questo account di

servizio alla macchina virtuale del connettore.

Fasi

1. Creare un ruolo personalizzato in Google Cloud:

   a. Creare un file YAML che includa il contenuto di "Autorizzazioni dell'account di servizio per il connettore".

   b. Da Google Cloud, attiva la shell cloud.

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

   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 e assegnare il ruolo all'account di servizio:

   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"

3. Se si prevede di implementare i sistemi Cloud Volumes ONTAP in progetti diversi da quello in cui si trova il connettore, è necessario fornire l'account di servizio del connettore per accedere a tali progetti.

   Ad esempio, supponiamo che il connettore si trovi nel progetto 1 e che si desideri creare sistemi Cloud Volumes ONTAP nel progetto 2. È necessario concedere l'accesso all'account di servizio nel progetto 2.

   a. Dal servizio IAM & Admin, selezionare il progetto Google Cloud in cui si desidera creare i sistemi Cloud Volumes ONTAP.

   b. Nella pagina **IAM**, selezionare **Concedi accesso** e fornire i dettagli richiesti.

      - Inserire l'indirizzo e-mail dell'account di servizio del connettore.
      - Selezionare il ruolo personalizzato del connettore.
      - Selezionare **Salva**.

   Per ulteriori informazioni, fare riferimento a. "Documentazione di Google Cloud"

Risultato

L'account di servizio per la macchina virtuale del connettore è impostato.

Passaggio 4: Impostare le autorizzazioni VPC condivise

Se si utilizza un VPC condiviso per distribuire le risorse in un progetto di servizio, è necessario preparare le autorizzazioni.

Questa tabella è di riferimento e l'ambiente deve riflettere la tabella delle autorizzazioni al termine della

configurazione IAM.

Visualizzare le autorizzazioni VPC condivise

Identità	Creatore	Ospitato in	Permessi del progetto di servizio	Permessi del progetto host	Scopo
Google per implementare il connettore	Personalizzato	Progetto di servizio	"Policy di implementazione del connettore"	compute.networkUser	Implementazione del connettore nel progetto di servizio
Account del servizio Connector	Personalizzato	Progetto di servizio	"Policy dell'account di servizio del connettore"	compute.networkUser deploymentmanager.editor	Implementazione e manutenzione di Cloud Volumes ONTAP e servizi nel progetto di servizio
Account del servizio Cloud Volumes ONTAP	Personalizzato	Progetto di servizio	storage.admin membro: Account di servizio BlueXP come serviceAccount.user	N/A.	(Opzionale) per il tiering dei dati e il backup e ripristino BlueXP
Agente del servizio API di Google	Google Cloud	Progetto di servizio	(Impostazione predefinita) Editor	compute.networkUser	Interagisce con le API di Google Cloud per conto dell'implementazione. Consente a BlueXP di utilizzare la rete condivisa.
Account di servizio predefinito di Google Compute Engine	Google Cloud	Progetto di servizio	(Impostazione predefinita) Editor	compute.networkUser	Implementa le istanze di Google Cloud e l'infrastruttura di calcolo per conto dell'implementazione. Consente a BlueXP di utilizzare la rete condivisa.

Note:

1. Deploymentmanager.editor è necessario solo per il progetto host se non si passano le regole del firewall alla distribuzione e si sceglie di consentire a BlueXP di crearle. BlueXP crea una distribuzione nel progetto host che contiene la regola firewall VPC0 se non viene specificata alcuna regola.
2. Firewall.create e firewall.delete sono necessari solo se non si passano le regole firewall all'implementazione e si sceglie di consentire a BlueXP di crearle. Queste autorizzazioni risiedono nel file .yaml dell'account BlueXP. Se si implementa una coppia ha utilizzando un VPC condiviso, queste autorizzazioni verranno utilizzate per creare le regole firewall per VPC1, 2 e 3. Per tutte le altre implementazioni, queste autorizzazioni verranno utilizzate anche per creare regole per VPC0.
3. Per il tiering dei dati, l'account del servizio di tiering deve avere il ruolo serviceAccount.user nell'account del servizio, non solo a livello di progetto. Attualmente, se si assegna serviceAccount.user a livello di progetto, le autorizzazioni non vengono visualizzate quando si esegue

una query all'account del servizio con getIAMPolicy.

Passaggio 5: Abilitare le API di Google Cloud

Prima di poter implementare Connector e Cloud Volumes ONTAP in Google Cloud, è necessario attivare diverse API di Google Cloud.

Fase

1. Abilita le seguenti API 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))

"Documentazione di Google Cloud: Abilitazione delle API"

Fase 6: Creare il connettore

Crea un connettore direttamente dalla console basata su web BlueXP o tramite gcloud.

A proposito di questa attività

La creazione di Connector implementa un'istanza di macchina virtuale in Google Cloud utilizzando una configurazione predefinita. Dopo aver creato il connettore, non si dovrebbe passare a un'istanza VM più piccola con meno CPU o RAM. "Informazioni sulla configurazione predefinita del connettore".

BlueXP

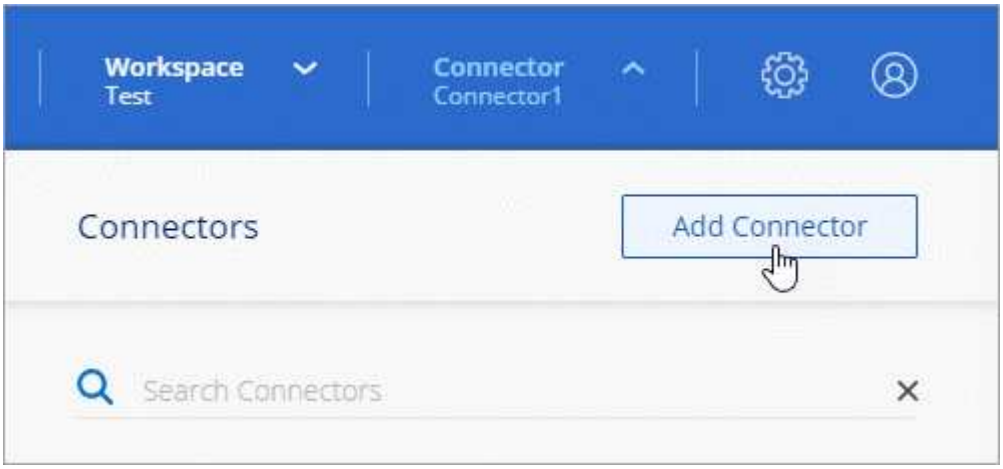
Prima di iniziare

Dovresti disporre di quanto segue:

- Le autorizzazioni necessarie per Google Cloud per creare il connettore e un account di servizio per la macchina virtuale del connettore.
- VPC e subnet che soddisfano i requisiti di rete.
- Dettagli su un server proxy, se è richiesto un proxy per l'accesso a Internet dal connettore.

Fasi

1. Selezionare l'elenco a discesa **Connector** (connettore) e selezionare **Add Connector** (Aggiungi connettore).



2. Scegli **Google Cloud Platform** come tuo cloud provider.
3. Nella pagina **Deploying a Connector** (implementazione di un connettore), consultare i dettagli relativi alle esigenze. Sono disponibili due opzioni:
   a. Selezionare **continua** per prepararsi all'implementazione utilizzando la guida all'interno del prodotto. Ogni fase della guida all'interno del prodotto include le informazioni contenute in questa pagina della documentazione.
   b. Selezionare **Skip to Deployment** (passa alla distribuzione) se si è già pronti seguendo la procedura riportata in questa pagina.
4. Seguire i passaggi della procedura guidata per creare il connettore:
   - Se richiesto, accedere all'account Google, che dovrebbe disporre delle autorizzazioni necessarie per creare l'istanza della macchina virtuale.

     Il modulo è di proprietà e ospitato da Google. Le tue credenziali non vengono fornite a NetApp.
   - **Dettagli**: Immettere un nome per l'istanza della macchina virtuale, specificare i tag, selezionare un progetto, quindi selezionare l'account del servizio che dispone delle autorizzazioni necessarie (per ulteriori informazioni, fare riferimento alla sezione precedente).
   - **Location**: Specificare una regione, una zona, un VPC e una subnet per l'istanza.
   - **Network** (rete): Scegliere se attivare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.
   - **Firewall Policy**: Scegliere se creare un nuovo criterio firewall o se selezionare un criterio firewall

esistente che consenta di utilizzare le regole in entrata e in uscita richieste.

"Regole del firewall in Google Cloud"

- **Revisione**: Controllare le selezioni per verificare che la configurazione sia corretta.

5. Selezionare **Aggiungi**.

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

Risultato

Una volta completato il processo, il connettore è disponibile per l'utilizzo da parte di BlueXP.

Se hai bucket di Google Cloud Storage nello stesso account Google Cloud in cui hai creato il connettore, vedrai comparire automaticamente un ambiente di lavoro di Google Cloud Storage su BlueXP Canvas. "Scopri come gestire Google Cloud Storage da BlueXP"

gcloud

Prima di iniziare

Dovresti disporre di quanto segue:

- Le autorizzazioni necessarie per Google Cloud per creare il connettore e un account di servizio per la macchina virtuale del connettore.
- VPC e subnet che soddisfano i requisiti di rete.
- Comprensione dei requisiti delle istanze di macchine virtuali.
  - **CPU**: 4 core o 4 vCPU
  - **RAM**: 14 GB
  - **Tipo di macchina**: Si consiglia n2-standard-4.

    Il connettore è supportato in Google Cloud su un'istanza VM con un sistema operativo che supporta funzioni VM schermate.

Fasi

1. Accedi a gcloud SDK utilizzando la tua metodologia preferita.

   Nei nostri esempi, utilizzeremo una shell locale con gcloud SDK installato, ma è possibile utilizzare Google Cloud Shell nativa nella console di Google Cloud.

   Per ulteriori informazioni su Google Cloud SDK, visitare il "Pagina della documentazione di Google Cloud SDK".

2. Verificare di aver effettuato l'accesso come utente con le autorizzazioni richieste definite nella sezione precedente:

   ```
   gcloud auth list
   ```

   L'output dovrebbe mostrare quanto segue dove l'account utente * è l'account utente desiderato per l'accesso:

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. Eseguire `gcloud compute instances create` comando:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

nome-istanza
: Il nome dell'istanza desiderata per l'istanza della macchina virtuale.

progetto
: (Facoltativo) il progetto in cui si desidera implementare la macchina virtuale.

account-servizio
: L'account del servizio specificato nell'output del passo 2.

zona
: La zona in cui si desidera implementare la macchina virtuale

no-address (indirizzo non assegnato)
: (Facoltativo) non viene utilizzato alcun indirizzo IP esterno (è necessario un NAT o un proxy cloud per instradare il traffico verso Internet pubblico)

tag-rete
: (Facoltativo) aggiungere tag di rete per collegare una regola firewall utilizzando tag all'istanza del connettore

percorso di rete

(Facoltativo) aggiungere il nome della rete in cui implementare il connettore (per un VPC condiviso, è necessario il percorso completo)

subnet-path

(Facoltativo) aggiungere il nome della subnet in cui implementare il connettore (per un VPC condiviso, è necessario il percorso completo)

percorso-chiave-kms

(Facoltativo) aggiungere una chiave KMS per crittografare i dischi del connettore (è necessario applicare anche le autorizzazioni IAM)

Per ulteriori informazioni su questi flag, visitare il "Documentazione di Google Cloud Compute SDK".

+
L'esecuzione del comando implementa il connettore utilizzando l'immagine Golden di NetApp. L'istanza di Connector e il software dovrebbero essere in esecuzione in circa cinque minuti.

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

   https://ipaddress

2. Dopo aver effettuato l'accesso, configurare il connettore:
   a. Specificare l'account BlueXP da associare al connettore.

      "Scopri di più sugli account BlueXP".

   b. Immettere un nome per il sistema.

Risultato

Il connettore è ora installato e configurato con l'account BlueXP.

Aprire un browser Web e accedere a. "Console BlueXP" Per iniziare a utilizzare il connettore con BlueXP.

Installare manualmente il connettore in Google Cloud

Per installare manualmente il connettore sul proprio host Linux, è necessario rivedere i requisiti dell'host, configurare la rete, preparare le autorizzazioni di Google Cloud, abilitare le API di Google Cloud, installare il connettore e quindi fornire le autorizzazioni preparate.

Prima di iniziare

Dovresti rivedere "Limitazioni del connettore".

Fase 1: 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 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 2: Configurare la rete

Configura il tuo networking in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud ibrido. Ad esempio, è necessario assicurarsi che le connessioni siano disponibili per le reti di

destinazione e che sia disponibile l'accesso a Internet in uscita.

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete alla posizione in cui si intende creare e gestire gli ambienti di lavoro. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema storage nel tuo ambiente on-premise.

Accesso a Internet in uscita

La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

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

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

Endpoint contattati dal connettore

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 per le operazioni quotidiane.

Si noti che gli endpoint elencati di seguito sono tutte le voci CNAME.

Endpoint	Scopo
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.

Endpoint	Scopo
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	Per aggiornare il connettore e i relativi componenti Docker.

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"

Passaggio 3: Impostare le autorizzazioni per il connettore

Un account di servizio Google Cloud è necessario per fornire a Connector le autorizzazioni necessarie per gestire le risorse in Google Cloud. Quando si crea il connettore, è necessario associare questo account di servizio alla macchina virtuale del connettore.

Fasi

1. Creare un ruolo personalizzato in Google Cloud:

   a. Creare un file YAML che includa il contenuto di "Autorizzazioni dell'account di servizio per il connettore".

   b. Da Google Cloud, attiva la shell cloud.

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

   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 e assegnare il ruolo all'account di servizio:

   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"

3. Se si prevede di implementare i sistemi Cloud Volumes ONTAP in progetti diversi da quello in cui si trova il connettore, è necessario fornire l'account di servizio del connettore per accedere a tali progetti.

   Ad esempio, supponiamo che il connettore si trovi nel progetto 1 e che si desideri creare sistemi Cloud Volumes ONTAP nel progetto 2. È necessario concedere l'accesso all'account di servizio nel progetto 2.

   a. Dal servizio IAM & Admin, selezionare il progetto Google Cloud in cui si desidera creare i sistemi Cloud Volumes ONTAP.

   b. Nella pagina **IAM**, selezionare **Concedi accesso** e fornire i dettagli richiesti.

      - Inserire l'indirizzo e-mail dell'account di servizio del connettore.
      - Selezionare il ruolo personalizzato del connettore.
      - Selezionare **Salva**.

   Per ulteriori informazioni, fare riferimento a. "Documentazione di Google Cloud"

Risultato

L'account di servizio per la macchina virtuale del connettore è impostato.

Passaggio 4: Impostare le autorizzazioni VPC condivise

Se si utilizza un VPC condiviso per distribuire le risorse in un progetto di servizio, è necessario preparare le autorizzazioni.

Questa tabella è di riferimento e l’ambiente deve riflettere la tabella delle autorizzazioni al termine della configurazione IAM.

Visualizzare le autorizzazioni VPC condivise

Identità	Creatore	Ospitato in	Permessi del progetto di servizio	Permessi del progetto host	Scopo
Google per implementare il connettore	Personalizzato	Progetto di servizio	"Policy di implementazione del connettore"	compute.networkUser	Implementazione del connettore nel progetto di servizio
Account del servizio Connector	Personalizzato	Progetto di servizio	"Policy dell'account di servizio del connettore"	compute.networkUser deploymentmanager.editor	Implementazione e manutenzione di Cloud Volumes ONTAP e servizi nel progetto di servizio
Account del servizio Cloud Volumes ONTAP	Personalizzato	Progetto di servizio	storage.admin membro: Account di servizio BlueXP come serviceAccount.user	N/A.	(Opzionale) per il tiering dei dati e il backup e ripristino BlueXP
Agente del servizio API di Google	Google Cloud	Progetto di servizio	(Impostazione predefinita) Editor	compute.networkUser	Interagisce con le API di Google Cloud per conto dell'implementazione. Consente a BlueXP di utilizzare la rete condivisa.
Account di servizio predefinito di Google Compute Engine	Google Cloud	Progetto di servizio	(Impostazione predefinita) Editor	compute.networkUser	Implementa le istanze di Google Cloud e l'infrastruttura di calcolo per conto dell'implementazione. Consente a BlueXP di utilizzare la rete condivisa.

Note:

1. Deploymentmanager.editor è necessario solo per il progetto host se non si passano le regole del firewall alla distribuzione e si sceglie di consentire a BlueXP di crearle. BlueXP crea una distribuzione nel progetto host che contiene la regola firewall VPC0 se non viene specificata alcuna regola.
2. Firewall.create e firewall.delete sono necessari solo se non si passano le regole firewall all'implementazione e si sceglie di consentire a BlueXP di crearle. Queste autorizzazioni risiedono nel file .yaml dell'account BlueXP. Se si implementa una coppia ha utilizzando un VPC condiviso, queste autorizzazioni verranno utilizzate per creare le regole firewall per VPC1, 2 e 3. Per tutte le altre implementazioni, queste autorizzazioni verranno utilizzate anche per creare regole per VPC0.
3. Per il tiering dei dati, l'account del servizio di tiering deve avere il ruolo serviceAccount.user nell'account del servizio, non solo a livello di progetto. Attualmente, se si assegna serviceAccount.user a livello di progetto, le autorizzazioni non vengono visualizzate quando si esegue

una query all'account del servizio con getIAMPolicy.

Passaggio 5: Abilitare le API di Google Cloud

Diverse API di Google Cloud devono essere abilitate prima di poter implementare i sistemi Cloud Volumes ONTAP in Google Cloud.

Fase

1. Abilita le seguenti API 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))

"Documentazione di Google Cloud: Abilitazione delle API"

Fase 6: Installare il connettore

Una volta completati i prerequisiti, è possibile installare manualmente il software sul proprio host Linux.

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.

6. Attendere il completamento dell'installazione.

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

7. Aprire un browser Web da un host connesso alla macchina virtuale Connector e immettere il seguente URL:

   https://ipaddress

8. Dopo aver effettuato l'accesso, configurare il connettore:
   a. Specificare l'account BlueXP da associare al connettore.
   b. Immettere un nome per il sistema.
   c. In **stai eseguendo in un ambiente protetto?** Mantieni disattivata la modalità limitata.

      La modalità limitata deve essere disattivata perché questa procedura descrive come utilizzare BlueXP in modalità standard. Attivare la modalità limitata solo se si dispone di un ambiente sicuro e si desidera disconnettere questo account dai servizi di back-end BlueXP. In tal caso, "Segui i passaggi per iniziare a utilizzare BlueXP in modalità limitata".

   d. Selezionare **Let's start**.

Risultato

Il connettore è ora installato e configurato con l'account BlueXP.

Se hai bucket di Google Cloud Storage nello stesso account Google Cloud in cui hai creato il connettore, vedrai comparire automaticamente un ambiente di lavoro di Google Cloud Storage su BlueXP Canvas. "Scopri come gestire Google Cloud Storage da BlueXP"

Fase 7: Fornire le autorizzazioni ad BlueXP

Devi fornire ad BlueXP le autorizzazioni di Google Cloud che hai precedentemente configurato. La fornitura delle autorizzazioni consente a BlueXP di gestire l'infrastruttura di dati e storage in Google Cloud.

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 Google Cloud, concedere l'accesso aggiungendo l'account del 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.

Installazione e configurazione di un connettore on-premise

Installare un connettore on-premise, quindi effettuare l'accesso e configurarlo per l'utilizzo con l'account BlueXP.

Prima di iniziare

Dovresti rivedere "Limitazioni del connettore".

Fase 1: 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. Assicurarsi che l'host soddisfi questi requisiti prima di installare il connettore.

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

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 2: Configurare la rete

Configura il tuo networking in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud ibrido. Ad esempio, è necessario assicurarsi che le connessioni siano disponibili per le reti di destinazione e che sia disponibile l'accesso a Internet in uscita.

Connessioni alle reti di destinazione

Un connettore richiede una connessione di rete alla posizione in cui si intende creare e gestire gli ambienti di lavoro. Ad esempio, la rete in cui intendi creare sistemi Cloud Volumes ONTAP o un sistema storage nel tuo ambiente on-premise.

Accesso a Internet in uscita

La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita per contattare endpoint specifici.

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

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

Endpoint contattati dal connettore

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 per le operazioni quotidiane.

Si noti che gli endpoint elencati di seguito sono tutte le voci CNAME.

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.
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	Per aggiornare il connettore e i relativi componenti Docker.

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"

Passaggio 3: Impostare le autorizzazioni cloud

Se si desidera utilizzare i servizi BlueXP in AWS o Azure con un connettore on-premise, è necessario impostare le autorizzazioni nel provider cloud in modo da poter aggiungere le credenziali al connettore dopo l'installazione.

Perché non Google Cloud? Quando il connettore viene installato in sede, non è in grado di gestire le risorse in Google Cloud. Il connettore deve essere installato in Google Cloud per gestire le risorse che vi risiedono.

AWS

Quando il connettore viene installato on-premise, è necessario fornire a BlueXP le autorizzazioni AWS aggiungendo le chiavi di accesso per un utente IAM che dispone delle autorizzazioni necessarie.

È necessario utilizzare questo metodo di autenticazione se il connettore è installato on-premise. Non puoi utilizzare un ruolo IAM.

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

A questo punto, si dovrebbero disporre delle chiavi di accesso per un utente IAM che dispone delle autorizzazioni necessarie. Dopo aver installato il connettore, è necessario associare queste credenziali al connettore di BlueXP.

Azure

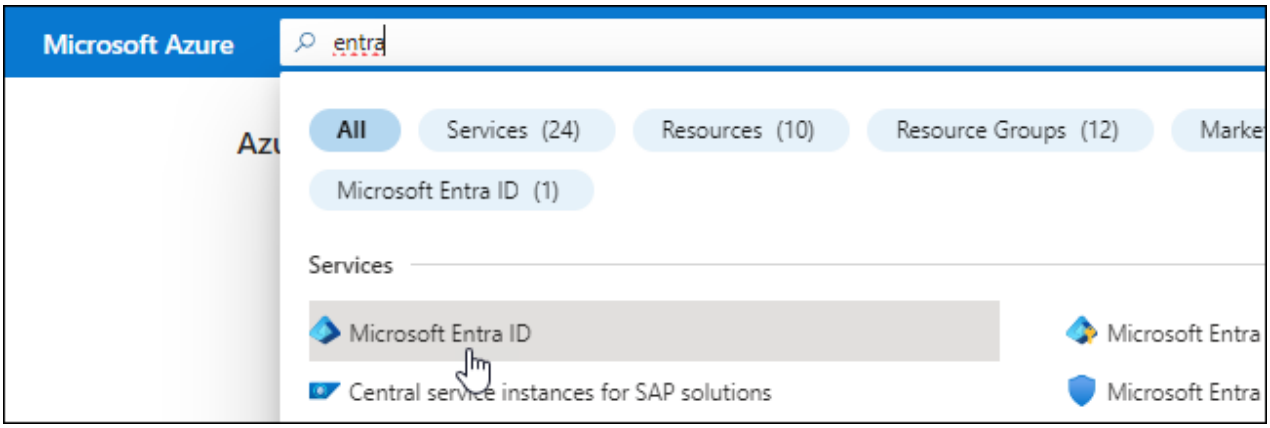
Quando il connettore è installato on-premise, devi fornire ad BlueXP le autorizzazioni di Azure, configurando un'identità di servizio in Microsoft Entra ID e ottenendo le credenziali di Azure di cui BlueXP ha bisogno.

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.

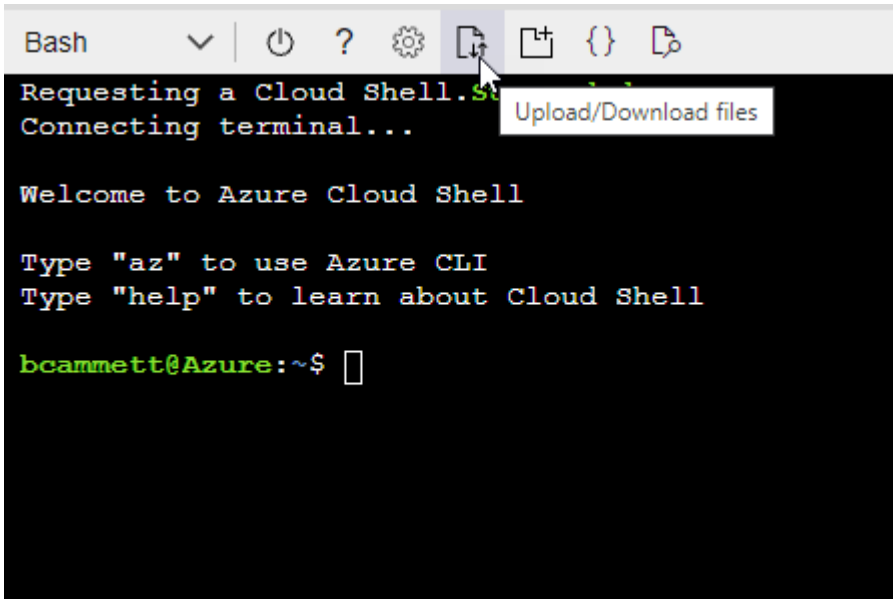
      Esempio

      ```
      "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:

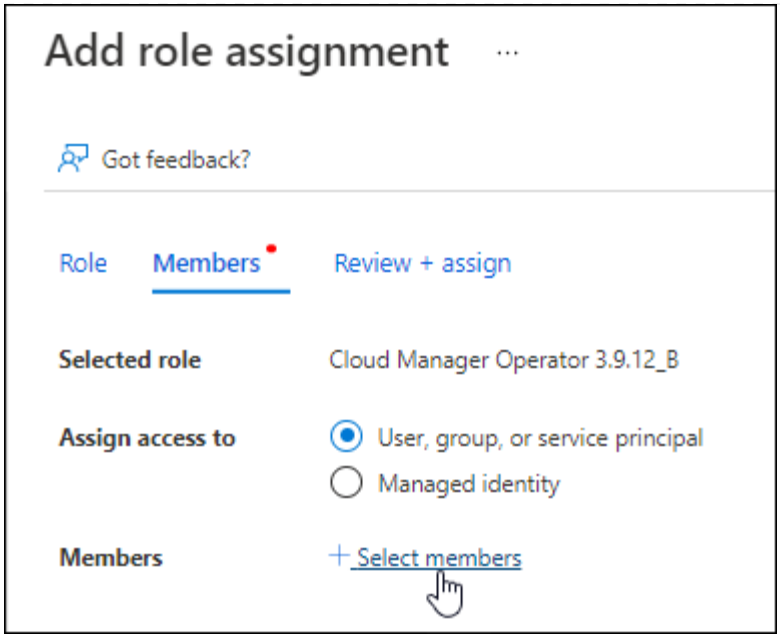
```
az role definition create --role-definition
Connector_Policy.json
```

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:

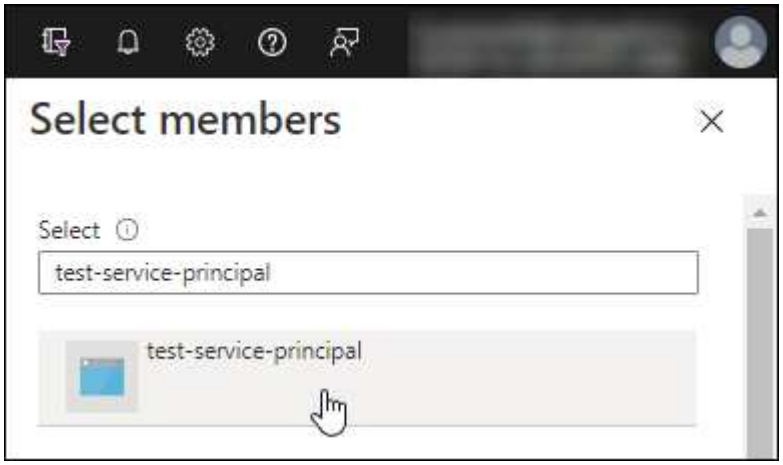
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

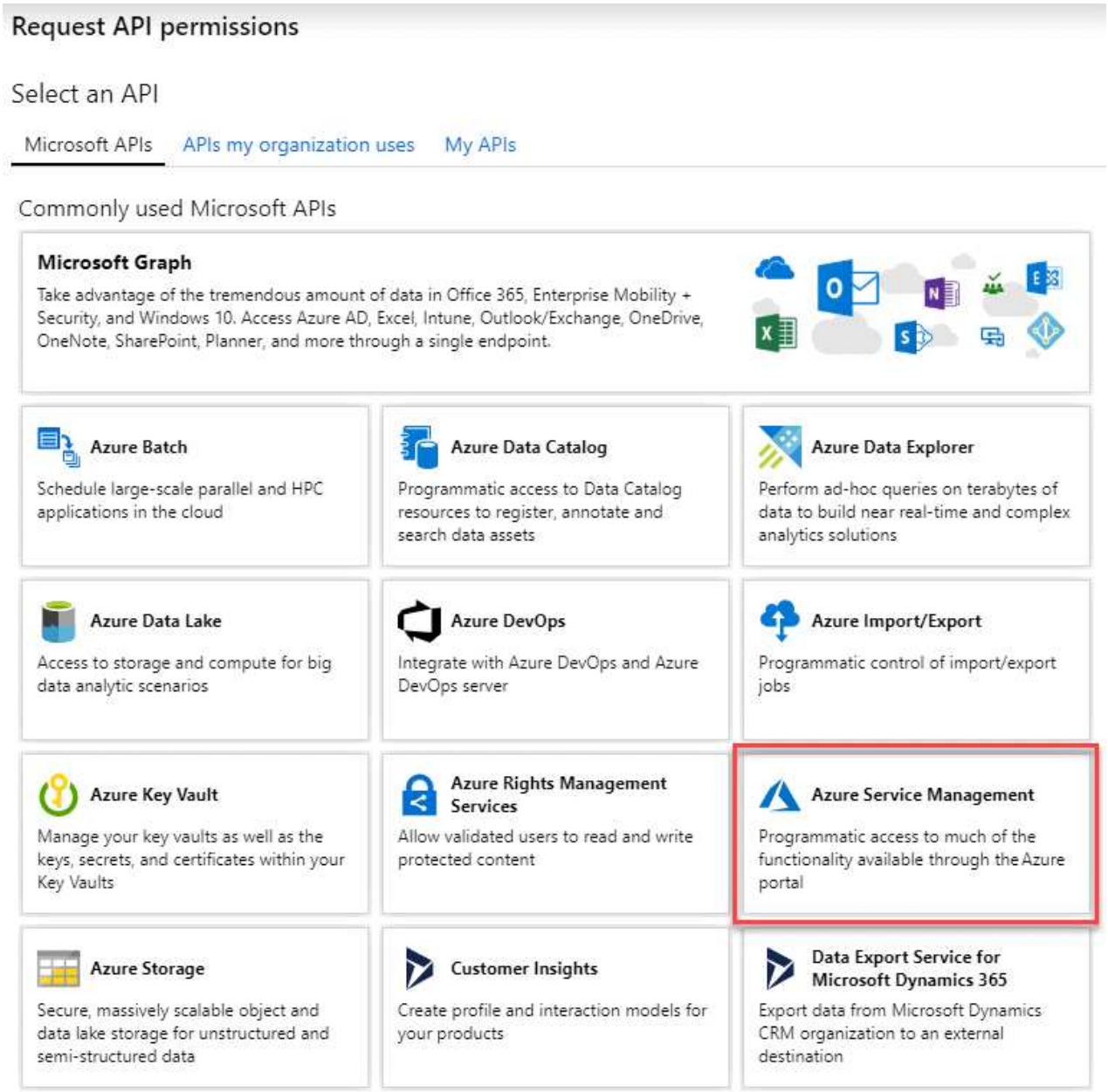
   L'entità del servizio dispone ora delle autorizzazioni Azure necessarie per implementare il connettore.

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.

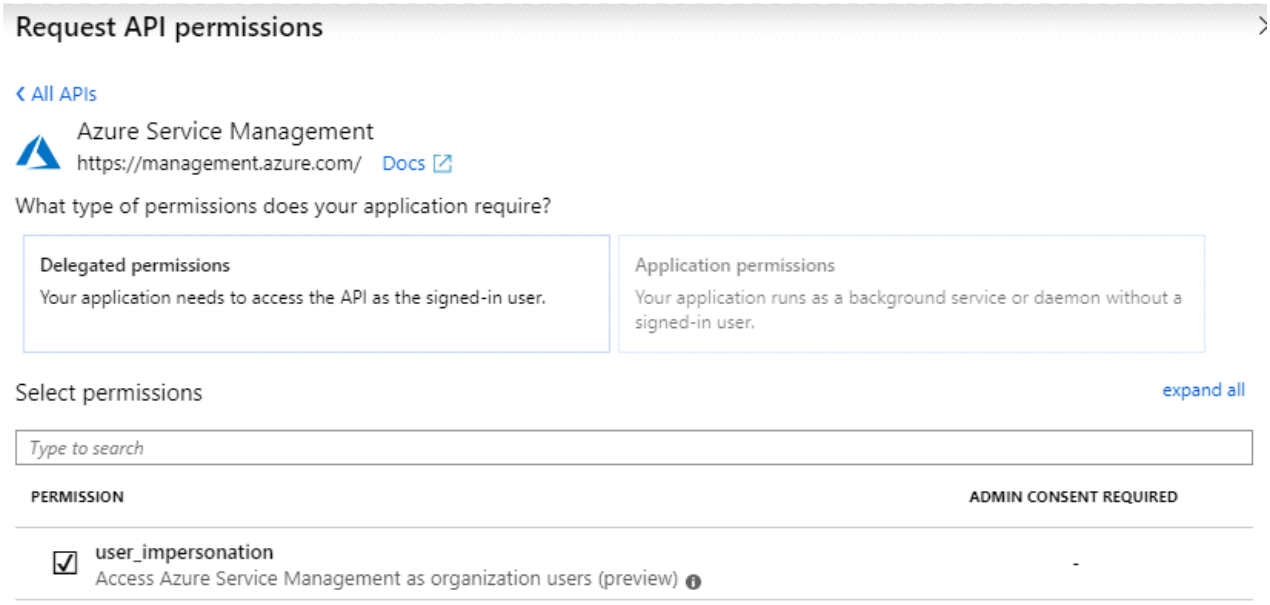
Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

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**.

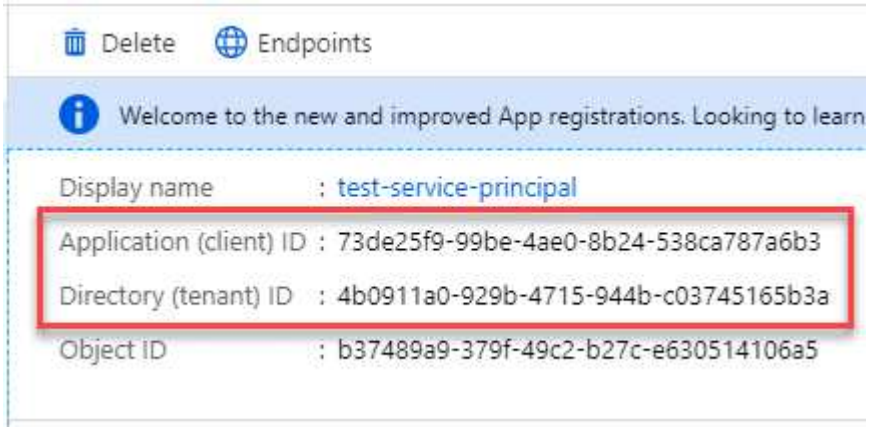


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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. Dopo aver installato il connettore, è necessario associare queste credenziali al connettore di BlueXP.

Fase 4: Installare il connettore

Scaricare e installare il software del connettore su un host Linux esistente on-premise.

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.

Fase 5: Configurare il connettore

Registrati o accedi e configura Connector per lavorare con l'account BlueXP.

Fasi

1. Aprire un browser Web e immettere il seguente URL:

   https://ipaddress

   Ipaddress può essere localhost, un indirizzo IP privato o un indirizzo IP pubblico, a seconda della configurazione dell'host. Ad esempio, se il connettore si trova nel cloud pubblico senza un indirizzo IP pubblico, è necessario inserire un indirizzo IP privato da un host che ha una connessione all'host del connettore.

2. Iscriviti o accedi.
3. Dopo aver effettuato l'accesso, configurare BlueXP:
   a. Specificare l'account BlueXP da associare al connettore.
   b. Immettere un nome per il sistema.
   c. In **stai eseguendo in un ambiente protetto?** Mantieni disattivata la modalità limitata.

      La modalità limitata deve essere disattivata perché questa procedura descrive come utilizzare BlueXP in modalità standard. Inoltre, la modalità limitata non è supportata quando il connettore viene installato on-premise.

   d. Selezionare **Let's start**.

Risultato

BlueXP è ora configurato con il connettore appena installato.

Fase 6: Fornire le autorizzazioni ad BlueXP

Dopo aver installato e configurato il connettore, Aggiungi le tue credenziali cloud in modo che BlueXP disponga delle autorizzazioni necessarie per eseguire azioni in AWS o Azure.

AWS

Prima di iniziare

Se queste credenziali sono state appena create in AWS, potrebbero essere necessari alcuni minuti prima che siano disponibili per l'utilizzo. Attendere alcuni minuti prima di aggiungere le credenziali a BlueXP.

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.

A questo punto, è possibile accedere alla "Console BlueXP" Per iniziare a utilizzare il connettore con BlueXP.

Azure

Prima di iniziare

Se queste credenziali sono state appena create in Azure, potrebbero essere necessari alcuni minuti prima che siano disponibili per l'utilizzo. Attendere alcuni minuti prima di aggiungere le credenziali a BlueXP.

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. A questo punto, è possibile accedere alla "Console BlueXP" Per iniziare a utilizzare il connettore con BlueXP.