Inizia subito

Setup and administration

NetApp
April 26, 2024

Sommario

Inizia subito

Scopri le nozioni di base

Scopri BlueXP

NetApp BlueXP offre alla tua organizzazione un singolo piano di controllo che ti aiuta a creare, proteggere e gestire i dati nei tuoi ambienti on-premise e cloud. La piattaforma SaaS BlueXP include servizi che forniscono gestione dello storage, mobilità dei dati, data Protection e analisi e controllo dei dati. Le funzionalità di gestione vengono fornite tramite una console basata su web e API.

Caratteristiche

La piattaforma BlueXP offre quattro pilastri principali per la gestione dei dati: Storage, mobilità, protezione, analisi e controllo.

Storage

Scopri, implementa e gestisci lo storage, sia in AWS, Azure, Google Cloud o on-premise.

- Configurazione e utilizzo "Cloud Volumes ONTAP" per una gestione dei dati efficiente e multiprotocollo tra i cloud.
- Configurare e utilizzare i servizi di file storage nel cloud:
  - "Azure NetApp Files"
  - "Amazon FSX per ONTAP"
  - "Cloud Volumes Service per Google Cloud"
- Rilevare e gestire "storage on-premise":
  - Sistemi e-Series
  - Cluster ONTAP
  - Sistemi StorageGRID

Mobilità

Sposta i dati dove servono sincronizzando, copiando, tiering e memorizzando i dati nella cache.

- "Copia e sincronizzazione"
- "Caching edge"
- "Tiering"

Protezione

Utilizza meccanismi di protezione automatici per proteggere i dati da perdita di dati, interruzioni non pianificate, ransomware e altre minacce informatiche.

- "Backup e recovery"
- "Replica"
- "Data Protection per i workload Kubernetes"

Analisi e controllo

Utilizza strumenti per monitorare, mappare e ottimizzare l'infrastruttura e lo storage dei dati. Ottieni informazioni utilizzabili per ottimizzare salute, resilienza e economia dello storage.

- "Classificazione"
- "Consulente digitale"
- "Efficienza economica"
- "Resilienza operativa"

"Scopri di più su come utilizzare BlueXP per aiutare la tua organizzazione"

Cloud provider supportati

BlueXP consente di gestire lo storage cloud e utilizzare i servizi cloud in Amazon Web Services, Microsoft Azure e Google Cloud.

Costo

I prezzi di BlueXP dipendono dai servizi che si intende utilizzare. "Scopri i prezzi di BlueXP"

Come funziona BlueXP

BlueXP include una console basata su web fornita tramite il layer SaaS, account che forniscono multi-tenancy e connettori che gestiscono gli ambienti di lavoro e abilitano i servizi cloud BlueXP.

Software-as-a-service

BlueXP è accessibile tramite un "console basata su web" E API. Questa esperienza SaaS ti consente di accedere automaticamente alle funzionalità più recenti non appena vengono rilasciate e di passare facilmente da un account BlueXP a un connettore e viceversa.

Account BlueXP

Quando si accede a BlueXP per la prima volta, viene richiesto di creare un *account BlueXP*. Questo account offre multi-tenancy e consente di organizzare utenti e risorse in *aree di lavoro* isolate.

"Scopri di più sugli account".

Connettori

Non è necessario un connettore per iniziare a utilizzare BlueXP, ma è necessario creare un connettore per sbloccare tutte le funzionalità e i servizi di BlueXP. Un connettore consente la gestione di risorse e processi in ambienti on-premise e cloud. È necessario gestire gli ambienti di lavoro (ad esempio, cluster Cloud Volumes ONTAP e ONTAP on-premise) e utilizzare molti servizi dati BlueXP.

"Scopri di più sui connettori".

Modalità limitata e modalità privata

BlueXP è supportato anche in ambienti con restrizioni di sicurezza e connettività. È possibile utilizzare *restricted mode* o *private mode* per limitare la connettività in uscita al layer BlueXP SaaS.

"Scopri di più sulle modalità di implementazione di BlueXP".

Certificazione SOC 2 tipo 2

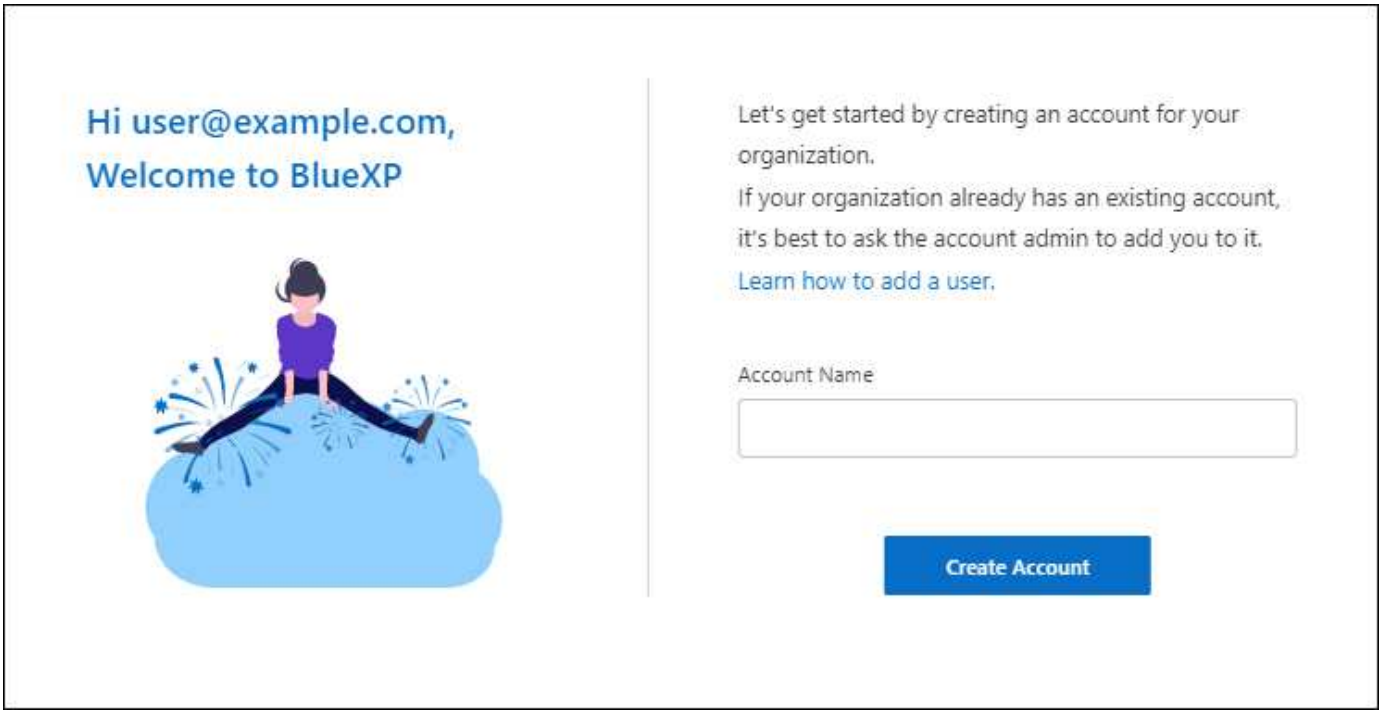
Un'azienda indipendente di contabili pubblici e un revisore dei servizi ha esaminato BlueXP e affermato di aver ottenuto report SOC 2 di tipo 2 sulla base dei criteri Trust Services applicabili.

"Visualizza i report SOC 2 di NetApp"

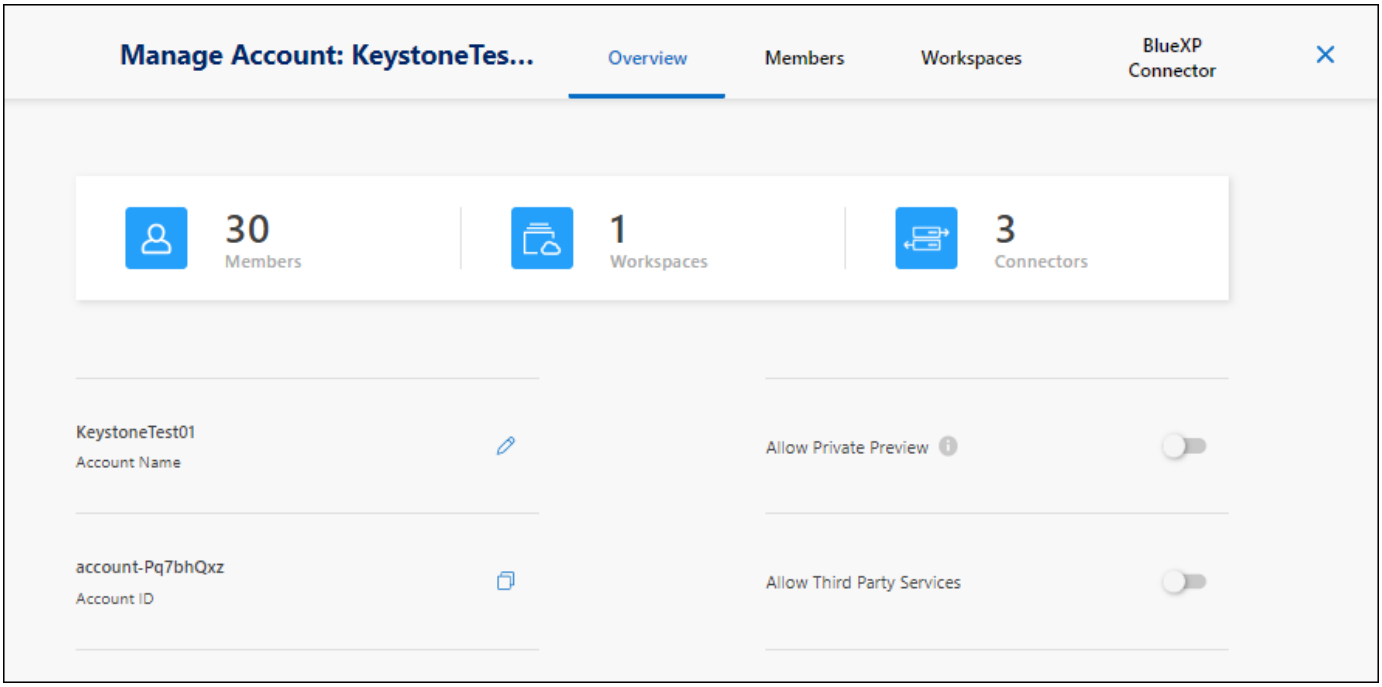
Scopri di più sugli account BlueXP

Un *account BlueXP* fornisce la multi-tenancy per la tua organizzazione, consentendo di organizzare utenti e risorse in *aree di lavoro* isolate. Ad esempio, un gruppo di utenti può distribuire e gestire ambienti di lavoro Cloud Volumes ONTAP in un'area di lavoro non visibile agli utenti che gestiscono ambienti di lavoro in un'altra area di lavoro.

Quando accedi per la prima volta a BlueXP, ti viene richiesto di selezionare o creare un account. Ad esempio, se non si dispone ancora di un account, viene visualizzata la seguente schermata:



BlueXP account Admins può quindi modificare le impostazioni per questo account gestendo utenti (membri), aree di lavoro e connettori:



"Scopri come gestire il tuo account BlueXP".

Modalità di implementazione

BlueXP offre le seguenti modalità di implementazione per l'account: Modalità standard, modalità limitata e modalità privata. Queste modalità supportano ambienti con diversi livelli di sicurezza e limitazioni di connettività.

"Scopri di più sulle modalità di implementazione di BlueXP".

Membri

I membri sono utenti BlueXP che si associano al proprio account BlueXP. L'associazione di un utente a un account e a una o più aree di lavoro in tale account consente a tali utenti di creare e gestire ambienti di lavoro in BlueXP.

Quando si associa un utente, viene assegnato un ruolo:

- *Account Admin*: Può eseguire qualsiasi azione in BlueXP.
- *Workspace Admin*: Consente di creare e gestire le risorse nell'area di lavoro assegnata.
- *Compliance Viewer*: È in grado di visualizzare solo le informazioni di conformità per la classificazione BlueXP e generare report per le aree di lavoro a cui sono autorizzati ad accedere.

"Scopri di più su questi ruoli".

Aree di lavoro

In BlueXP, un'area di lavoro isola qualsiasi numero di *ambienti di lavoro* da altri utenti dell'account. Gli amministratori dell'area di lavoro non possono accedere agli ambienti di lavoro in un'area di lavoro a meno che l'amministratore dell'account non colleghi l'amministratore a tale area di lavoro.

Un ambiente di lavoro rappresenta un sistema storage. Ad esempio:

- Un sistema Cloud Volumes ONTAP
- Un cluster ONTAP on-premise
- Un cluster Kubernetes

"Scopri come aggiungere un'area di lavoro".

Connettori

Un connettore esegue le azioni che BlueXP deve eseguire per gestire l'infrastruttura dati. Il connettore viene eseguito su un'istanza di macchina virtuale implementata nel cloud provider o su un host on-premise configurato.

È possibile utilizzare un connettore con più di un servizio BlueXP. Ad esempio, se si utilizza un connettore per gestire Cloud Volumes ONTAP, è possibile utilizzare lo stesso connettore con un altro servizio come il tiering BlueXP.

"Scopri di più sui connettori".

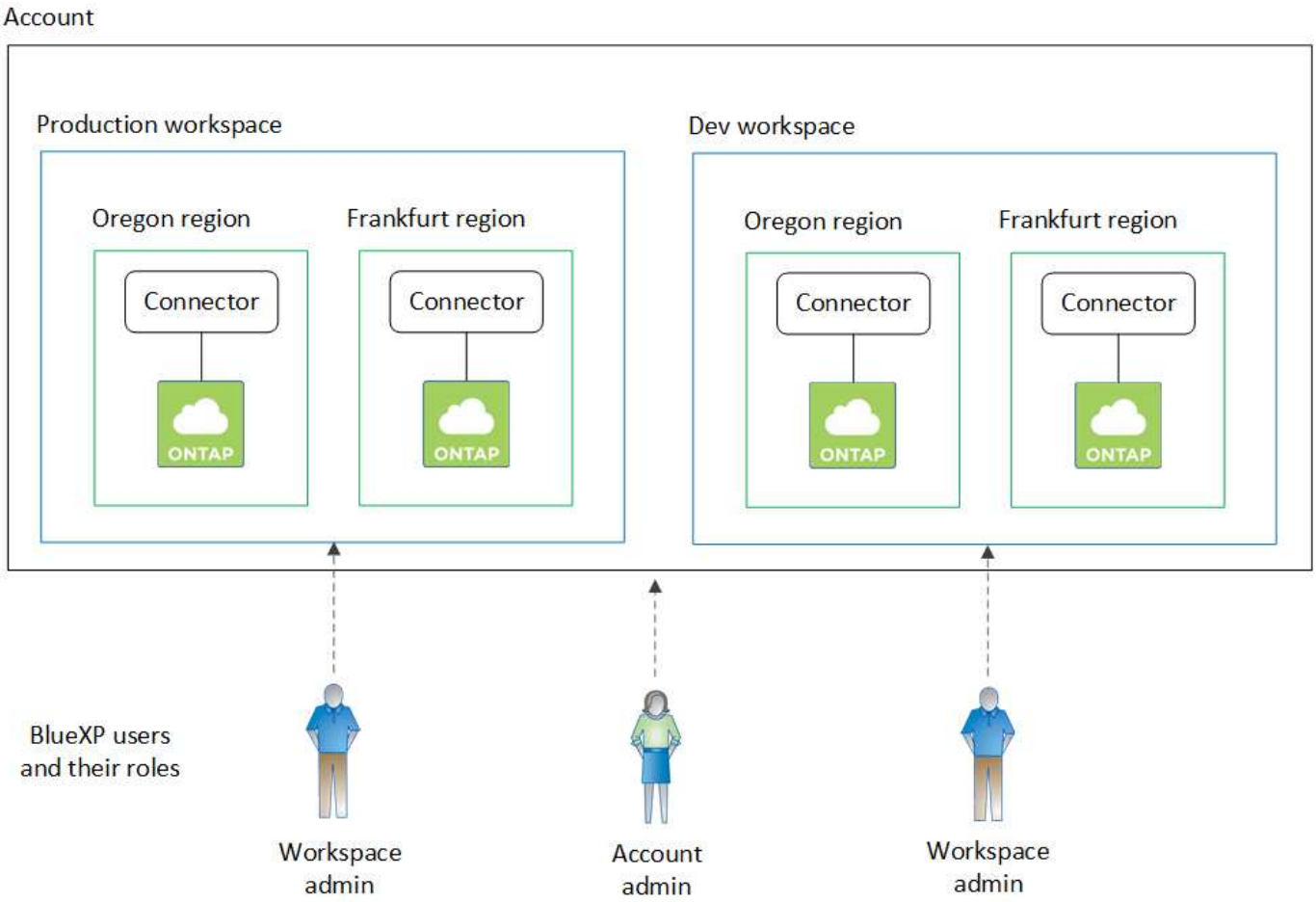
Esempi

I seguenti esempi illustrano come configurare gli account.

> In entrambe le immagini di esempio che seguono, il connettore e i sistemi Cloud Volumes ONTAP non risiedono in realtà _nell'account BlueXP—sono in esecuzione in un provider cloud. Si tratta di una rappresentazione concettuale della relazione tra ciascun componente.

Più aree di lavoro

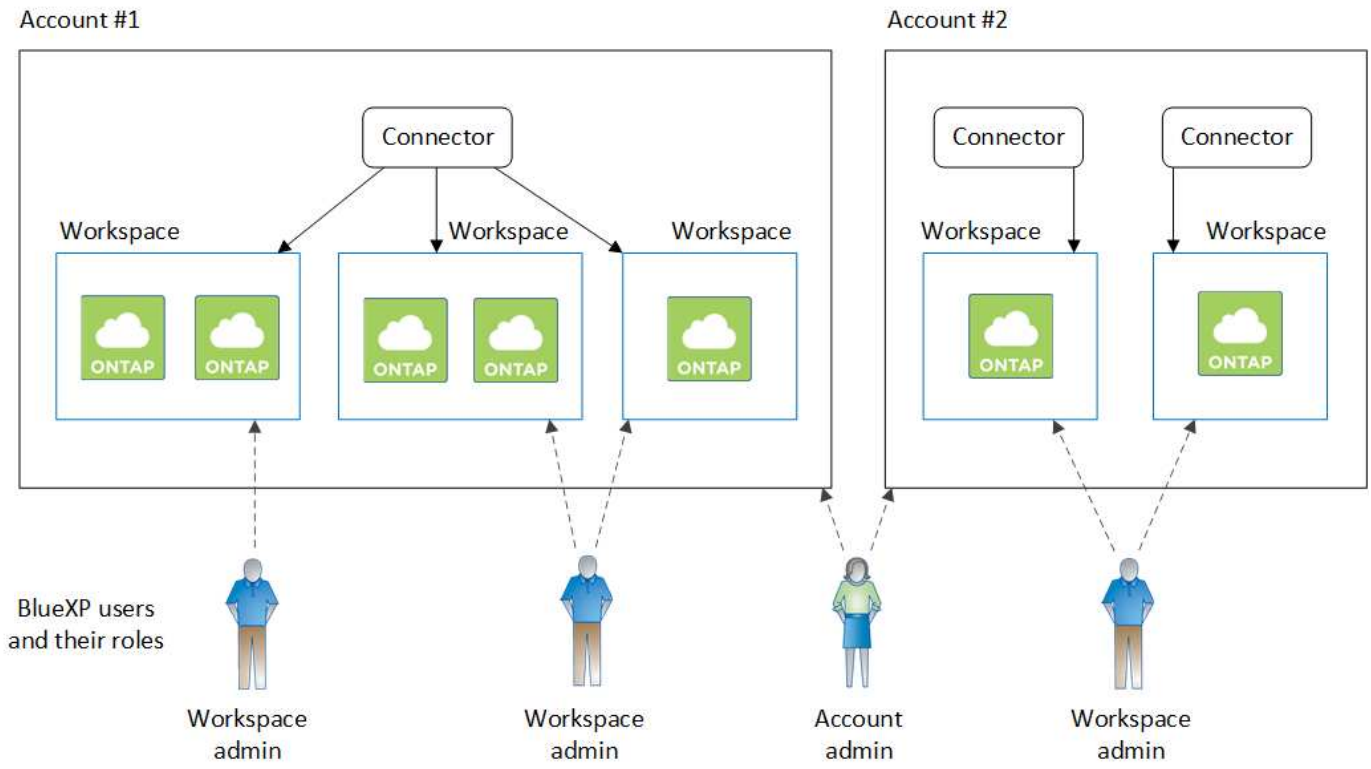
Nell'esempio riportato di seguito viene illustrato un account che utilizza due aree di lavoro per creare ambienti isolati. Il primo spazio di lavoro è per un ambiente di produzione e il secondo per un ambiente di sviluppo.



Account multipli

Ecco un altro esempio che mostra il più alto livello di multi-tenancy utilizzando due account BlueXP separati. Ad esempio, un provider di servizi potrebbe utilizzare BlueXP in un account per fornire servizi ai propri clienti, mentre un altro account per fornire il disaster recovery per una delle proprie business unit.

L'account 2 include due connettori separati. Questo potrebbe verificarsi se i sistemi sono in regioni separate o in provider cloud separati.



Scopri di più sui connettori

Un *connettore* è il software NetApp in esecuzione nella rete cloud o on-premise. Esegue le azioni che BlueXP deve eseguire per gestire l'infrastruttura dati. Il connettore esegue costantemente il polling del livello BlueXP SaaS per individuare eventuali azioni da intraprendere. Non è necessario un connettore per iniziare a utilizzare BlueXP, ma è necessario creare un connettore per sbloccare tutte le funzionalità e i servizi di BlueXP.

Cosa puoi fare senza un connettore

Non è necessario un connettore per iniziare a utilizzare BlueXP. È possibile utilizzare diverse funzionalità e servizi in BlueXP senza creare alcun connettore.

È possibile utilizzare le seguenti funzionalità e servizi BlueXP senza un connettore:

- Creazione dell'ambiente di lavoro Amazon FSX per NetApp ONTAP

  Sebbene non sia necessario un connettore per creare un ambiente di lavoro, è necessario creare e gestire volumi, replicare i dati e integrare FSX per ONTAP con servizi come la classificazione BlueXP e la copia e la sincronizzazione BlueXP.

- Catalogo di automazione
- Azure NetApp Files

  Sebbene non sia necessario un connettore per configurare e gestire Azure NetApp Files, è necessario un connettore per utilizzare la classificazione BlueXP per eseguire la scansione dei dati Azure NetApp Files.

- Cloud Volumes Service per Google Cloud

- Copia e sincronizzazione
- Consulente digitale
- Portafoglio digitale

  In quasi tutti i casi, è possibile aggiungere una licenza al portafoglio digitale senza un connettore.

  Per aggiungere una licenza al portafoglio digitale è necessario un connettore solo per le licenze Cloud Volumes ONTAP *basate su nodo*. In questo caso, è necessario un connettore perché i dati provengono dalle licenze installate sui sistemi Cloud Volumes ONTAP.

- Rilevamento diretto dei cluster ONTAP on-premise

  Sebbene non sia necessario un connettore per il rilevamento diretto di un cluster ONTAP on-premise, è necessario un connettore per sfruttare le funzionalità aggiuntive di BlueXP.

  "Scopri di più sulle opzioni di rilevamento e gestione dei cluster ONTAP on-premise"

- Sostenibilità

Quando è necessario un connettore

Quando si utilizza BlueXP in modalità standard, è necessario un connettore per le seguenti funzionalità e servizi in BlueXP:

- Funzionalità di gestione di Amazon FSX per ONTAP
- Storage Amazon S3
- Storage Azure Blob
- Backup e recovery
- Classificazione
- Cloud Volumes ONTAP
- Disaster recovery
- Sistemi e-Series
- Efficienza economica [1]
- Caching edge
- Bucket di storage Google Cloud
- Cluster Kubernetes
- Report sulla migrazione
- Integrazione del cluster ONTAP on-premise con i servizi dati BlueXP
- Resilienza operativa [1]
- Protezione ransomware
- Sistemi StorageGRID
- Tiering
- Caching dei volumi

[1] sebbene sia possibile accedere a questi servizi senza un connettore, è necessario un connettore per avviare azioni dai servizi.

Per utilizzare BlueXP in modalità limitata o privata è necessario un connettore.

I connettori devono essere sempre operativi

I connettori sono una parte fondamentale dell'architettura del servizio BlueXP. È tua responsabilità garantire che i connettori pertinenti siano sempre attivi, operativi e accessibili. Sebbene il servizio sia progettato per superare brevi interruzioni della disponibilità del connettore, è necessario intraprendere azioni immediate quando è necessario rimediare ai guasti dell'infrastruttura.

La presente documentazione è disciplinata dall'EULA. Se il prodotto non viene utilizzato in conformità con la documentazione, la funzionalità e il funzionamento del prodotto, nonché i diritti dell'utente previsti dal Contratto di licenza con l'utente finale, potrebbero risentire negativamente.

Impatto su Cloud Volumes ONTAP

Un connettore è un componente chiave per lo stato e il funzionamento di Cloud Volumes ONTAP. Se un connettore viene spento, i sistemi PAYGO Cloud Volumes ONTAP e i sistemi BYOL basati sulla capacità si arrestano dopo aver perso la comunicazione con un connettore per più di 14 giorni. Questo accade perché il connettore aggiorna le licenze sul sistema ogni giorno.

Se il sistema Cloud Volumes ONTAP dispone di una licenza BYOL basata su nodo, il sistema rimane in esecuzione dopo 14 giorni perché la licenza è installata sul sistema Cloud Volumes ONTAP.

Posizioni supportate

Un connettore è supportato nelle seguenti posizioni:

- Amazon Web Services
- Microsoft Azure

  Un connettore in Azure deve essere implementato nella stessa regione di Azure dei sistemi Cloud Volumes ONTAP che gestisce 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"

- Google Cloud

  Se si desidera utilizzare i servizi BlueXP con Google Cloud, è necessario utilizzare un connettore in esecuzione in Google Cloud.

- On-premise

Modalità limitata e modalità privata

Per utilizzare BlueXP in modalità limitata o privata, è possibile iniziare a utilizzare BlueXP installando il connettore e accedendo all'interfaccia utente in esecuzione localmente sul connettore.

"Scopri le modalità di implementazione di BlueXP".

Come creare un connettore

Un account Admin BlueXP può creare un connettore direttamente da BlueXP, dal mercato del tuo cloud provider o installando manualmente il software sul tuo host Linux. Il modo in cui iniziare dipende dall'utilizzo di BlueXP in modalità standard, limitata o privata.

- "Scopri le modalità di implementazione di BlueXP"
- "Inizia subito con BlueXP in modalità standard"
- "Inizia subito con BlueXP in modalità limitata"
- "Inizia subito con BlueXP in modalità privata"

Permessi

Sono necessarie autorizzazioni specifiche per creare il connettore direttamente da BlueXP e un altro set di autorizzazioni per l'istanza del connettore stesso. Se si crea il connettore in AWS o Azure direttamente da BlueXP, BlueXP crea il connettore con le autorizzazioni necessarie.

Quando si utilizza BlueXP in modalità standard, il modo in cui si forniscono le autorizzazioni dipende da come si intende creare il connettore.

Per informazioni su come impostare le autorizzazioni, fare riferimento a quanto segue:

- Modalità standard
  - "Opzioni di installazione del connettore in AWS"
  - "Opzioni di installazione del connettore in Azure"
  - "Opzioni di installazione del connettore in Google Cloud"
  - "Impostare le autorizzazioni cloud per le implementazioni on-premise"
- "Impostare le autorizzazioni per la modalità limitata"
- "Impostare le autorizzazioni per la modalità privata"

Per visualizzare le autorizzazioni esatte necessarie al connettore per le operazioni quotidiane, fare riferimento alle pagine seguenti:

- "Scopri come il connettore utilizza le autorizzazioni AWS"
- "Scopri come il connettore utilizza le autorizzazioni Azure"
- "Scopri come Connector utilizza le autorizzazioni Google Cloud"

Aggiornamenti del connettore

Di solito aggiorniamo il software del connettore ogni mese per introdurre nuove funzionalità e migliorare la stabilità. Sebbene la maggior parte dei servizi e delle funzionalità della piattaforma BlueXP sia offerta tramite software basato su SaaS, alcune funzionalità dipendono dalla versione del connettore. Che include la gestione Cloud Volumes ONTAP, la gestione del cluster ONTAP on-premise, le impostazioni e la guida.

Quando si utilizza BlueXP in modalità standard o limitata, il connettore aggiorna automaticamente il proprio software all'ultima versione, a condizione che disponga di accesso a Internet outbound per ottenere l'aggiornamento software. Se si utilizza BlueXP in modalità privata, è necessario aggiornare manualmente il connettore.

"Scopri come aggiornare manualmente il software del connettore".

Manutenzione del sistema operativo e delle macchine virtuali

La manutenzione del sistema operativo sull'host del connettore è responsabilità dell'utente. Ad esempio, è necessario applicare gli aggiornamenti per la protezione al sistema operativo sull'host del connettore seguendo le procedure standard dell'azienda per la distribuzione del sistema operativo.

Tenere presente che non è necessario interrompere alcun servizio sull'host del connettore quando si esegue un aggiornamento del sistema operativo.

Se è necessario arrestare e avviare la macchina virtuale del connettore, è necessario farlo dalla console del provider di cloud o utilizzando le procedure standard per la gestione on-premise.

Tenere presente che il connettore deve essere sempre operativo.

Ambienti di lavoro multipli

Un connettore può gestire più ambienti di lavoro in BlueXP. Il numero massimo di ambienti di lavoro che un singolo connettore deve gestire varia. Dipende dal tipo di ambiente di lavoro, dal numero di volumi, dalla quantità di capacità gestita e dal numero di utenti.

Se disponi di un'implementazione su larga scala, collabora con il tuo rappresentante NetApp per dimensionare il tuo ambiente. In caso di problemi durante il percorso, contattaci utilizzando la chat integrata nel prodotto.

Connettori multipli

In alcuni casi, potrebbe essere necessario un solo connettore, ma potrebbero essere necessari due o più connettori.

Ecco alcuni esempi:

- Si dispone di un ambiente multi-cloud (ad esempio, AWS e Azure) e si preferisce avere un connettore in AWS e un altro in Azure. Ciascuno di essi gestisce i sistemi Cloud Volumes ONTAP in esecuzione in tali ambienti.
- Un provider di servizi potrebbe utilizzare un account BlueXP per fornire servizi ai propri clienti, mentre utilizza un altro account per fornire il disaster recovery per una delle proprie business unit. Ciascun account dispone di connettori separati.

Quando cambiare

Quando si crea il primo connettore, BlueXP utilizza automaticamente tale connettore per ogni ambiente di lavoro aggiuntivo creato. Una volta creato un connettore aggiuntivo, è necessario passare da un connettore all'altro per visualizzare gli ambienti di lavoro specifici di ciascun connettore.

"Scopri come passare da un connettore all'altro".

Disaster recovery

È possibile gestire un ambiente di lavoro con più connettori contemporaneamente per scopi di disaster recovery. Se un connettore si spegne, è possibile passare all'altro connettore per gestire immediatamente l'ambiente di lavoro.

Per impostare questa configurazione:

1. "Passare a un altro connettore".
2. Scopri l'ambiente di lavoro esistente.
    - "Aggiungere sistemi Cloud Volumes ONTAP esistenti a BlueXP"
    - "Scopri i cluster ONTAP"
3. Impostare "Modalità di gestione della capacità"

Solo il connettore principale deve essere impostato su **Automatic Mode** (modalità automatica). Se si passa a un altro connettore per scopi di DR, è possibile modificare la modalità di gestione della capacità in base alle esigenze.

Scopri le modalità di implementazione di BlueXP

BlueXP offre varie *modalità di implementazione* che consentono di utilizzare BlueXP in modo da soddisfare i requisiti di sicurezza e di business. *Standard mode* sfrutta il layer BlueXP SaaS per fornire funzionalità complete, mentre *restricted mode* e *private mode* sono disponibili per le organizzazioni con restrizioni di connettività.

Mentre BlueXP inibisce il flusso di traffico, comunicazione e dati quando si utilizza la modalità limitata o privata, è tua responsabilità garantire che il tuo ambiente (on-premise e nel cloud) sia conforme alle normative richieste.

Panoramica

BlueXP offre le seguenti modalità di implementazione per il tuo account. Ciascuna modalità differisce in termini di requisiti di connettività in uscita, posizione di implementazione, processo di installazione, metodo di autenticazione, servizi di storage e dati disponibili e metodi di addebito.

Modalità standard

BlueXP è accessibile agli utenti come servizio cloud dalla console basata su web. A seconda dei servizi BlueXP che intendi utilizzare, un amministratore di BlueXP crea uno o più connettori per gestire i dati all'interno del tuo ambiente di cloud ibrido.

Questa modalità utilizza la trasmissione di dati crittografati su Internet pubblico.

Modalità limitata

Nel cloud viene installato un connettore BlueXP (in un'area governativa, in un'area di cloud sovrana o in un'area commerciale) e la connettività in uscita al layer BlueXP SaaS è limitata. Gli utenti accedono a BlueXP localmente dalla console basata sul web disponibile dal connettore, non dal layer SaaS.

Questa modalità viene generalmente utilizzata dagli enti pubblici statali e locali e dalle aziende regolamentate.

Scopri di più sulla connettività in uscita al livello SaaS.

Modalità privata

Un connettore BlueXP viene installato on-premise o nel cloud (in un'area sicura, in un'area di cloud sovrana o in un'area commerciale) e dispone di *no* connettività al layer BlueXP SaaS. Gli utenti accedono a BlueXP localmente dalla console basata sul web disponibile dal connettore, non dal layer SaaS.

Una regione sicura include "Cloud segreto AWS", "Cloud AWS top secret", e. "Azure IL6"

Nella tabella seguente viene fornito un confronto di queste modalità.

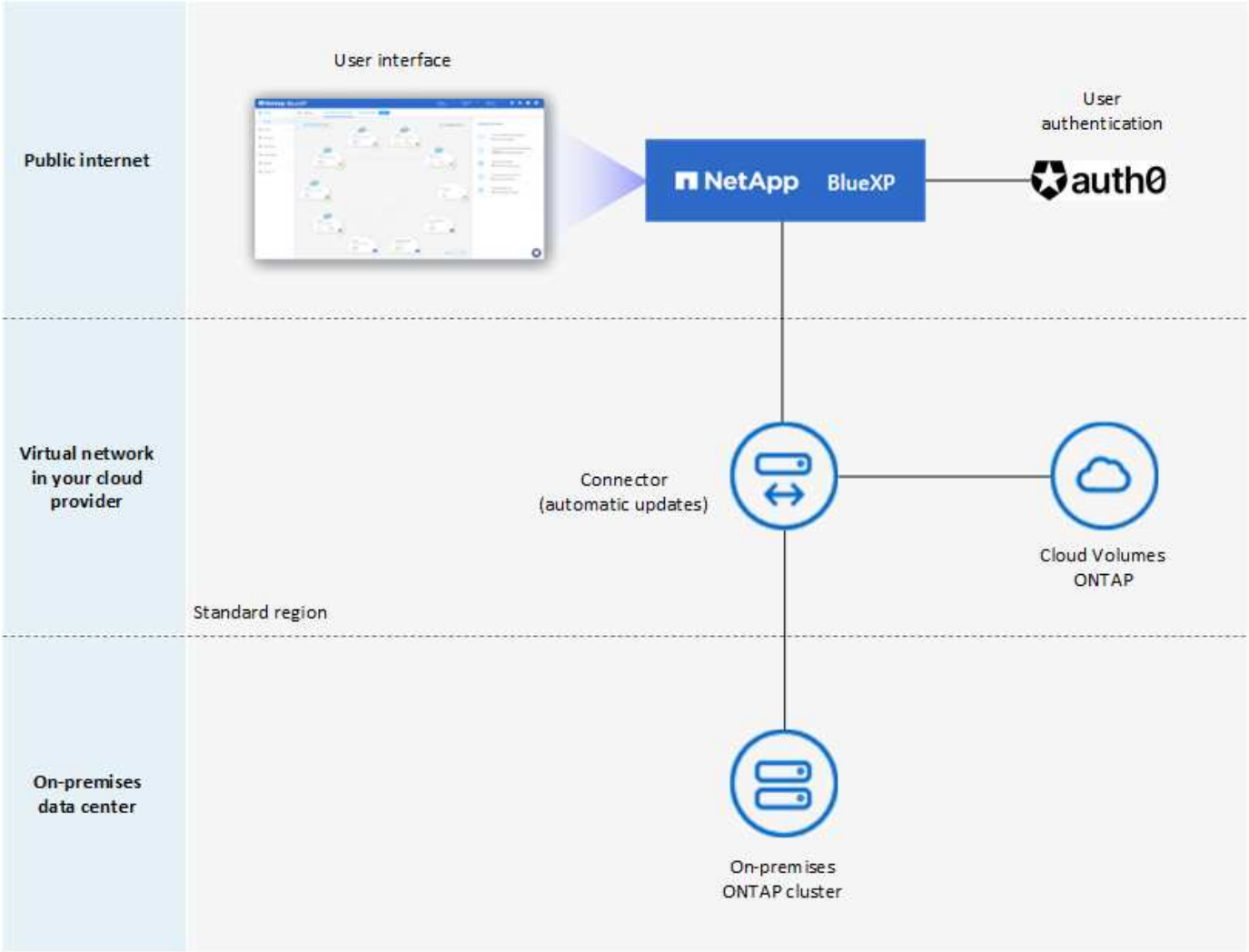
	Modalità standard	Modalità limitata	Modalità privata
Connessione richiesta a BlueXP SaaS Layer?	Sì	Solo in uscita	No

	Modalità standard	Modalità limitata	Modalità privata
Connessione richiesta al tuo cloud provider?	Sì	Sì, all'interno della regione	Sì, all'interno della regione (se si utilizza Cloud Volumes ONTAP)
Installazione del connettore	Da BlueXP, cloud marketplace o installazione manuale	Cloud marketplace o installazione manuale	Installazione manuale
Aggiornamenti del connettore	Aggiornamenti automatici del software NetApp Connector	Aggiornamenti automatici del software NetApp Connector	È richiesto l'aggiornamento manuale
Accesso all'interfaccia utente	Dal livello SaaS BlueXP	Localmente dal connettore VM	Localmente dal connettore VM
Endpoint API	Il livello BlueXP SaaS	Il connettore	Il connettore
Autenticazione	Tramite SaaS utilizzando auth0, accesso NSS o federazione di identità	Attraverso SaaS utilizzando auth0 o Identity Federation	Autenticazione utente locale
Storage e servizi dati	Sono supportati tutti	Molti sono supportati	Ne sono supportati diversi
Opzioni di licenza	Abbonamenti Marketplace e BYOL	Abbonamenti Marketplace e BYOL	BYOL

Leggi le sezioni seguenti per ulteriori informazioni su queste modalità, tra cui le funzionalità e i servizi di BlueXP supportati.

Modalità standard

L'immagine seguente è un esempio di implementazione in modalità standard.



BlueXP funziona come segue in modalità standard:

Comunicazione in uscita

La connettività è necessaria dal connettore al layer BlueXP SaaS, alle risorse pubblicamente disponibili del tuo cloud provider e ad altri componenti essenziali per le operazioni quotidiane.

- "Endpoint che il connettore contatta in AWS"
- "Endpoint che il connettore contatta in Azure"
- "Endpoint che il connettore contatta in Google Cloud"

Posizione supportata per il connettore

In modalità standard, il connettore è supportato nel cloud o on-premise.

Installazione del connettore

L'installazione del connettore è possibile da una procedura di installazione guidata in BlueXP, da AWS o Azure Marketplace, o utilizzando un programma di installazione per installare manualmente il connettore sul proprio host Linux nel data center o nel cloud.

Aggiornamenti del connettore

Gli aggiornamenti automatici del software del connettore sono disponibili da BlueXP con aggiornamenti mensili.

Accesso all'interfaccia utente

L'interfaccia utente è accessibile dalla console basata sul web fornita attraverso il layer SaaS.

Endpoint API

Le chiamate API vengono effettuate al seguente endpoint:
https://cloudmanager.cloud.netapp.com

Autenticazione

L'autenticazione viene fornita tramite il servizio cloud di BlueXP utilizzando auth0 o tramite gli accessi al NetApp Support Site (NSS). È disponibile la federazione delle identità.

Servizi BlueXP supportati

Tutti i servizi BlueXP sono disponibili per gli utenti.

Opzioni di licenza supportate

Gli abbonamenti Marketplace e BYOL sono supportati con la modalità standard; tuttavia, le opzioni di licenza supportate dipendono dal servizio BlueXP in uso. Consulta la documentazione relativa a ciascun servizio per ulteriori informazioni sulle opzioni di licenza disponibili.

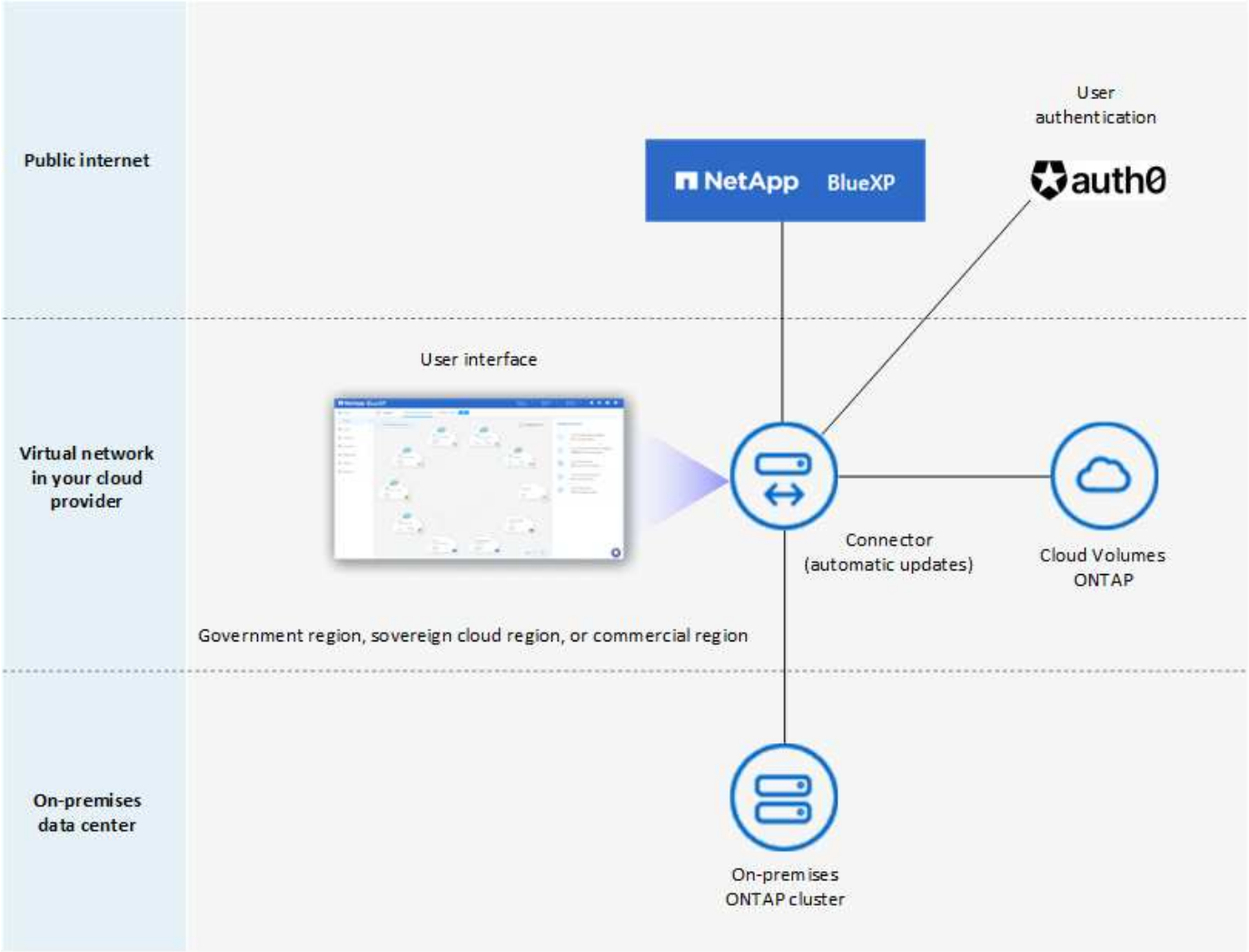
Come iniziare con la modalità standard

Accedere alla "Console BlueXP basata su web" e iscriverti.

"Scopri come iniziare a utilizzare la modalità standard".

Modalità limitata

L'immagine seguente è un esempio di implementazione in modalità limitata.



BlueXP funziona come segue in modalità limitata:

Comunicazione in uscita

La connettività in uscita è necessaria dal connettore al livello BlueXP SaaS per utilizzare i servizi dati BlueXP, per abilitare gli aggiornamenti software automatici del connettore, per utilizzare l'autenticazione basata su auth0 e per inviare metadati a scopo di addebito (nome della VM di storage, capacità allocata e UUID volume, tipo e IOPS).

Il layer BlueXP SaaS non avvia la comunicazione con il connettore. Tutte le comunicazioni vengono avviate dal connettore, che può estrarre o trasferire i dati da o verso il layer SaaS secondo necessità.

È inoltre necessaria una connessione per le risorse del cloud provider dall'interno della regione.

Posizione supportata per il connettore

In modalità limitata, il connettore è supportato nel cloud: In un'area governativa, in un'area sovrana o in un'area commerciale.

Installazione del connettore

L'installazione del connettore è possibile da AWS o Azure Marketplace o da un'installazione manuale sul proprio host Linux.

Aggiornamenti del connettore

Gli aggiornamenti automatici del software del connettore sono disponibili da BlueXP con aggiornamenti mensili.

Accesso all'interfaccia utente

L'interfaccia utente è accessibile dalla macchina virtuale del connettore implementata nella regione del cloud.

Endpoint API

Le chiamate API vengono effettuate alla macchina virtuale del connettore.

Autenticazione

L'autenticazione viene fornita tramite il servizio cloud di BlueXP utilizzando auth0. È disponibile anche la federazione delle identità.

Servizi BlueXP supportati

BlueXP supporta i seguenti servizi di storage e dati in modalità limitata:

Servizi supportati	Note
Amazon FSX per ONTAP	Supporto completo
Azure NetApp Files	Supporto completo
Backup e recovery	Supportato in regioni governative e commerciali con modalità limitata. Non supportato nelle regioni sovrane con modalità limitata. In modalità limitata, il backup e recovery di BlueXP supporta il backup e il ripristino dei soli dati del volume ONTAP. "Consente di visualizzare l'elenco delle destinazioni di backup supportate per i dati ONTAP" Il backup e il ripristino dei dati applicativi, dei dati delle macchine virtuali e dei dati Kubernetes non sono supportati.
Classificazione	Supportato nelle regioni governative con modalità limitata. Non supportato in aree commerciali o in aree sovrane con modalità limitata. Si applicano le seguenti limitazioni: • Impossibile eseguire la scansione di account OneDrive, SharePoint e Google Drive. • La funzionalità dell'etichetta AIP (Microsoft Azure Information Protection) non può essere integrata.
Cloud Volumes ONTAP	Supporto completo

Servizi supportati	Note
Portafoglio digitale	Per la modalità limitata, puoi utilizzare il portafoglio digitale con le opzioni di licenza supportate elencate di seguito.
Cluster ONTAP on-premise	Sono supportati sia il rilevamento con un connettore che il rilevamento senza un connettore (rilevamento diretto). Quando si rileva un cluster on-premise con un connettore, la visualizzazione avanzata (System Manager) non è supportata.
Replica	Supportato nelle regioni governative con modalità limitata. Non supportato in aree commerciali o in aree sovrane con modalità limitata.

Opzioni di licenza supportate

Con la modalità limitata sono supportate le seguenti opzioni di licenza:

- Abbonamenti al marketplace (contratti orari e annuali)

  Tenere presente quanto segue:

  - Per Cloud Volumes ONTAP, sono supportate solo le licenze basate sulla capacità.
  - In Azure, i contratti annuali non sono supportati dalle regioni governative.
- BYOL

  Per Cloud Volumes ONTAP, BYOL supporta sia licenze basate su capacità che licenze basate su nodo.

Come iniziare con la modalità limitata

È necessario attivare la modalità limitata quando si crea l'account BlueXP.

Se non disponi ancora di un account, ti verrà richiesto di creare il tuo account e attivare la modalità limitata quando accedi a BlueXP per la prima volta da un connettore che hai installato manualmente o che hai creato dal mercato del tuo provider di servizi cloud.

Se si dispone già di un account e si desidera crearne un altro, è necessario utilizzare l'API tenancy.

Tenere presente che non è possibile modificare l'impostazione della modalità limitata dopo la creazione dell'account da parte di BlueXP. Non puoi attivare la modalità limitata in un secondo momento e non puoi disattivarla in un secondo momento. Deve essere impostato al momento della creazione dell'account.

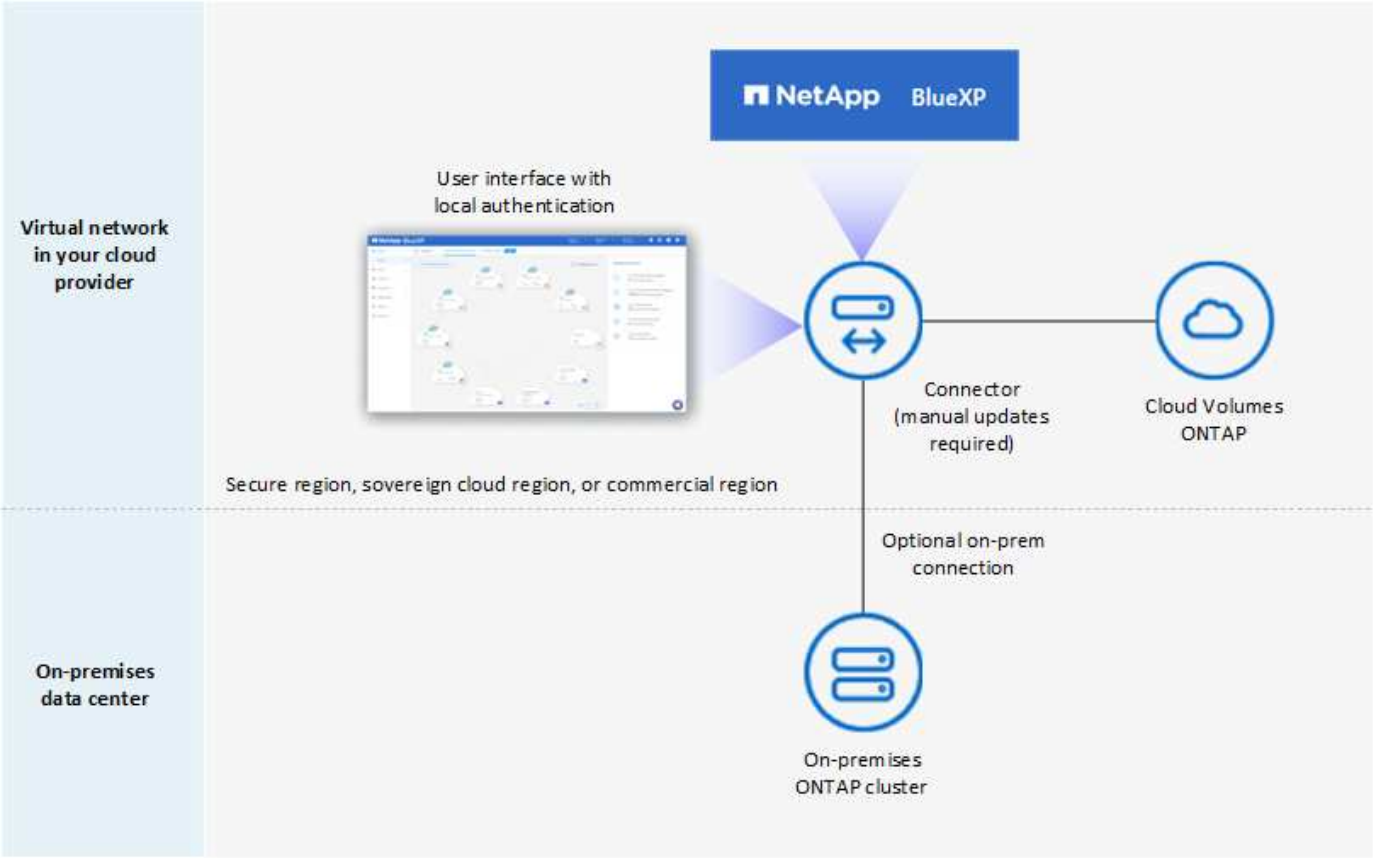
- "Scopri come iniziare a utilizzare la modalità limitata".
- "Scopri come creare un account BlueXP aggiuntivo".

Modalità privata

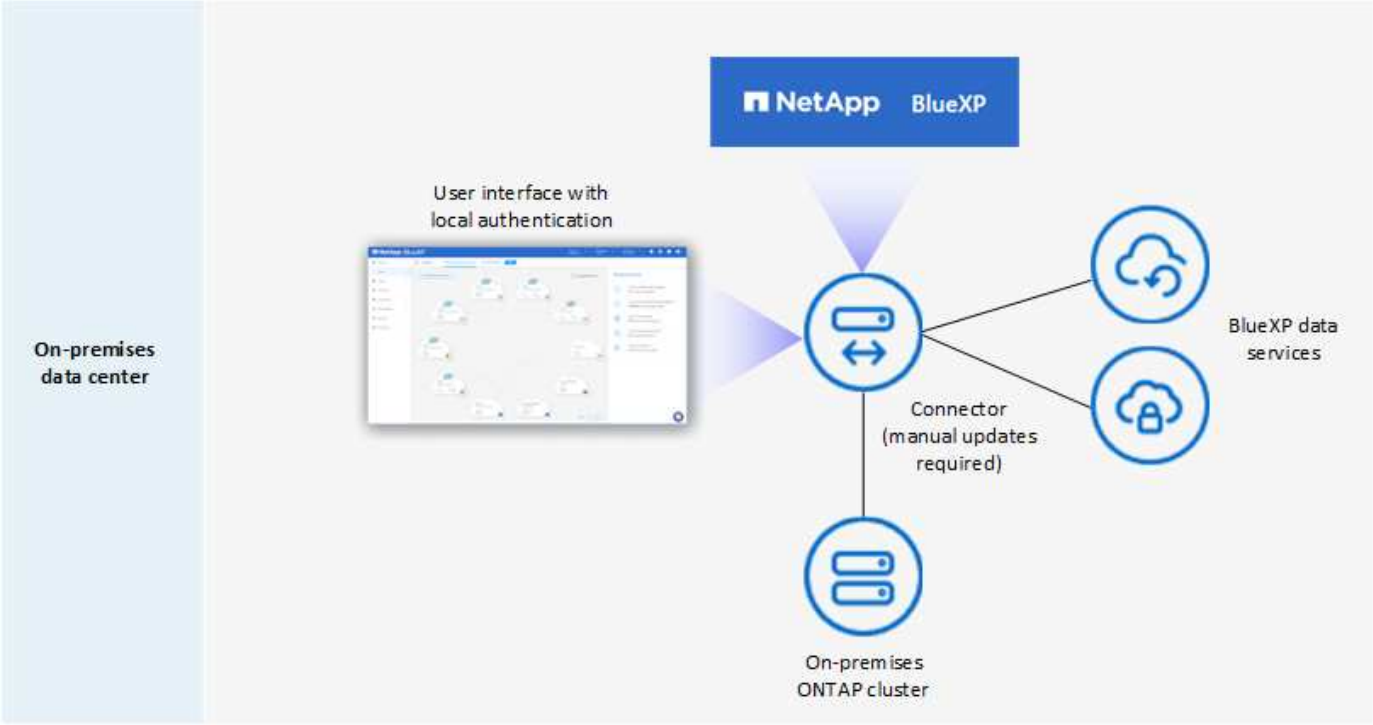
In modalità privata, è possibile installare un connettore on-premise o nel cloud e utilizzare BlueXP per gestire i dati nel cloud ibrido. Non è disponibile alcuna connettività al livello BlueXP SaaS.

L'immagine seguente mostra un esempio di implementazione in modalità privata in cui il connettore è installato

nel cloud e gestisce sia Cloud Volumes ONTAP che un cluster ONTAP on-premise.



Nel frattempo, la seconda immagine mostra un esempio di implementazione in modalità privata in cui il connettore viene installato on-premise, gestisce un cluster ONTAP on-premise e fornisce l'accesso ai servizi dati BlueXP supportati.



BlueXP funziona come segue in modalità privata:

Comunicazione in uscita

Non è richiesta alcuna connettività in uscita per il layer BlueXP SaaS. Tutti i pacchetti, le dipendenze e i componenti essenziali vengono forniti con il connettore e forniti dalla macchina locale. La connettività alle risorse pubblicamente disponibili del tuo cloud provider è necessaria solo se stai implementando Cloud Volumes ONTAP.

Posizione supportata per il connettore

In modalità privata, il connettore è supportato nel cloud o on-premise.

Installazione del connettore

Le installazioni manuali del connettore sono supportate sul proprio host Linux nel cloud o on-premise.

Aggiornamenti del connettore

È necessario aggiornare manualmente il software del connettore. Il software Connector viene pubblicato sul sito di supporto NetApp a intervalli non definiti.

Accesso all'interfaccia utente

L'interfaccia utente è accessibile dal connettore implementato nella tua area cloud o on-premise.

Endpoint API

Le chiamate API vengono effettuate alla macchina virtuale del connettore.

Autenticazione

L'autenticazione viene fornita attraverso la gestione e l'accesso degli utenti locali. L'autenticazione non viene fornita attraverso il servizio cloud di BlueXP.

Servizi BlueXP supportati nelle implementazioni cloud

BlueXP supporta i seguenti servizi di storage e dati in modalità privata quando il connettore viene installato nel cloud:

Servizi supportati	Note
Backup e recovery	Supportato nelle aree commerciali di AWS e Azure. Non supportato in Google Cloud o in "Cloud segreto AWS", "Cloud AWS top secret", o. "Azure IL6" In modalità privata, il backup e recovery di BlueXP supporta il backup e il ripristino dei soli dati del volume ONTAP. "Consente di visualizzare l'elenco delle destinazioni di backup supportate per i dati ONTAP" Il backup e il ripristino dei dati applicativi, dei dati delle macchine virtuali e dei dati Kubernetes non sono supportati.
Cloud Volumes ONTAP	Poiché non è disponibile l'accesso a Internet, non sono disponibili le seguenti funzioni: Aggiornamenti software automatici e AutoSupport.

Servizi supportati	Note
Portafoglio digitale	È possibile utilizzare il portafoglio digitale con le opzioni di licenza supportate elencate di seguito per la modalità privata.
Cluster ONTAP on-premise	Richiede la connettività dal cloud (dove è installato il connettore) all'ambiente on-premise. Il rilevamento senza connettore (rilevamento diretto) non è supportato.

Servizi BlueXP supportati nelle implementazioni on-premise

BlueXP supporta i seguenti servizi di storage e dati con modalità privata quando il connettore viene installato in sede:

Servizi supportati	Note
Backup e recovery	In modalità privata, il backup e recovery di BlueXP supporta il backup e il ripristino dei soli dati del volume ONTAP. "Visualizza l'elenco delle destinazioni di backup supportate per i dati dei volumi ONTAP" Il backup e il ripristino dei dati applicativi, dei dati delle macchine virtuali e dei dati Kubernetes non sono supportati.
Classificazione	• Le uniche origini dati supportate sono quelle che è possibile rilevare localmente. "Visualizzare le fonti che è possibile scoprire localmente" • Le funzioni che richiedono l'accesso a Internet in uscita non sono supportate. "Visualizza le limitazioni delle funzioni"
Portafoglio digitale	È possibile utilizzare il portafoglio digitale con le opzioni di licenza supportate elencate di seguito per la modalità privata.
Cluster ONTAP on-premise	Il rilevamento senza connettore (rilevamento diretto) non è supportato.
Replica	Supporto completo

Opzioni di licenza supportate

Solo BYOL è supportato in modalità privata.

Per Cloud Volumes ONTAP BYOL, è supportata solo la licenza basata su nodo. Le licenze basate sulla capacità non sono supportate. Poiché non è disponibile una connessione Internet in uscita, è necessario caricare manualmente il file di licenza Cloud Volumes ONTAP nel portafoglio digitale BlueXP.

"Scopri come aggiungere licenze al portafoglio digitale BlueXP"

Come iniziare con la modalità privata

La modalità privata è disponibile scaricando il programma di installazione "offline" dal NetApp Support Site.

"Scopri come iniziare a utilizzare la modalità privata".

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

Confronto tra servizi e funzionalità

La seguente tabella consente di identificare rapidamente i servizi e le funzionalità di BlueXP supportati in modalità limitata e privata.

Alcuni servizi potrebbero essere supportati con limitazioni. Per ulteriori informazioni su come questi servizi sono supportati in modalità limitata e privata, fare riferimento alle sezioni precedenti.

Area di prodotto	Servizio o funzione BlueXP	Modalità limitata	Modalità privata
Ambienti di lavoro Questa parte della tabella elenca il supporto per la gestione dell'ambiente di lavoro da BlueXP Canvas. Non indica le destinazioni di backup supportate per backup e recovery BlueXP.	Amazon FSX per ONTAP	Sì	No
	Amazon S3	No	No
	Azure Blob	No	No
	Azure NetApp Files	Sì	No
	Cloud Volumes ONTAP	Sì	Sì
	Cloud Volumes Service per Google Cloud	No	No
	Storage Google Cloud	No	No
	Cluster Kubernetes	No	No
	Cluster ONTAP on-premise	Sì	Sì
	E-Series	No	No
	StorageGRID	No	No

Area di prodotto	Servizio o funzione BlueXP	Modalità limitata	Modalità privata
Servizi	Backup e recovery	Sì "Visualizza l'elenco delle destinazioni di backup supportate per i dati dei volumi ONTAP"	Sì "Visualizza l'elenco delle destinazioni di backup supportate per i dati dei volumi ONTAP"
	Classificazione	Sì	Sì
	Operazioni cloud	No	No
	Copia e sincronizzazione	No	No
	Consulente digitale	No	No
	Portafoglio digitale	Sì	Sì
	Disaster recovery	No	No
	Efficienza economica	No	No
	Caching edge	No	No
	Report sulla migrazione	No	No
	Resilienza operativa	No	No
	Protezione ransomware	No	No
	Replica	Sì	Sì
	Sostenibilità	No	No
	Tiering	No	No
	Caching dei volumi	No	No
Caratteristiche	Credenziali	Sì	Sì
	Account NSS	Sì	No
	Notifiche	Sì	No
	Cerca	Sì	No
	Tempistiche	Sì	Sì

Inizia con la modalità standard

Flusso di lavoro introduttivo (modalità standard)

Inizia con BlueXP in modalità standard preparando il networking per la console BlueXP, iscrivendoti e creando un account, creando facoltativamente un connettore e iscrivendoti a BlueXP.

In modalità standard, BlueXP è accessibile agli utenti come servizio cloud dalla console basata su web. Prima di iniziare, dovresti avere una conoscenza di "BlueXP", "Connettori", e. "modalità di distribuzione".

1 **"Preparazione del networking per l'utilizzo della console BlueXP"**

I computer che accedono alla console BlueXP devono disporre di connessioni a endpoint specifici per completare alcune attività amministrative. Se la rete limita l'accesso in uscita, è necessario assicurarsi che questi endpoint siano consentiti.

2 **"Registrati e crea un account"**

Accedere alla "Console BlueXP" e iscriverti. Ti verrà offerta la possibilità di creare un account, ma puoi saltare questo passaggio se sei invitato a un account esistente.

A questo punto, hai effettuato l'accesso e puoi iniziare a utilizzare diversi servizi BlueXP come Consulente digitale, Amazon FSX per ONTAP, Azure NetApp Files e altri ancora. "Scopri cosa puoi fare senza un connettore".

3 **Creare un connettore**

Non è necessario un connettore per iniziare a utilizzare BlueXP, ma è possibile creare un connettore per sbloccare tutte le funzionalità e i servizi di BlueXP. Il connettore è il software NetApp che consente a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud ibrido.

Un account Admin BlueXP può creare un connettore nel cloud o nella rete on-premise.

- "Scopri di più su quando sono necessari i connettori e sul loro funzionamento"
- "Scopri come creare un connettore in AWS"
- "Scopri come creare un connettore in Azure"
- "Scopri come creare un connettore in Google Cloud"
- "Scopri come creare un connettore on-premise"

Nota: Se si desidera utilizzare i servizi BlueXP per gestire lo storage e i dati in Google Cloud, il connettore deve essere in esecuzione in Google Cloud.

4 **"Iscriviti a BlueXP"**

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

Preparazione del networking per l'utilizzo della console BlueXP

Quando utilizzi la console basata sul web BlueXP fornita attraverso il livello SaaS, contatta diversi endpoint quando completi alcuni task amministrativi. I computer che accedono alla console BlueXP devono disporre di connessioni a questi endpoint.

Questi endpoint vengono contattati dal computer di un utente quando si completano azioni specifiche dalla console BlueXP. Fai anche riferimento ai requisiti di rete per il connettore e per servizi BlueXP specifici. Per ulteriori informazioni, fare riferimento ai link correlati alla fine di questa pagina.

Endpoint	Scopo
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	Il browser Web contatta questi URL quando si utilizza la console basata su Web BlueXP.
https://aiq.netapp.com	Richieste per accedere al Digital Advisor di BlueXP.
Servizi AWS (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • S3 (Simple Storage Service)	Necessario per implementare un connettore da BlueXP in AWS. L'endpoint esatto dipende dalla regione in cui viene implementato il connettore. "Per ulteriori informazioni, fare riferimento alla documentazione AWS."
https://management.azure.com https://login.microsoftonline.com	Necessario per implementare un connettore da BlueXP nella maggior parte delle regioni Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Necessario per implementare un connettore da BlueXP nelle regioni di Azure Germania.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Necessario per implementare un connettore da BlueXP nelle regioni Azure US Gov.
https://www.googleapis.com	Necessario per implementare un connettore di BlueXP in Google Cloud.
https://signin.b2c.netapp.com	Necessario per aggiornare le credenziali NetApp Support Site (NSS) o per aggiungere nuove credenziali NSS a BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite BlueXP.
https://widget.intercom.io	Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp.

Oltre a questi endpoint, è anche necessario garantire che il connettore disponga dell'accesso a Internet in uscita per contattare endpoint specifici per le operazioni quotidiane. Puoi trovare l'elenco di questi endpoint seguendo i link nella sezione successiva.

Link correlati

- Preparare il collegamento in rete per il connettore
  - "Configurare la rete AWS"
  - "Configurare il networking Azure"
  - "Configurare il networking Google Cloud"
  - "Configurare il networking on-premise"

- Preparare il networking per i servizi BlueXP

  Fai riferimento alla documentazione di ogni servizio BlueXP.

  "Documentazione BlueXP"

Iscriviti a BlueXP

BlueXP è accessibile da una console basata su web. Una volta iniziato a utilizzare BlueXP, il primo passo consiste nell'iscriversi utilizzando le credenziali del sito di supporto NetApp o creando un login cloud NetApp.

A proposito di questa attività

È possibile iscriversi a BlueXP utilizzando una delle seguenti opzioni:

- Le tue credenziali NetApp Support Site (NSS) esistenti
- Un login cloud NetApp specificando il tuo indirizzo e-mail e una password

Entrambe le opzioni supportano una connessione federated, che consente il single sign-on utilizzando le credenziali della directory aziendale (identità federata). È possibile configurare una connessione federativa dopo l'iscrizione. "Scopri come utilizzare la federazione delle identità con BlueXP".

Fasi

1. Aprire un browser Web e accedere a. "Console BlueXP"
2. Se disponi di un account NetApp Support Site, inserisci l'indirizzo e-mail associato al tuo account NSS direttamente nella pagina **Log in**.

   Se disponi di un account NSS, puoi saltare la pagina di registrazione. BlueXP ti iscriverà come parte di questo login iniziale.

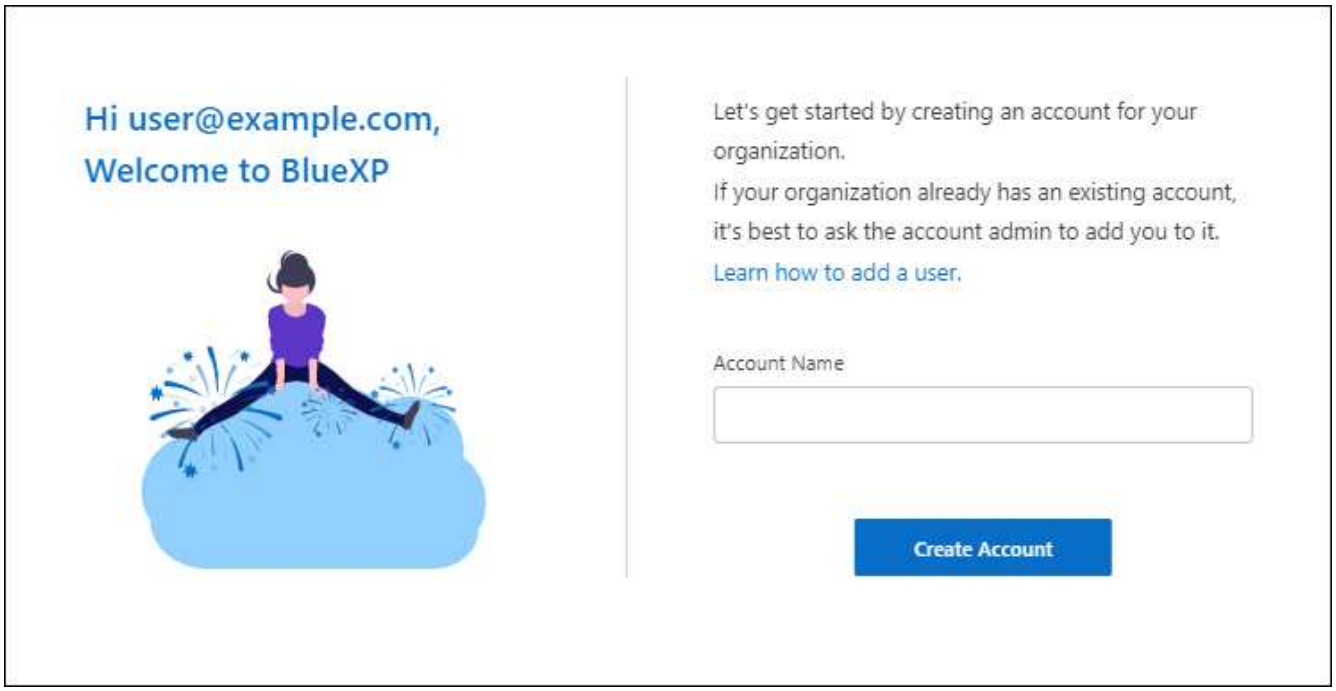
3. Se non disponi di un account NSS e desideri registrarti creando un login cloud NetApp, seleziona **Registrati**.
4. Nella pagina **Registrati**, inserisci le informazioni richieste per creare un login al cloud NetApp.

   Nel modulo di iscrizione sono consentiti solo caratteri inglesi.

5. Quando richiesto, leggere il Contratto di licenza con l'utente finale e accettare i termini.
6. Nella pagina **Benvenuto**, immettere un nome per l'account.

   Se la tua azienda dispone già di un account e vuoi iscriverti, devi chiudere BlueXP e chiedere al proprietario di associarti all'account. Dopo che il proprietario ti ha aggiunto, puoi accedere e accedere all'account. "Scopri come aggiungere membri a un account esistente".

   Un account è l'elemento di primo livello della piattaforma per le identità di NetApp. Consente di aggiungere e gestire utenti, ruoli, autorizzazioni e ambienti di lavoro.



7. Selezionare **Crea account**.

Risultato

Ora disponi di un account e di un account di accesso BlueXP. Nella maggior parte dei casi, il passaggio successivo consiste nella creazione di un connettore che connette i servizi di BlueXP al tuo ambiente di cloud ibrido.

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.

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.

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.

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".

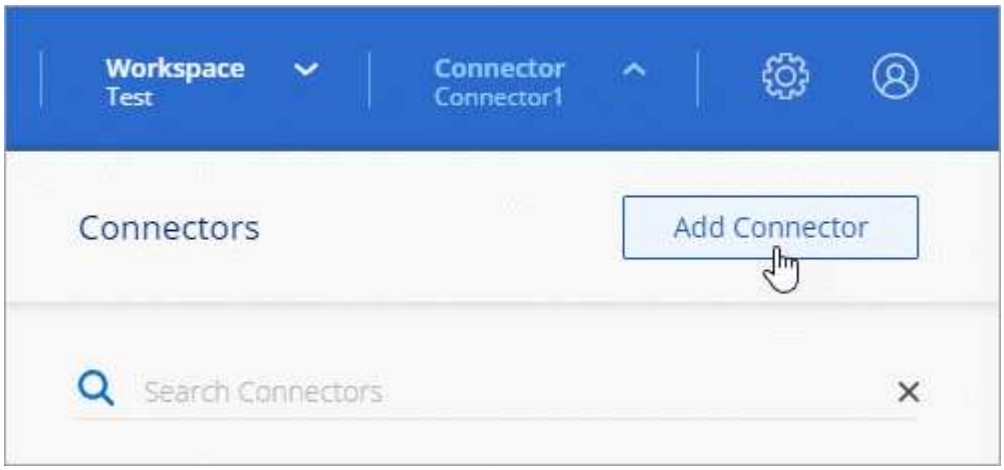
Prima di iniziare

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".

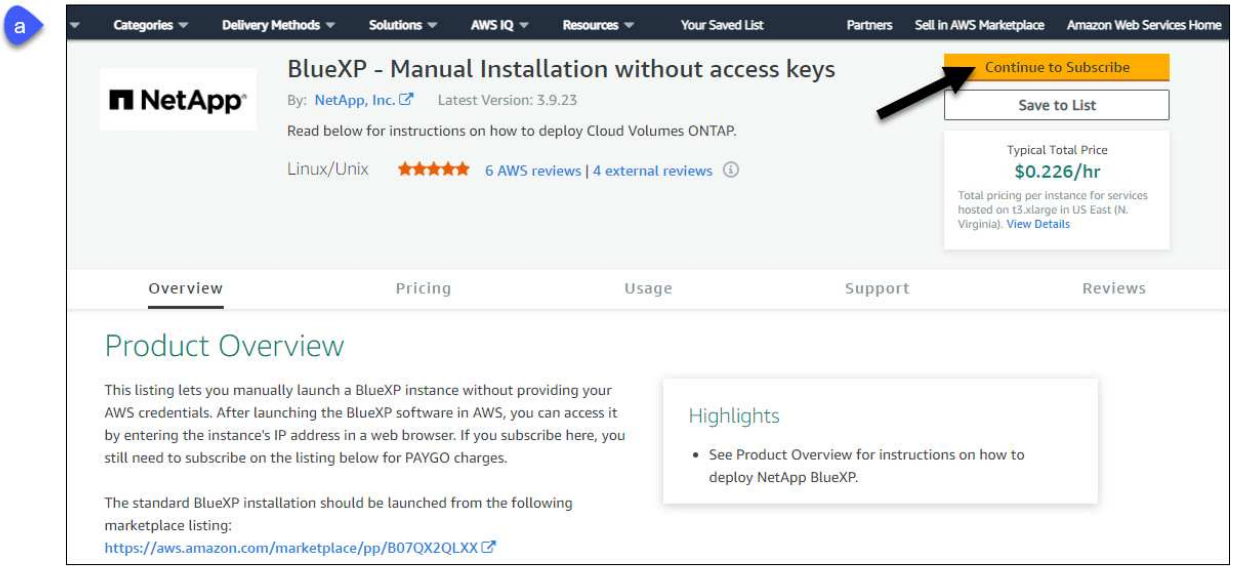
Prima di iniziare

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.

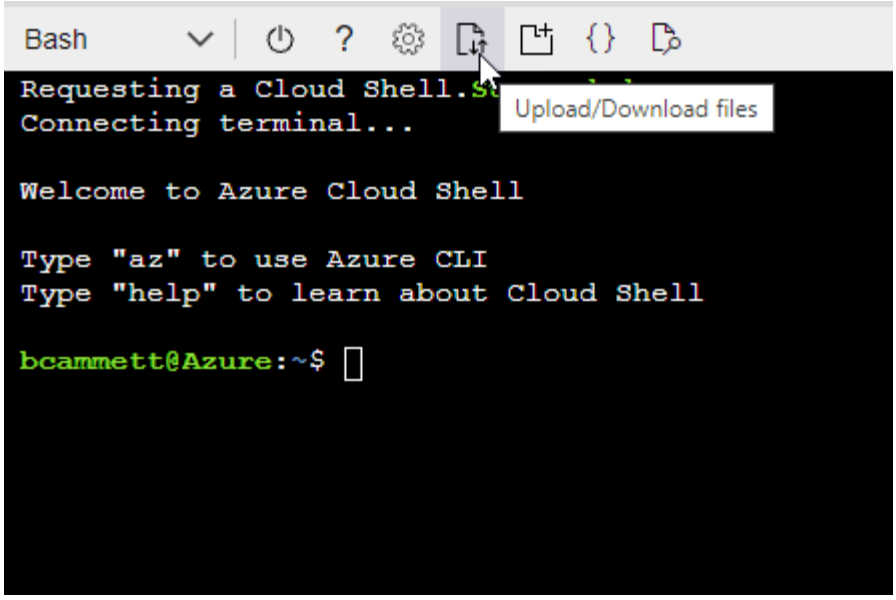
   Esempio

```
"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.

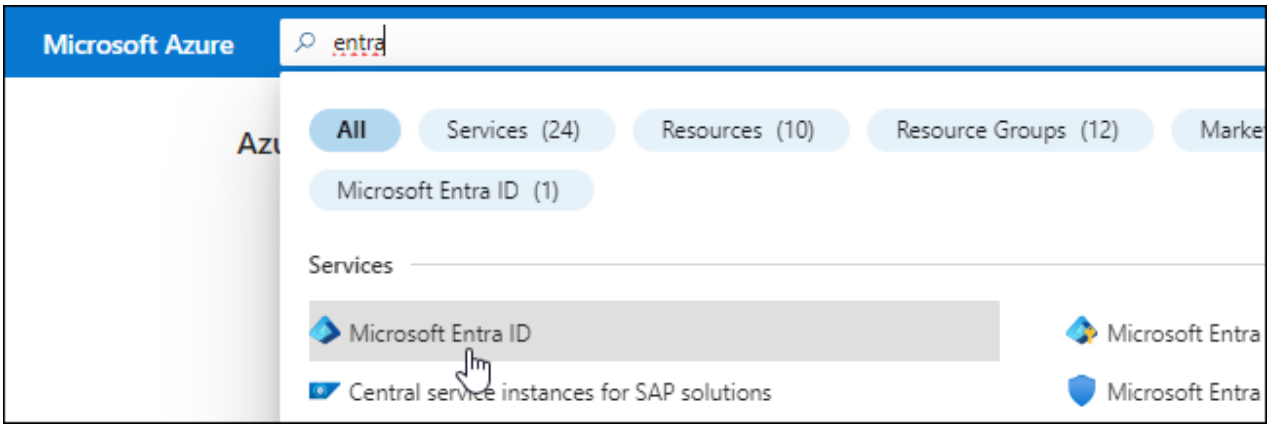
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP.

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**.

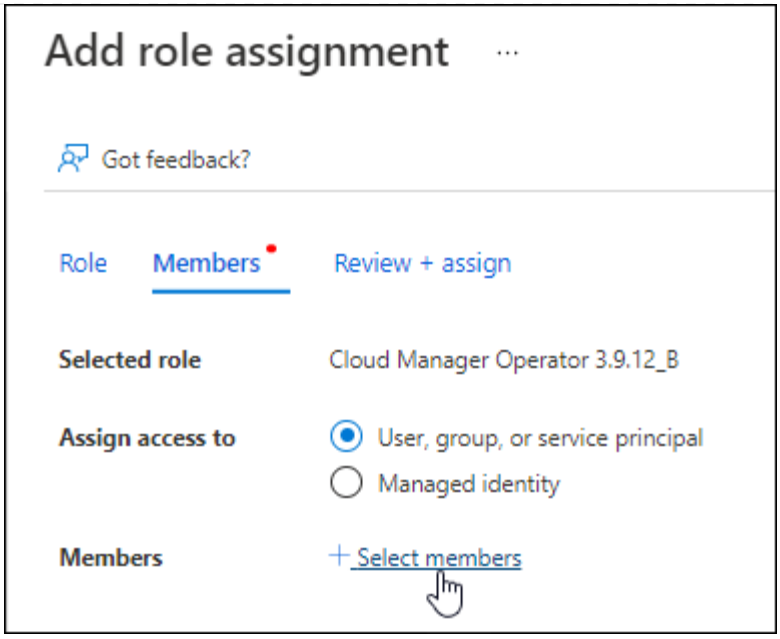
   Hai creato l'applicazione ad e il service principal.

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:

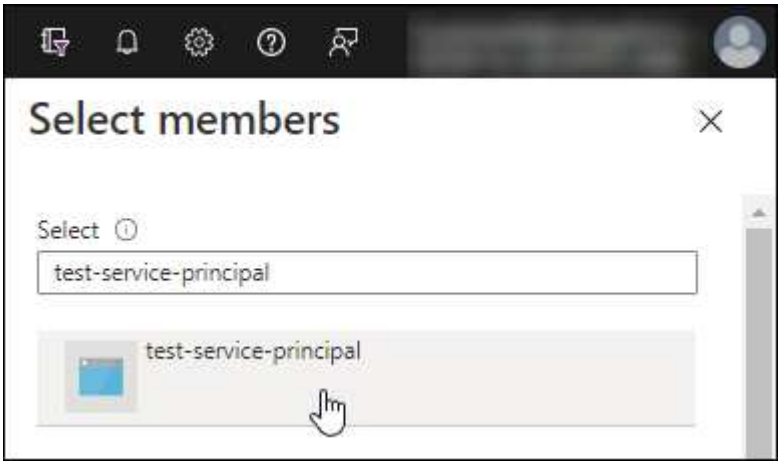
   a. Mantieni selezionata l'opzione **User, group o service principal**.

   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**.

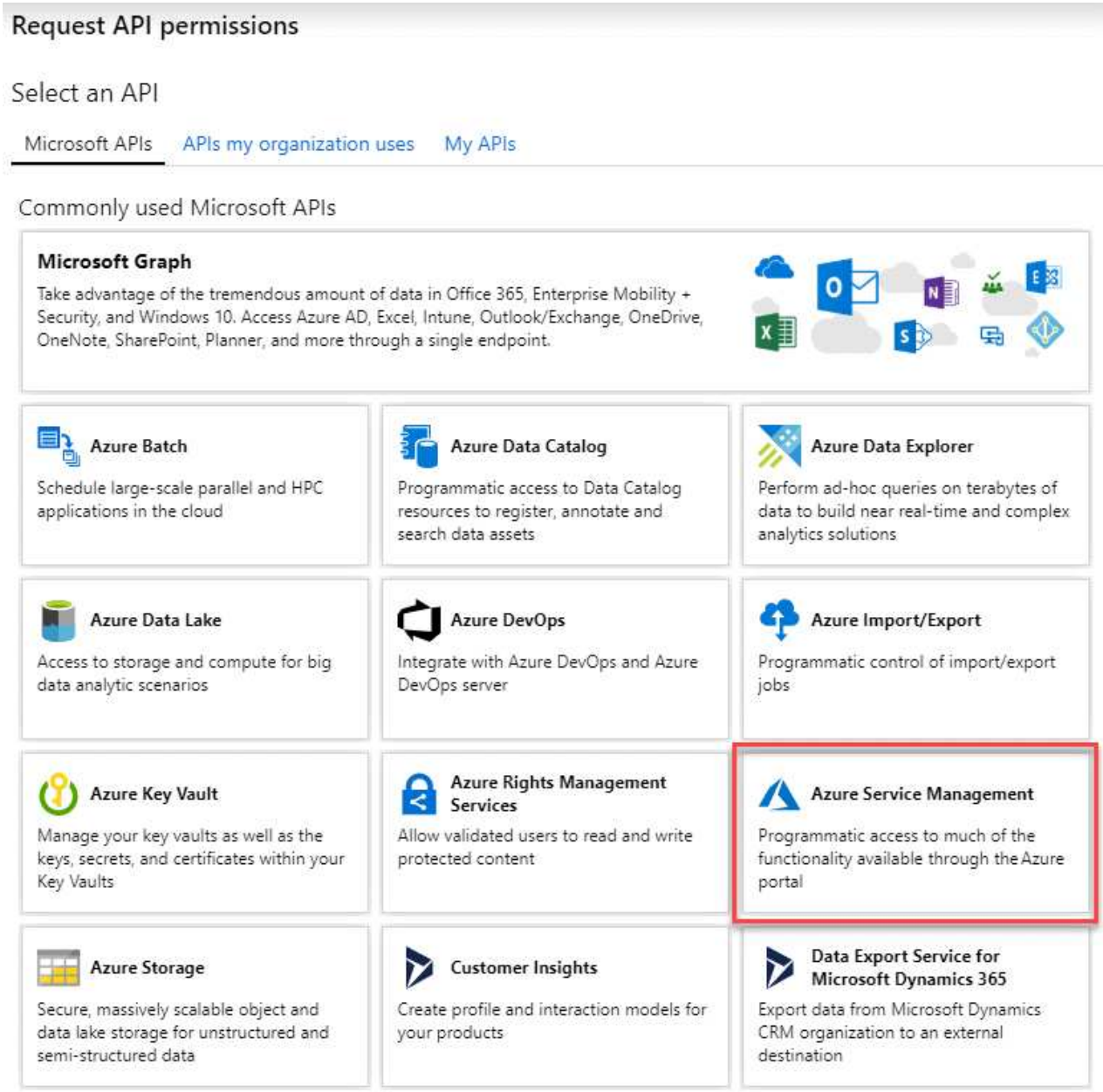
6. Fare clic su **Rivedi + assegna**.

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

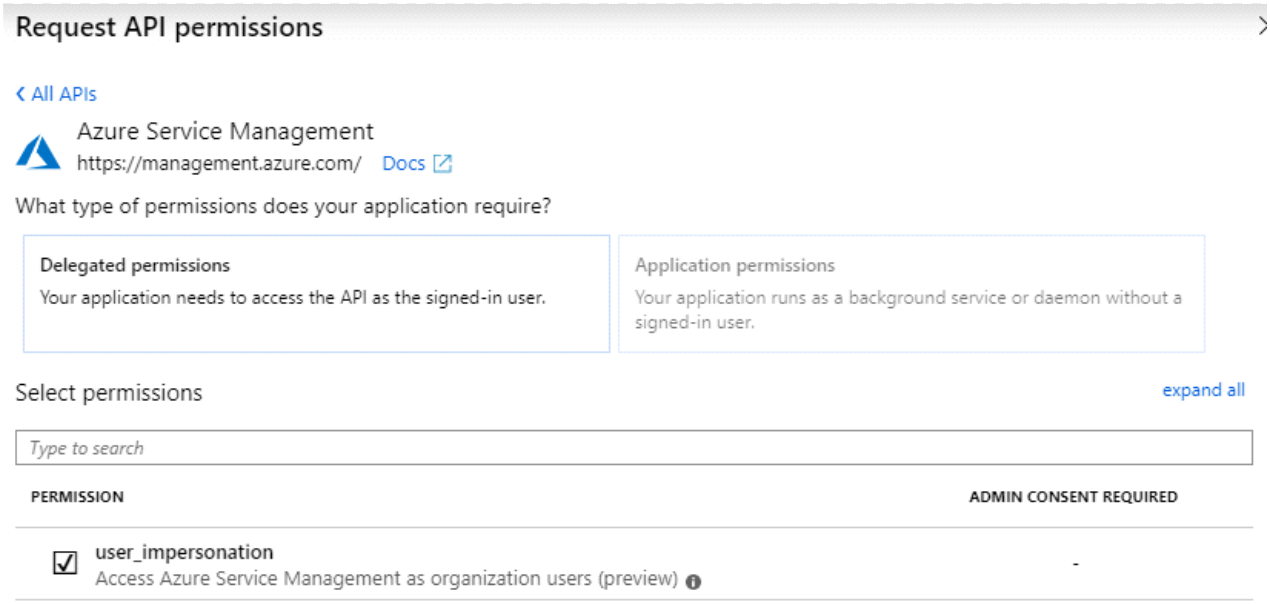
   Se si desidera gestire le risorse in più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. Ad esempio, BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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**.

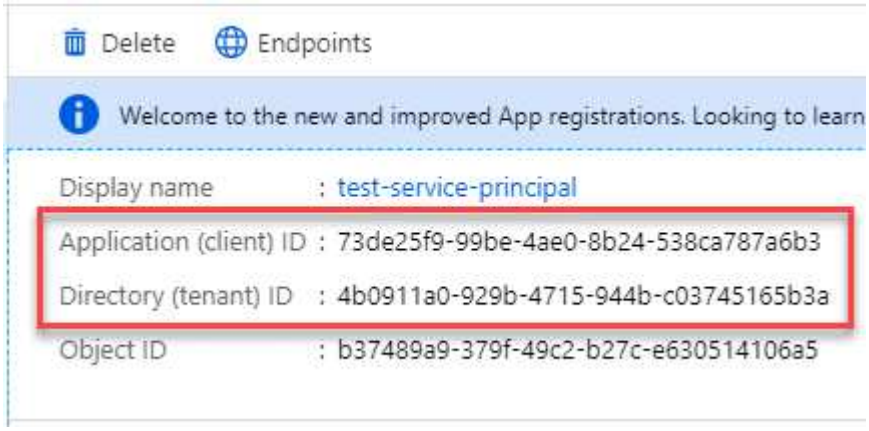


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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.

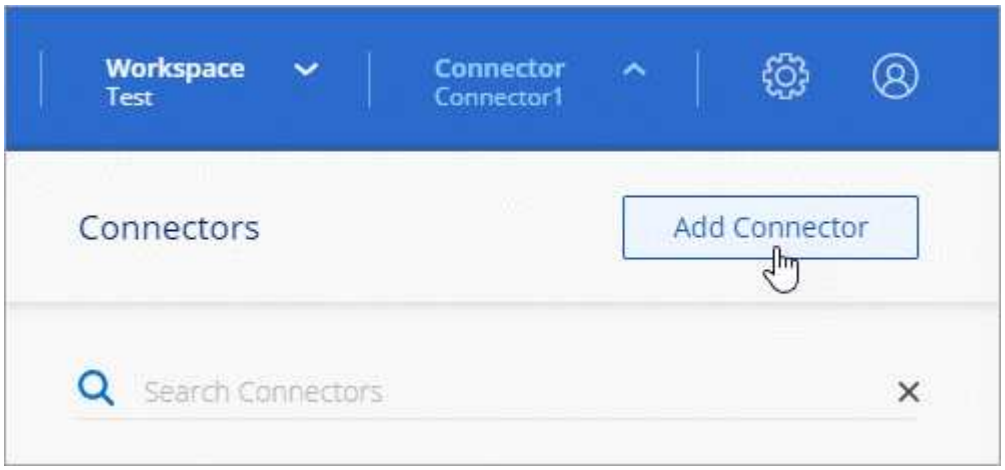
  "Scopri di più sulla connessione a una macchina virtuale Linux in Azure"

- 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.

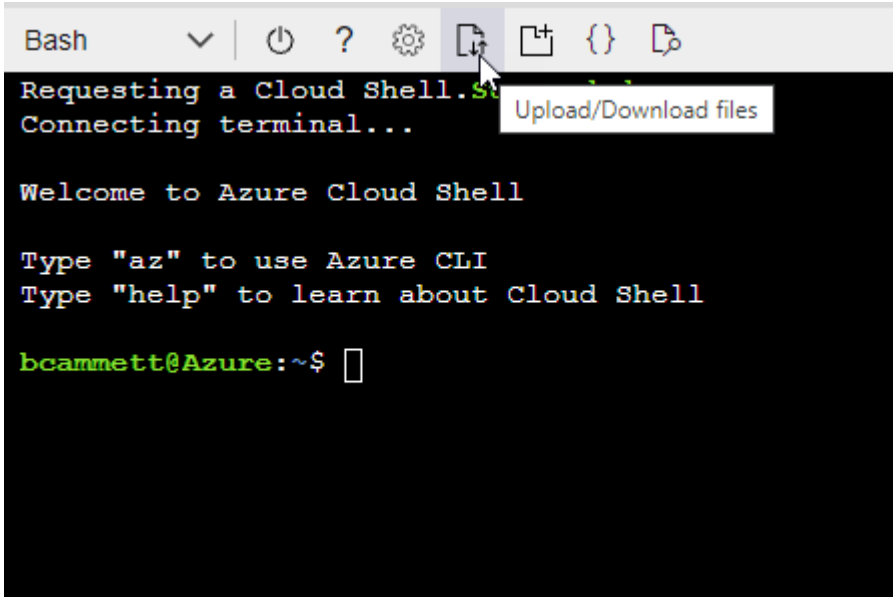
   Esempio

   ```
   "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

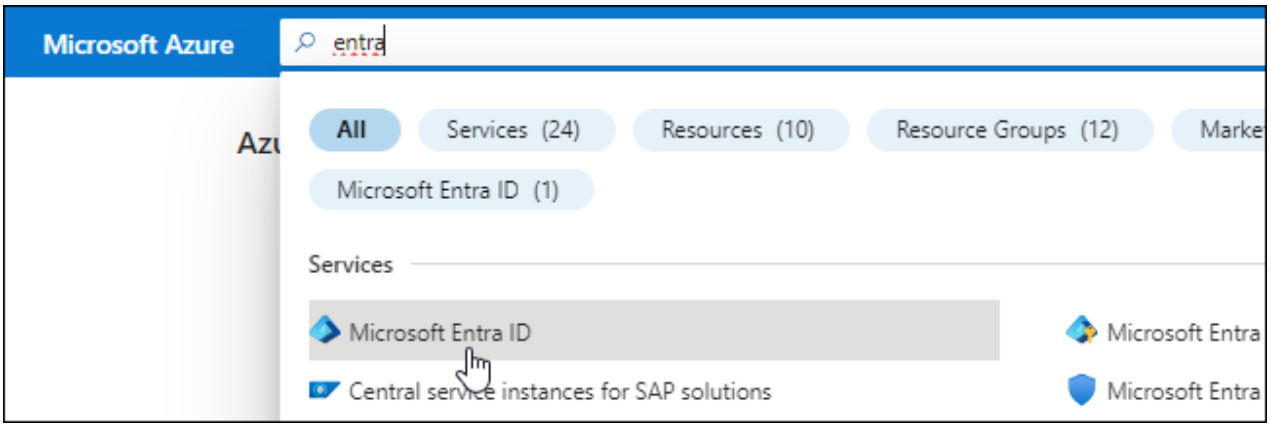
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP.

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.

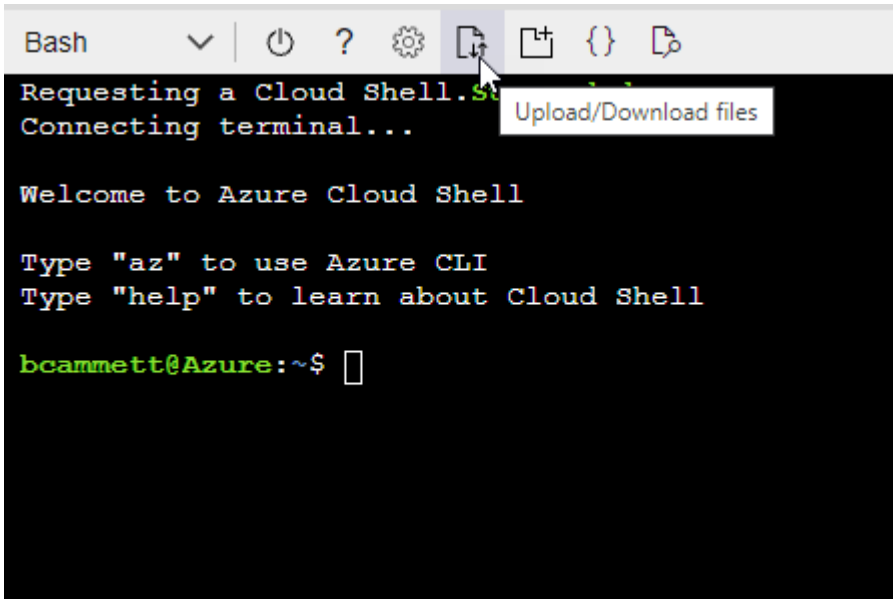
   Esempio

```
"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
```

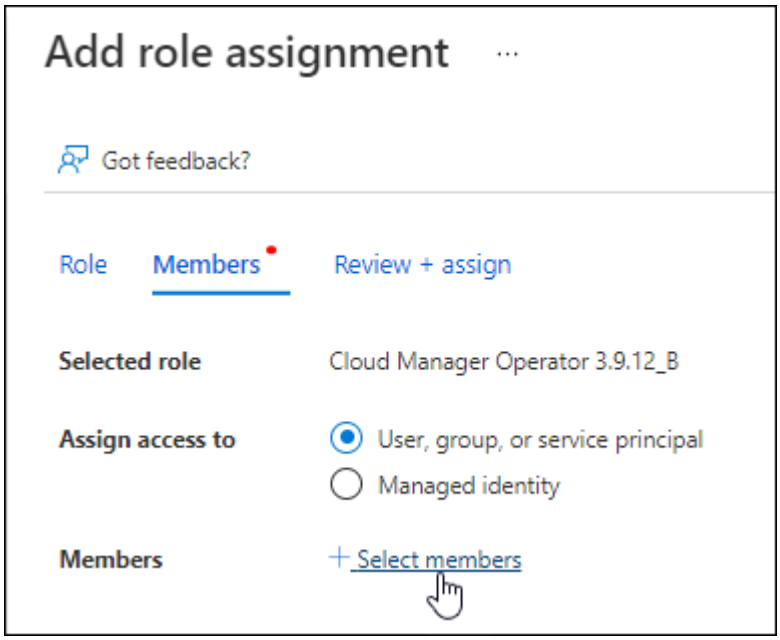
   A questo punto, dovrebbe essere disponibile un ruolo personalizzato denominato BlueXP

Operator che è possibile assegnare alla macchina virtuale Connector.

2. Assegnare l'applicazione al ruolo:

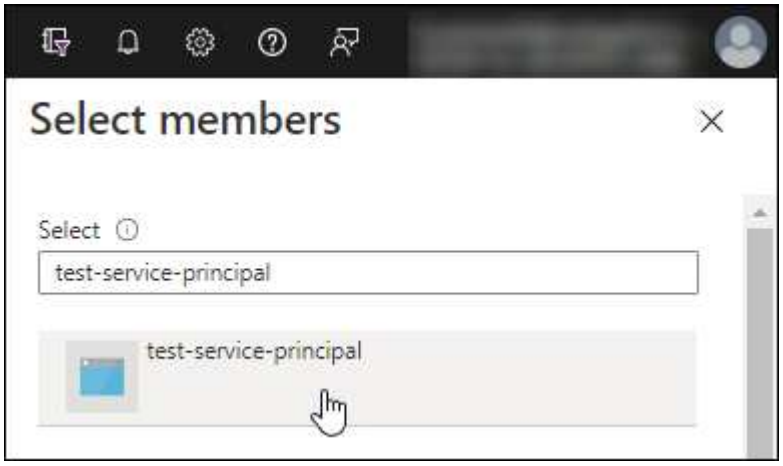
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

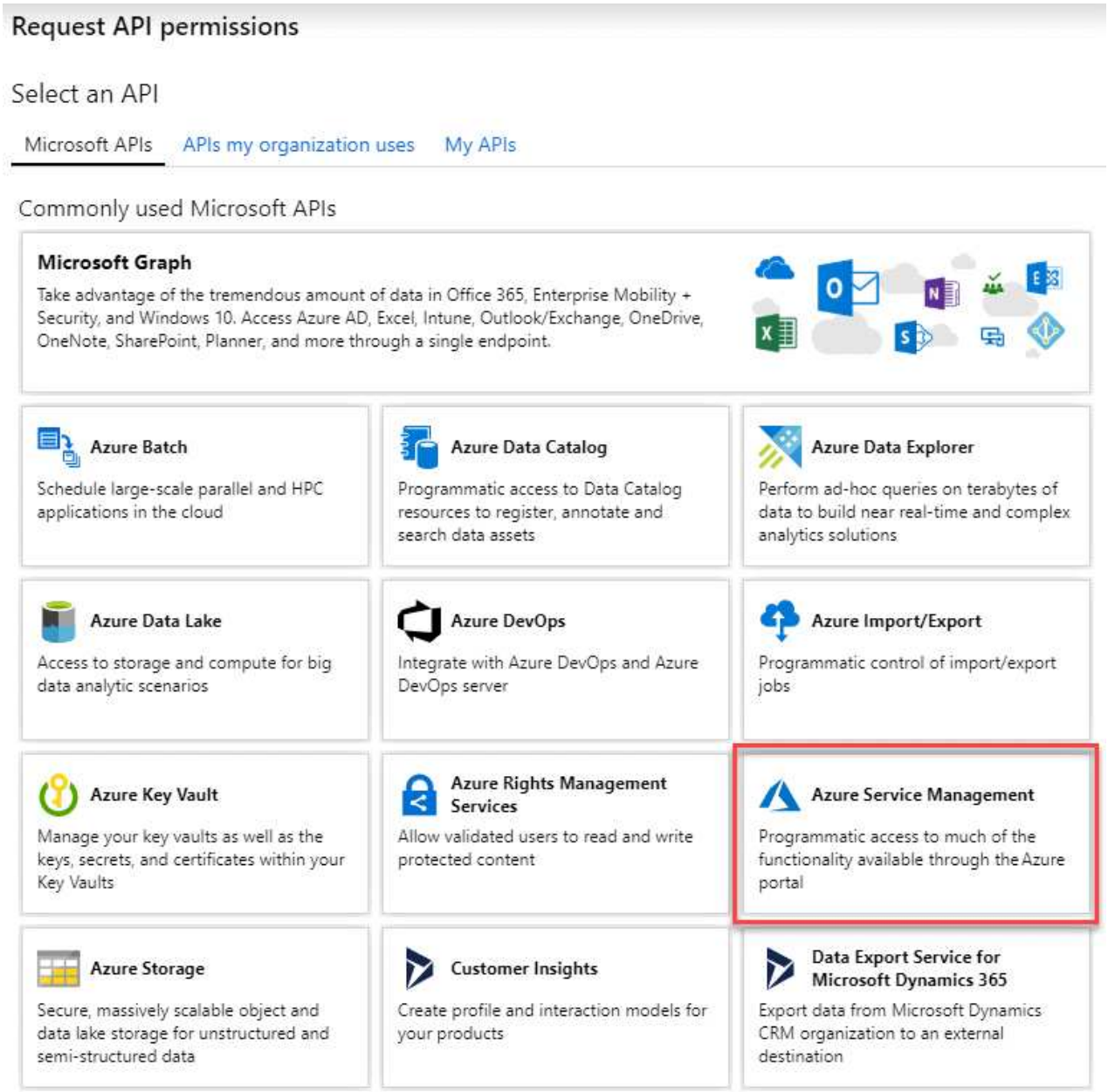
f. Selezionare **Rivedi + assegna**.

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

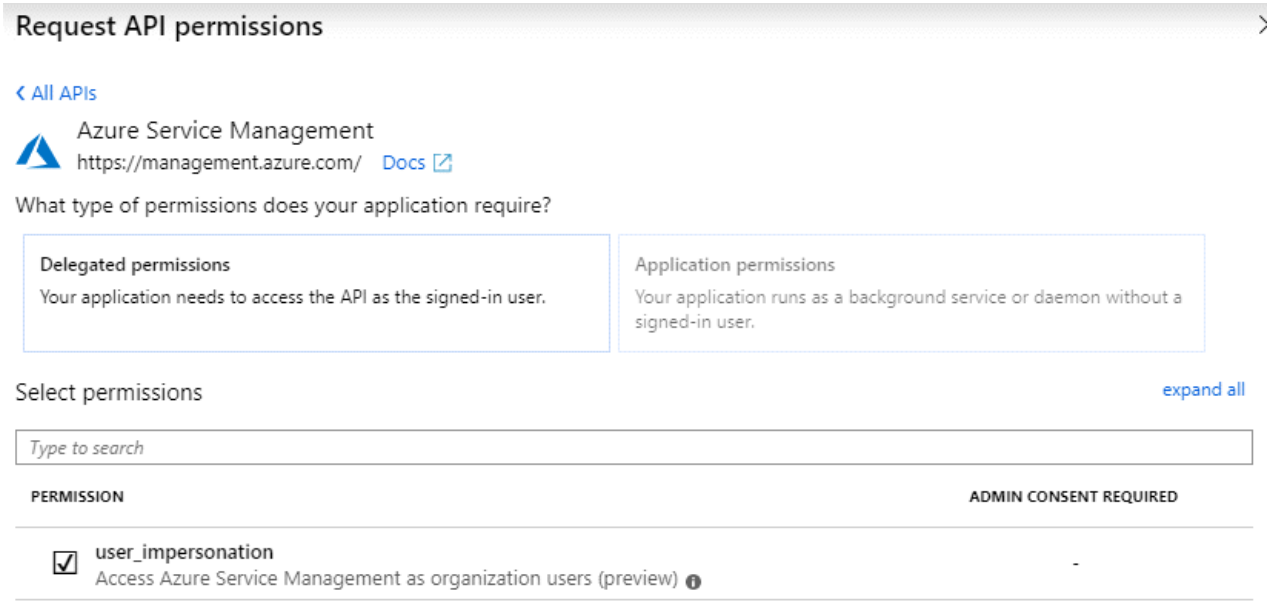
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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**.

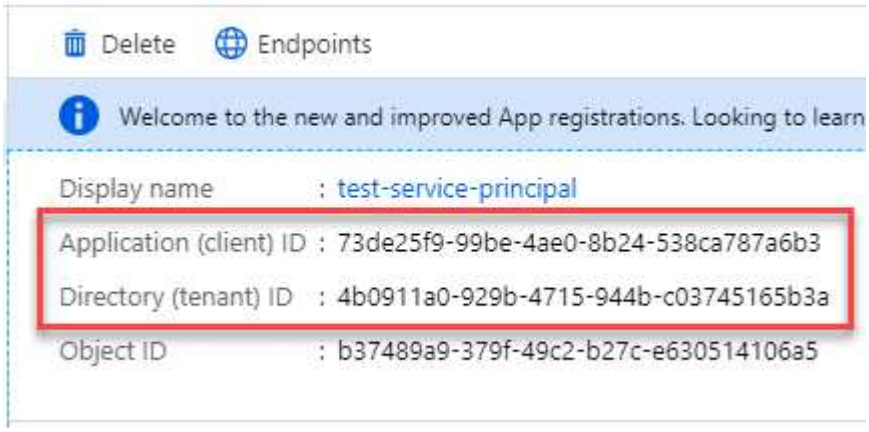


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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.

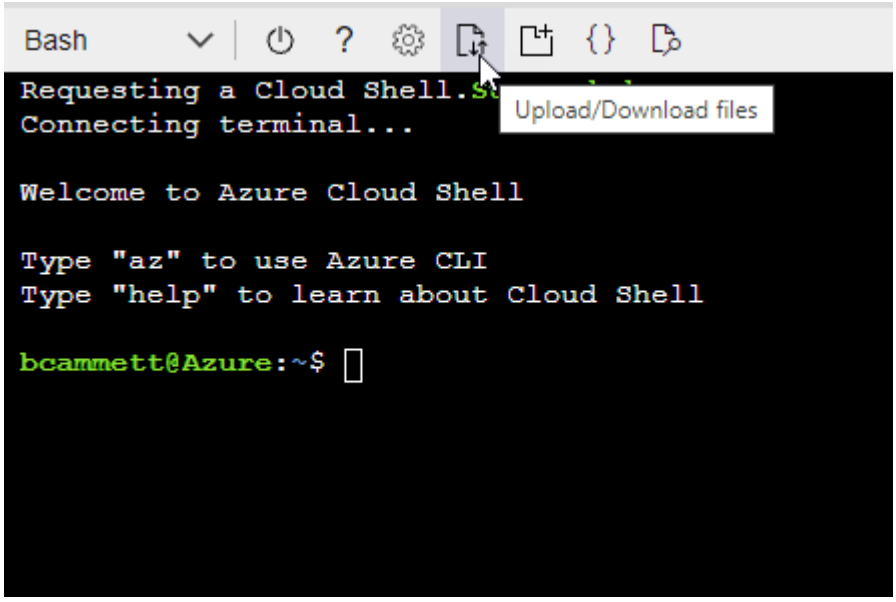
   Esempio

   ```
   "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

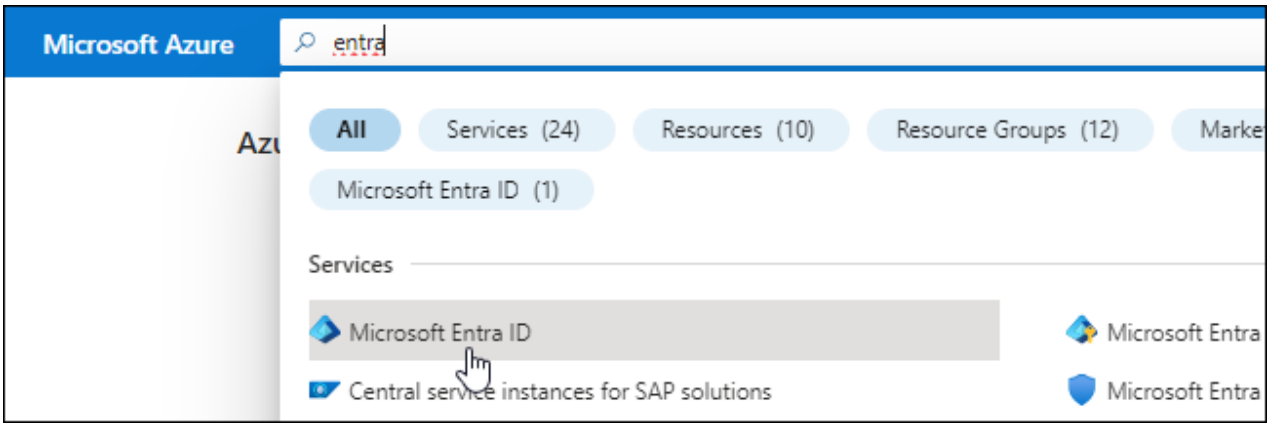
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP.

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.

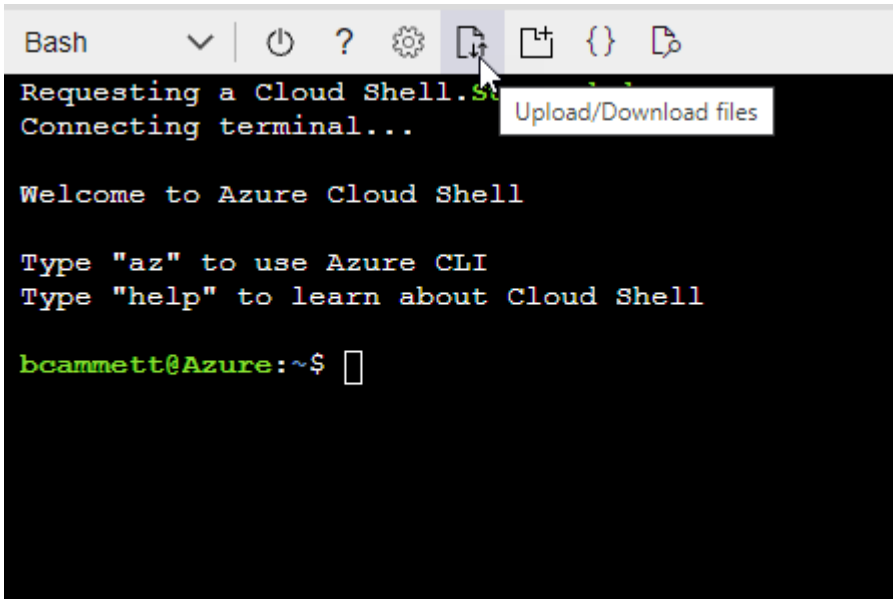
   Esempio

```
"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
```

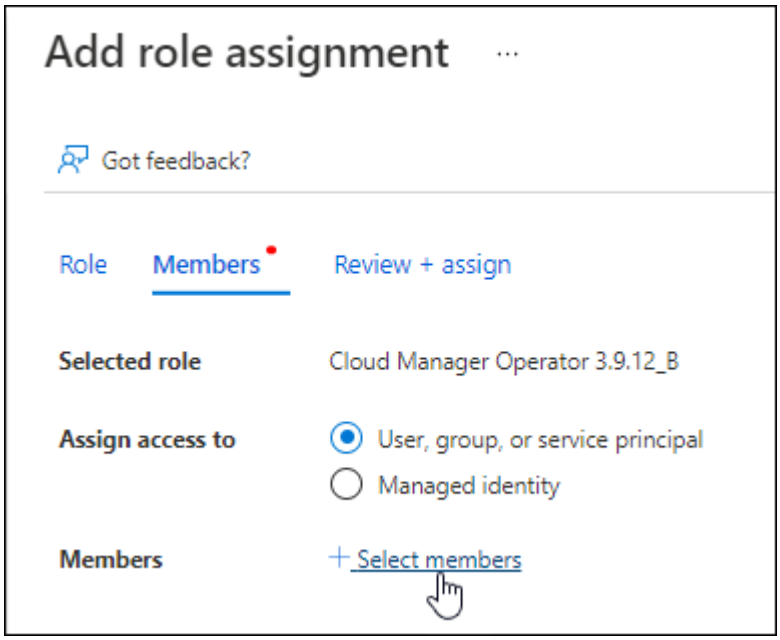
   A questo punto, dovrebbe essere disponibile un ruolo personalizzato denominato BlueXP

Operator che è possibile assegnare alla macchina virtuale Connector.

2. Assegnare l'applicazione al ruolo:

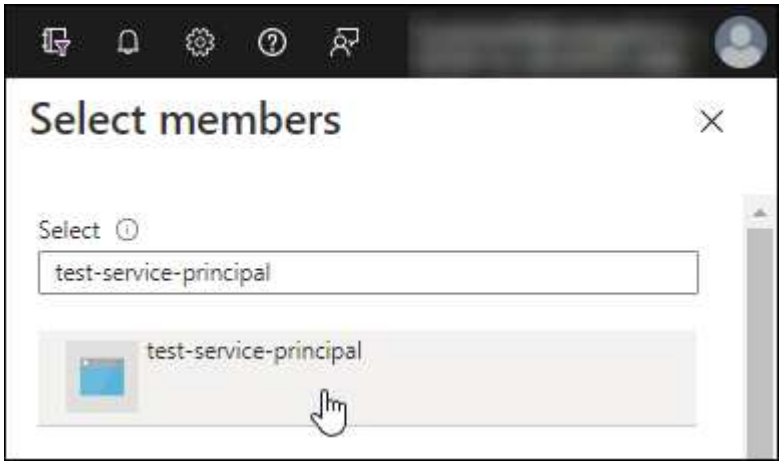
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

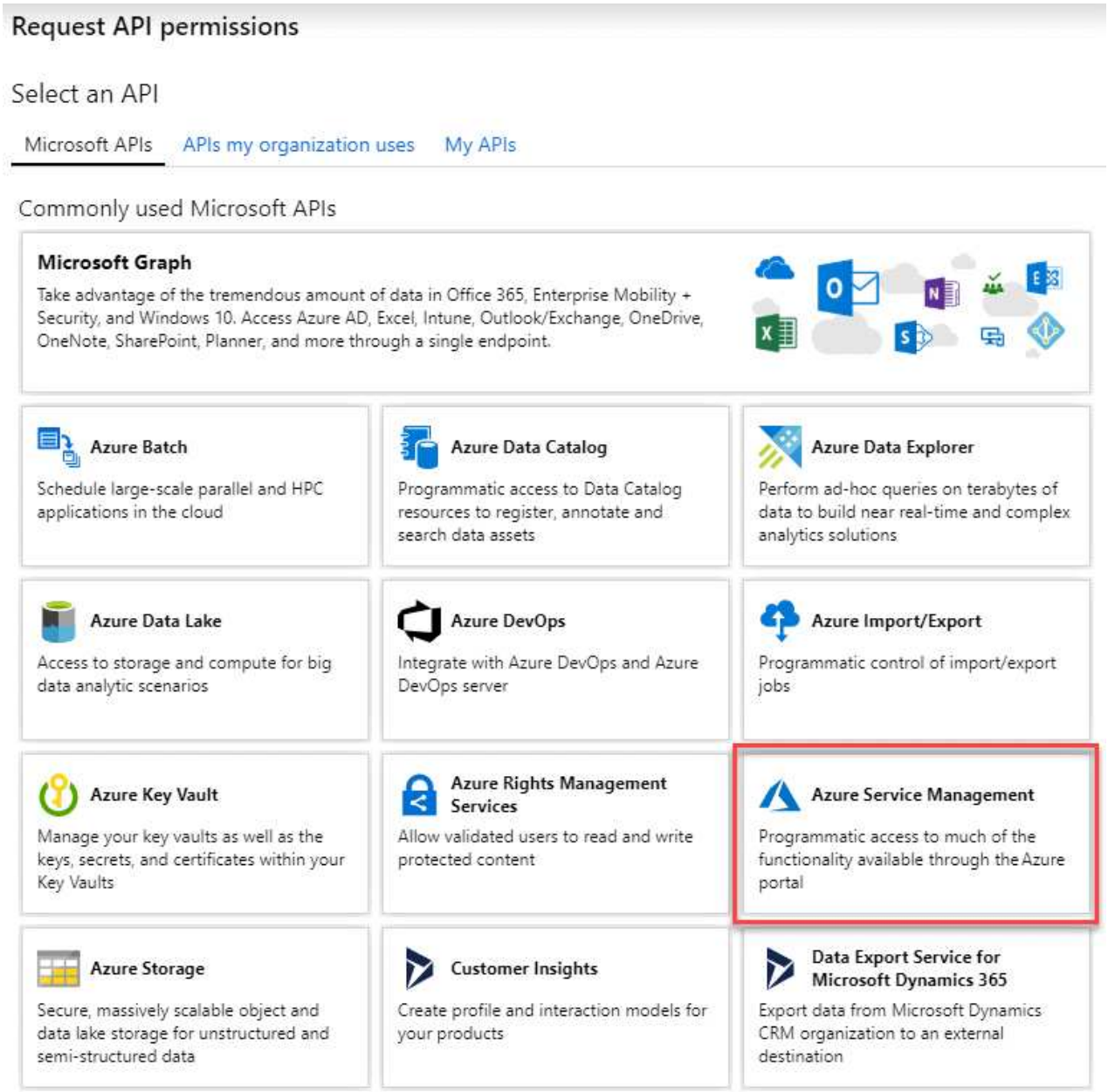
f. Selezionare **Rivedi + assegna**.

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

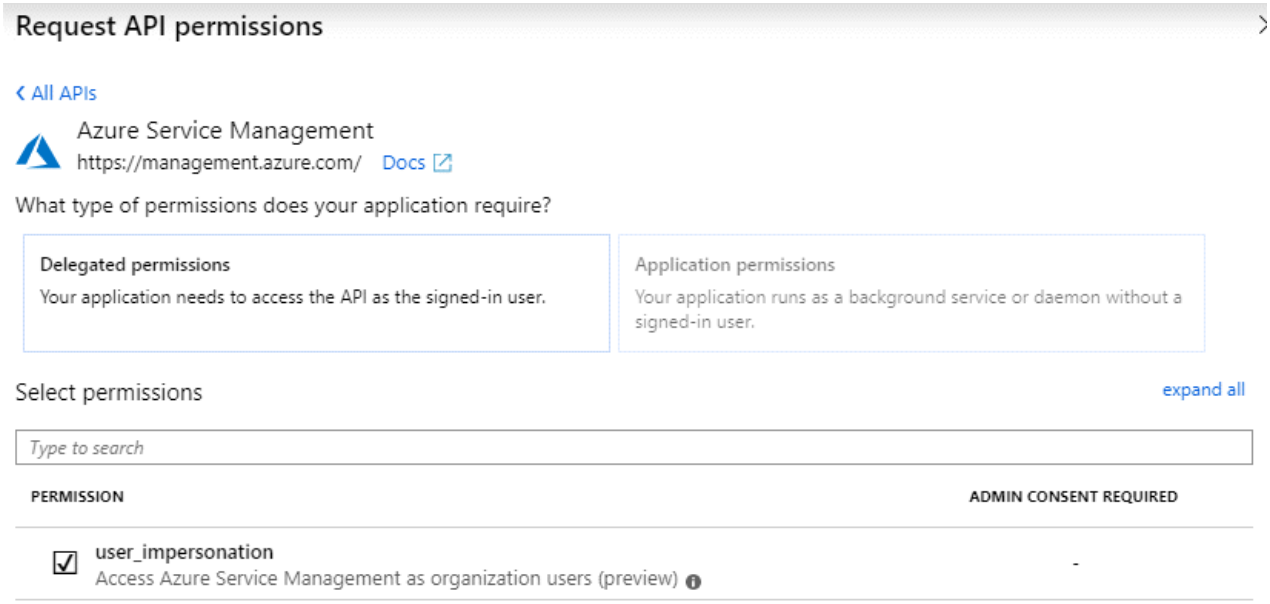
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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**.

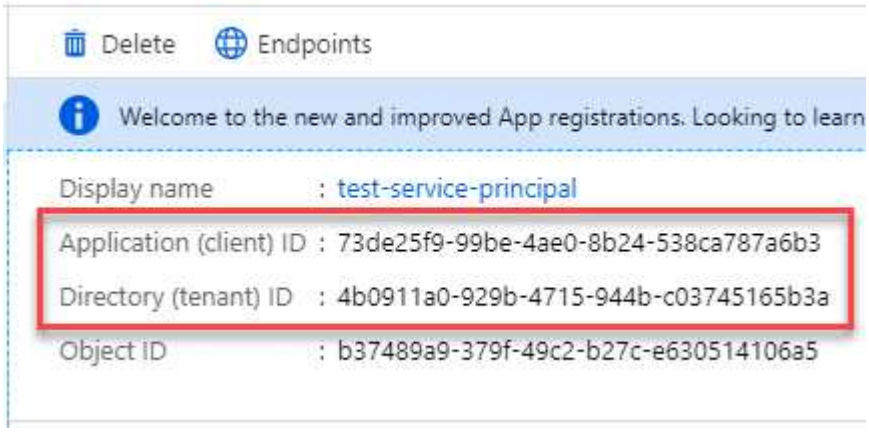


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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.
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

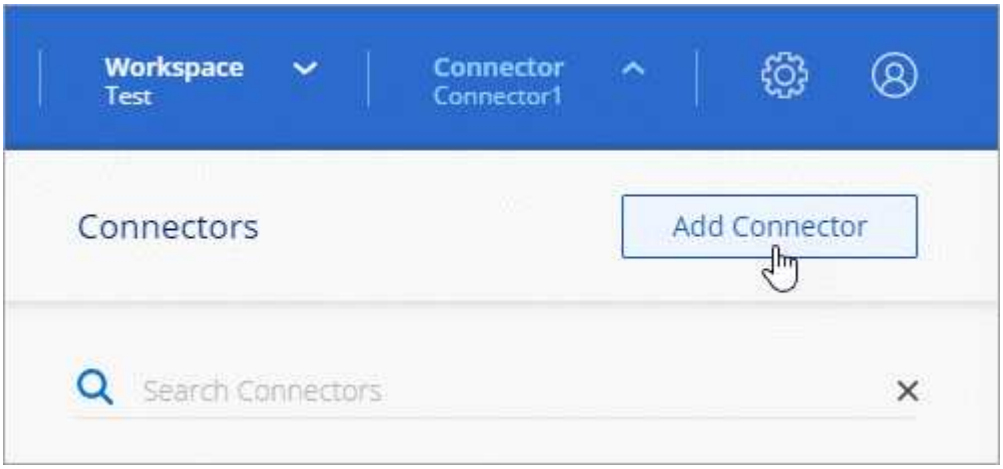
Prima di iniziare

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

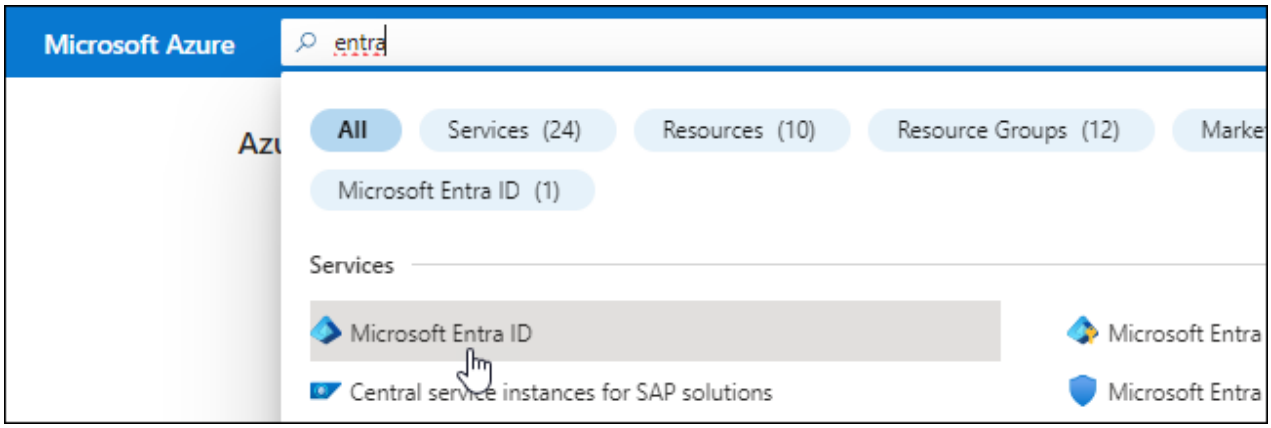
Quando il connettore è installato on-premise, devi fornire ad BlueXP le autorizzazioni di Azure, configurando un'identità di servizio in Microsoft Entra ID e ottenendo le credenziali di Azure di cui BlueXP ha bisogno.

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.

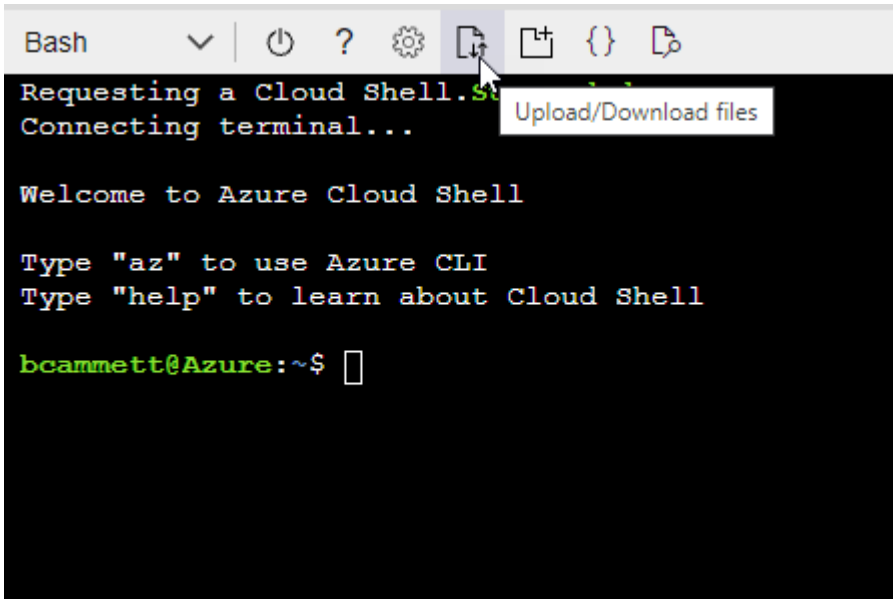
      Esempio

      ```
      "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:

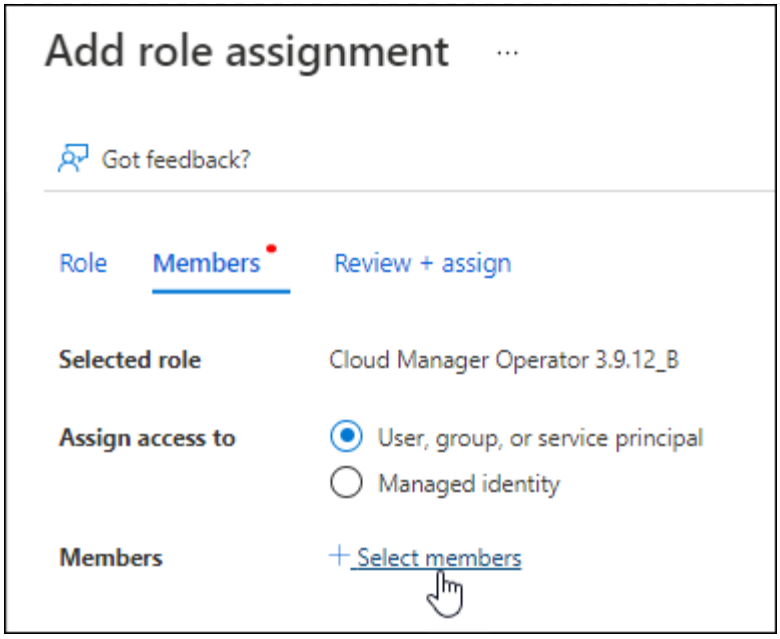
```
az role definition create --role-definition
Connector_Policy.json
```

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:

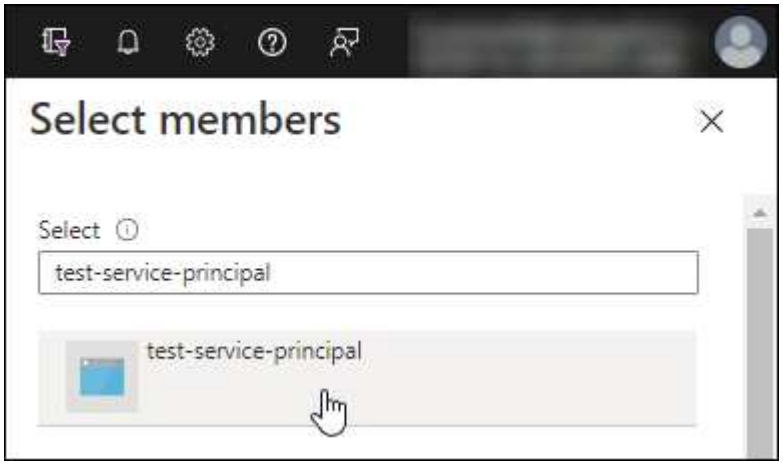
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

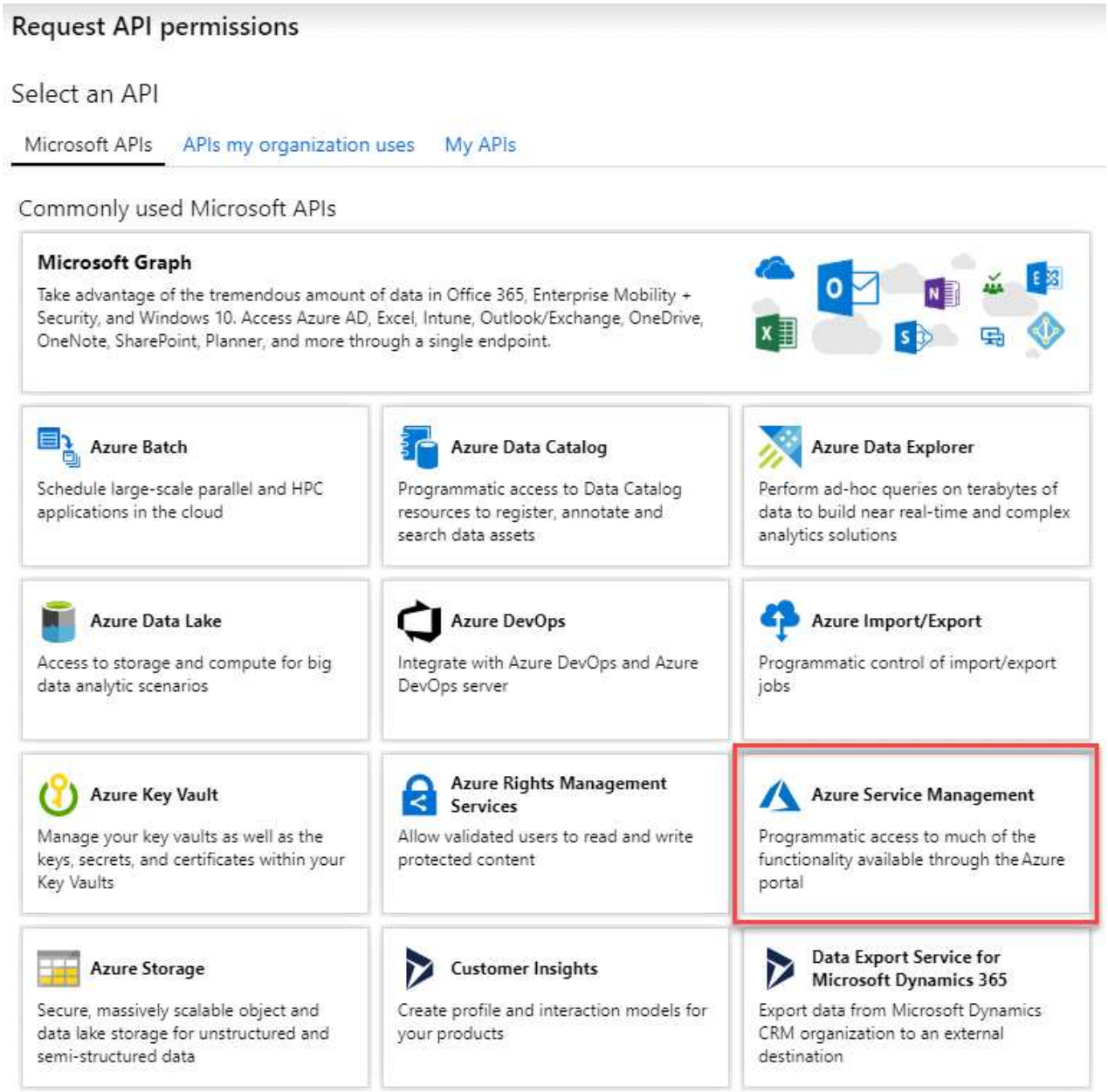
   L'entità del servizio dispone ora delle autorizzazioni Azure necessarie per implementare il connettore.

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.

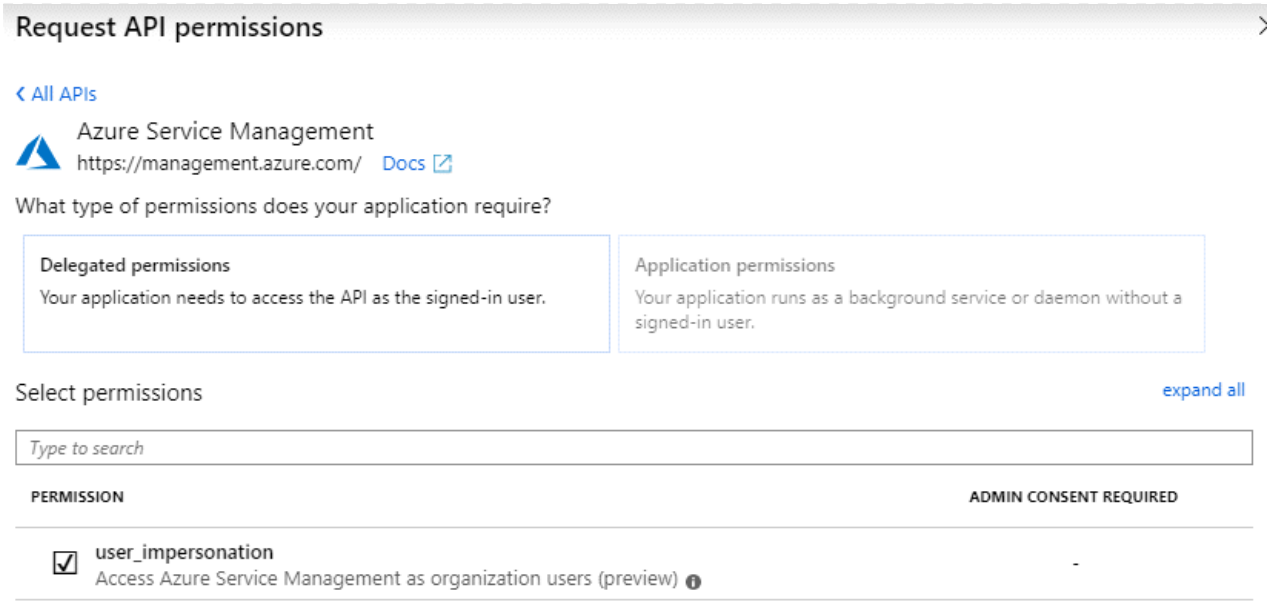
Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

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**.

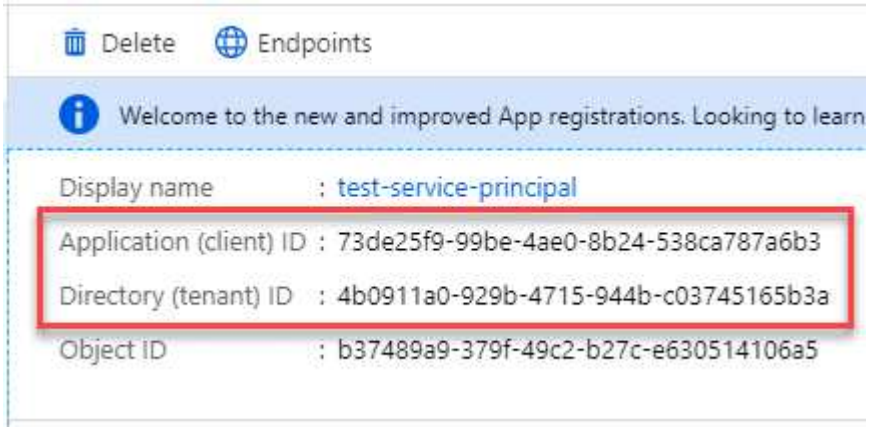


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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.

Iscriviti a BlueXP (modalità standard)

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

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

- Backup e recovery
- Classificazione
- Cloud Volumes ONTAP
- Tiering

Prima di iniziare

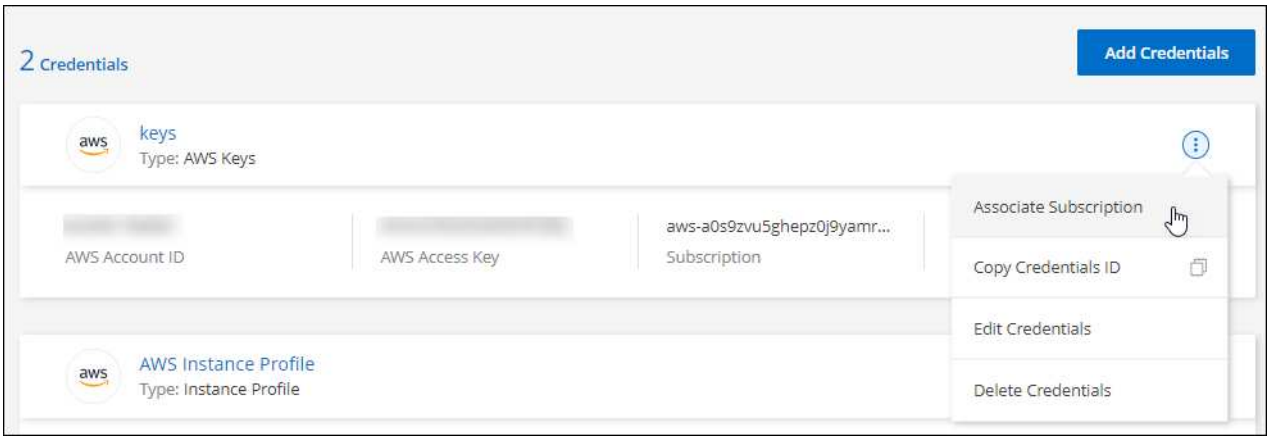
L'iscrizione a BlueXP implica l'associazione di un abbonamento Marketplace alle credenziali cloud associate a un connettore. Se hai seguito il flusso di lavoro "Get Started with standard mode" (inizia con la modalità standard), dovresti già disporre di un connettore. Per ulteriori informazioni, consulta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

AWS

Fasi

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

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



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

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

   b. Selezionare **Iscriviti**.

   c. Selezionare **Configura account**.

      Verrai reindirizzato al sito Web di BlueXP.

   d. Dalla pagina **Subscription Assignment**:

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

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

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

      - Selezionare **Salva**.

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

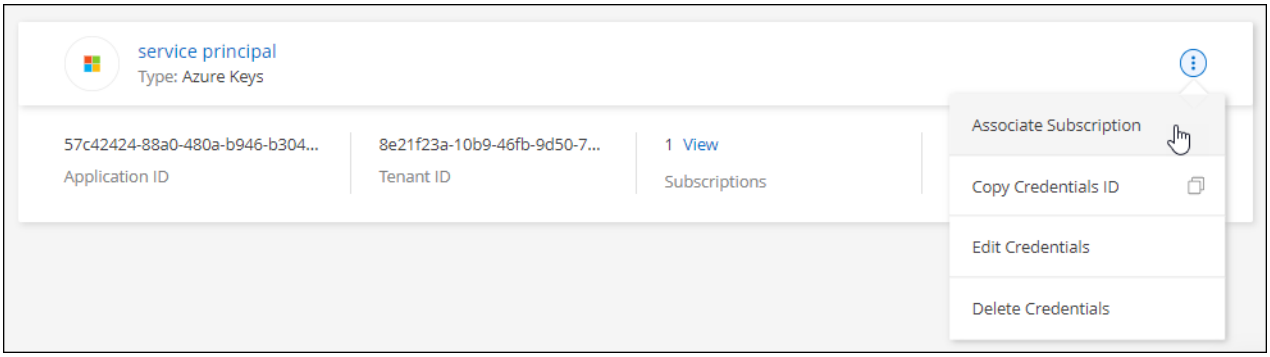
Iscriviti a BlueXP dal marketplace AWS

Azure

Fasi

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

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



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

   a. Se richiesto, accedere all'account Azure.

   b. Selezionare **Iscriviti**.

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

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

      Verrai reindirizzato al sito Web di BlueXP.

   e. Dalla pagina **Subscription Assignment**:

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

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

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

      - Selezionare **Salva**.

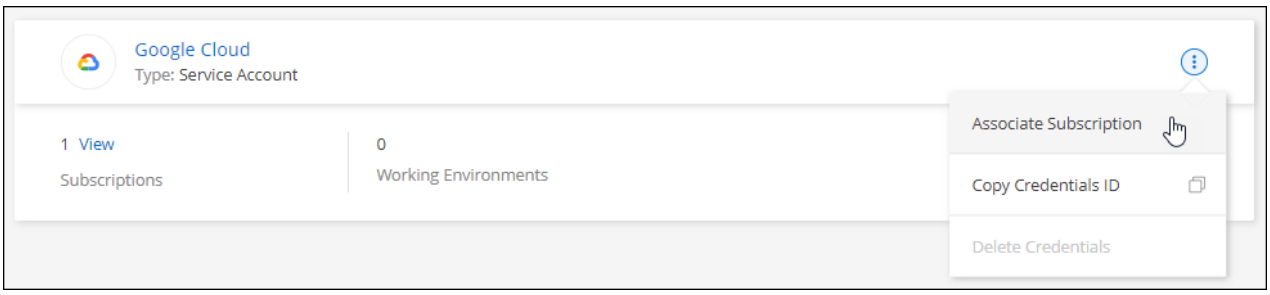
        Il seguente video mostra i passaggi per iscriversi a Azure Marketplace:

Iscriviti a BlueXP da Azure Marketplace

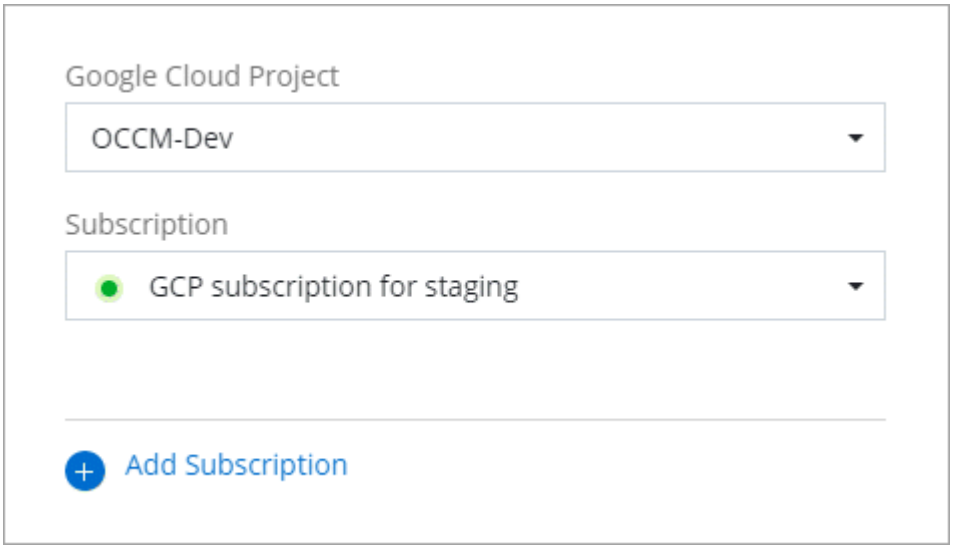
Google Cloud

Fasi

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



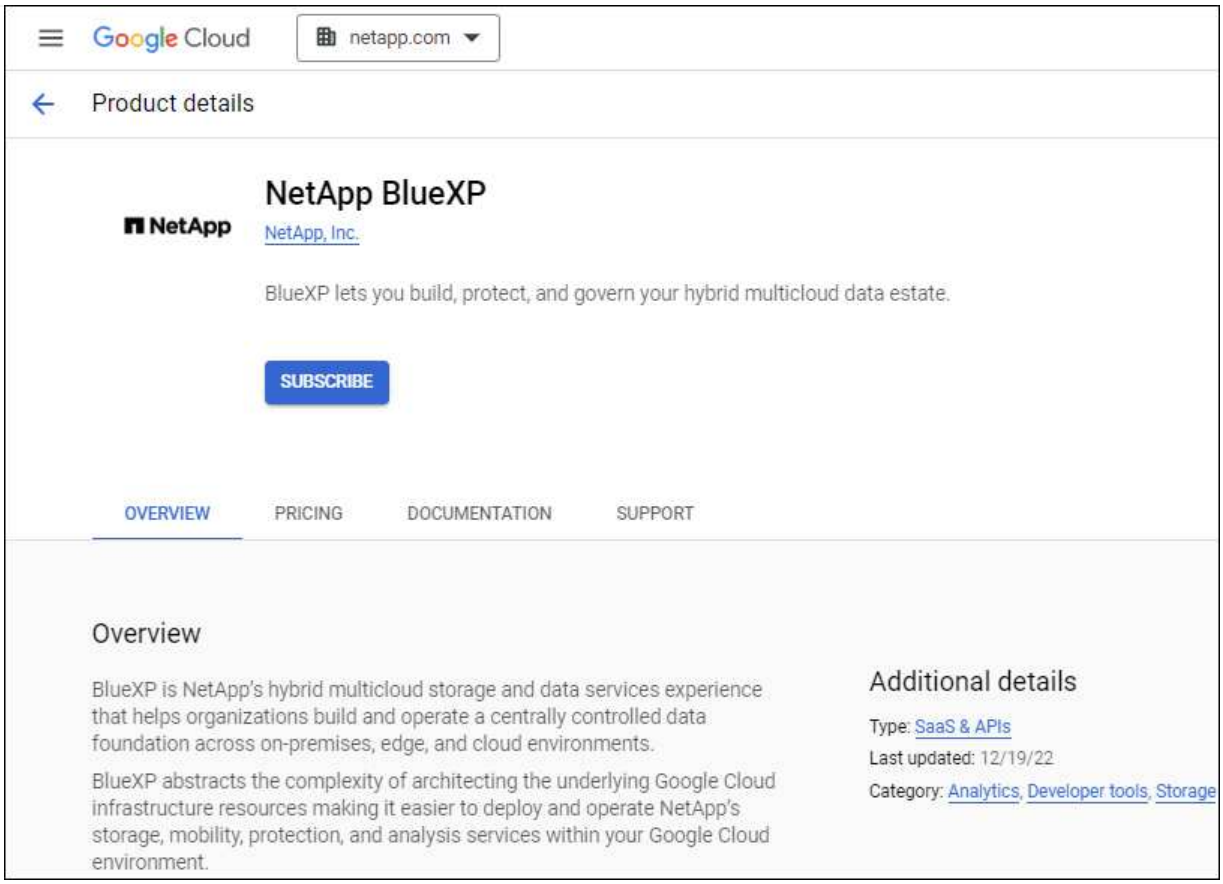
3. Per associare le credenziali a un abbonamento esistente, selezionare un progetto e un abbonamento Google Cloud dall'elenco a discesa, quindi selezionare **Associa**.



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

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

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



b. Selezionare **Iscriviti**.

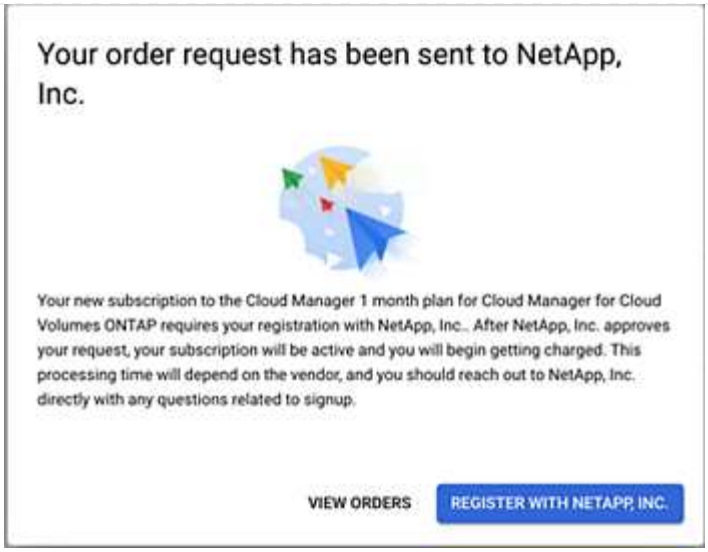
c. Selezionare l'account di fatturazione appropriato e accettare i termini e le condizioni.

d. Selezionare **Iscriviti**.

   Questa fase invia la richiesta di trasferimento a NetApp.

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

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



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

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

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

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

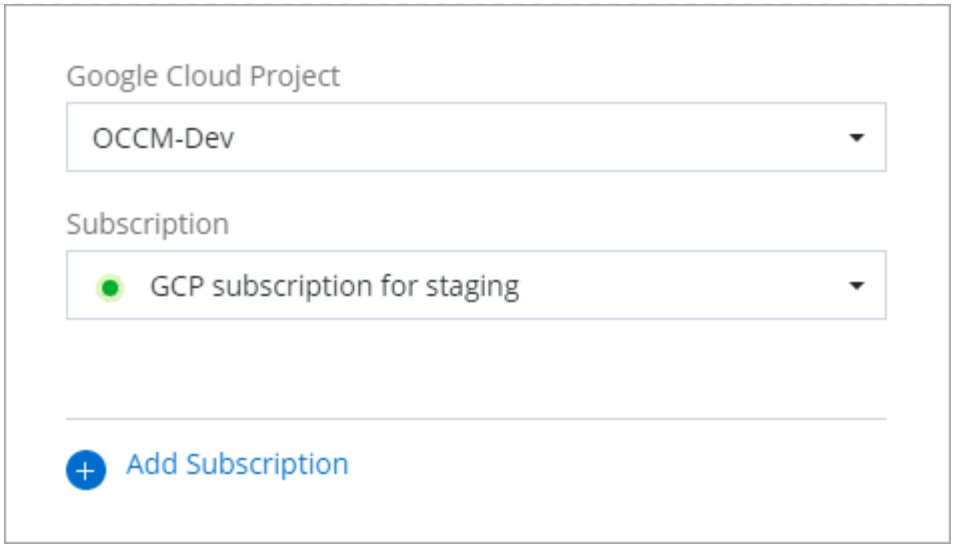
Per tutti gli altri account, è necessario associare manualmente l'abbonamento ripetendo questa procedura.

- Selezionare **Salva**.

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

Iscriviti a BlueXP da Google Cloud Marketplace

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



Link correlati

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

Operazioni successive (modalità standard)

Dopo aver effettuato l'accesso e configurato BlueXP in modalità standard, gli utenti possono creare e rilevare ambienti di lavoro e utilizzare i servizi dati BlueXP.

> Se hai installato un connettore in AWS, Microsoft Azure o Google Cloud, BlueXP scopre automaticamente le informazioni sui bucket Amazon S3, sull'archiviazione BLOB di Azure o sui bucket Google Cloud Storage nella posizione in cui è installato il connettore. Un ambiente di lavoro viene aggiunto automaticamente a BlueXP Canvas.

Per assistenza, consultare "home page della documentazione BlueXP" Per visualizzare i documenti relativi a tutti i servizi BlueXP.

Link correlato

"Modalità di implementazione di BlueXP"

Inizia con la modalità limitata

Flusso di lavoro introduttivo (modalità limitata)

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

La modalità limitata viene generalmente utilizzata dai governi locali e statali e da società regolamentate,

comprese le implementazioni nelle aree pubbliche di AWS GovCloud e Azure. Prima di iniziare, dovresti avere una conoscenza di "BlueXP", "Connettori", e. "modalità di distribuzione".

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

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

2 **"Implementare il connettore"**

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

3 **"Iscriviti a BlueXP"**

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

Prepararsi per l'implementazione in modalità limitata

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

Fase 1: Comprendere il funzionamento della modalità limitata

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

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

Inoltre, non tutti i servizi BlueXP sono disponibili.

"Scopri come funziona la modalità limitata".

Passaggio 2: Esaminare le opzioni di installazione

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

- Da AWS Marketplace
- Da Azure Marketplace

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

Fase 3: Esaminare i requisiti dell'host

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

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

Host dedicato

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

Sistemi operativi supportati

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

  L'host deve essere registrato con Red Hat Subscription Management. Se non è registrato, l'host non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione del connettore.

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

Hypervisor

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

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

CPU

4 core o 4 vCPU

RAM

14 GB

Tipo di istanza AWS EC2

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

Dimensione delle macchine virtuali Azure

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

Tipo di macchina Google Cloud

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

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

Spazio su disco in /opz

100 GiB di spazio deve essere disponibile

Spazio su disco in /var

20 GiB di spazio deve essere disponibile

Motore Docker

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

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

"Visualizzare le istruzioni di installazione"

Fase 4: Preparare il collegamento in rete

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

Connessioni alle reti di destinazione

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

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

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

Endpoint	Scopo
https://signin.b2c.netapp.com	Necessario per aggiornare le credenziali NetApp Support Site (NSS) o per aggiungere nuove credenziali NSS a BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite BlueXP.
https://widget.intercom.io	Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp.

Endpoint contattati durante l'installazione manuale

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

- https://support.netapp.com
- https://mysupport.netapp.com

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

  Questo endpoint non è richiesto nelle regioni governative di Azure.

- https://occmclientinfragov.azurecr.us

  Questo endpoint è richiesto solo nelle regioni governative di Azure.

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

Accesso a Internet in uscita per le operazioni quotidiane

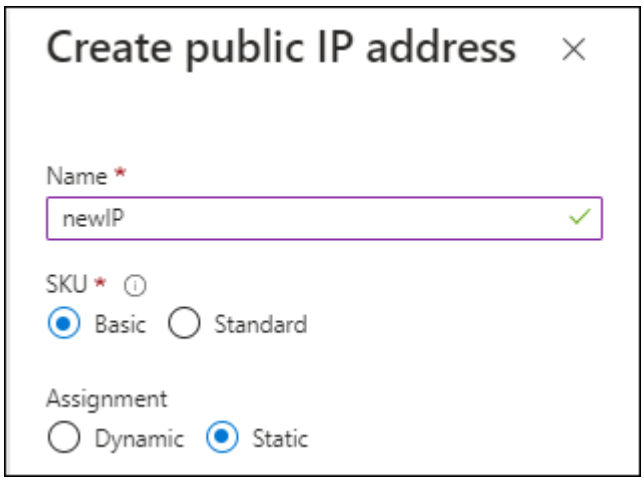
La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita. Il connettore richiede l'accesso a Internet in uscita per contattare i seguenti endpoint al fine di gestire risorse e processi all'interno dell'ambiente di cloud pubblico.

Endpoint	Scopo
Servizi AWS (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Gestione delle identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • S3 (Simple Storage Service)	Per gestire le risorse in AWS. L'endpoint esatto dipende dall'area AWS che stai utilizzando. "Per ulteriori informazioni, fare riferimento alla documentazione AWS"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Per gestire le risorse nelle aree pubbliche di Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Per gestire le risorse nelle regioni governative di Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Per gestire le risorse nelle regioni Azure China.

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.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io Questo endpoint non è richiesto nelle regioni governative di Azure. https://occmclientinfragov.azurecr.us Questo endpoint è richiesto solo nelle regioni governative di Azure.	Per aggiornare il connettore e i relativi componenti Docker.

Indirizzo IP pubblico in Azure

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



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

"Documentazione di Azure: SKU IP pubblico"

Server proxy

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

- Indirizzo IP
- Credenziali
- Certificato HTTPS

BlueXP non supporta i server proxy trasparenti.

Porte

Non c'è traffico in entrata verso il connettore, a meno che non venga avviato o se il connettore viene utilizzato come proxy per inviare messaggi AutoSupport da Cloud Volumes ONTAP al supporto NetApp.

- HTTP (80) e HTTPS (443) forniscono l'accesso all'interfaccia utente locale, che verrà utilizzata in rare circostanze.
- SSH (22) è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.
- Le connessioni in entrata sulla porta 3128 sono necessarie se si implementano sistemi Cloud Volumes ONTAP in una subnet in cui non è disponibile una connessione Internet in uscita.

  Se i sistemi Cloud Volumes ONTAP non dispongono di una connessione a Internet in uscita per inviare messaggi AutoSupport, BlueXP configura automaticamente tali sistemi in modo che utilizzino un server proxy incluso nel connettore. L'unico requisito è garantire che il gruppo di sicurezza del connettore consenta le connessioni in entrata sulla porta 3128. Dopo aver implementato il connettore, aprire questa porta.

Enable NTP (attiva NTP)

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

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

Passaggio: 5 preparare le autorizzazioni del cloud

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

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

Ruolo AWS IAM

Utilizzare un ruolo IAM per fornire al connettore le autorizzazioni.

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

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

Fasi

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

Risultato

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

Chiave di accesso AWS

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

Fasi

1. Accedere alla console AWS e accedere al servizio IAM.
2. Creare una policy:
   a. Selezionare **Criteri > Crea policy**.
   b. Selezionare **JSON** e copiare e incollare il contenuto di "Policy IAM per il connettore".
   c. Completare i passaggi rimanenti per creare il criterio.

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

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

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

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

Risultato

L'account dispone ora delle autorizzazioni necessarie.

Ruolo di Azure

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

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

Fasi

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

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

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

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

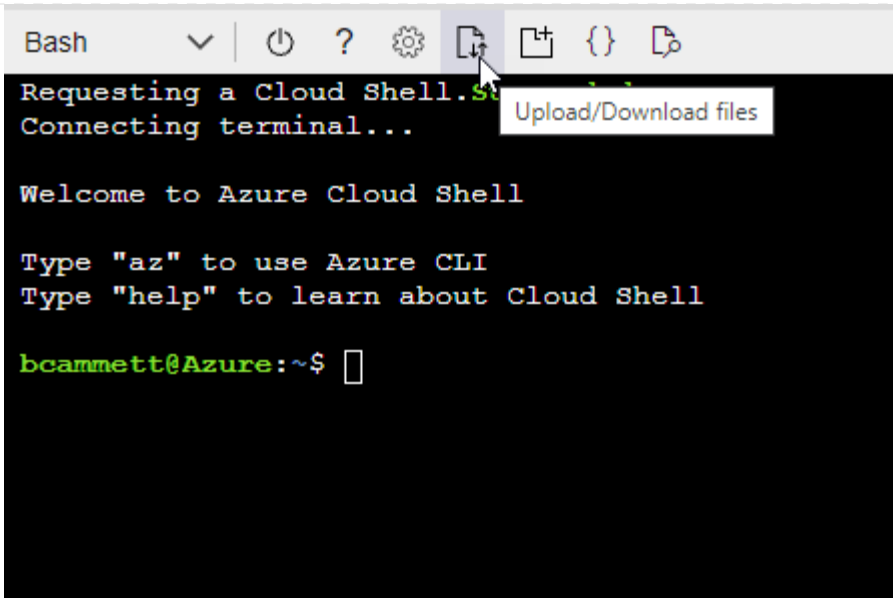
   Esempio

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

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

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

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



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

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

Risultato

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

Entità del servizio Azure

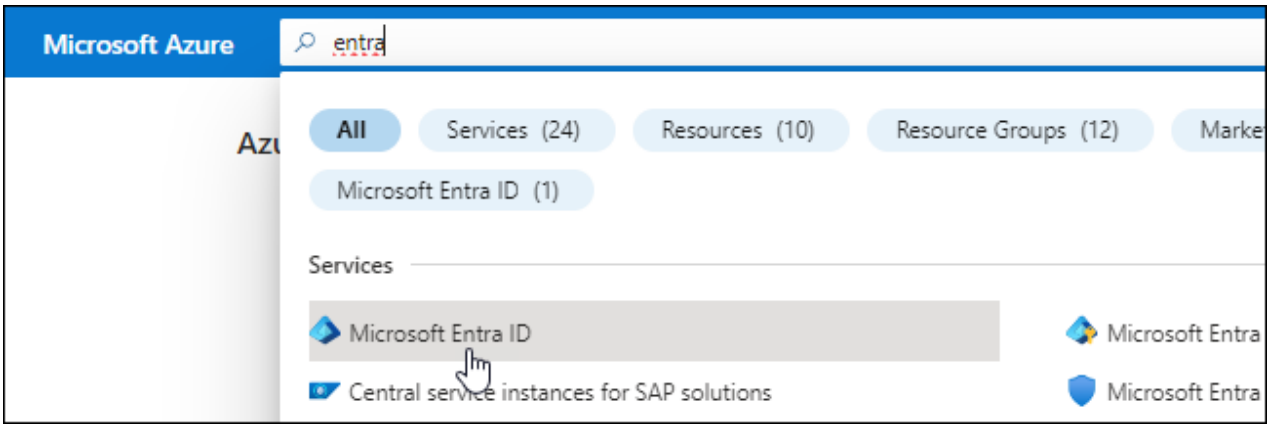
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP. È necessario fornire queste credenziali a BlueXP dopo aver installato il connettore e configurato BlueXP.

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

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

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

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



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

   Hai creato l'applicazione ad e il service principal.

Assegnare l'applicazione a un ruolo

1. Creare un ruolo personalizzato:

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

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

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

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

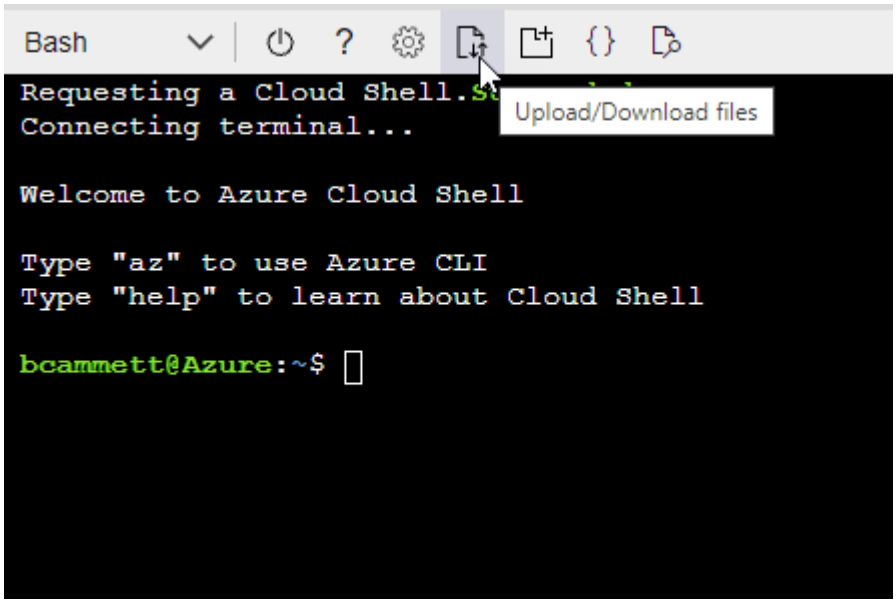
      Esempio

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

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

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

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



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

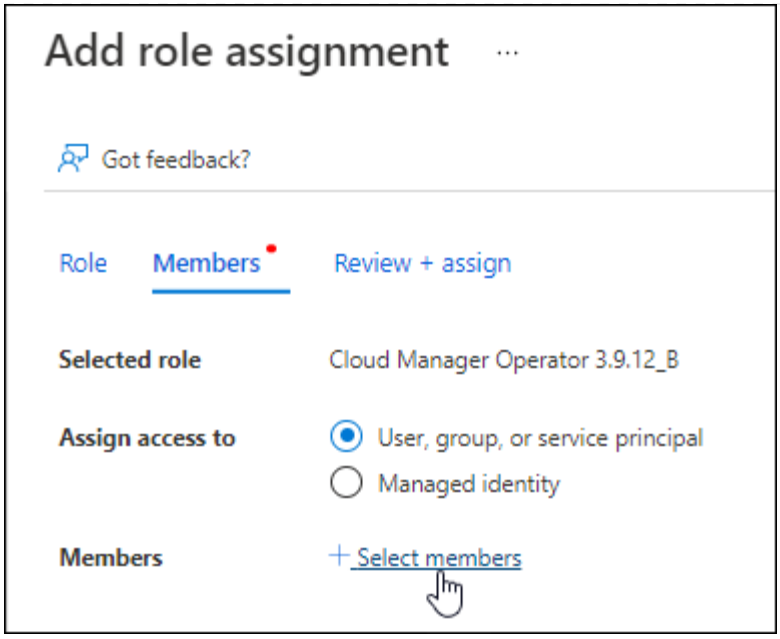
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Assegnare l'applicazione al ruolo:

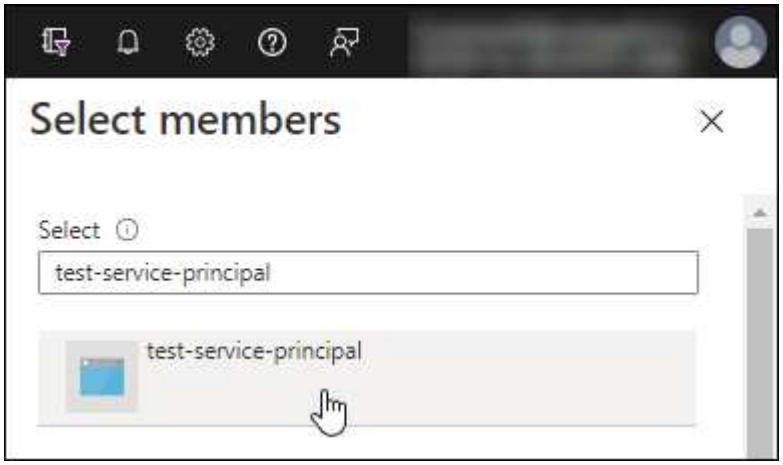
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

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



- Cercare il nome dell'applicazione.

  Ecco un esempio:



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

f. Selezionare **Rivedi + assegna**.

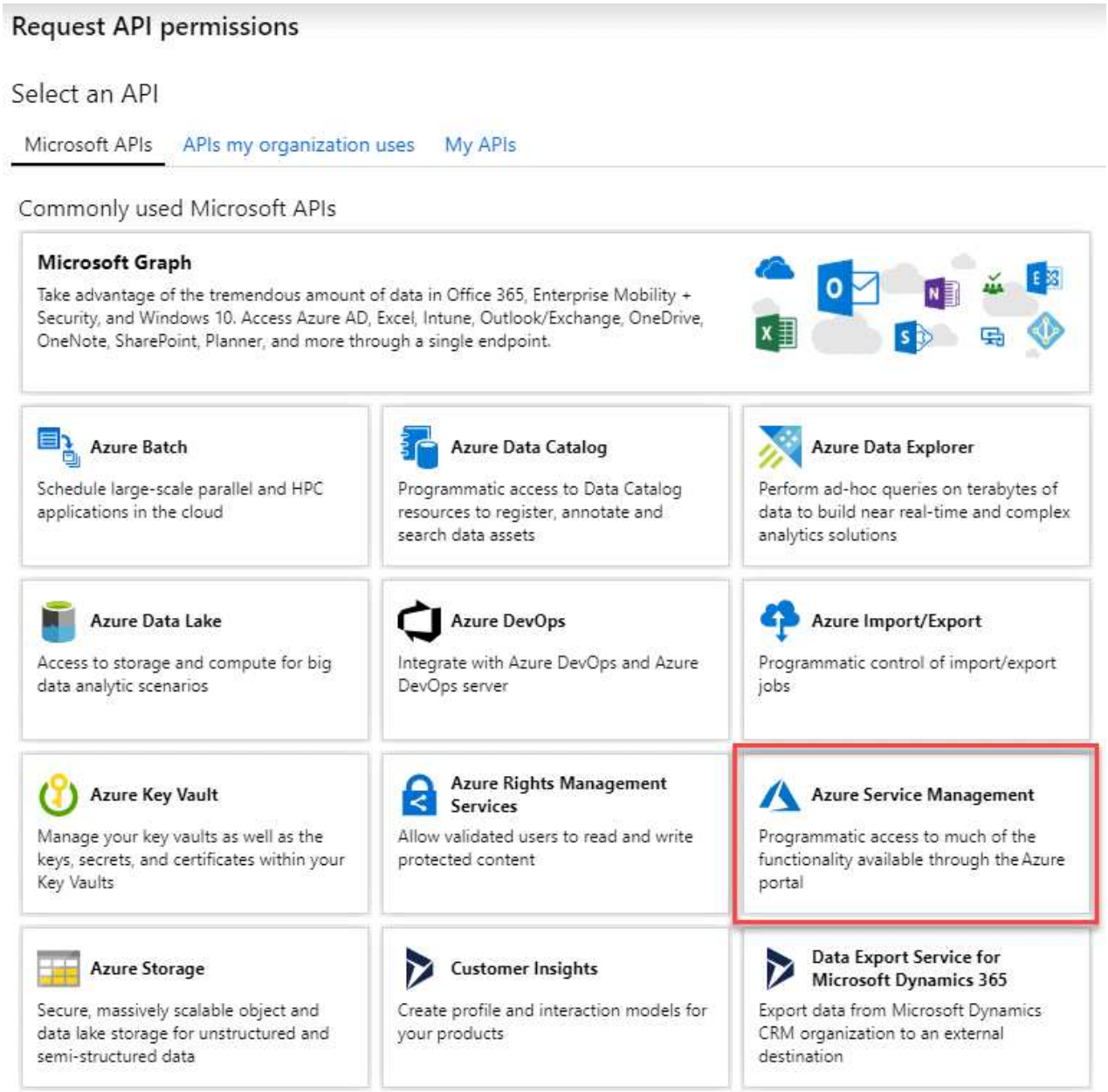
   L'entità del servizio dispone ora delle autorizzazioni Azure necessarie per implementare il connettore.

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

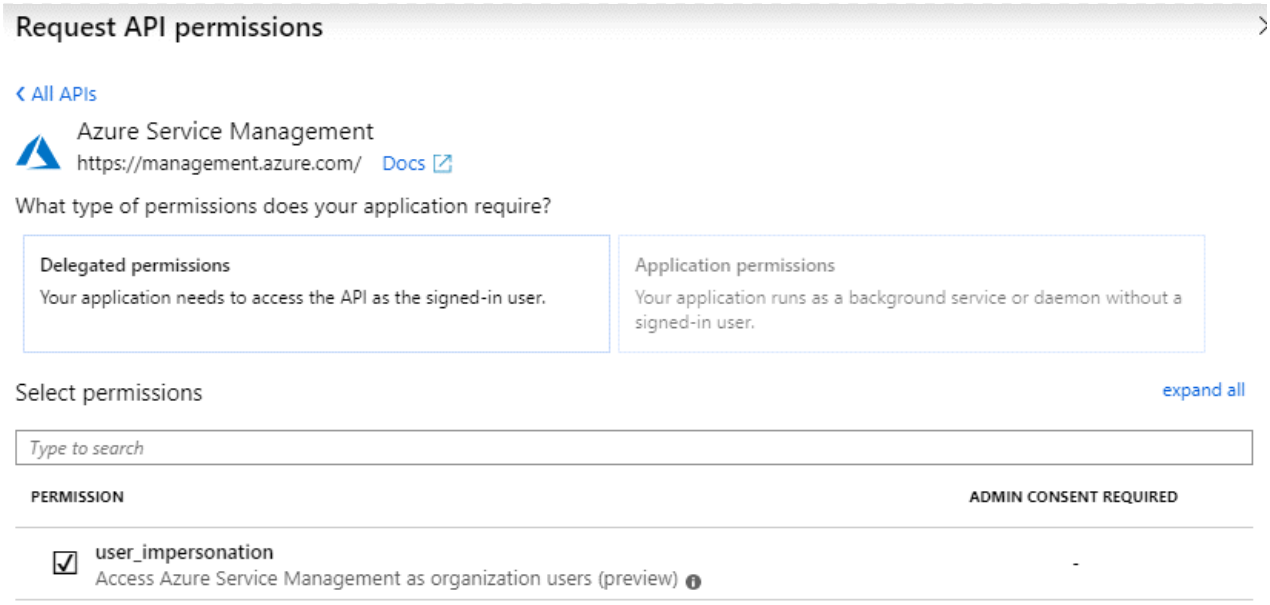
Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

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

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

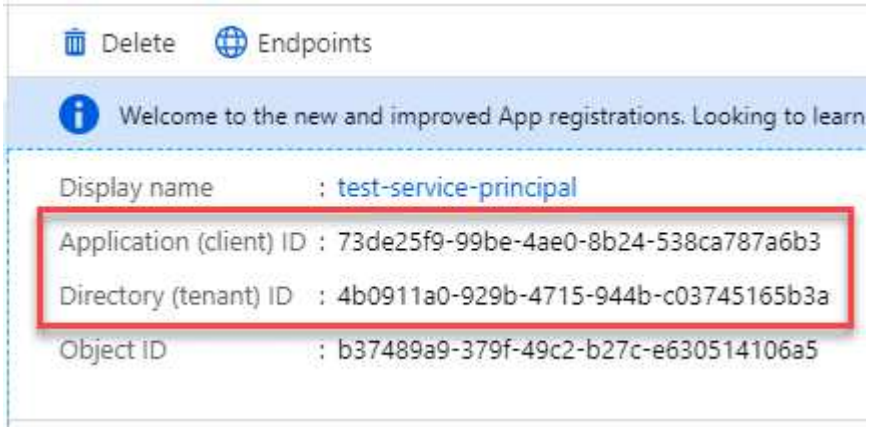


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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

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



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

Creare un client segreto

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

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

Risultato

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

Account del servizio Google Cloud

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

Fasi

1. Creare un ruolo personalizzato in Google Cloud:

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

   b. Da Google Cloud, attiva la shell cloud.

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

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

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

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

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

2. Creare un account di servizio in Google Cloud:

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

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

   c. Selezionare il ruolo appena creato.

   d. Completare i passaggi rimanenti per creare il ruolo.

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

Risultato

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

Passaggio 6: Abilitare le API di Google Cloud

Per implementare Cloud Volumes ONTAP in Google Cloud sono necessarie diverse API.

Fase

1. "Abilita le seguenti API di Google Cloud nel tuo progetto"
    - API di Cloud Deployment Manager V2
    - API Cloud Logging
    - API Cloud Resource Manager
    - API di Compute Engine
    - API IAM (Identity and Access Management)
    - API di Cloud Key Management Service (KMS)

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

Implementare il connettore in modalità limitata

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

Fase 1: Installare il connettore

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

Mercato commerciale AWS

Prima di iniziare

Dovresti disporre di quanto segue:

- VPC e subnet che soddisfano i requisiti di rete.

  "Scopri i requisiti di rete"

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

  "Scopri come impostare le autorizzazioni AWS"

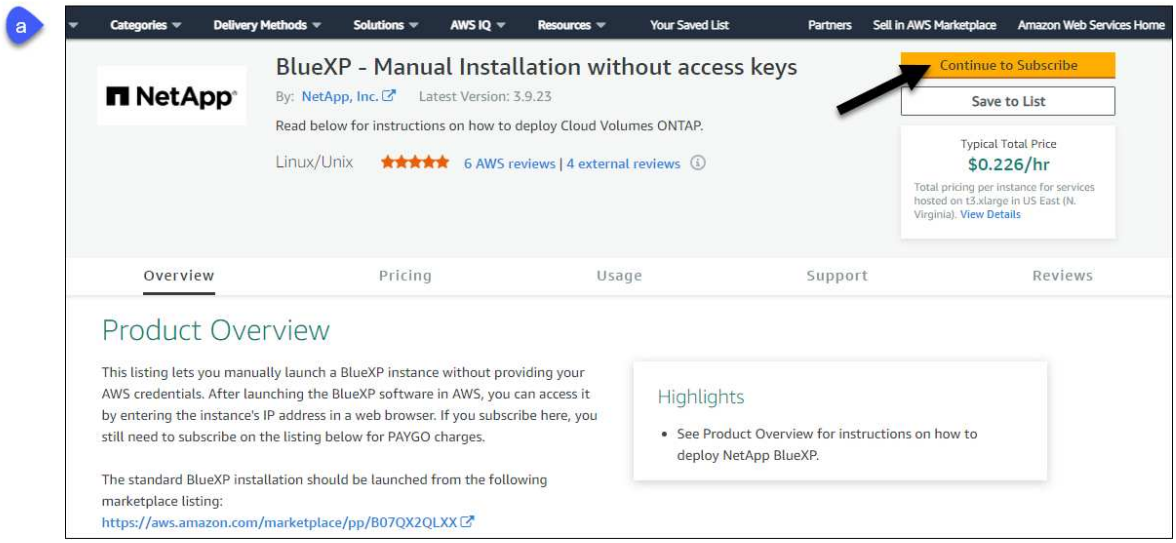
- Autorizzazioni per iscriversi e annullare l'iscrizione da AWS Marketplace per l'utente IAM.
- Comprensione dei requisiti di CPU e RAM per l'istanza.

  "Esaminare i requisiti dell'istanza".

- Coppia di chiavi per l'istanza EC2.

Fasi

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



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

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

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

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

       Sono necessarie altre regole per configurazioni specifiche.

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

   - **Configura archiviazione**: Mantenere le dimensioni e il tipo di disco predefiniti per il volume root.

     Se si desidera abilitare la crittografia Amazon EBS sul volume root, selezionare **Avanzate**, espandere **Volume 1**, selezionare **crittografato**, quindi scegliere una chiave KMS.

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

Risultato

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

Quali sono le prossime novità?

Configurare BlueXP.

Mercato AWS Gov

Prima di iniziare

Dovresti disporre di quanto segue:

- VPC e subnet che soddisfano i requisiti di rete.

  "Scopri i requisiti di rete"

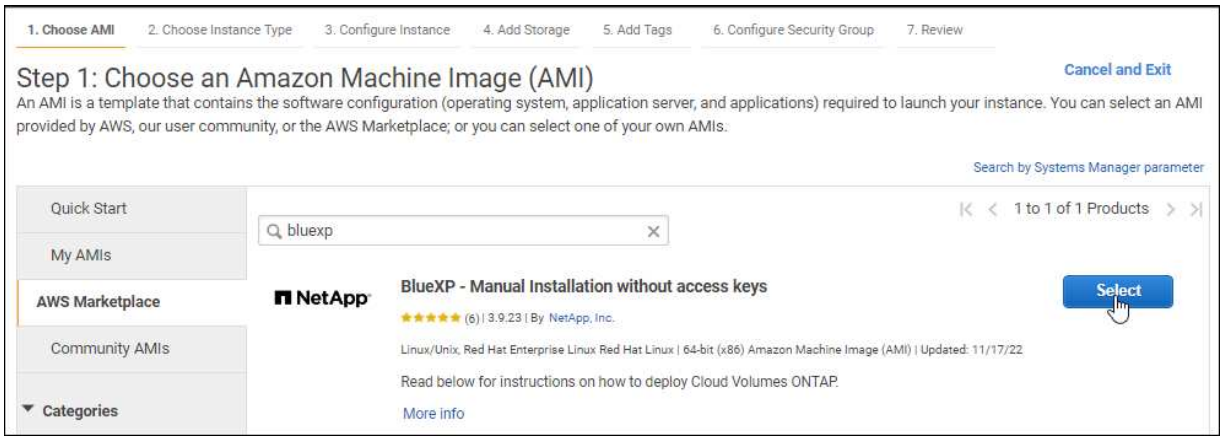
- Un ruolo IAM con un criterio allegato che include le autorizzazioni richieste per il connettore.

  "Scopri come impostare le autorizzazioni AWS"

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

Fasi

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

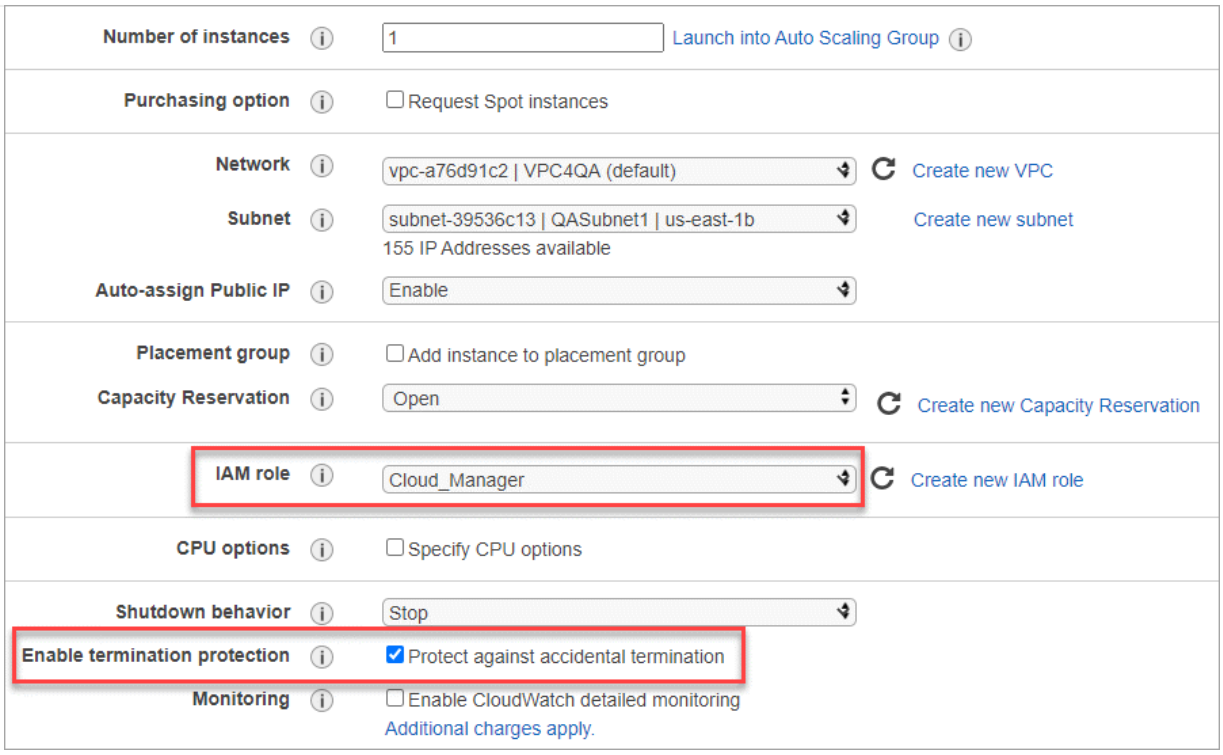


   d. Selezionare **continua**.

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

     "Esaminare i requisiti dell'istanza".

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



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

Risultato

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

Quali sono le prossime novità?

Configurare BlueXP.

Azure Marketplace

Prima di iniziare

Dovresti disporre di quanto segue:

- VNET e subnet che soddisfano i requisiti di rete.

  "Scopri i requisiti di rete"

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

  "Scopri come impostare le autorizzazioni Azure"

Fasi

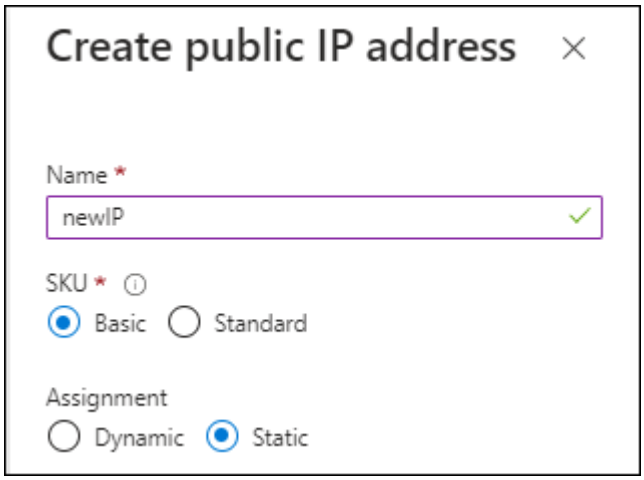
1. Accedere alla pagina NetApp Connector VM in Azure Marketplace.
   - "Pagina di Azure Marketplace per le regioni commerciali"

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

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

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

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



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

   "Documentazione di Azure: SKU IP pubblico"

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

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

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

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

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

Risultato

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

Quali sono le prossime novità?

Configurare BlueXP.

Installazione manuale

Prima di iniziare

Dovresti disporre di quanto segue:

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

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

  BlueXP non supporta i server proxy trasparenti.

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

A proposito di questa attività

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

Fasi

1. Verificare che docker sia attivato e in esecuzione.

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

2. Se le variabili di sistema *http_proxy* o *https_proxy* sono impostate sull'host, rimuoverle:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Se non si rimuovono queste variabili di sistema, l'installazione avrà esito negativo.

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

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

4. Assegnare le autorizzazioni per eseguire lo script.

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

   Dove <version> è la versione del connettore scaricato.

5. Eseguire lo script di installazione.

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

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

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

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

--proxy configura il connettore per l'utilizzo di un server proxy HTTP o HTTPS utilizzando uno dei seguenti formati:

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Tenere presente quanto segue:

  - L'utente può essere un utente locale o un utente di dominio.
  - Per un utente di dominio, è necessario utilizzare il codice ASCII per \ come illustrato sopra.
  - BlueXP non supporta password che includono il carattere @.

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

Risultato

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

Quali sono le prossime novità?

Configurare BlueXP.

Fase 2: Configurare BlueXP

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

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

Fasi

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

   https://ipaddress

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

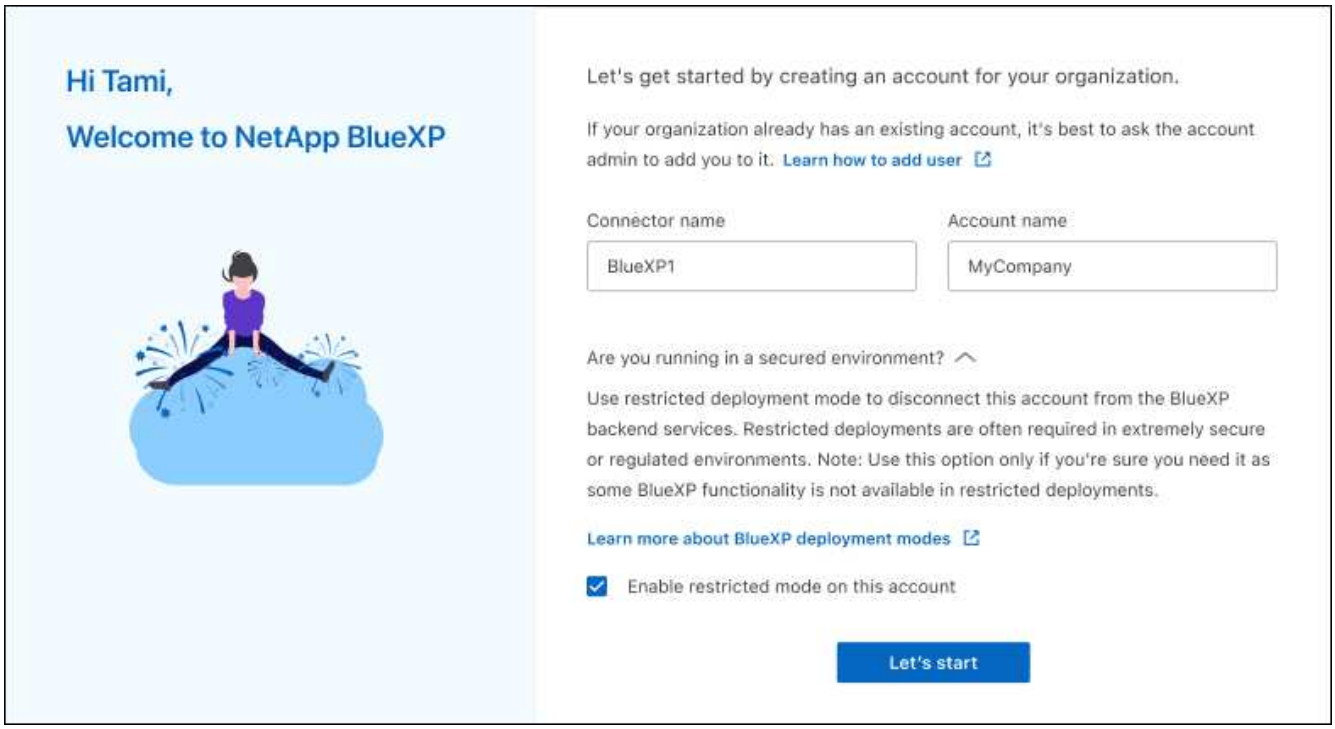
   a. Inserire un nome per il connettore.
   b. Immettere un nome per un nuovo account BlueXP o selezionare un account esistente.

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

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

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

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



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

Risultato

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

Quali sono le prossime novità?

Fornire a BlueXP le autorizzazioni precedentemente impostate.

Fase 3: Fornire le autorizzazioni ad BlueXP

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

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

"Scopri come preparare le autorizzazioni cloud".

Ruolo AWS IAM

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

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

Fasi

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

Risultato

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

Chiave di accesso AWS

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

Fasi

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

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

Risultato

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

Ruolo di Azure

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

Fasi

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

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

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

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

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

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

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

Risultato

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

Entità del servizio Azure

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

Fasi

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

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

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

Risultato

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

Account del servizio Google Cloud

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

Fasi

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

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

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

Risultato

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

Iscriviti a BlueXP (modalità limitata)

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

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

- Backup e recovery
- Classificazione
- Cloud Volumes ONTAP

Prima di iniziare

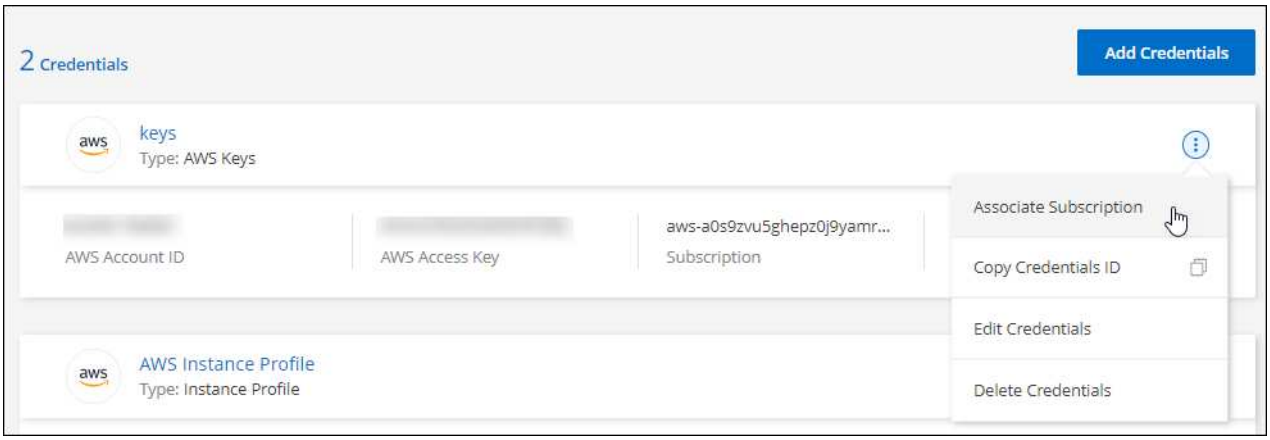
L'iscrizione a BlueXP implica l'associazione di un abbonamento Marketplace alle credenziali cloud associate a un connettore. Se hai seguito il flusso di lavoro "Get Started with Restricted mode" (inizia con la modalità limitata), dovresti già disporre di un connettore. Per ulteriori informazioni, consulta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

AWS

Fasi

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

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



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

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

   b. Selezionare **Iscriviti**.

   c. Selezionare **Configura account**.

      Verrai reindirizzato al sito Web di BlueXP.

   d. Dalla pagina **Subscription Assignment**:

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

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

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

      - Selezionare **Salva**.

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

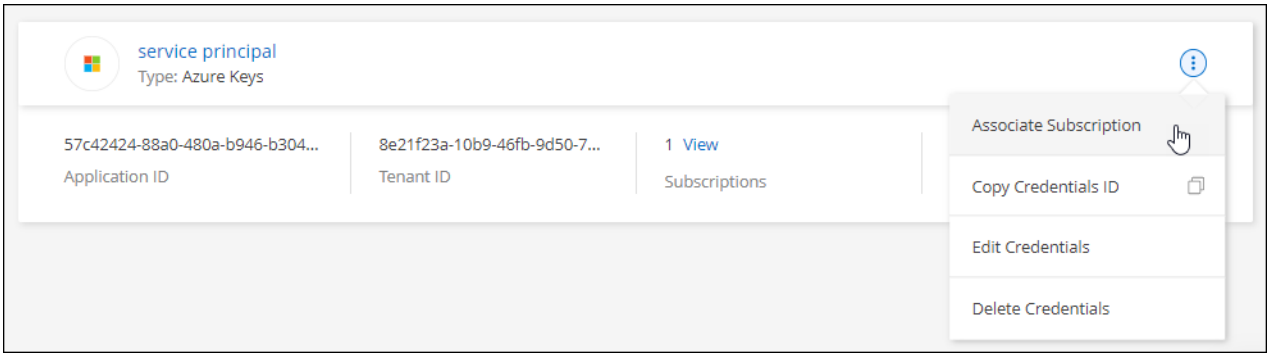
Iscriviti a BlueXP dal marketplace AWS

Azure

Fasi

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

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



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

   a. Se richiesto, accedere all'account Azure.

   b. Selezionare **Iscriviti**.

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

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

      Verrai reindirizzato al sito Web di BlueXP.

   e. Dalla pagina **Subscription Assignment**:

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

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

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

      - Selezionare **Salva**.

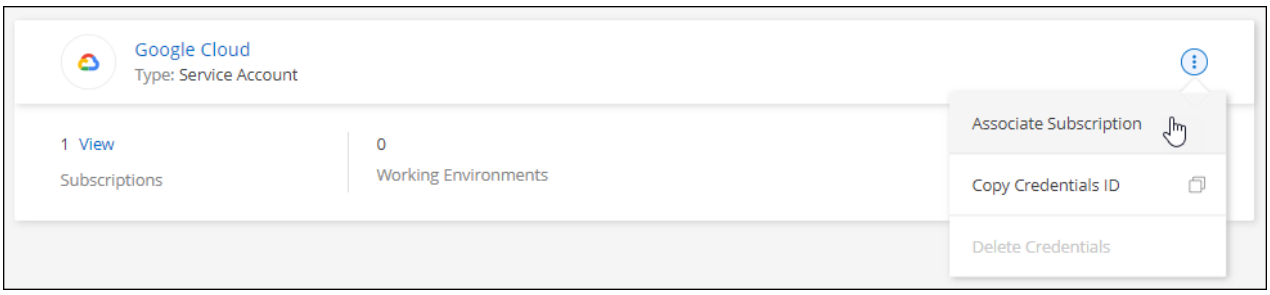
        Il seguente video mostra i passaggi per iscriversi a Azure Marketplace:

Iscriviti a BlueXP da Azure Marketplace

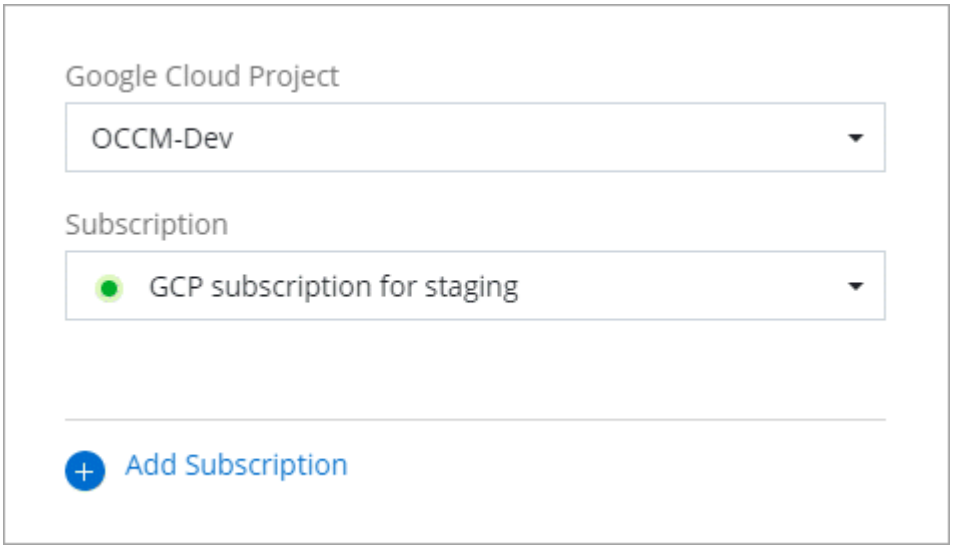
Google Cloud

Fasi

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



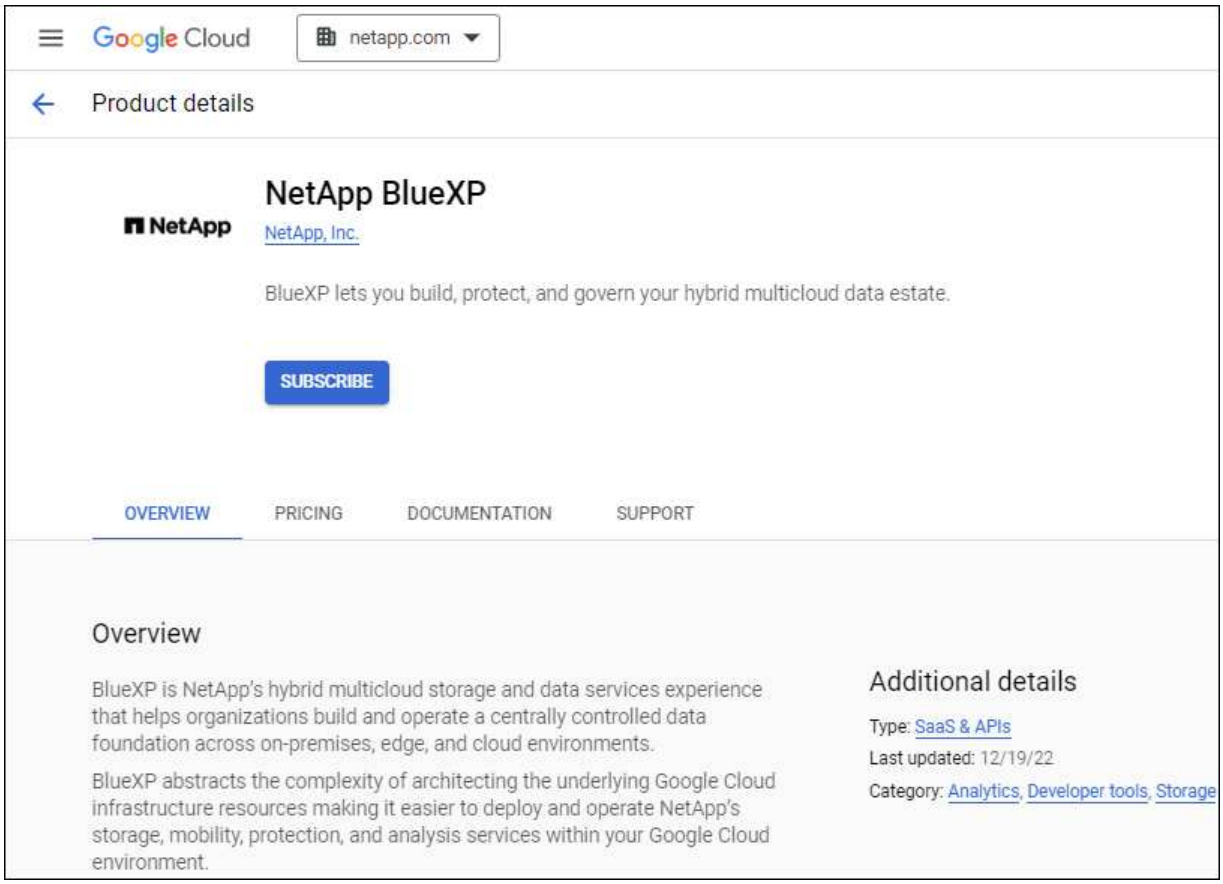
3. Per associare le credenziali a un abbonamento esistente, selezionare un progetto e un abbonamento Google Cloud dall'elenco a discesa, quindi selezionare **Associa**.



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

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

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



b. Selezionare **Iscriviti**.

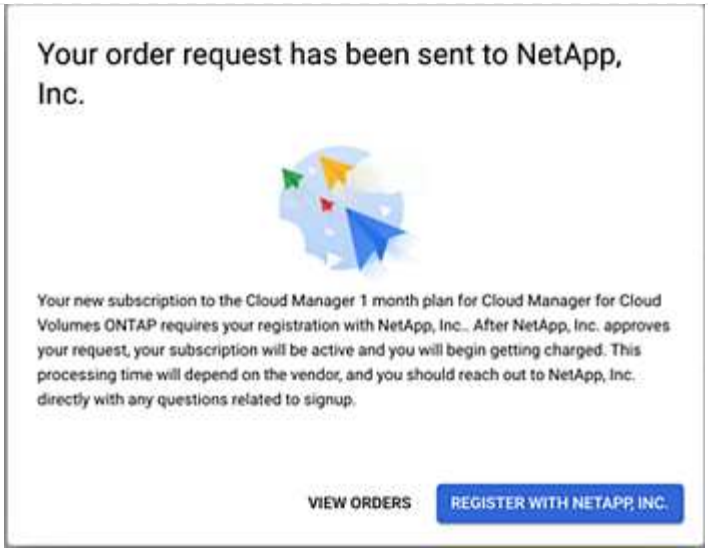
c. Selezionare l'account di fatturazione appropriato e accettare i termini e le condizioni.

d. Selezionare **Iscriviti**.

   Questa fase invia la richiesta di trasferimento a NetApp.

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

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



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

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

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

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

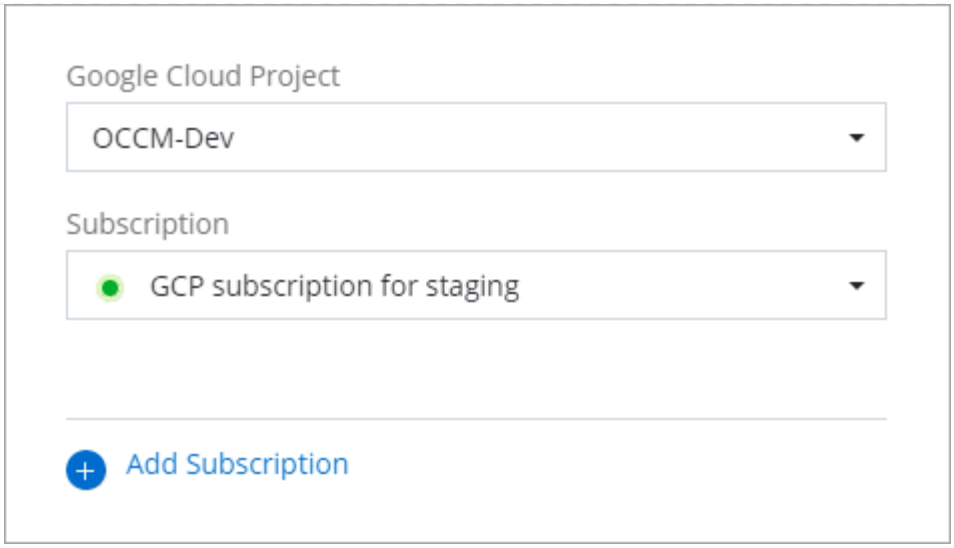
Per tutti gli altri account, è necessario associare manualmente l'abbonamento ripetendo questa procedura.

- Selezionare **Salva**.

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

Iscriviti a BlueXP da Google Cloud Marketplace

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



Link correlati

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

Operazioni successive (modalità limitata)

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

Per assistenza, consultare la documentazione relativa a questi servizi:

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

Link correlato

"Modalità di implementazione di BlueXP"

Inizia con la modalità privata

Flusso di lavoro introduttivo (modalità privata)

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

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

Prima di iniziare, dovresti avere una conoscenza di "BlueXP", "Connettori", e. "modalità di distribuzione".

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

1. Prepara un host Linux dedicato che soddisfi i requisiti di CPU, RAM, spazio su disco, motore Docker e altro ancora.
2. Configurare una rete che fornisca accesso alle reti di destinazione.
3. Per le implementazioni cloud, imposta le autorizzazioni nel tuo cloud provider in modo da poter associare tali autorizzazioni al connettore dopo l'installazione del software.

2 **"Implementare il connettore"**

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

Prepararsi per l'implementazione in modalità privata

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

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

Passaggio 1: Comprendere il funzionamento della modalità privata

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

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

Inoltre, non tutti i servizi BlueXP sono disponibili.

"Scopri come funziona la modalità privata".

Passaggio 2: Esaminare le opzioni di installazione

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

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

Fase 3: Esaminare i requisiti dell'host

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

Host dedicato

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

Sistemi operativi supportati

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

  L'host deve essere registrato con Red Hat Subscription Management. Se non è registrato, l'host non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione del connettore.

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

Hypervisor

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

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

CPU

4 core o 4 vCPU

RAM

14 GB

Tipo di istanza AWS EC2

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

Dimensione delle macchine virtuali Azure

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

Tipo di macchina Google Cloud

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

Il connettore è supportato in Google Cloud su un'istanza di macchina virtuale con un sistema operativo che

supporta "Funzioni di VM schermate"

Spazio su disco in /opz

100 GiB di spazio deve essere disponibile

Spazio su disco in /var

20 GiB di spazio deve essere disponibile

Motore Docker

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

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

"Visualizzare le istruzioni di installazione"

Fase 4: Preparare il collegamento in rete per il connettore

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

Connessioni alle reti di destinazione

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

Endpoint per le operazioni quotidiane

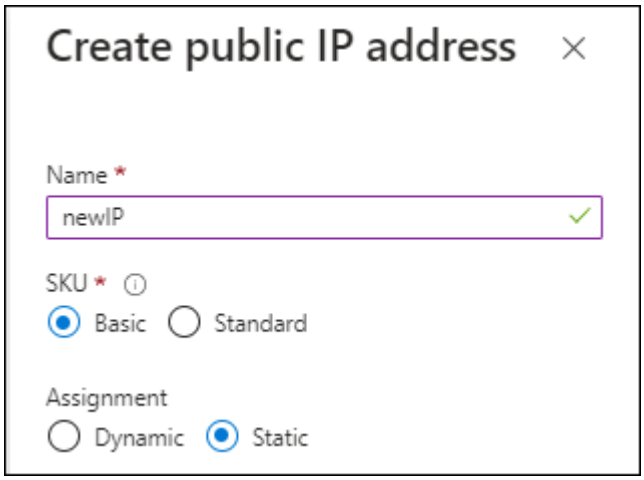
Il connettore contatta i seguenti endpoint per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

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

Endpoint	Scopo
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Per gestire le risorse nell'area Azure IL6.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Per gestire le risorse nelle regioni Azure China.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Per gestire le risorse in Google Cloud.

Indirizzo IP pubblico in Azure

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



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

"Documentazione di Azure: SKU IP pubblico"

Server proxy

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

- Indirizzo IP
- Credenziali
- Certificato HTTPS

BlueXP non supporta i server proxy trasparenti.

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

Porte

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

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

Enable NTP (attiva NTP)

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

Passaggio 5: Preparare le autorizzazioni del cloud

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

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

Ruolo AWS IAM

Utilizzare un ruolo IAM per fornire al connettore le autorizzazioni. Sarà necessario associare manualmente il ruolo all'istanza EC2 per il connettore.

Fasi

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

Risultato

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

Chiave di accesso AWS

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

Fasi

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

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

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

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

3. Allegare i criteri a un utente IAM.
   - "Documentazione AWS: Creazione dei ruoli IAM"
   - "Documentazione di AWS: Aggiunta e rimozione dei criteri IAM"
4. Assicurarsi che l'utente disponga di una chiave di accesso che è possibile aggiungere a BlueXP dopo aver installato il connettore.

Risultato

L'account dispone ora delle autorizzazioni necessarie.

Ruolo di Azure

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

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

Fasi

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

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

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

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

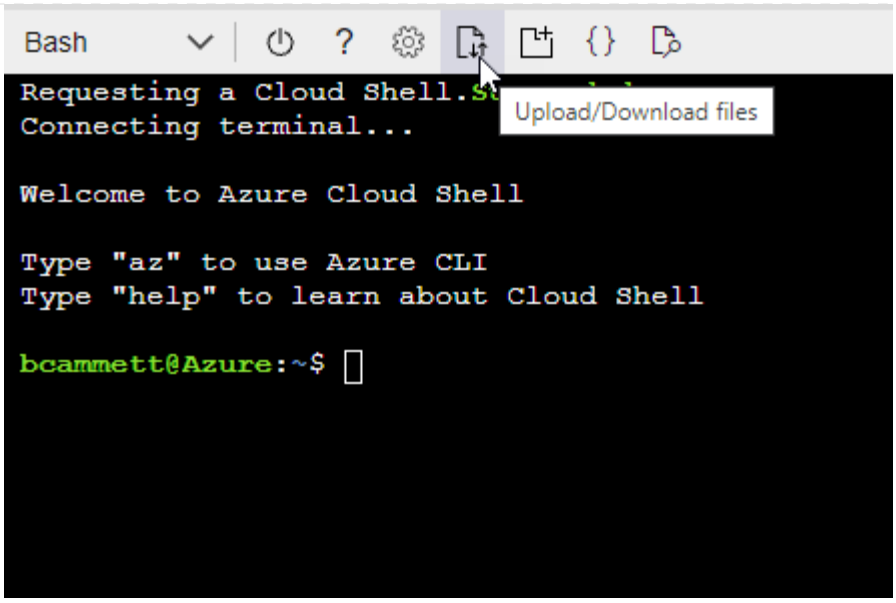
   Esempio

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

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

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

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



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

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

Risultato

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

Entità del servizio Azure

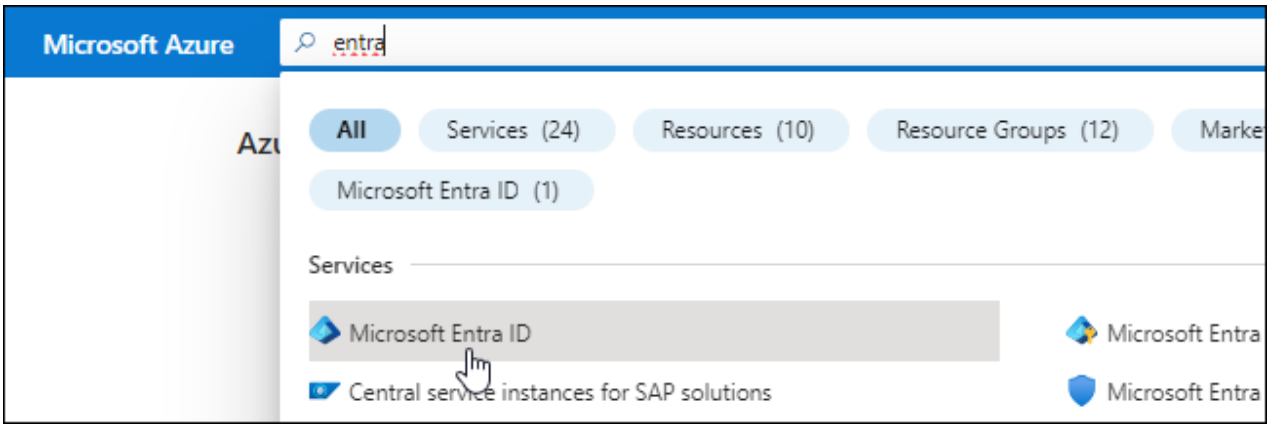
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP. È necessario fornire queste credenziali a BlueXP dopo aver installato il connettore e configurato BlueXP.

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

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

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

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



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

   Hai creato l'applicazione ad e il service principal.

Assegnare l'applicazione a un ruolo

1. Creare un ruolo personalizzato:

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

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

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

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

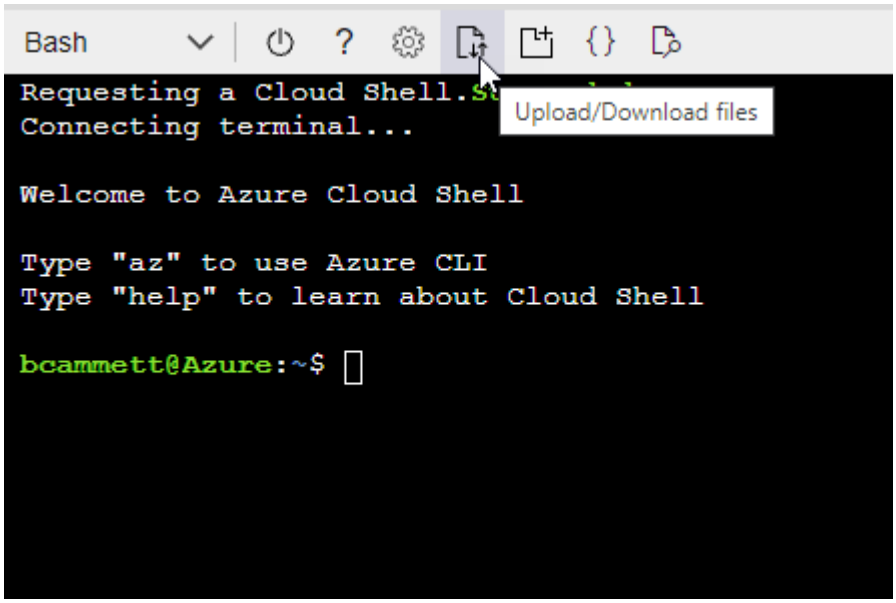
      Esempio

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

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

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

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



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

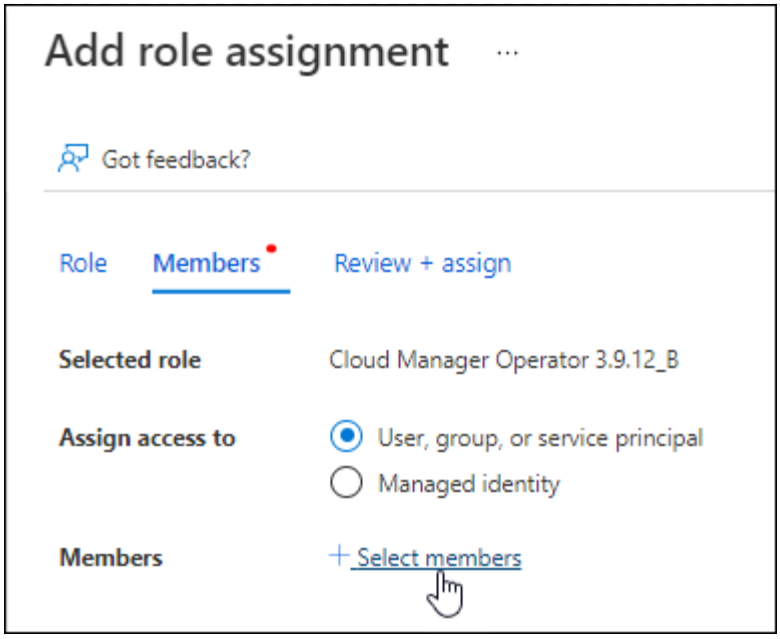
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Assegnare l'applicazione al ruolo:

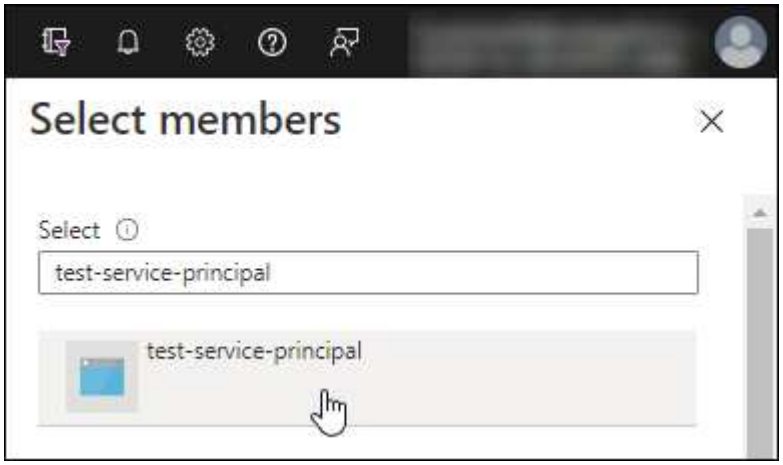
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

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



- Cercare il nome dell'applicazione.

  Ecco un esempio:



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

f. Selezionare **Rivedi + assegna**.

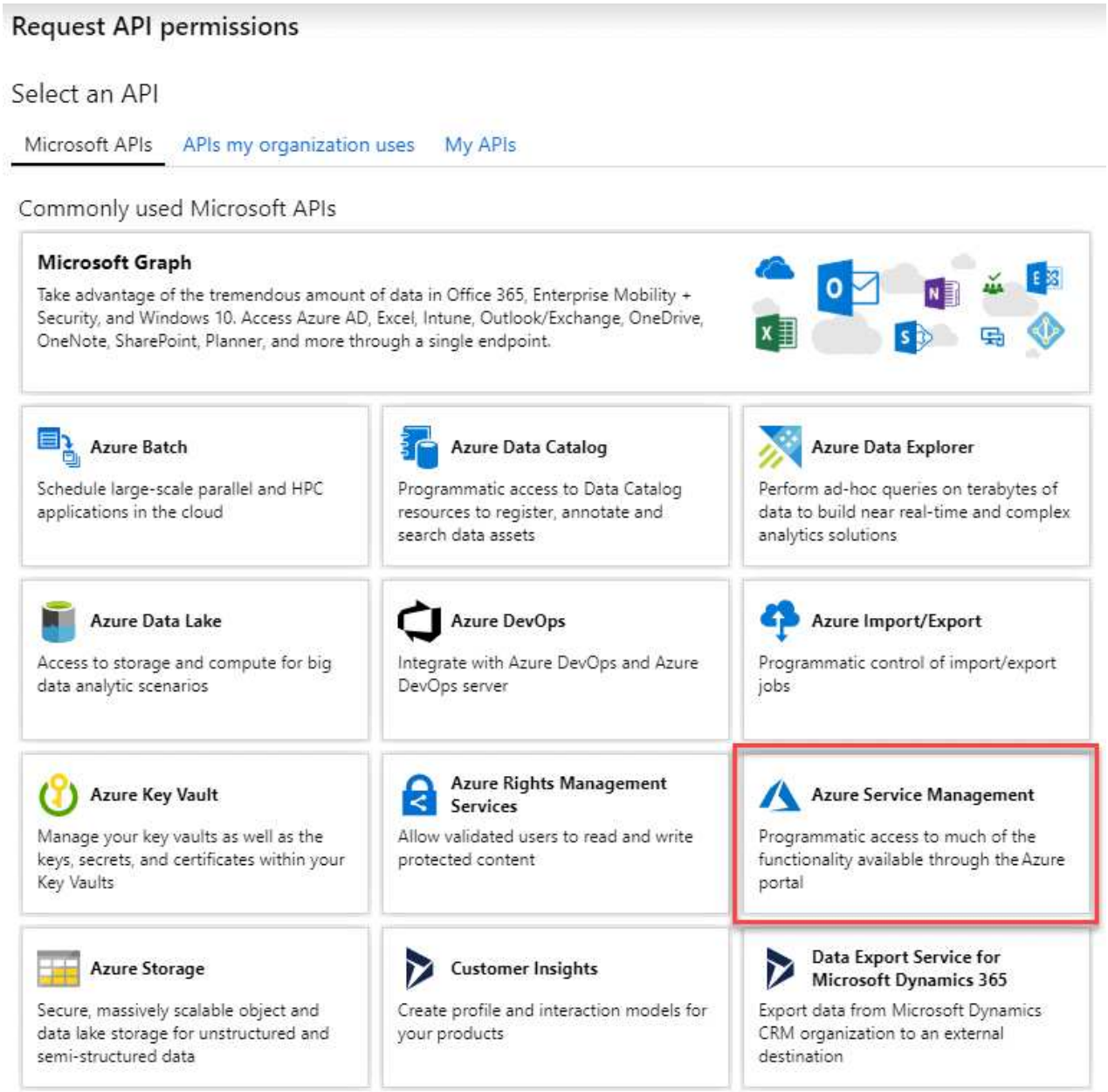
   L'entità del servizio dispone ora delle autorizzazioni Azure necessarie per implementare il connettore.

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

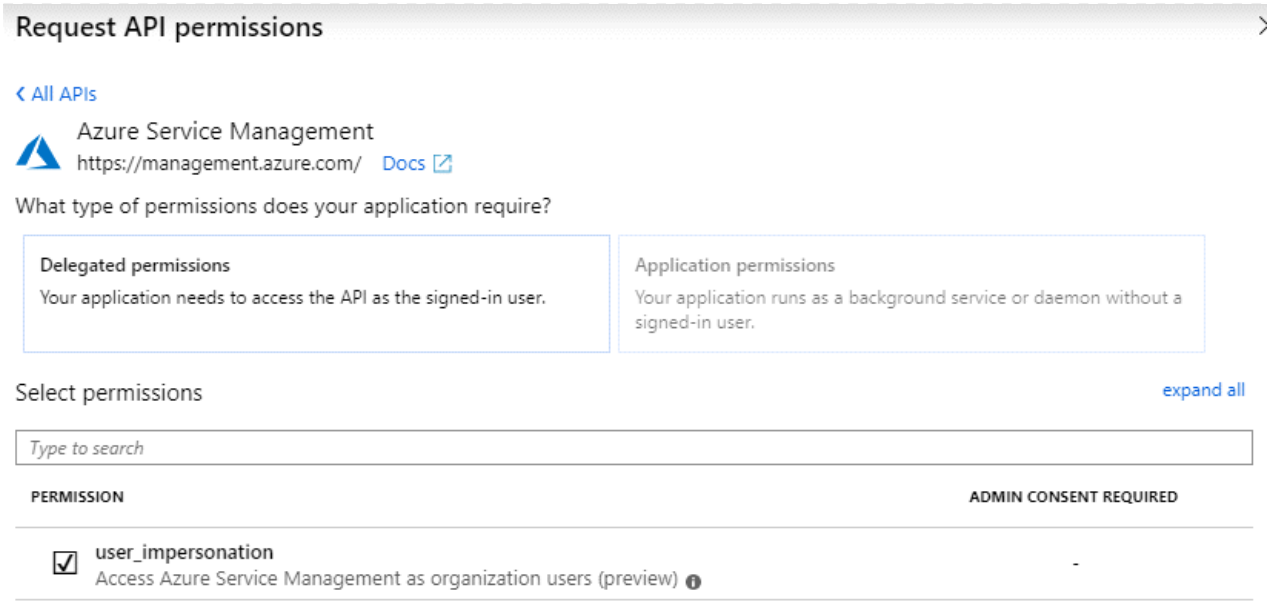
Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

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

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

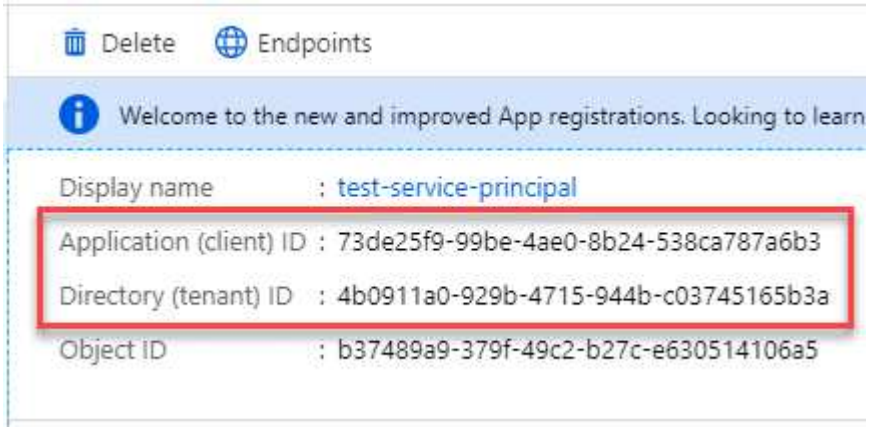


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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

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



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

Creare un client segreto

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

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

Risultato

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

Account del servizio Google Cloud

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

Fasi

1. Creare un ruolo personalizzato in Google Cloud:

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

   b. Da Google Cloud, attiva la shell cloud.

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

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

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

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

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

2. Creare un account di servizio in Google Cloud:

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

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

   c. Selezionare il ruolo appena creato.

   d. Completare i passaggi rimanenti per creare il ruolo.

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

Risultato

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

Passaggio 6: Abilitare le API di Google Cloud

Per implementare Cloud Volumes ONTAP in Google Cloud sono necessarie diverse API.

Fase

1. "Abilita le seguenti API di Google Cloud nel tuo progetto"
    - API di Cloud Deployment Manager V2
    - API Cloud Logging
    - API Cloud Resource Manager
    - API di Compute Engine
    - API IAM (Identity and Access Management)
    - API di Cloud Key Management Service (KMS)

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

Implementare il connettore in modalità privata

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

Fase 1: Installare il connettore

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

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

Prima di iniziare

Per installare il connettore sono necessari i privilegi di root.

Fasi

1. Verificare che docker sia attivato e in esecuzione.

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

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

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

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

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

   Dove <version> è la versione del connettore scaricato.

5. Eseguire lo script di installazione:

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

   Dove <version> è la versione del connettore scaricato.

Risultato

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

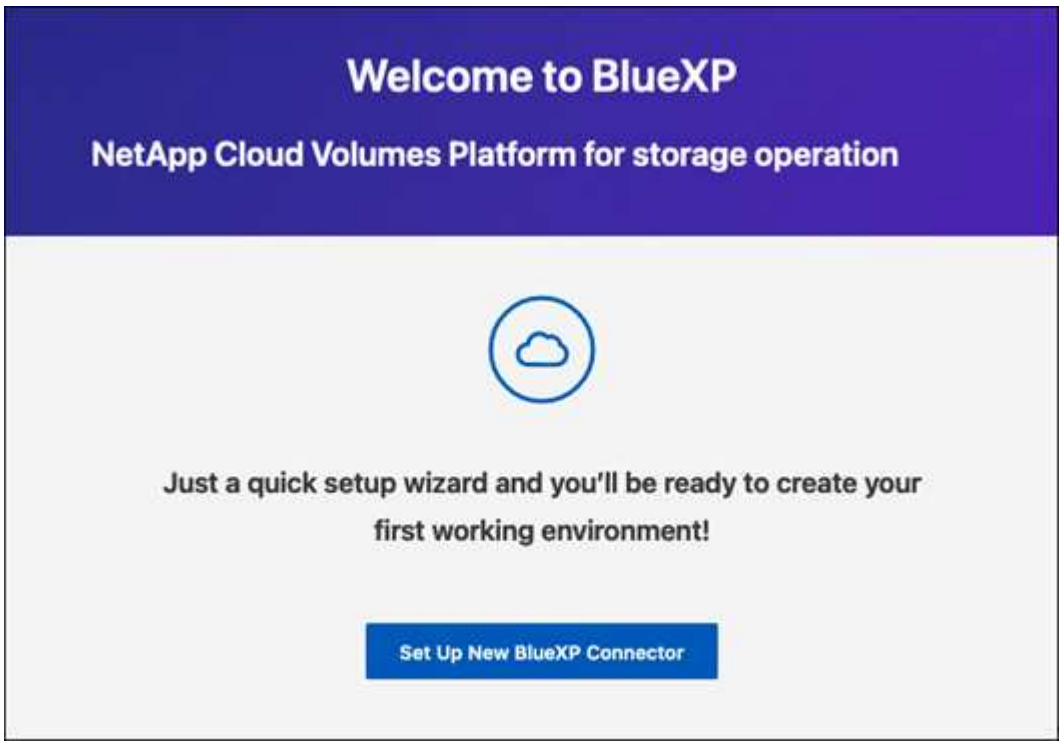
Fase 2: Configurare BlueXP

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

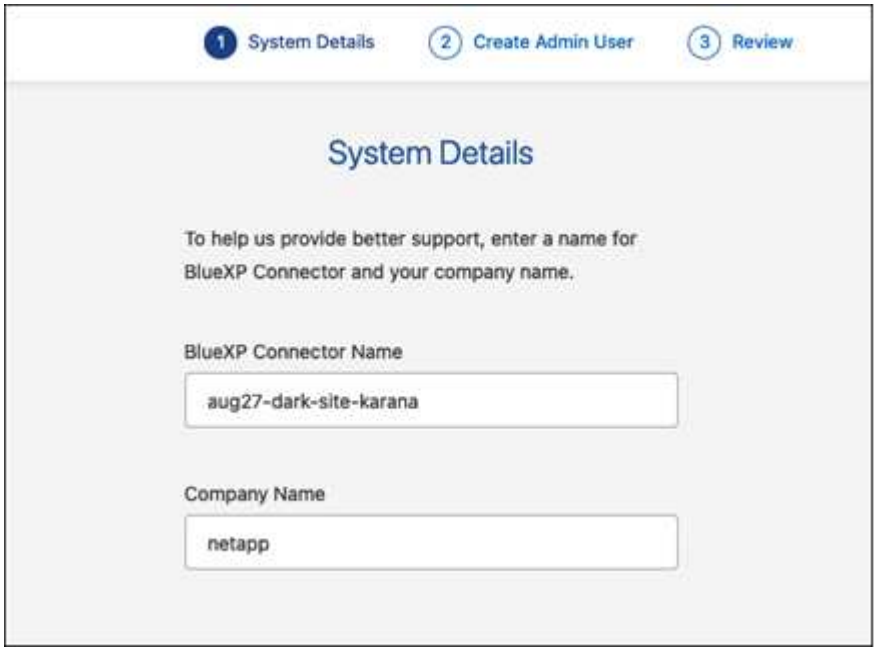
Fasi

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

   Viene visualizzata la seguente schermata.



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



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

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

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

Risultato

Il connettore è stato installato e configurato.

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

Quali sono le prossime novità?

Fornire a BlueXP le autorizzazioni precedentemente impostate.

Fase 3: Fornire le autorizzazioni ad BlueXP

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

"Scopri come preparare le autorizzazioni cloud".

Ruolo AWS IAM

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

Fasi

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

Risultato

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

Chiave di accesso AWS

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

Fasi

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

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

Risultato

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

Ruolo di Azure

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

Fasi

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

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

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

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

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

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

Risultato

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

Entità del servizio Azure

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

Fasi

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

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

Risultato

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

Account del servizio Google Cloud

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

Fasi

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

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

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

Risultato

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

Operazioni successive (modalità privata)

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

Per assistenza, consultare la seguente documentazione:

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

Link correlato

"Modalità di implementazione di BlueXP"

Accedere a BlueXP

Il modo in cui accedi ad BlueXP dipende dalla modalità di implementazione di BlueXP che stai utilizzando per l'account.

Modalità standard

Dopo aver effettuato la registrazione a BlueXP, è possibile accedere dalla console basata su Web per iniziare a gestire l'infrastruttura di dati e storage.

A proposito di questa attività

È possibile accedere alla console basata su Web di BlueXP utilizzando una delle seguenti opzioni:

- Le tue credenziali NetApp Support Site (NSS) esistenti
- Un login cloud NetApp utilizzando il tuo indirizzo e-mail e una password
- Una connessione federata

  È possibile utilizzare il Single Sign-on per accedere utilizzando le credenziali della directory aziendale (identità federata). "Scopri come utilizzare la federazione delle identità con BlueXP".

Fasi

1. Aprire un browser Web e accedere a. "Console BlueXP"
2. Nella pagina **Log in**, inserire l'indirizzo e-mail associato al login.
3. A seconda del metodo di autenticazione associato all'accesso, viene richiesto di inserire le credenziali:
   - Credenziali cloud NetApp: Inserire la password
   - Federated User (utente federato): Immettere le credenziali di identità federated
   - Account NetApp Support Site: Immettere le credenziali del NetApp Support Site

Risultato

Ora hai effettuato l'accesso e puoi iniziare a utilizzare BlueXP per gestire la tua infrastruttura multi-cloud ibrida.

Modalità limitata

Quando si utilizza BlueXP in modalità limitata, è necessario accedere alla console BlueXP dall'interfaccia utente che viene eseguita localmente sul connettore.

A proposito di questa attività

BlueXP supporta l'accesso con una delle seguenti opzioni quando l'account è impostato in modalità limitata:

- Un login cloud NetApp utilizzando il tuo indirizzo e-mail e una password
- Una connessione federata

  È possibile utilizzare il Single Sign-on per accedere utilizzando le credenziali della directory aziendale (identità federata). "Scopri come utilizzare la federazione delle identità con 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 in cui è stato installato il connettore. Ad esempio, potrebbe essere necessario

inserire un indirizzo IP privato da un host connesso all’host del connettore.

2. Immettere il nome utente e la password per accedere.

Risultato

Ora hai effettuato l’accesso e puoi iniziare a utilizzare BlueXP per gestire la tua infrastruttura multi-cloud ibrida.

Modalità privata

Quando si utilizza BlueXP in modalità privata, è necessario accedere alla console BlueXP dall’interfaccia utente che viene eseguita localmente sul connettore.

A proposito di questa attività

La modalità privata supporta la gestione e l’accesso degli utenti locali. L’autenticazione non viene fornita attraverso il servizio cloud di 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 in cui è stato installato il connettore. Ad esempio, potrebbe essere necessario inserire un indirizzo IP privato da un host connesso all’host del connettore.

2. Immettere il nome utente e la password per accedere.

Risultato

Ora hai effettuato l’accesso e puoi iniziare a utilizzare BlueXP per gestire la tua infrastruttura multi-cloud ibrida.