Documentazione di installazione e amministrazione di BlueXP

Setup and administration

NetApp
April 26, 2024

Sommario

Documentazione di installazione e amministrazione di BlueXP . . . 1
Note di rilascio . . . 2
- Novità . . . 2
- Limitazioni note . . . 27

Inizia subito . . . 29
- Scopri le nozioni di base . . . 29
- Inizia con la modalità standard . . . 51
- Inizia con la modalità limitata . . . 159
- Inizia con la modalità privata . . . 193
- Accedere a BlueXP . . . 213

Amministrare BlueXP . . . 216
- Utilizzo della federazione delle identità con BlueXP . . . 216
- BlueXP . . . 222
- Connettori . . . 236
- Credenziali e iscrizioni . . . 255

Riferimento . . . 297
- Permessi . . . 297
- Porte . . . 356

Conoscenza e supporto . . . 362
- Registrati per ricevere assistenza . . . 362
- Richiedi assistenza . . . 366

Note legali . . . 372
- Copyright . . . 372
- Marchi . . . 372
- Brevetti . . . 372
- Direttiva sulla privacy . . . 372
- Open source . . . 372

Documentazione di installazione e amministrazione di BlueXP

Note di rilascio

Novità

Scopri le novità delle funzionalità di amministrazione di BlueXP: Account BlueXP, connettori, credenziali del cloud provider e altro ancora.

22 aprile 2024

Connettore 3.9.39

Questa versione di BlueXP Connector include piccoli miglioramenti alla sicurezza e correzioni di bug.

A questo punto, la versione 3.9.39 è disponibile per la modalità standard e la modalità limitata.

Autorizzazioni AWS per creare un connettore

Sono necessarie due autorizzazioni aggiuntive per creare un connettore in AWS da BlueXP:

```
"ec2:DescribeLaunchTemplates",
"ec2:CreateLaunchTemplate",
```

Queste autorizzazioni sono necessarie per abilitare IMDSv2 sull'istanza EC2 per il connettore.

Queste autorizzazioni sono state incluse nella policy visualizzata nell'interfaccia utente BlueXP durante la creazione di un connettore e nella stessa policy fornita nella documentazione.

> Questo criterio contiene solo le autorizzazioni necessarie per avviare l'istanza di Connector in AWS da BlueXP. Non è lo stesso criterio che viene assegnato all'istanza del connettore.

"Scopri come configurare le autorizzazioni AWS per creare un connettore da AWS".

11 aprile 2024

Update di Docker Engine

Abbiamo aggiornato i requisiti di Docker Engine per specificare la versione massima supportata del connettore, ovvero 25,0.5. La versione minima supportata è ancora 19,3.1.

"Visualizza i requisiti dell'host del connettore".

26 marzo 2024

Rilascio in modalità privata (3,9.38)

Una nuova release in modalità privata è ora disponibile per BlueXP. Questa release include le seguenti versioni dei servizi BlueXP che sono supportate in modalità privata.

Servizio	Versione inclusa
Connettore	3.9.38
Backup e recovery	12 marzo 2024
Classificazione	4 marzo 2024
Gestione di Cloud Volumes ONTAP	8 marzo 2024
Portafoglio digitale	30 luglio 2023
Gestione del cluster ONTAP on-premise	30 luglio 2023
Replica	18 settembre 2022

Questa nuova versione è disponibile per il download dal sito del supporto NetApp.

- "Informazioni sulla modalità privata"
- "Scopri come iniziare a utilizzare BlueXP in modalità privata"
- "Informazioni su come aggiornare il connettore quando si utilizza la modalità privata"

8 marzo 2024

Connettore 3.9.38

A questo punto, la versione 3.9.38 è disponibile per la modalità standard e la modalità limitata. Questa release include il supporto per IMDSv2 in AWS e un aggiornamento dei permessi AWS.

Supporto di IMDSv2

BlueXP ora supporta Amazon EC2 Instance Metadata Service versione 2 (IMDSv2) con l'istanza del connettore e con le istanze di Cloud Volumes ONTAP. IMDSv2 fornisce una maggiore protezione contro le vulnerabilità. In precedenza era supportato solo IMDSv1.

"Scopri di più su IMDSv2 dal blog sulla sicurezza AWS"

Il servizio IMDS (Instance Metadata Service) viene attivato come segue nelle istanze EC2:

- Per implementazioni di nuovi connettori da BlueXP o che utilizzano "Script di terraform", IMDSv2 è attivato per impostazione predefinita nell'istanza EC2.
- Se si avvia una nuova istanza EC2 in AWS e quindi si installa manualmente il software del connettore, anche IMDSv2 viene attivato per impostazione predefinita.
- Se si avvia il connettore da AWS Marketplace, IMDSv1 viene attivato per impostazione predefinita. È possibile configurare manualmente IMDSv2 sull'istanza EC2.
- Per i connettori esistenti, IMDSv1 è ancora supportato, ma è possibile configurare manualmente IMDSv2 sull'istanza EC2, se si preferisce.
- Per Cloud Volumes ONTAP, IMDSv1 è attivato per impostazione predefinita sulle istanze nuove ed esistenti. Se si preferisce, è possibile configurare manualmente IMDSv2 sulle istanze EC2.

"Scopri come configurare IMDSv2 sulle istanze esistenti".

Aggiornamento delle autorizzazioni AWS

Abbiamo aggiornato la policy del connettore per AWS in modo da includere l'autorizzazione "EC2:DescribeAvailabilityZones". Questa autorizzazione è necessaria per una prossima release. Aggiorneremo le note di rilascio con ulteriori dettagli quando tale release sarà disponibile.

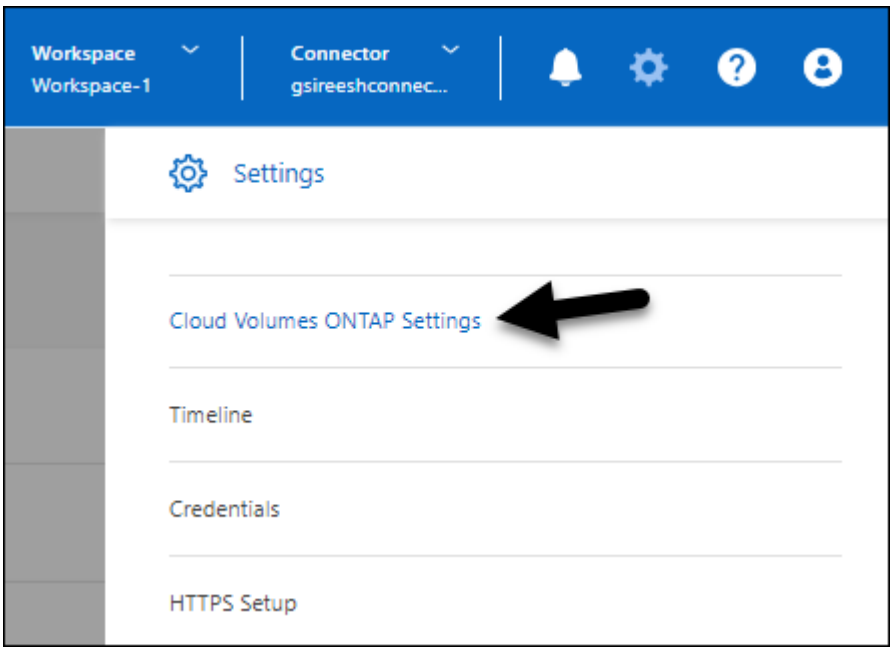
"Visualizza le autorizzazioni AWS per il connettore".

Impostazioni proxy e Cloud Volumes ONTAP

Le impostazioni del server proxy per il connettore sono ora disponibili nella pagina **Gestisci connettori** (modalità standard) o nella pagina **Modifica connettori** (modalità limitata e modalità privata).

"Informazioni su come configurare il connettore per l'utilizzo di un server proxy".

Inoltre, abbiamo rinominato la pagina **Impostazioni connettore** in **Impostazioni Cloud Volumes ONTAP**.



15 febbraio 2024

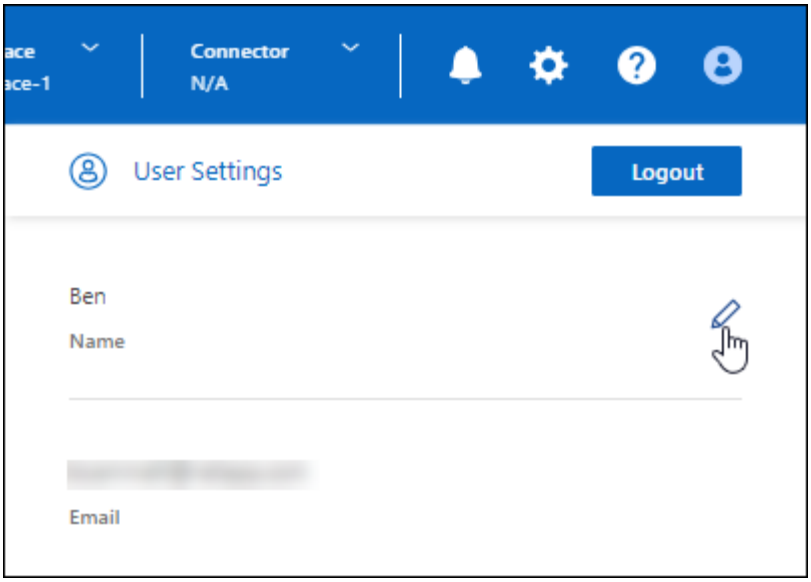
Connettore 3.9.37

Questa versione di BlueXP Connector include piccoli miglioramenti alla sicurezza e correzioni di bug.

A questo punto, la versione 3.9.37 è disponibile per la modalità standard e la modalità limitata.

Modifica nome

Se utilizzi le credenziali cloud di NetApp per accedere a BlueXP, puoi modificare il tuo nome in **Impostazioni utente**.



La modifica del nome non è supportata se si effettua l'accesso con una connessione federata o con l'account del sito di supporto NetApp.

11 gennaio 2024

Connettore 3.9.36

Questa release include miglioramenti minori, correzioni di bug e supporto per il connettore nelle seguenti aree cloud:

- La regione di Israele (Tel Aviv) in AWS
- L'Arabia Saudita in Google Cloud

5 dicembre 2023

Rilascio in modalità privata (3,9.35)

Una nuova release in modalità privata è ora disponibile per BlueXP. Questa release include la versione 3.9.35 del connettore e le versioni dei servizi BlueXP che sono supportate dalla modalità privata a ottobre 2023.

Questa nuova versione è disponibile per il download dal sito del supporto NetApp.

- "Scopri di più sui servizi BlueXP inclusi nella modalità privata"
- "Scopri come iniziare a utilizzare BlueXP in modalità privata"
- "Informazioni su come aggiornare il connettore quando si utilizza la modalità privata"

8 novembre 2023

Connettore 3.9.35

Questa versione contiene piccoli miglioramenti alla sicurezza e correzioni di bug.

6 ottobre 2023

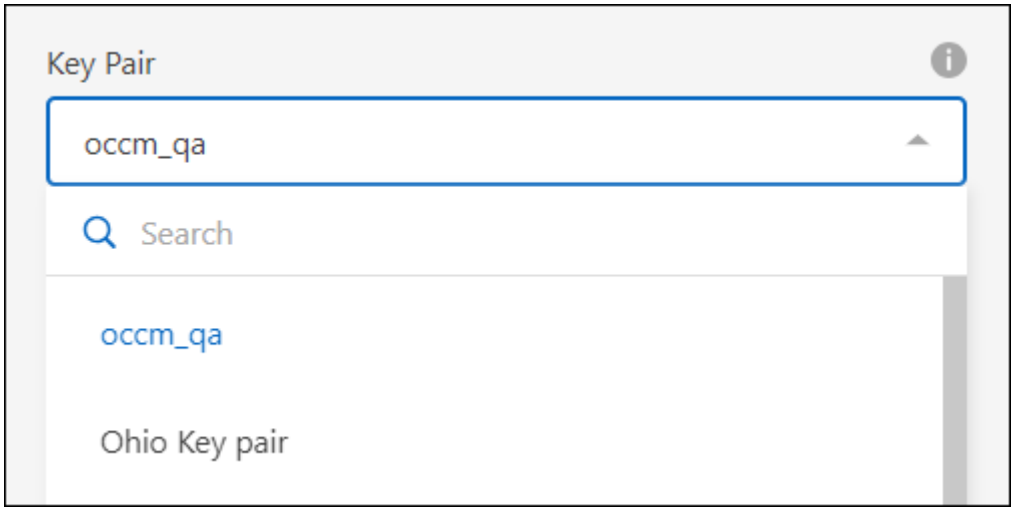
Connettore 3.9.34

Questa versione contiene piccoli miglioramenti e correzioni di bug.

10 settembre 2023

Connettore 3.9.33

- Quando crei un connettore in AWS da BlueXP, puoi cercare nel campo Coppia di chiavi per trovare più facilmente la coppia di chiavi da utilizzare con l'istanza del connettore.



- Questo aggiornamento include anche le correzioni dei bug.

30 luglio 2023

Connettore 3.9.32

- È ora possibile utilizzare l'API del servizio di audit BlueXP per esportare i registri di audit.

  Il servizio di audit registra le informazioni sulle operazioni eseguite dai servizi BlueXP. Sono inclusi spazi di lavoro, connettori utilizzati e altri dati di telemetria. È possibile utilizzare questi dati per determinare quali azioni sono state eseguite, chi le ha eseguite e quando si sono verificate.

  "Scopri di più sull'utilizzo dell'API del servizio di audit"

  Questo collegamento è accessibile anche dall'interfaccia utente di BlueXP nella pagina Timeline.

- Questa versione del connettore include anche miglioramenti Cloud Volumes ONTAP e miglioramenti del cluster ONTAP on-premise.
  - "Scopri i miglioramenti di Cloud Volumes ONTAP"
  - "Scopri i miglioramenti del cluster on-premise di ONTAP"

2 luglio 2023

Connettore 3.9.31

- Ora puoi scoprire i cluster ONTAP on-premise dalla scheda **My estate** (in precedenza **My Opportunities**)

  "Scopri come scoprire i cluster dalla pagina My estate".

- Se si utilizza il connettore in un'area governativa di Azure, assicurarsi che il connettore possa contattare il seguente endpoint:

  https://occmclientinfragov.azurecr.us

  Questo endpoint è necessario per installare manualmente il connettore e per aggiornare il connettore e i relativi componenti Docker.

  A seguito di questa modifica, un connettore in un'area governativa di Azure non contatta più il seguente endpoint:

  https://cloudmanagerinfraprod.azurecr.io

  Si noti che questo endpoint è ancora necessario per tutte le altre configurazioni in modalità limitata e per la modalità standard.

4 giugno 2023

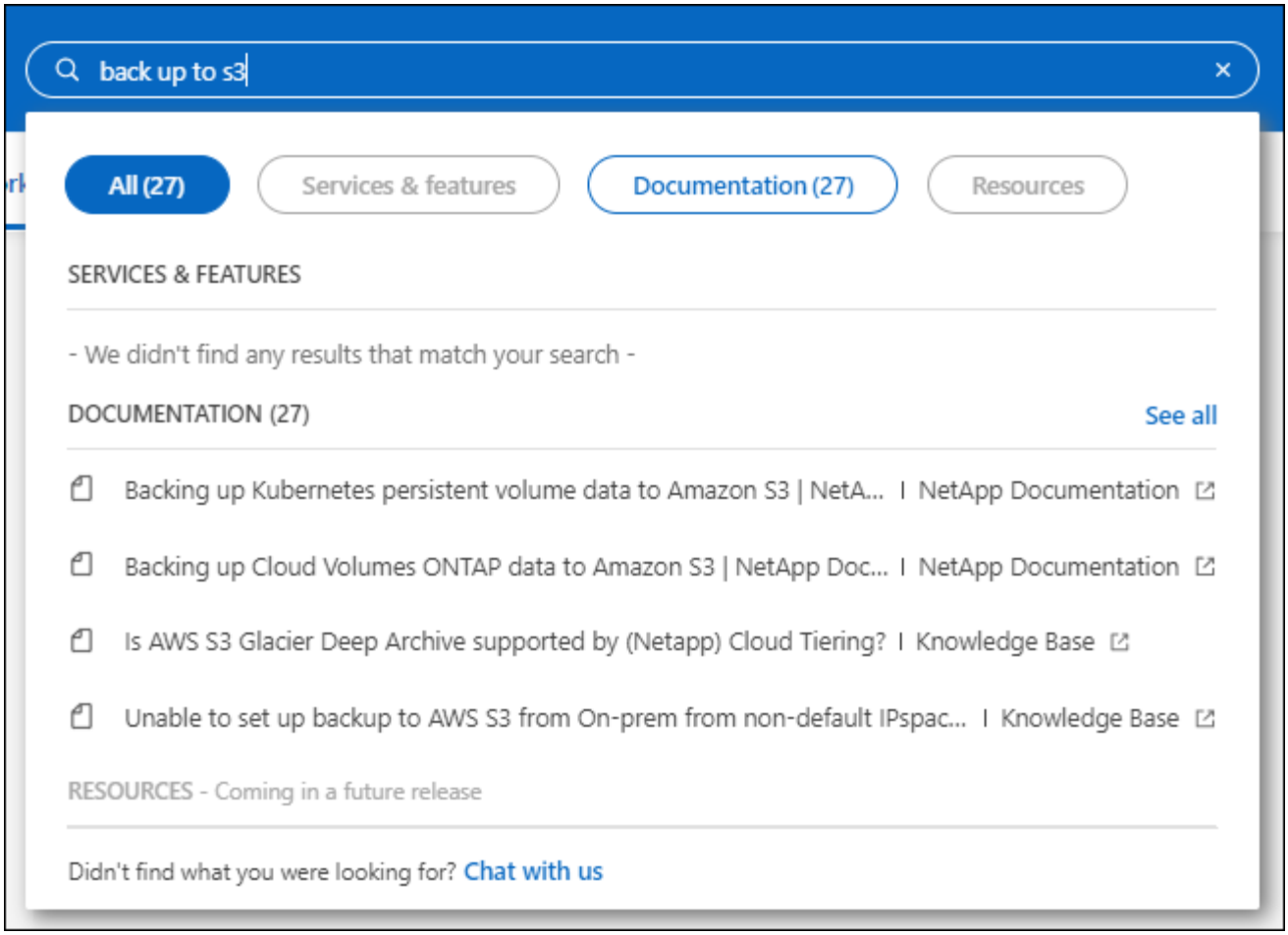
Connettore 3.9.30

- Quando si apre un caso di supporto NetApp dalla dashboard di supporto, BlueXP apre il caso utilizzando l'account del sito di supporto NetApp associato all'accesso a BlueXP. In precedenza, BlueXP ha utilizzato l'account del sito di supporto NetApp associato all'intero account BlueXP.

  Nell'ambito di questa modifica, la registrazione al supporto per un account BlueXP viene ora effettuata tramite l'account del sito di supporto NetApp associato all'accesso BlueXP di un utente. In precedenza, la registrazione al supporto era effettuata tramite un account NSS associato all'intero account BlueXP. Di conseguenza, altri utenti di BlueXP non visualizzeranno lo stesso stato di registrazione del supporto se non hanno associato un account del sito di supporto NetApp al proprio login BlueXP. Se in precedenza hai registrato il tuo account BlueXP per il supporto, lo stato di registrazione è ancora valido. Basta aggiungere un account NSS a livello utente per visualizzare lo stato.

  - "Scopri come creare un caso con il supporto NetApp"
  - "Scopri come gestire le credenziali associate all'accesso a BlueXP"
  - "Scopri come registrarti per il supporto"

- Ora puoi cercare la documentazione da BlueXP. I risultati della ricerca ora forniscono link ai contenuti su docs.netapp.com e kb.netapp.com, che potrebbero aiutare a rispondere a una domanda che hai.



- Il connettore consente ora di aggiungere e gestire gli account di storage Azure da BlueXP.

  "Scopri come aggiungere nuovi account di storage Azure negli abbonamenti Azure di BlueXP".

- Il connettore è ora supportato nelle seguenti aree AWS:
  - Hyderabad (ap-sud-2)
  - Melbourne (ap-sud-est-4)
  - Spagna (ue-Sud-2)
  - Emirati Arabi Uniti (me-Central-1)
  - Zurigo (eu-Central-2)
- Il connettore è ora supportato nelle seguenti aree di Azure:
  - Brasile Sud
  - Francia Sud
  - Jio India Central
  - Jio India ovest
  - Polonia centrale
  - Qatar Central
- Il connettore è ora supportato nelle seguenti aree di Google Cloud:
  - Columbus (US-east5)

- Dallas (US-South1)

"Visualizza l'elenco completo delle regioni supportate"

7 maggio 2023

Connettore 3.9.29

- Ubuntu 22.04 è il nuovo sistema operativo per il connettore quando si implementa un connettore da BlueXP o dal mercato del cloud provider.

  È inoltre possibile installare manualmente il connettore sul proprio host Linux su cui è in esecuzione Ubuntu 22.04.

- Red Hat Enterprise Linux 8.6 e 8.7 non sono più supportati con le nuove implementazioni di connettori.

  Queste versioni non sono supportate con le nuove implementazioni perché Red Hat non supporta più Docker, necessario per il connettore. Se si dispone di un connettore esistente in esecuzione su RHEL 8.6 o 8.7, NetApp continuerà a supportare la configurazione.

  Red Hat 7.6, 7.7, 7.8 e 7.9 sono ancora supportati con connettori nuovi ed esistenti.

- Il connettore è ora supportato nell'area Qatar di Google Cloud.
- Il connettore è supportato anche nella regione Sweden Central di Microsoft Azure.

  "Visualizza l'elenco completo delle regioni supportate"

- Questa versione del connettore include i miglioramenti di Cloud Volumes ONTAP.

  "Scopri i miglioramenti di Cloud Volumes ONTAP"

4 aprile 2023

Modalità di implementazione

Le *modalità di implementazione* di BlueXP consentono di utilizzare BlueXP in modo da soddisfare i requisiti di sicurezza e di business. È possibile scegliere tra tre modalità:

- Modalità standard
- Modalità limitata
- Modalità privata

"Scopri di più su queste modalità di implementazione".

> L'introduzione della modalità limitata sostituisce l'opzione di attivazione o disattivazione della piattaforma SaaS. È possibile attivare la modalità limitata al momento della creazione dell'account. Non può essere attivato o disattivato in un secondo momento.

3 aprile 2023

Connettore 3.9.28

- Le notifiche e-mail sono ora supportate con il portafoglio digitale BlueXP.

  Se si configurano le impostazioni di notifica, è possibile ricevere notifiche via email quando le licenze BYOL stanno per scadere (una notifica di "avviso") o se sono già scadute (una notifica di "errore").

  "Scopri come configurare le notifiche via e-mail".

- Il connettore è ora supportato nella regione di Google Cloud Turin.

  "Visualizza l'elenco completo delle regioni supportate"

- È ora possibile gestire le credenziali utente associate all'accesso BlueXP: Credenziali ONTAP e credenziali del sito di supporto NetApp.

  Quando si seleziona **Impostazioni > credenziali**, è possibile visualizzare le credenziali, aggiornare le credenziali ed eliminarle. Ad esempio, se si modifica la password per queste credenziali, sarà necessario aggiornare la password in BlueXP.

  "Scopri come gestire le credenziali utente".

- È ora possibile caricare gli allegati quando si crea un caso di supporto o quando si aggiornano le note del caso per un caso di supporto esistente.

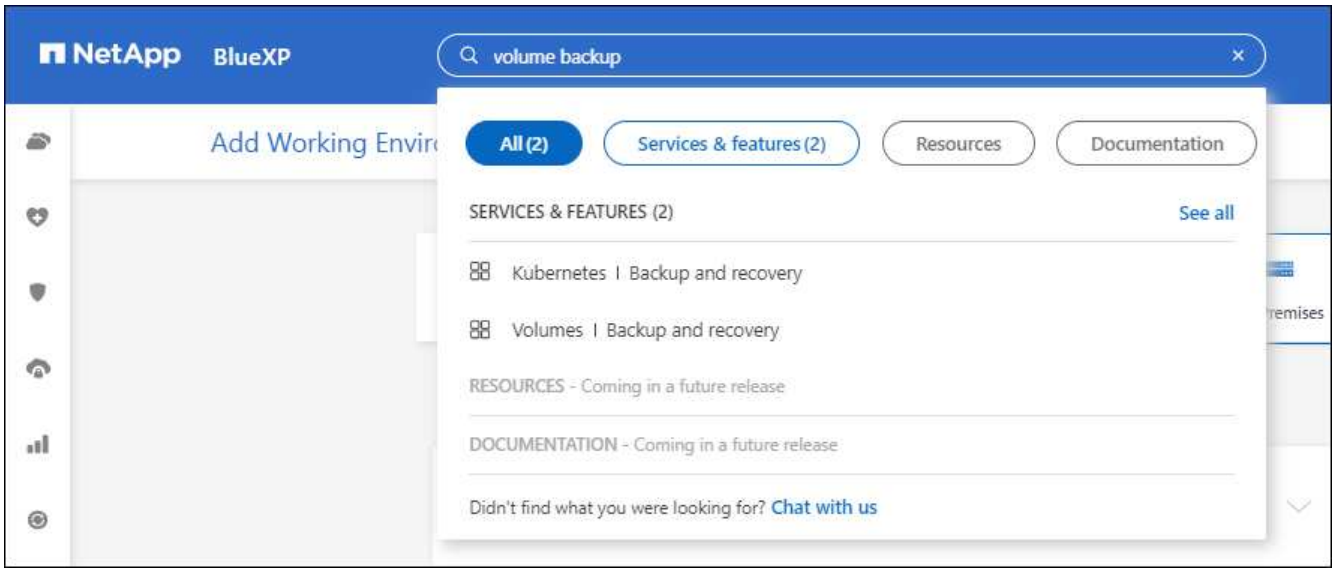
  "Scopri come creare e gestire i casi di supporto".

- Questa versione del connettore include anche miglioramenti Cloud Volumes ONTAP e miglioramenti del cluster ONTAP on-premise.
  - "Scopri i miglioramenti di Cloud Volumes ONTAP"
  - "Scopri i miglioramenti del cluster on-premise di ONTAP"

5 marzo 2023

Connettore 3.9.27

- La funzione di ricerca è ora disponibile nella console BlueXP. A questo punto, è possibile utilizzare la ricerca per trovare i servizi e le funzionalità di BlueXP.



- È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente da BlueXP. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

  "Scopri come gestire i tuoi casi di supporto".

- Il connettore è ora supportato in qualsiasi ambiente cloud con isolamento completo da Internet. È quindi possibile utilizzare la console BlueXP in esecuzione sul connettore per implementare Cloud Volumes ONTAP nella stessa posizione e per rilevare i cluster ONTAP on-premise (se si dispone di una connessione dall'ambiente cloud all'ambiente on-premise). È inoltre possibile utilizzare il backup e il ripristino BlueXP per eseguire il backup dei volumi Cloud Volumes ONTAP nelle aree commerciali di AWS e Azure. Nessun altro servizio BlueXP è supportato in questo tipo di implementazione, ad eccezione del portafoglio digitale BlueXP.

  La regione cloud può essere un'area per agenzie statunitensi sicure come AWS Top Secret Cloud, AWS Secret Cloud, Azure IL6 o qualsiasi regione commerciale.

  Per iniziare, installare manualmente il software Connector, accedere alla console BlueXP in esecuzione sul connettore, aggiungere la licenza BYOL al portafoglio digitale BlueXP, quindi implementare Cloud Volumes ONTAP.

  - "Installare il connettore in una posizione senza accesso a Internet"
  - "Accedere alla console BlueXP sul connettore"
  - "Aggiungere una licenza non assegnata"
  - "Inizia a utilizzare Cloud Volumes ONTAP"

- Il connettore consente ora di aggiungere e gestire i bucket Amazon S3 da BlueXP.

  "Scopri come aggiungere nuovi bucket Amazon S3 nel tuo account AWS da BlueXP".

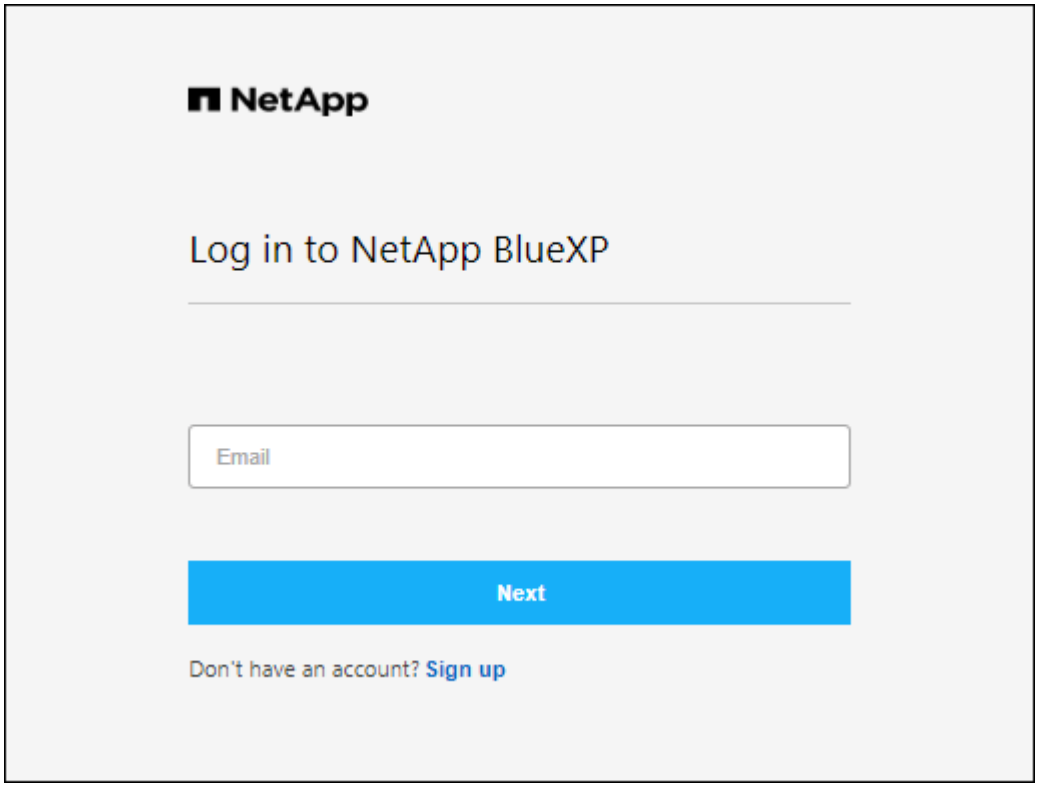
- Questa versione del connettore include i miglioramenti di Cloud Volumes ONTAP.

  "Scopri i miglioramenti di Cloud Volumes ONTAP"

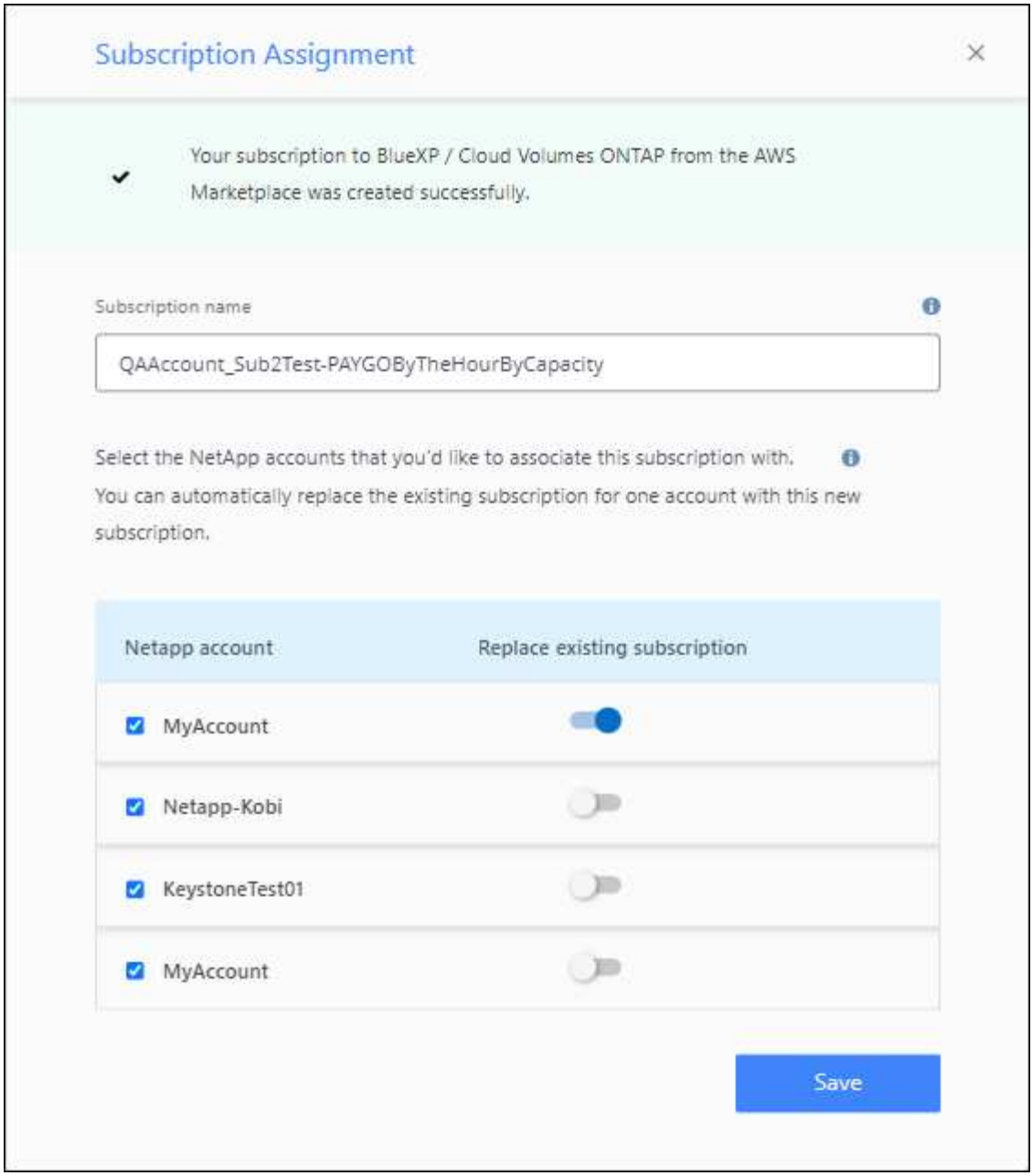
5 febbraio 2023

Connettore 3.9.26

- Nella pagina **Log in**, viene richiesto di inserire l'indirizzo e-mail associato al login. Dopo aver selezionato **Avanti**, BlueXP richiede di autenticare utilizzando il metodo di autenticazione associato all'accesso:
  - La password per le tue credenziali cloud NetApp
  - Le tue credenziali di identità federate
  - Le tue credenziali del NetApp Support Site



- Se non hai ancora utilizzato BlueXP e disponi delle credenziali NetApp Support Site (NSS), puoi saltare la pagina di registrazione e inserire il tuo indirizzo e-mail direttamente nella pagina di accesso. BlueXP ti iscriverà come parte di questo login iniziale.
- Quando ti iscrivi a BlueXP dal mercato del tuo provider cloud, ora hai la possibilità di sostituire l'abbonamento esistente per un account con il nuovo abbonamento.



  - "Scopri come associare un abbonamento AWS"
  - "Scopri come associare un abbonamento Azure"
  - "Scopri come associare un abbonamento a Google Cloud"
- BlueXP avviserà l'utente se il connettore è stato spento per 14 giorni o più.
  - "Informazioni sulle notifiche BlueXP"
  - "Scopri perché i connettori devono rimanere in esecuzione"
- Abbiamo aggiornato la policy di connessione per Google Cloud per includere un'autorizzazione necessaria per creare e gestire le VM di storage su coppie Cloud Volumes ONTAP ha:

  compute.instances.updateNetworkInterface

  "Visualizzare le autorizzazioni Google Cloud per il connettore".

- Questa versione del connettore include i miglioramenti di Cloud Volumes ONTAP.

  "Scopri i miglioramenti di Cloud Volumes ONTAP"

1 gennaio 2023

Connettore 3.9.25

Questa versione del connettore include miglioramenti Cloud Volumes ONTAP e correzioni di bug.

"Scopri i miglioramenti di Cloud Volumes ONTAP"

4 dicembre 2022

Connettore 3.9.24

- L'URL della console BlueXP è stato aggiornato a. https://console.bluexp.netapp.com
- Il connettore è ora supportato nella regione di Google Cloud Israele.
- Questa versione del connettore include anche miglioramenti Cloud Volumes ONTAP e miglioramenti del cluster ONTAP on-premise.
  - "Scopri i miglioramenti di Cloud Volumes ONTAP"
  - "Scopri i miglioramenti del cluster on-premise di ONTAP"

6 novembre 2022

Connettore 3.9.23

- Gli abbonamenti PAYGO e i contratti annuali per BlueXP sono ora disponibili per la visualizzazione e la gestione dal portafoglio digitale.

  "Scopri come gestire gli abbonamenti"

- Questa versione del connettore include anche i miglioramenti di Cloud Volumes ONTAP.

  "Scopri i miglioramenti di Cloud Volumes ONTAP"

1° novembre 2022

Introduzione di BlueXP

NetApp BlueXP estende e migliora le funzionalità fornite tramite Cloud Manager. BlueXP è un piano di controllo unificato che offre un'esperienza multicloud ibrida per servizi di storage e dati in ambienti on-premise e cloud.

Esperienza di gestione unificata

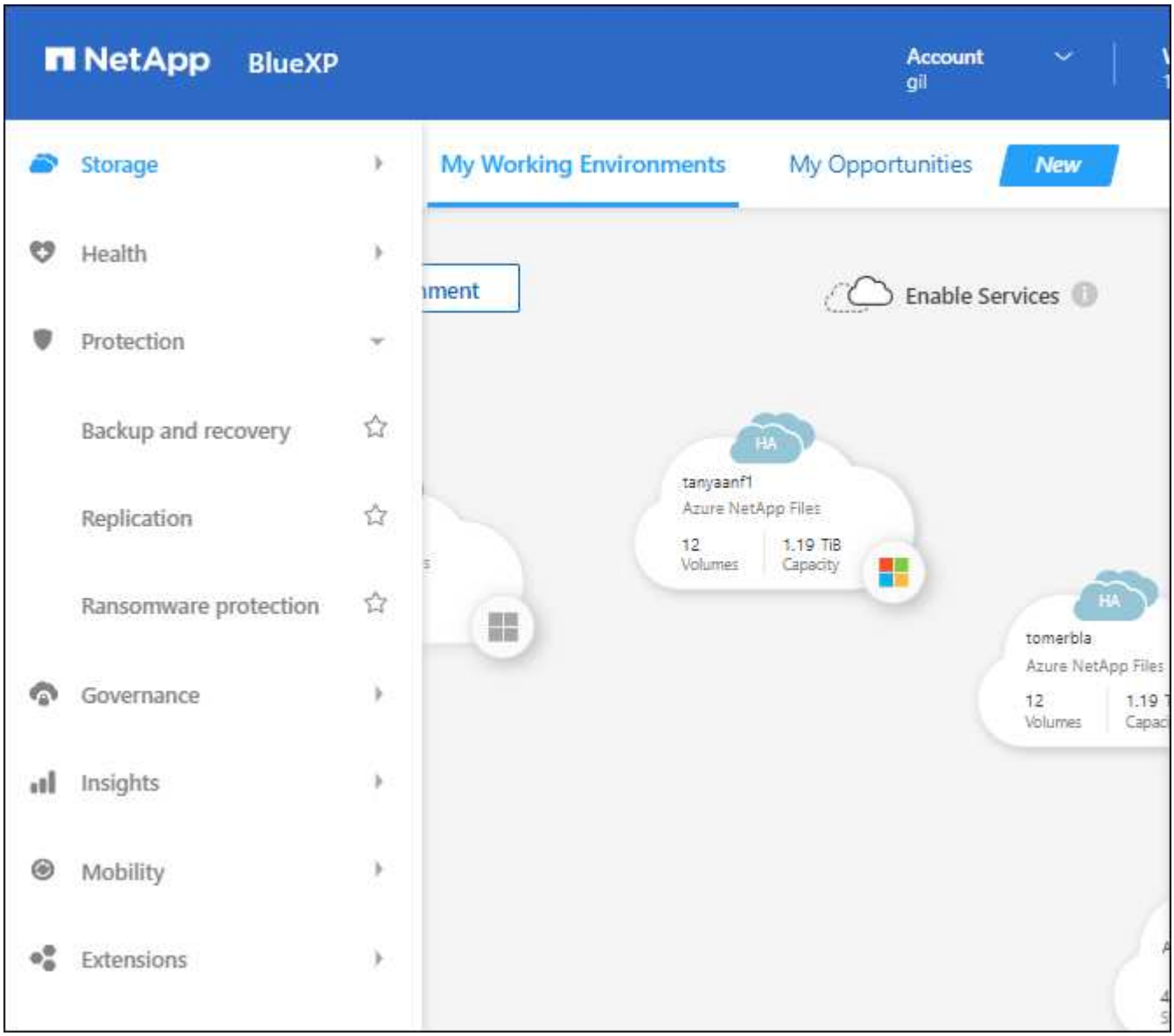
BlueXP consente di gestire tutte le risorse di storage e dati da un'unica interfaccia.

È possibile utilizzare BlueXP per creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi storage on-premise e edge.

"Scopri di più dal sito Web BlueXP"

Nuovo menu di navigazione

Nel menu di navigazione di BlueXP, i servizi sono ora organizzati in base alle categorie e sono denominati in base alle loro funzionalità. Ad esempio, puoi accedere al backup e al ripristino BlueXP dalla categoria **protezione**.



Integrazioni di nuovi prodotti

- Ora puoi gestire i bucket Amazon S3 negli account AWS in cui è installato il connettore.
- Ora puoi gestire più sistemi storage on-premise, come e-Series e StorageGRID.
- Ora è possibile utilizzare i servizi dati precedentemente disponibili solo come servizio standalone con un'interfaccia utente separata, come BlueXP Digital Advisor (Active IQ).

Scopri di più

- "Gestire i bucket Amazon S3"
- "Gestire i sistemi storage e-Series"
- "Gestire i sistemi storage StorageGRID"

- "Scopri di più sull'integrazione di Digital Advisor"

Richiedi di aggiornare le credenziali NSS

Cloud Manager richiede ora di aggiornare le credenziali associate ai tuoi account NetApp Support Site quando il token di refresh associato al tuo account scade dopo 3 mesi. "Scopri come gestire gli account NSS"

18 settembre 2022

Connettore 3.9.22

- Abbiamo migliorato la procedura guidata di implementazione del connettore aggiungendo una *guida in-product* che fornisce i passaggi necessari per soddisfare i requisiti minimi per l'installazione del connettore: Autorizzazioni, autenticazione e rete.
- È ora possibile creare un caso di supporto NetApp direttamente da Cloud Manager nella dashboard di supporto*.

  "Scopri come creare un caso".

- Questa versione del connettore include anche i miglioramenti di Cloud Volumes ONTAP.

  "Scopri i miglioramenti di Cloud Volumes ONTAP"

31 luglio 2022

Connettore 3.9.21

- Abbiamo introdotto un nuovo modo per scoprire le risorse cloud esistenti che non stai ancora gestendo in Cloud Manager.

  In Canvas, la scheda **My Opportunities** fornisce una posizione centralizzata per scoprire le risorse esistenti che è possibile aggiungere a Cloud Manager per operazioni e servizi dati coerenti nel tuo multicloud ibrido.

  In questa versione iniziale, My Opportunities consente di scoprire i file system FSX per ONTAP esistenti nel proprio account AWS.

  "Scopri come scoprire FSX per ONTAP utilizzando le mie opportunità"

- Questa versione del connettore include anche i miglioramenti di Cloud Volumes ONTAP.

  "Scopri i miglioramenti di Cloud Volumes ONTAP"

15 luglio 2022

Modifiche alle policy

Abbiamo aggiornato la documentazione aggiungendo le policy di Cloud Manager direttamente all'interno dei documenti. Ciò significa che ora è possibile visualizzare le autorizzazioni richieste per Connector e Cloud Volumes ONTAP insieme ai passaggi che descrivono come configurarle. Queste policy erano precedentemente accessibili da una pagina del sito di supporto NetApp.

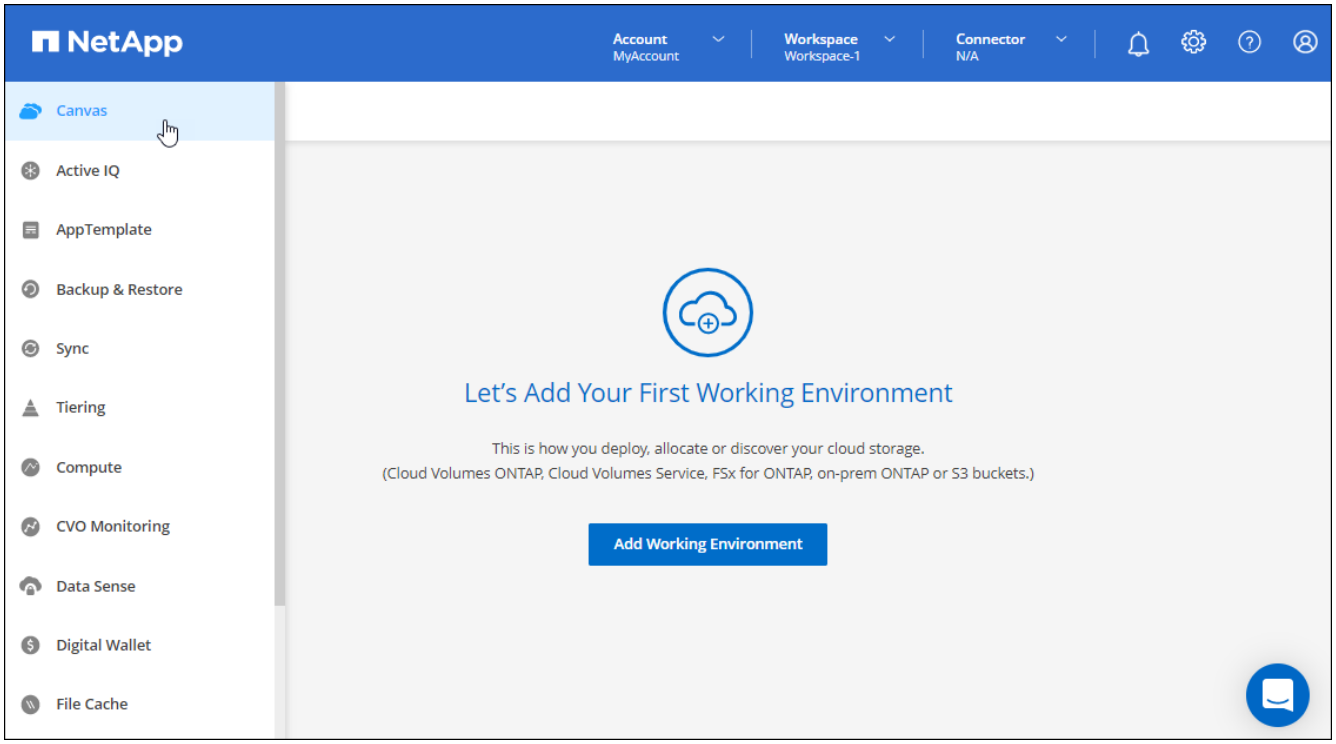
"Ecco un esempio che mostra le autorizzazioni del ruolo AWS IAM utilizzate per creare un connettore".

Abbiamo anche creato una pagina che fornisce collegamenti a ciascuna policy. "Visualizza il riepilogo delle autorizzazioni per Cloud Manager".

3 luglio 2022

Connettore 3.9.20

- Abbiamo introdotto un nuovo modo per accedere all'elenco crescente di funzionalità nell'interfaccia di Cloud Manager. Tutte le funzionalità di Cloud Manager sono ora facilmente reperibili passando il mouse sul pannello di sinistra.



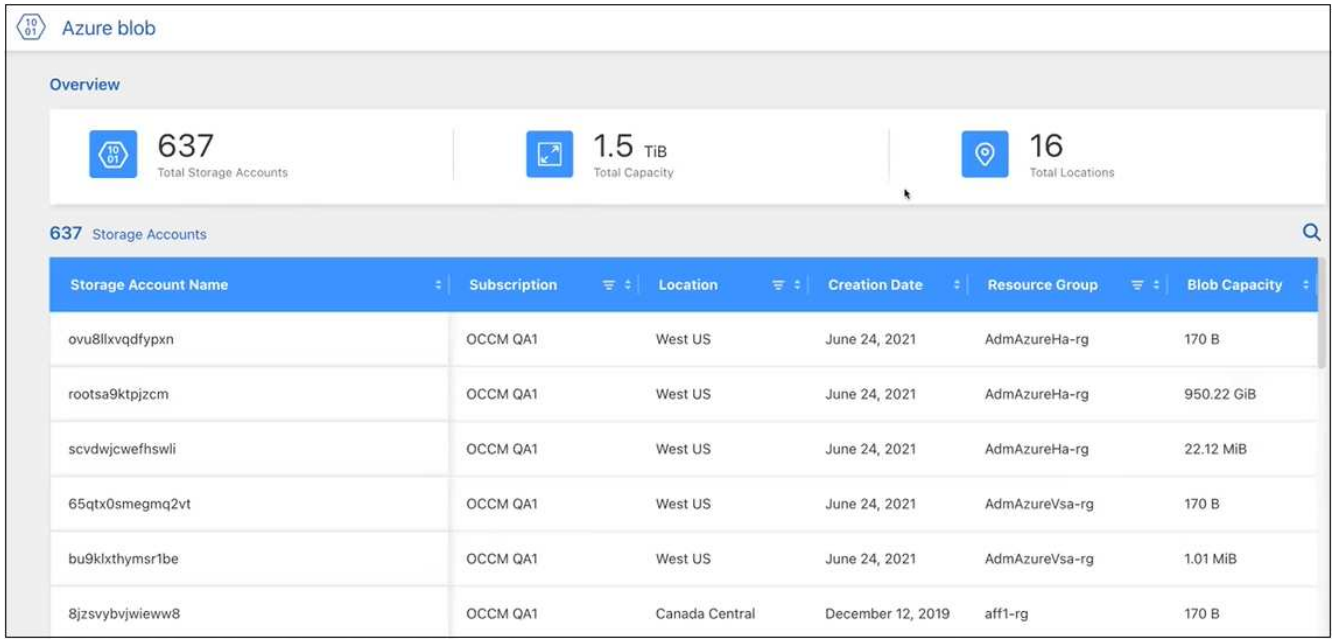
- Ora puoi configurare Cloud Manager per inviare notifiche via email in modo da essere informato di importanti attività del sistema anche quando non sei connesso al sistema.

  "Scopri di più sul monitoraggio delle operazioni nel tuo account".

- Cloud Manager ora supporta lo storage Azure Blob e Google Cloud Storage come ambienti di lavoro, in modo simile al supporto di Amazon S3.

  Dopo aver installato un connettore in Azure o Google Cloud, Cloud Manager rileva automaticamente le informazioni sullo storage Azure Blob nell'abbonamento Azure o in Google Cloud Storage nel progetto in cui è installato il connettore. Cloud Manager visualizza lo storage a oggetti come un ambiente di lavoro che è possibile aprire per visualizzare informazioni più dettagliate.

  Ecco un esempio di ambiente di lavoro Azure Blob:



- Abbiamo riprogettato la pagina delle risorse per un ambiente di lavoro Amazon S3 fornendo informazioni più dettagliate sui bucket S3, come capacità, dettagli di crittografia e altro ancora.
- Il connettore è ora supportato nelle seguenti aree di Google Cloud:
  - Madrid (europa-Sud-Sance1)
  - Parigi (europa-ovest 9)
  - Varsavia (Europa centrale2)
- Il connettore è ora supportato nella regione Azure West US 3.

  "Visualizza l'elenco completo delle regioni supportate"

- Questa versione del connettore include anche i miglioramenti di Cloud Volumes ONTAP.

  "Scopri i miglioramenti di Cloud Volumes ONTAP"

28 giugno 2022

Accedi con le credenziali NetApp

Quando i nuovi utenti si iscrivono a Cloud Central, possono ora selezionare l'opzione **Accedi con NetApp** per accedere con le credenziali del NetApp Support Site. In alternativa all'immissione di un indirizzo e-mail e di una password.

> Gli accessi esistenti che utilizzano un indirizzo e-mail e una password devono continuare a utilizzare tale metodo di accesso. L'opzione Accedi con NetApp è disponibile per i nuovi utenti che si iscrivono.

7 giugno 2022

Connettore 3.9.19

- Il connettore è ora supportato nella regione di AWS Jakarta (ap-sud-est-3).

- Il connettore è ora supportato nella regione sud-orientale del Brasile Azure.

  "Visualizza l'elenco completo delle regioni supportate"

- Questa versione del connettore include anche miglioramenti Cloud Volumes ONTAP e miglioramenti del cluster ONTAP on-premise.
  - "Scopri i miglioramenti di Cloud Volumes ONTAP"
  - "Scopri i miglioramenti del cluster on-premise di ONTAP"

12 maggio 2022

Patch del connettore 3.9.18

Abbiamo aggiornato il connettore per introdurre correzioni di bug. La soluzione più importante è un problema che influisce sull'implementazione di Cloud Volumes ONTAP in Google Cloud quando il connettore si trova in un VPC condiviso.

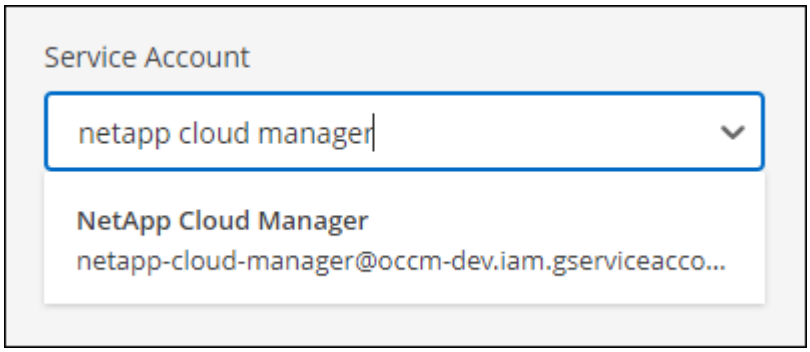
2 maggio 2022

Connettore 3.9.18

- Il connettore è ora supportato nelle seguenti aree di Google Cloud:
  - Delhi (asia-Sud 2)
  - Melbourne (australia-sud-est 2)
  - Milano (europa-ovest 8)
  - Santiago (america del sud-ovest 1)

  "Visualizza l'elenco completo delle regioni supportate"

- Quando si seleziona l'account del servizio Google Cloud da utilizzare con il connettore, Cloud Manager visualizza ora l'indirizzo e-mail associato a ciascun account del servizio. La visualizzazione dell'indirizzo di posta elettronica consente di distinguere più facilmente gli account di servizio che condividono lo stesso nome.



- Abbiamo certificato il connettore in Google Cloud su un'istanza di macchina virtuale con un sistema operativo che supporta "Funzioni di VM schermate"
- Questa versione del connettore include anche i miglioramenti di Cloud Volumes ONTAP. "Scopri di più su questi miglioramenti"
- Sono necessarie nuove autorizzazioni AWS per consentire al connettore di implementare Cloud Volumes

ONTAP.

Le seguenti autorizzazioni sono ora necessarie per creare un gruppo di posizionamento AWS Spread quando si implementa una coppia ha in una singola zona di disponibilità (AZ):

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

Queste autorizzazioni sono ora necessarie per ottimizzare il modo in cui Cloud Manager crea il gruppo di posizionamento.

Assicurati di fornire queste autorizzazioni a ogni set di credenziali AWS aggiunto a Cloud Manager. "Visualizzare la policy IAM più recente per il connettore".

3 aprile 2022

Connettore 3.9.17

- Ora puoi creare un connettore lasciando che Cloud Manager assuma un ruolo IAM impostato nel tuo ambiente. Questo metodo di autenticazione è più sicuro della condivisione di una chiave di accesso AWS e di una chiave segreta.

  "Scopri come creare un connettore utilizzando un ruolo IAM".

- Questa versione del connettore include anche i miglioramenti di Cloud Volumes ONTAP. "Scopri di più su questi miglioramenti"

27 febbraio 2022

Connettore 3.9.16

- Quando crei un nuovo connettore in Google Cloud, Cloud Manager visualizzerà tutte le policy firewall esistenti. In precedenza, Cloud Manager non visualizzava policy che non disponevano di tag di destinazione.
- Questa versione del connettore include anche i miglioramenti di Cloud Volumes ONTAP. "Scopri di più su questi miglioramenti"

30 gennaio 2022

Connettore 3.9.15

Questa versione del connettore include i miglioramenti di Cloud Volumes ONTAP. "Scopri di più su questi miglioramenti"

2 gennaio 2022

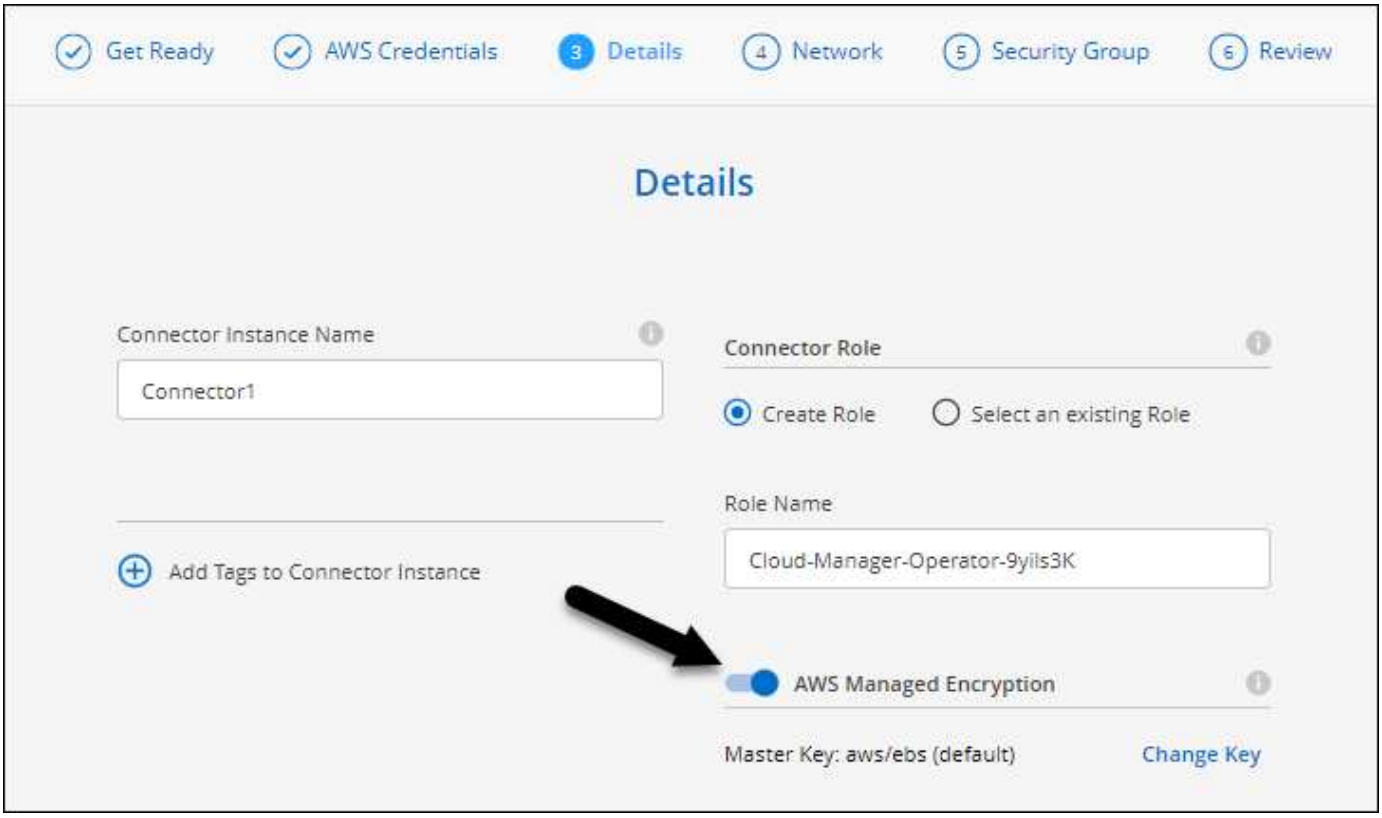
Endpoint ridotti per il connettore

Abbiamo ridotto il numero di endpoint che un connettore deve contattare per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

"Visualizzare l'elenco degli endpoint richiesti"

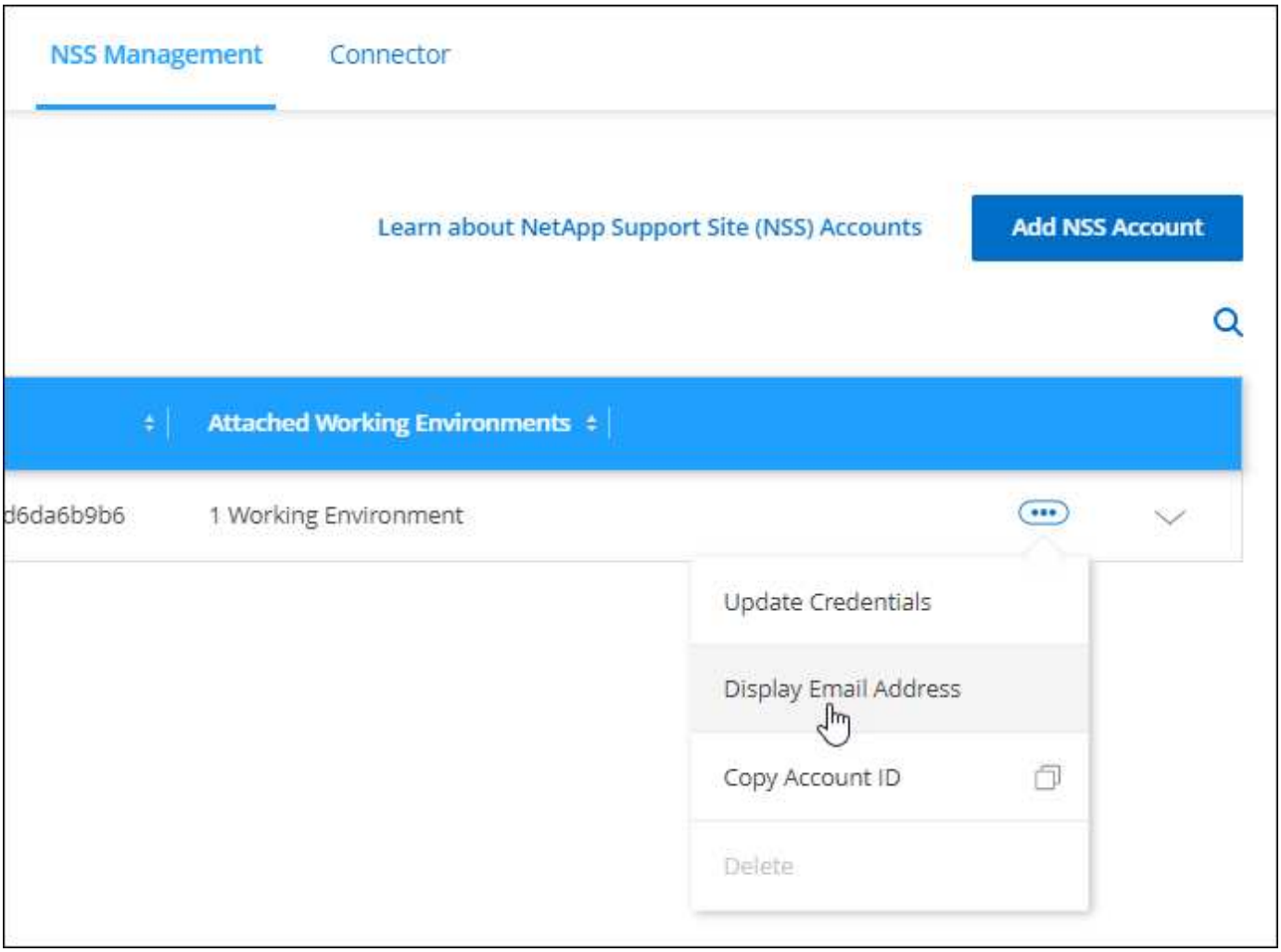
Crittografia del disco EBS per il connettore

Quando si implementa un nuovo connettore in AWS da Cloud Manager, è ora possibile scegliere di crittografare i dischi EBS del connettore utilizzando la chiave master predefinita o una chiave gestita.



Indirizzo e-mail per gli account NSS

Ora Cloud Manager può visualizzare l'indirizzo e-mail associato a un account NetApp Support Site.



28 novembre 2021

Aggiornamento necessario per gli account del NetApp Support Site

A partire da dicembre 2021, NetApp utilizza ora Microsoft Azure Active Directory come provider di identità per i servizi di autenticazione specifici per il supporto e la concessione di licenze. In seguito a questo aggiornamento, Cloud Manager richiederà di aggiornare le credenziali per gli account NetApp Support Site già aggiunti in precedenza.

Se non hai ancora eseguito la migrazione dell'account NSS a IDaaS, devi prima migrare l'account e poi aggiornare le tue credenziali in Cloud Manager.

"Scopri di più sull'utilizzo di Microsoft Azure Active Directory per la gestione delle identità da parte di NetApp"

Modificare gli account NSS per Cloud Volumes ONTAP

Se la tua organizzazione dispone di più account del sito di supporto NetApp, ora puoi modificare l'account associato a un sistema Cloud Volumes ONTAP.

"Scopri come collegare un ambiente di lavoro a un altro account NSS".

4 novembre 2021

Certificazione SOC 2 tipo 2

Un'azienda indipendente di contabili pubblici e un revisore dei servizi ha esaminato Cloud Manager, Cloud Sync, Cloud Tiering, Cloud Data Sense e Cloud Backup (piattaforma Cloud Manager) e ha affermato di aver ottenuto report SOC 2 di tipo 2 in base ai criteri applicabili per i servizi di trust.

"Visualizza i report SOC 2 di NetApp".

Il connettore non è più supportato come proxy

Non è più possibile utilizzare Cloud Manager Connector come server proxy per inviare messaggi AutoSupport da Cloud Volumes ONTAP. Questa funzionalità è stata rimossa e non è più supportata. È necessario fornire la connettività AutoSupport tramite un'istanza NAT o i servizi proxy dell'ambiente.

"Scopri di più sulla verifica di AutoSupport con Cloud Volumes ONTAP"

31 ottobre 2021

Autenticazione con service principal

Quando si crea un nuovo connettore in Microsoft Azure, è ora possibile autenticarsi con un'entità del servizio Azure, anziché con le credenziali dell'account Azure.

"Scopri come eseguire l'autenticazione con un service principal Azure".

Miglioramento delle credenziali

Abbiamo riprogettato la pagina delle credenziali per una maggiore facilità di utilizzo e per adattarsi all'aspetto attuale dell'interfaccia di Cloud Manager.

2 settembre 2021

È stato aggiunto un nuovo servizio di notifica

Il servizio di notifica è stato introdotto per visualizzare lo stato delle operazioni di Cloud Manager avviate durante la sessione di accesso corrente. È possibile verificare se l'operazione è stata eseguita correttamente o se non è riuscita. "Scopri come monitorare le operazioni nell'account".

7 luglio 2021

Miglioramenti alla procedura guidata Aggiungi connettore

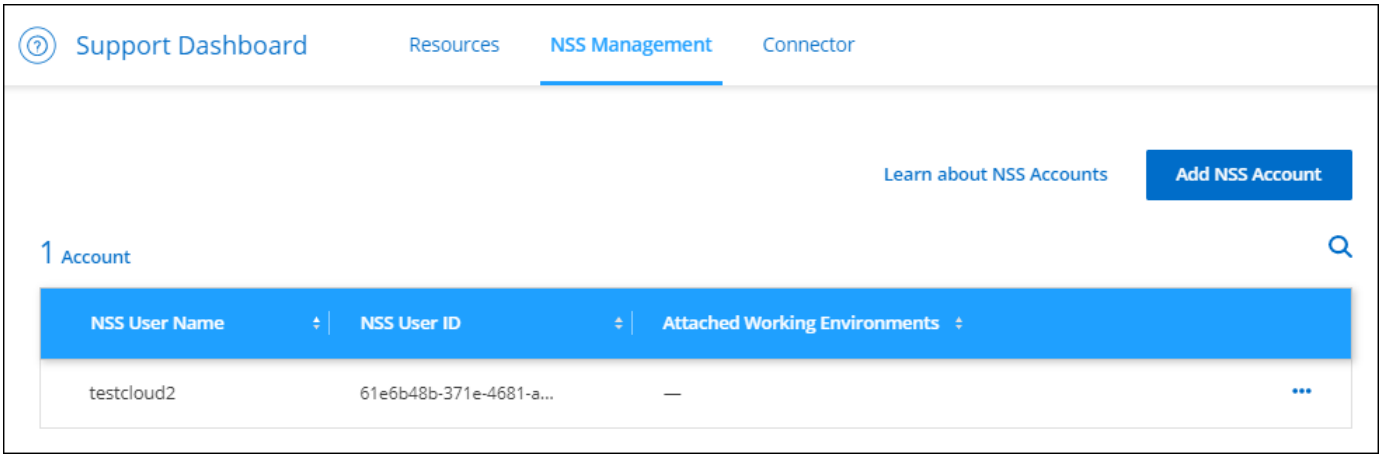
Abbiamo riprogettato la procedura guidata **Add Connector** per aggiungere nuove opzioni e semplificarne l'utilizzo. È ora possibile aggiungere tag, specificare un ruolo (per AWS o Azure), caricare un certificato root per un server proxy, visualizzare il codice per l'automazione Terraform, visualizzare i dettagli di avanzamento e molto altro ancora.

- "Creare un connettore in AWS"
- "Creare un connettore in Azure"
- "Creare un connettore in Google Cloud"

Gestione dell'account NSS da Support Dashboard

Gli account NetApp Support Site (NSS) sono ora gestiti dalla dashboard di supporto, anziché dal menu Impostazioni. Questa modifica semplifica la ricerca e la gestione di tutte le informazioni relative al supporto da un'unica posizione.

"Scopri come gestire gli account NSS".



5 maggio 2021

Account nella timeline

La cronologia di Cloud Manager mostra ora le azioni e gli eventi relativi alla gestione dell'account. Le azioni includono elementi come l'associazione degli utenti, la creazione di aree di lavoro e la creazione di connettori. Controllare la cronologia può essere utile se è necessario identificare chi ha eseguito un'azione specifica o se è necessario identificare lo stato di un'azione.

"Scopri come filtrare la timeline per il servizio tenancy".

11 aprile 2021

API chiama direttamente Cloud Manager

Se è stato configurato un server proxy, è ora possibile attivare un'opzione per inviare chiamate API direttamente a Cloud Manager senza utilizzare il proxy. Questa opzione è supportata con i connettori in esecuzione in AWS o in Google Cloud.

"Scopri di più su questa impostazione".

Utenti dell'account di servizio

È ora possibile creare un utente dell'account di servizio.

Un account di servizio agisce come un "utente" che può effettuare chiamate API autorizzate a Cloud Manager per scopi di automazione. In questo modo è più semplice gestire l'automazione, poiché non è necessario creare script di automazione basati sull'account utente di una persona reale che può lasciare l'azienda in qualsiasi momento. E se utilizzi la federazione, puoi creare un token senza generare un token di refresh dal cloud.

"Scopri di più sull'utilizzo degli account di servizio".

Anteprime private

Ora puoi consentire anteprime private nel tuo account per accedere ai nuovi servizi cloud di NetApp man mano che vengono resi disponibili come anteprima in Cloud Manager.

"Scopri di più su questa opzione".

Servizi di terze parti

Puoi anche consentire ai servizi di terze parti del tuo account di accedere ai servizi di terze parti disponibili in Cloud Manager.

"Scopri di più su questa opzione".

8 marzo 2021

Questo aggiornamento include miglioramenti a diverse funzioni e servizi.

Miglioramenti di Cloud Volumes ONTAP

Questa release di Cloud Manager include miglioramenti alla gestione di Cloud Volumes ONTAP.

Miglioramenti disponibili in tutti i cloud provider

Cloud Manager è ora in grado di implementare e gestire Cloud Volumes ONTAP 9,9.0.

"Scopri le nuove funzionalità incluse in questa release di Cloud Volumes ONTAP".

Miglioramenti disponibili in AWS

- È ora possibile implementare Cloud Volumes ONTAP 9.8 nell'ambiente dei servizi cloud commerciali AWS (C2S).

  "Scopri come iniziare a utilizzare C2S"

- Cloud Manager ti ha sempre abilitato per crittografare i dati Cloud Volumes ONTAP utilizzando il servizio di gestione delle chiavi (KMS) di AWS. A partire da Cloud Volumes ONTAP 9.9.0, i dati sui dischi EBS e i dati a livelli S3 vengono crittografati se si seleziona un CMK gestito dal cliente. In precedenza, solo i dati EBS sarebbero stati crittografati.

  Tenere presente che è necessario fornire al ruolo IAM Cloud Volumes ONTAP l'accesso per utilizzare il CMK.

  "Scopri di più sulla configurazione di AWS KMS con Cloud Volumes ONTAP"

Potenziamento disponibile in Azure

È ora possibile implementare Cloud Volumes ONTAP 9.8 nel dipartimento della difesa di Azure (DOD) Impact Level 6 (IL6).

Miglioramenti disponibili in Google Cloud

- Abbiamo ridotto il numero di indirizzi IP richiesti per Cloud Volumes ONTAP 9.8 e versioni successive in Google Cloud. Per impostazione predefinita, è richiesto un indirizzo IP in meno (abbiamo unificato la LIF di intercluster con la LIF di gestione dei nodi). È inoltre possibile saltare la creazione della LIF di gestione

SVM quando si utilizza l'API, riducendo la necessità di un indirizzo IP aggiuntivo.

"Scopri di più sui requisiti degli indirizzi IP in Google Cloud"

- Quando si implementa una coppia Cloud Volumes ONTAP ha in Google Cloud, è ora possibile scegliere VPC condivisi per VPC-1, VPC-2 e VPC-3. In precedenza, solo VPC-0 poteva essere un VPC condiviso. Questa modifica è supportata con Cloud Volumes ONTAP 9.8 e versioni successive.

  "Scopri di più sui requisiti di rete di Google Cloud"

Miglioramenti al connettore

- Cloud Manager invia ora una notifica agli utenti Admin tramite un'e-mail quando un connettore non è in esecuzione.

  Mantenere i connettori attivi e funzionanti consente di garantire la migliore gestione di Cloud Volumes ONTAP e altri servizi cloud NetApp.

- Ora Cloud Manager visualizza una notifica se è necessario modificare il tipo di istanza per il connettore.

  La modifica del tipo di istanza consente di utilizzare le nuove funzioni e funzionalità attualmente mancanti.

Miglioramenti apportati a Cloud Sync

- Cloud Sync ora supporta le relazioni di sincronizzazione tra lo storage ONTAP S3 e i server SMB:
  - Storage ONTAP S3 su un server SMB
  - Un server per PMI nello storage ONTAP S3

    "Visualizzare le relazioni di sincronizzazione supportate"

- Cloud Sync consente ora di unificare la configurazione di un gruppo di broker dati direttamente dall'interfaccia utente.

  Si sconsiglia di modificare la configurazione autonomamente. È necessario consultare NetApp per capire quando modificare la configurazione e come modificarla.

  "Scopri di più su come definire una configurazione unificata"

Miglioramenti al tiering cloud

- Durante il tiering in Google Cloud Storage, è possibile applicare una regola del ciclo di vita in modo che i dati su più livelli passino da una classe di storage Standard a uno storage nearline, Coldline o di archivio a costi più bassi dopo 30 giorni.
- Cloud Tiering ora viene visualizzato se hai dei cluster ONTAP on-premise non rilevati, in modo che puoi aggiungerli a Cloud Manager per abilitare il tiering o altri servizi in questi cluster.

  "Scopri come scoprire questi cluster aggiuntivi"

Miglioramenti di Azure NetApp Files

Ora puoi modificare in maniera dinamica il livello di servizio per un volume per soddisfare le esigenze dei carichi di lavoro e ottimizzare i costi. Il volume viene spostato nell'altro pool di capacità senza alcun impatto sul

volume. "Scopri di più"

9 febbraio 2021

Miglioramenti della dashboard di supporto

Abbiamo aggiornato il Support Dashboard, consentendoti di aggiungere le tue credenziali NetApp Support Site, che ti registrano per il supporto. Puoi anche avviare un caso di supporto NetApp direttamente dalla dashboard. Fare clic sull'icona Guida e quindi su **supporto**.

Limitazioni note

Le limitazioni note identificano piattaforme, dispositivi o funzioni non supportate da questa versione del prodotto o che non interagiscono correttamente con esso. Esaminare attentamente queste limitazioni.

Queste limitazioni sono specifiche per l'installazione e l'amministrazione di BlueXP: Il connettore, la piattaforma SaaS e molto altro ancora.

Limitazioni del connettore

I server proxy trasparenti non sono supportati

BlueXP non supporta i server proxy trasparenti con il connettore.

"Ulteriori informazioni sull'utilizzo di un server proxy con il connettore".

Possibile conflitto con gli indirizzi IP compresi nell'intervallo 172

BlueXP implementa il connettore con due interfacce che hanno indirizzi IP negli intervalli 172.17.0.0/16 e 172.18.0.0/16.

Se la rete dispone di una subnet configurata con uno di questi intervalli, potrebbero verificarsi errori di connettività da BlueXP. Ad esempio, il rilevamento dei cluster ONTAP on-premise in BlueXP potrebbe non riuscire.

Consultare l'articolo della Knowledge base "Conflitto IP del connettore BlueXP con la rete esistente" Per istruzioni su come modificare l'indirizzo IP delle interfacce del connettore.

La decrittografia SSL non è supportata

BlueXP non supporta configurazioni firewall con crittografia SSL attivata. Se la decrittografia SSL è attivata, vengono visualizzati messaggi di errore in BlueXP e l'istanza del connettore viene visualizzata come inattiva.

Per una maggiore sicurezza, è possibile scegliere tra "Installare un certificato HTTPS firmato da un'autorità di certificazione (CA)".

Pagina vuota durante il caricamento dell'interfaccia utente locale

Se si carica la console basata su Web in esecuzione su un connettore, l'interfaccia potrebbe non essere visualizzata e viene visualizzata solo una pagina vuota.

Questo problema è correlato a un problema di caching. La soluzione è utilizzare una sessione di browser Web

privato o in incognito.

Gli host Linux condivisi non sono supportati

Il connettore non è supportato su una macchina virtuale condivisa con altre applicazioni. La macchina virtuale deve essere dedicata al software del connettore.

agenti ed interni di terze parti

Gli agenti di terze parti o le estensioni delle macchine virtuali non sono supportati sulla macchina virtuale del connettore.

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

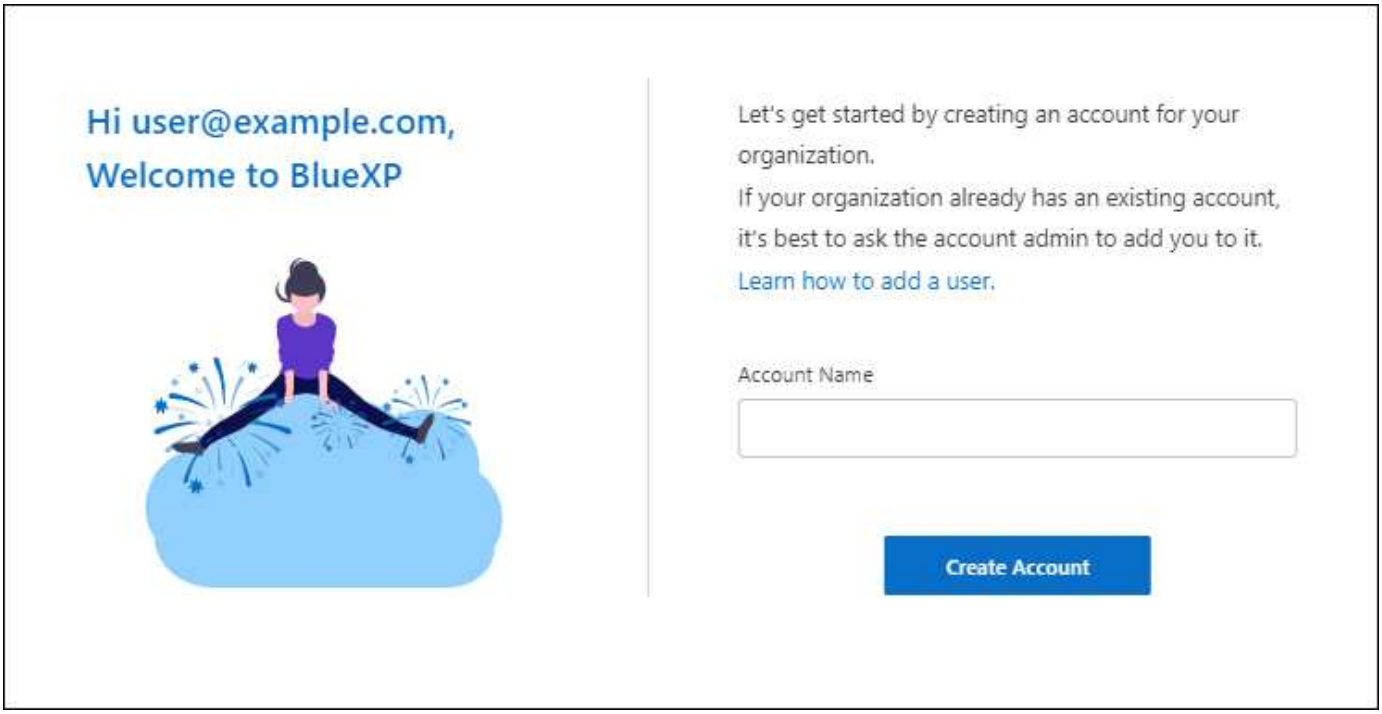
Un'azienda indipendente di contabili pubblici e un revisore dei servizi ha esaminato BlueXP e affermato di aver ottenuto report SOC 2 di tipo 2 sulla base dei criteri Trust Services applicabili.

"Visualizza i report SOC 2 di NetApp"

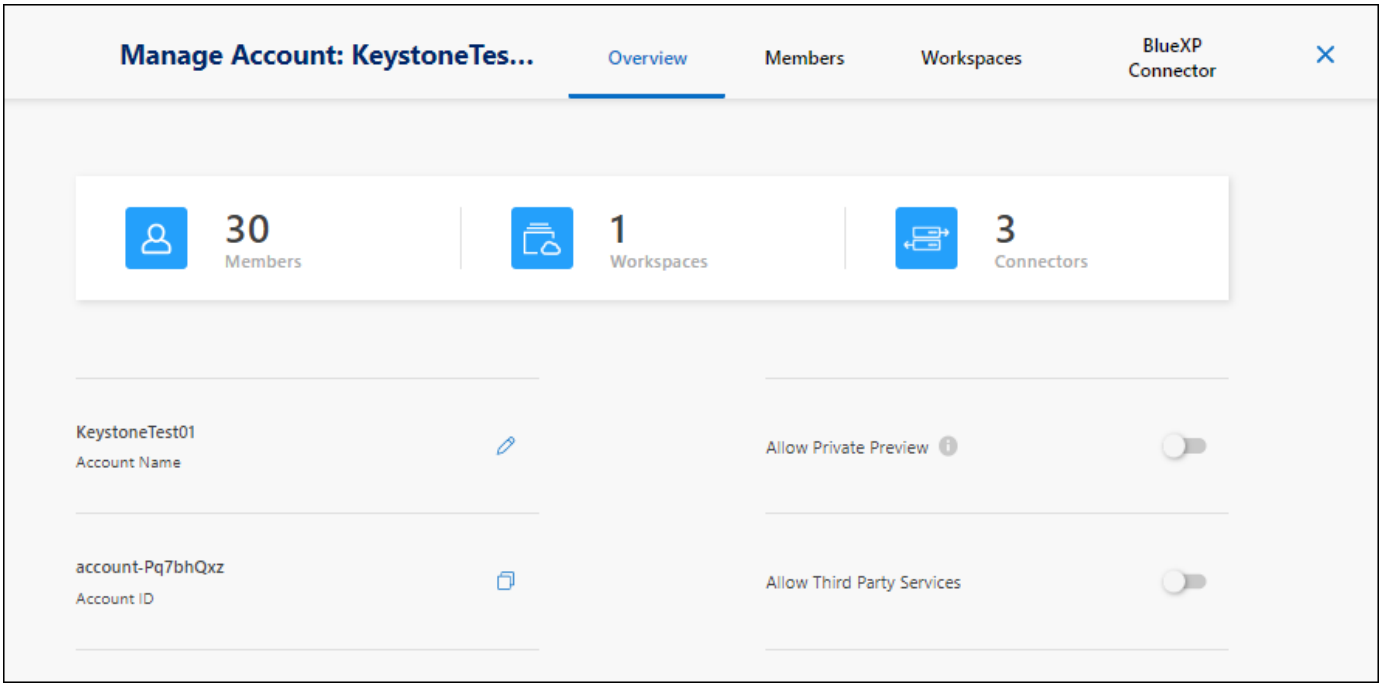
Scopri di più sugli account BlueXP

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".

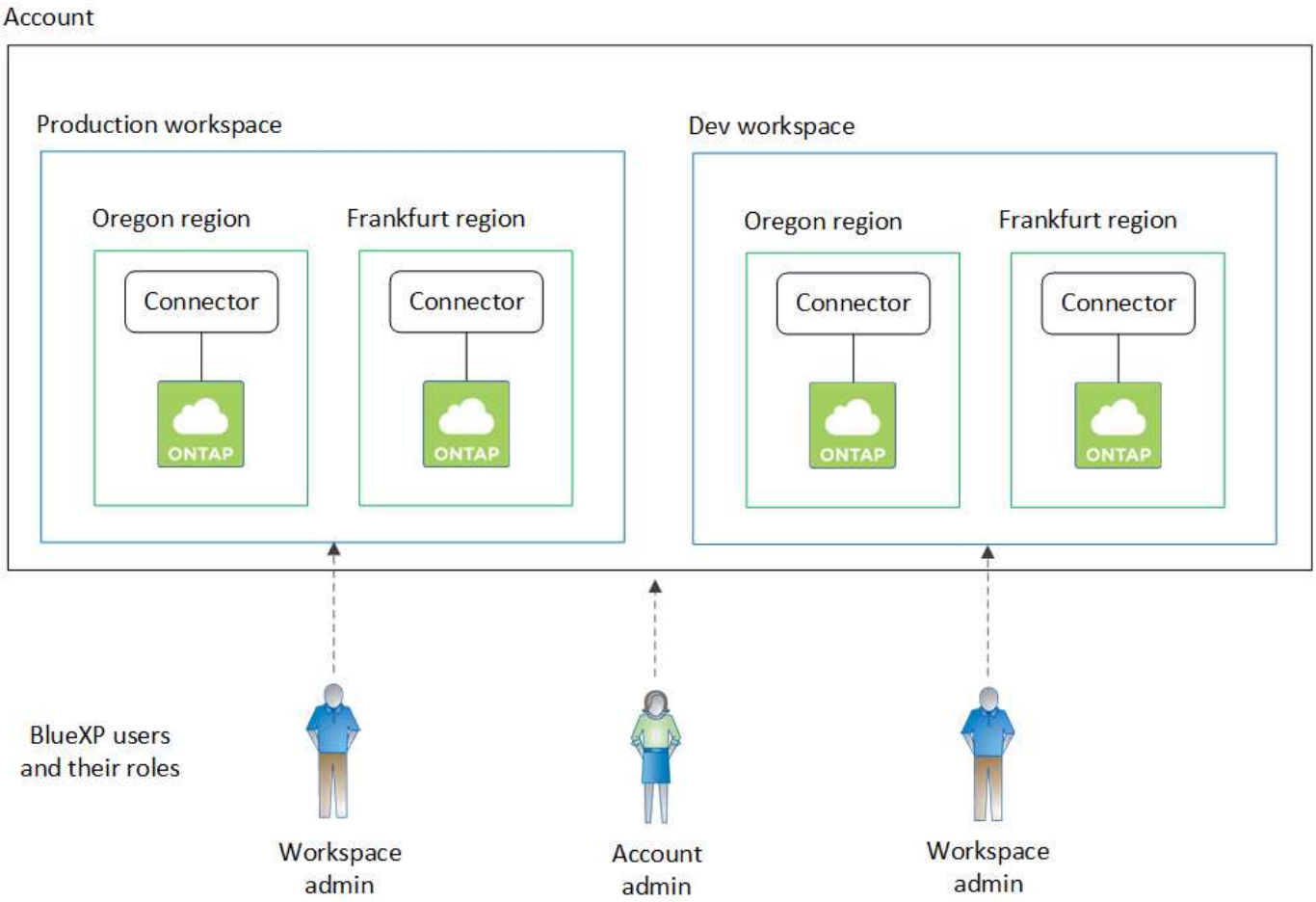
Esempi

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

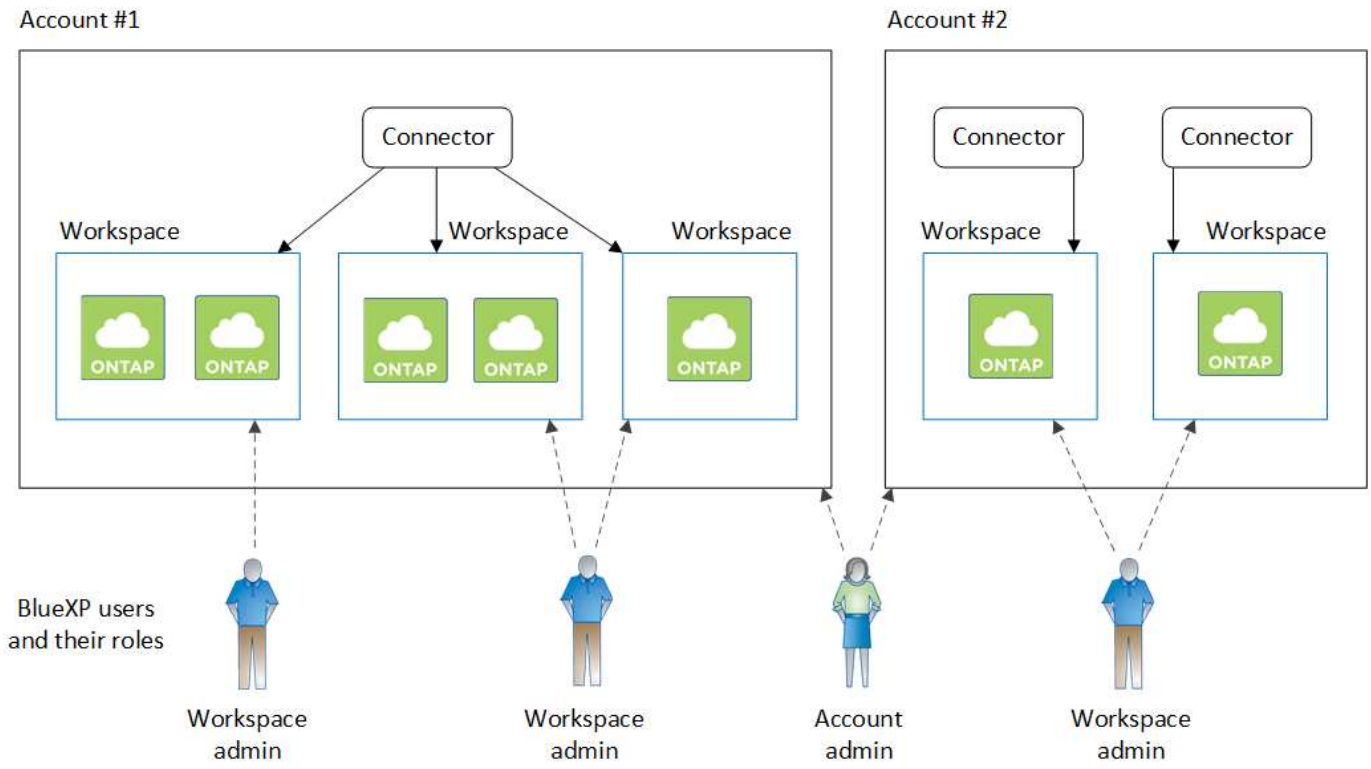
Nell'esempio riportato di seguito viene illustrato un account che utilizza due aree di lavoro per creare ambienti isolati. Il primo spazio di lavoro è per un ambiente di produzione e il secondo per un ambiente di sviluppo.



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.

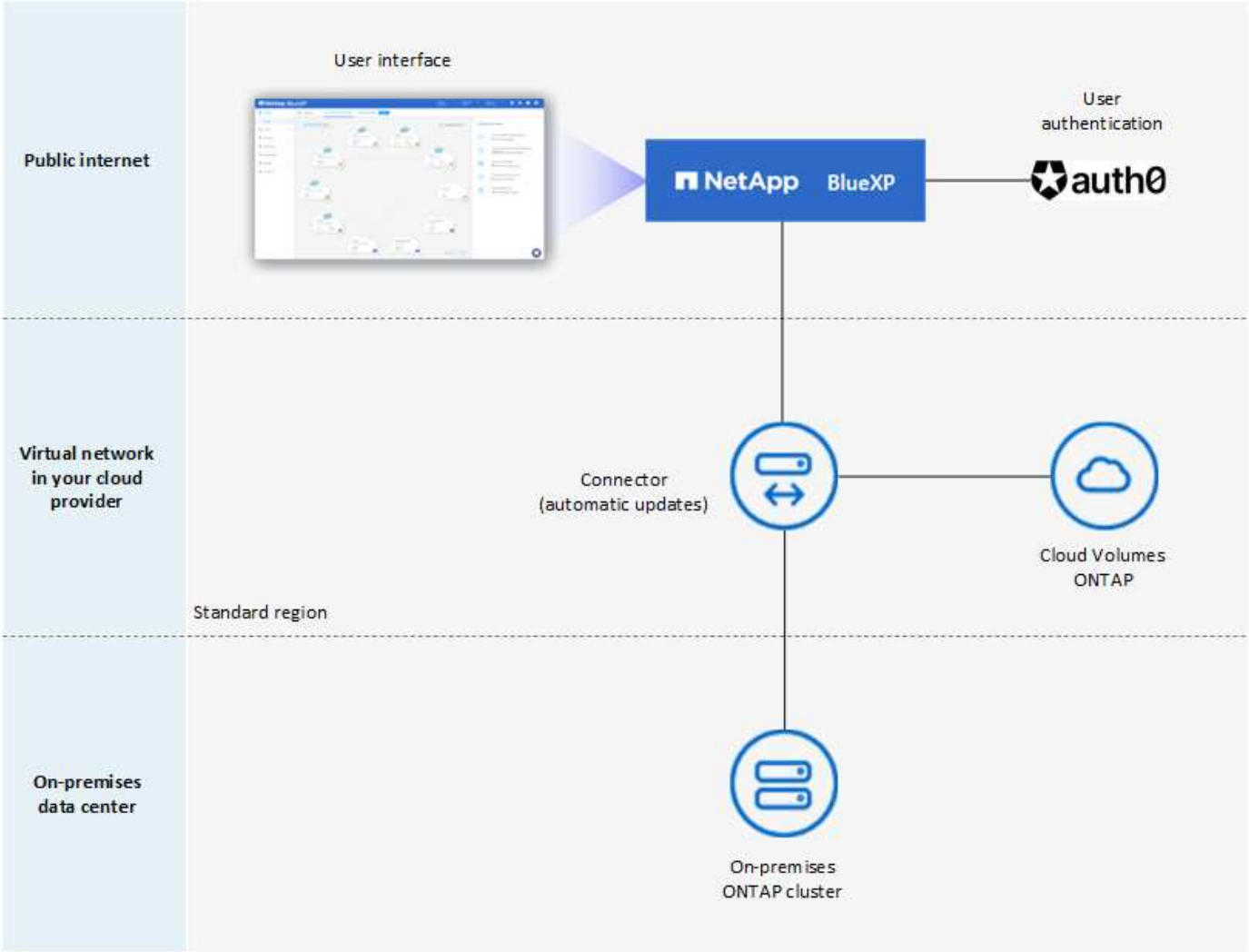
	Modalità standard	Modalità limitata	Modalità privata
Connessione richiesta a BlueXP SaaS Layer?	Sì	Solo in uscita	No

	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.

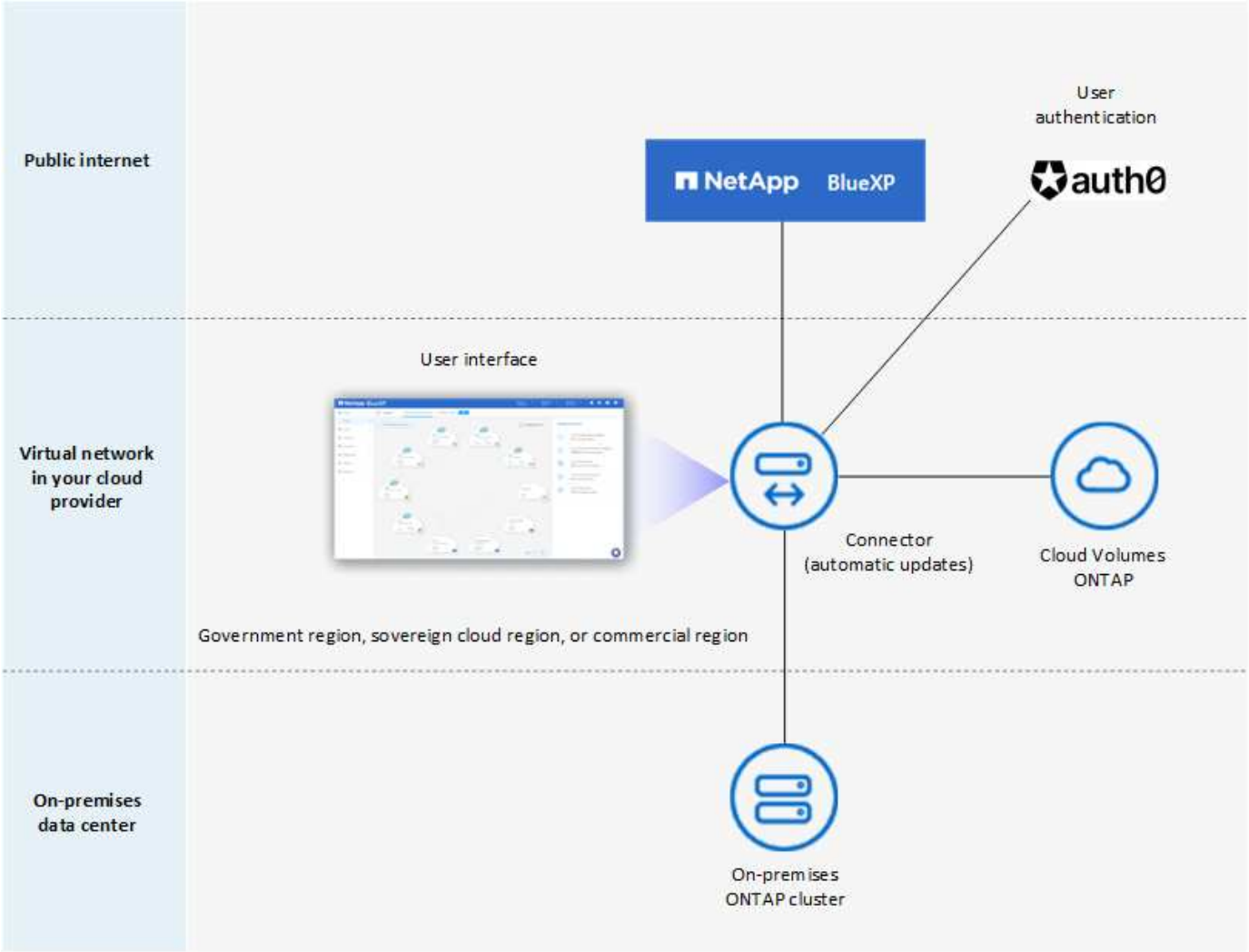
Come iniziare con la modalità standard

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.

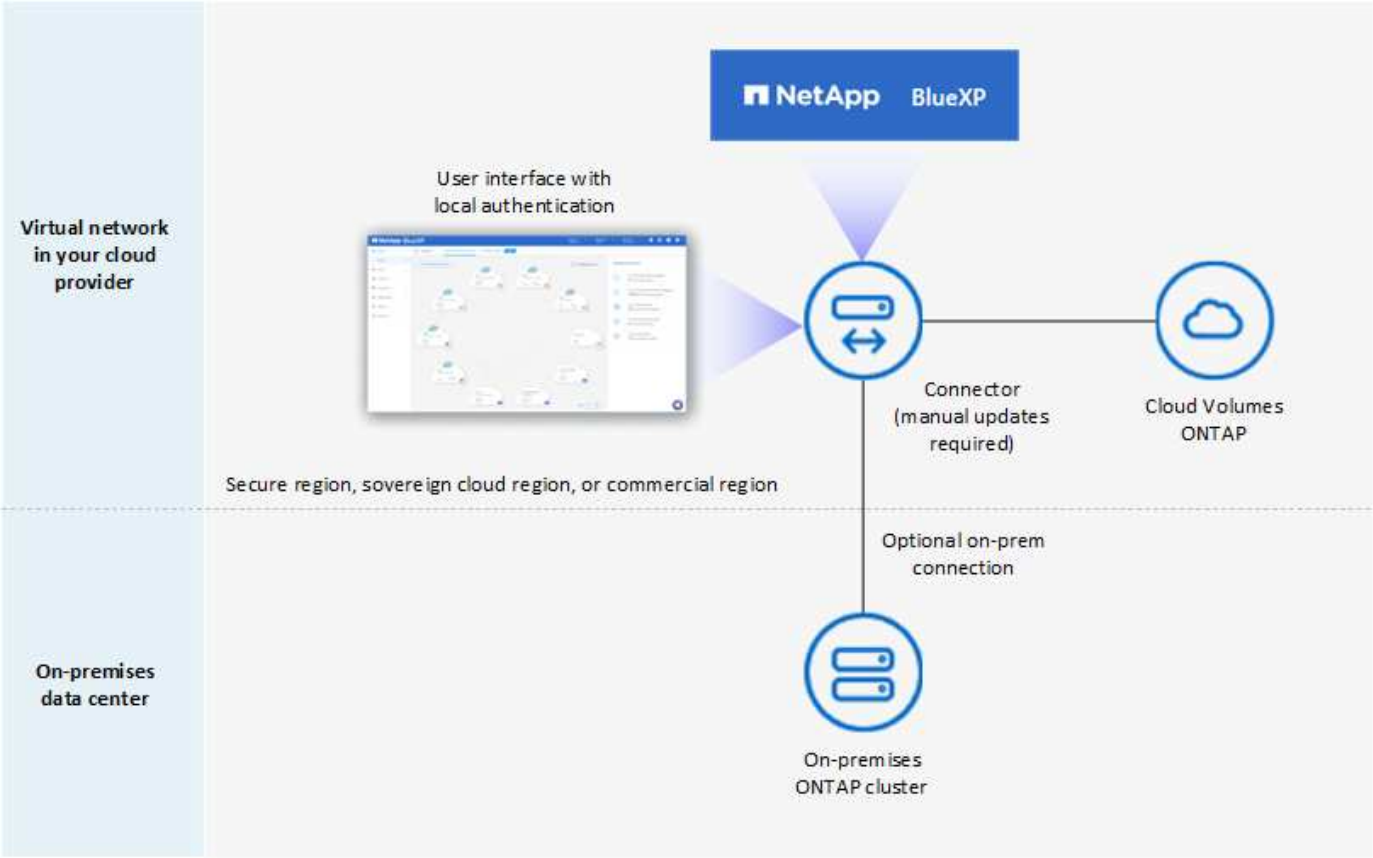
- "Scopri come iniziare a utilizzare la modalità limitata".
- "Scopri come creare un account BlueXP aggiuntivo".

Modalità privata

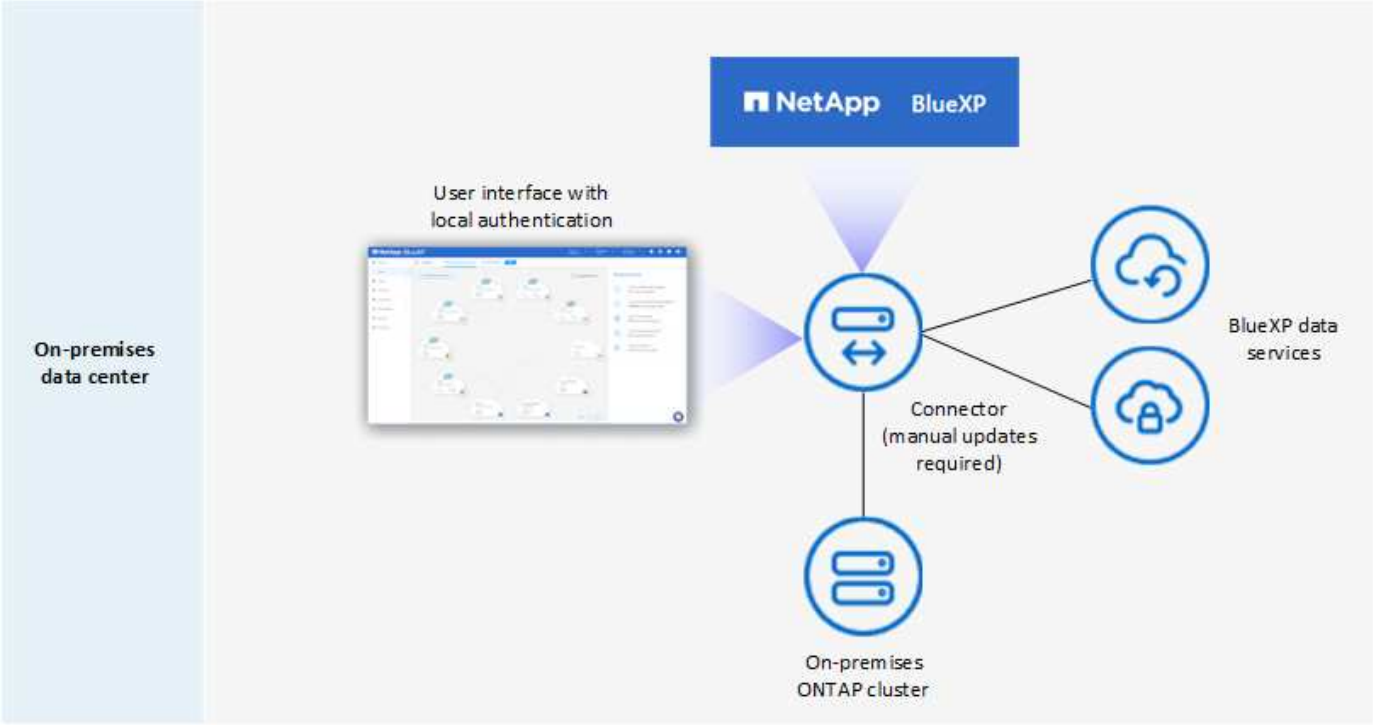
In modalità privata, è possibile installare un connettore on-premise o nel cloud e utilizzare BlueXP per gestire i dati nel cloud ibrido. Non è disponibile alcuna connettività al livello BlueXP SaaS.

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.

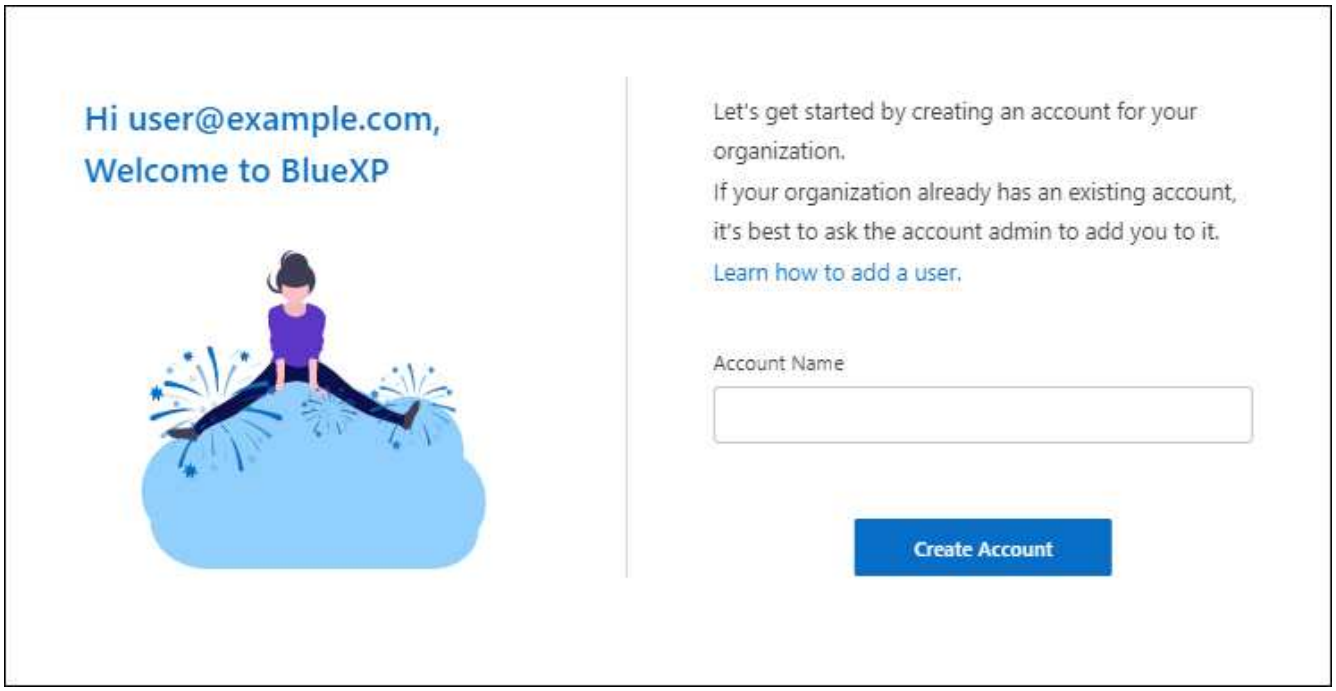
3. Se non disponi di un account NSS e desideri registrarti creando un login cloud NetApp, seleziona **Registrati**.
4. Nella pagina **Registrati**, inserisci le informazioni richieste per creare un login al cloud NetApp.

   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".

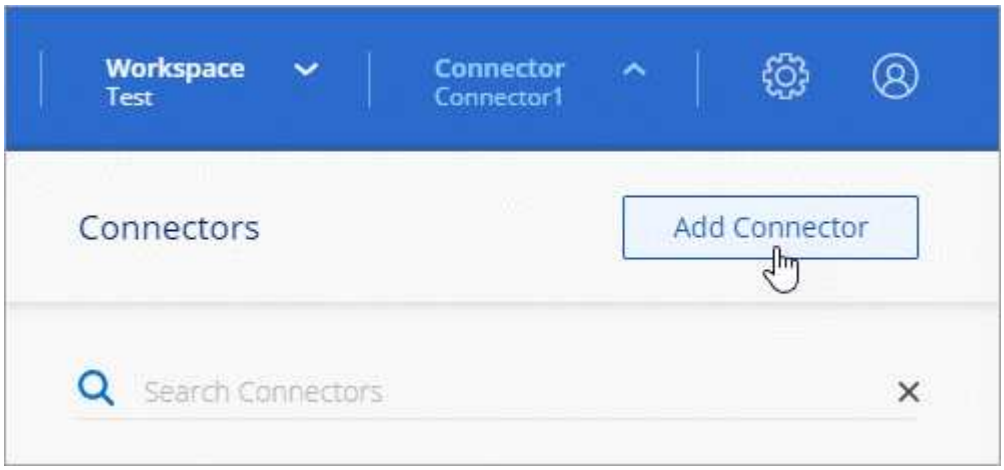
Prima di iniziare

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".

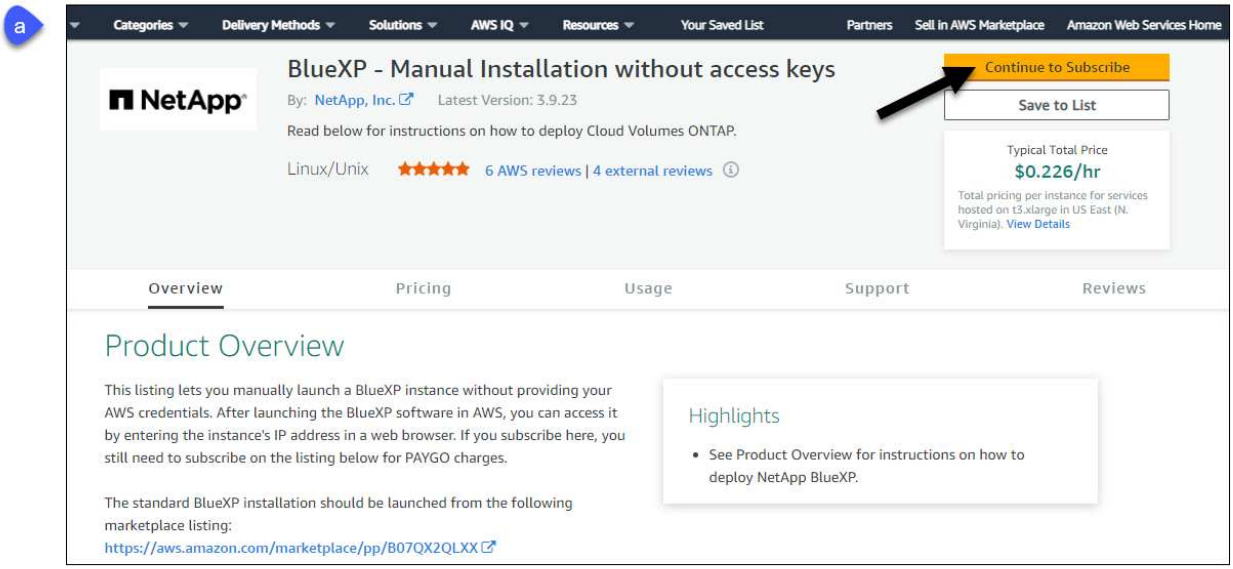
Prima di iniziare

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.

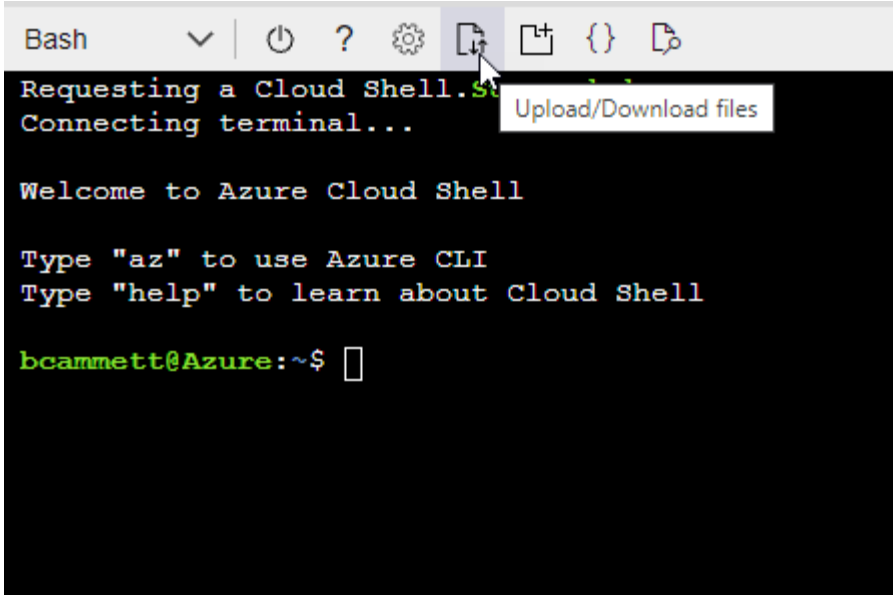
   Esempio

```
"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.

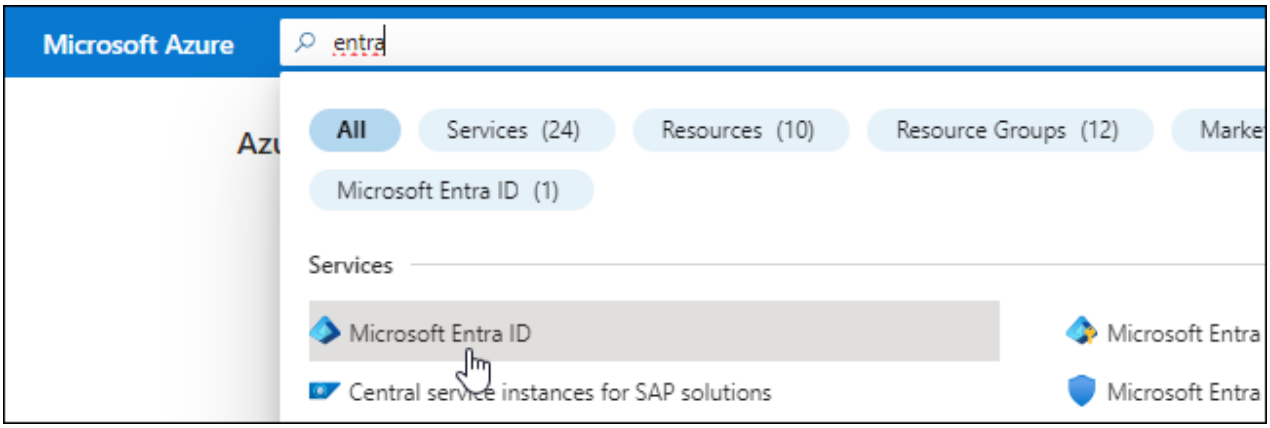
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP.

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**.

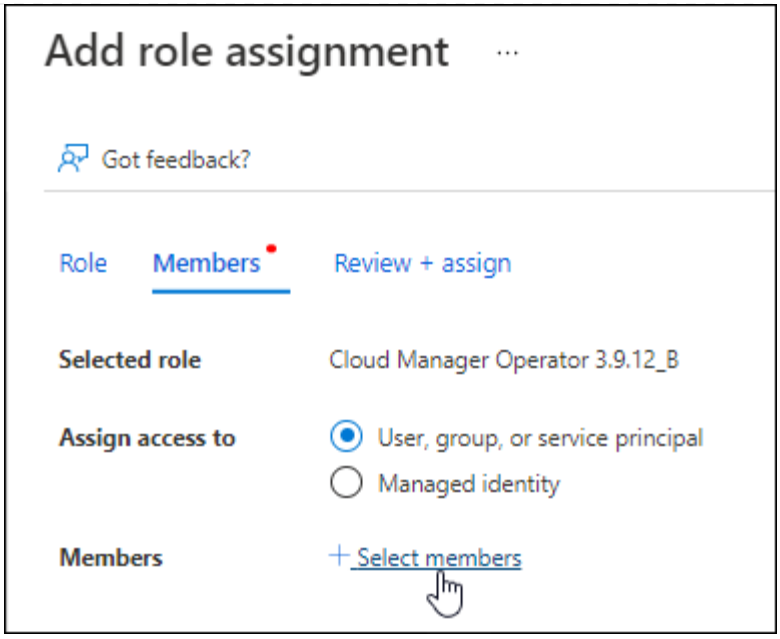
   Hai creato l'applicazione ad e il service principal.

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:

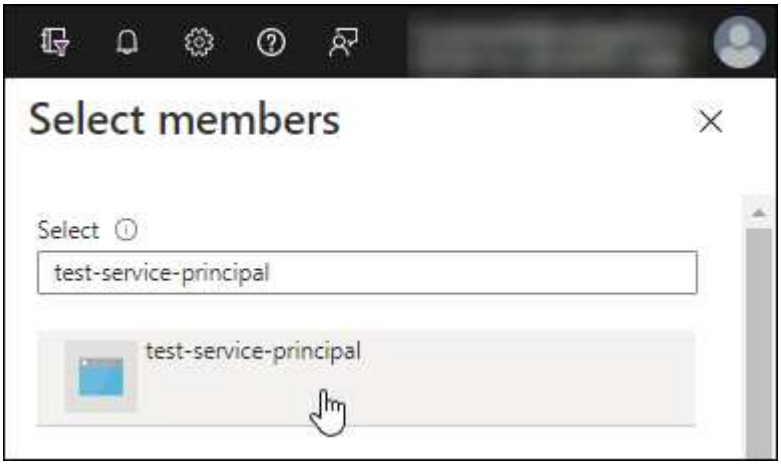
   a. Mantieni selezionata l'opzione **User, group o service principal**.

   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**.

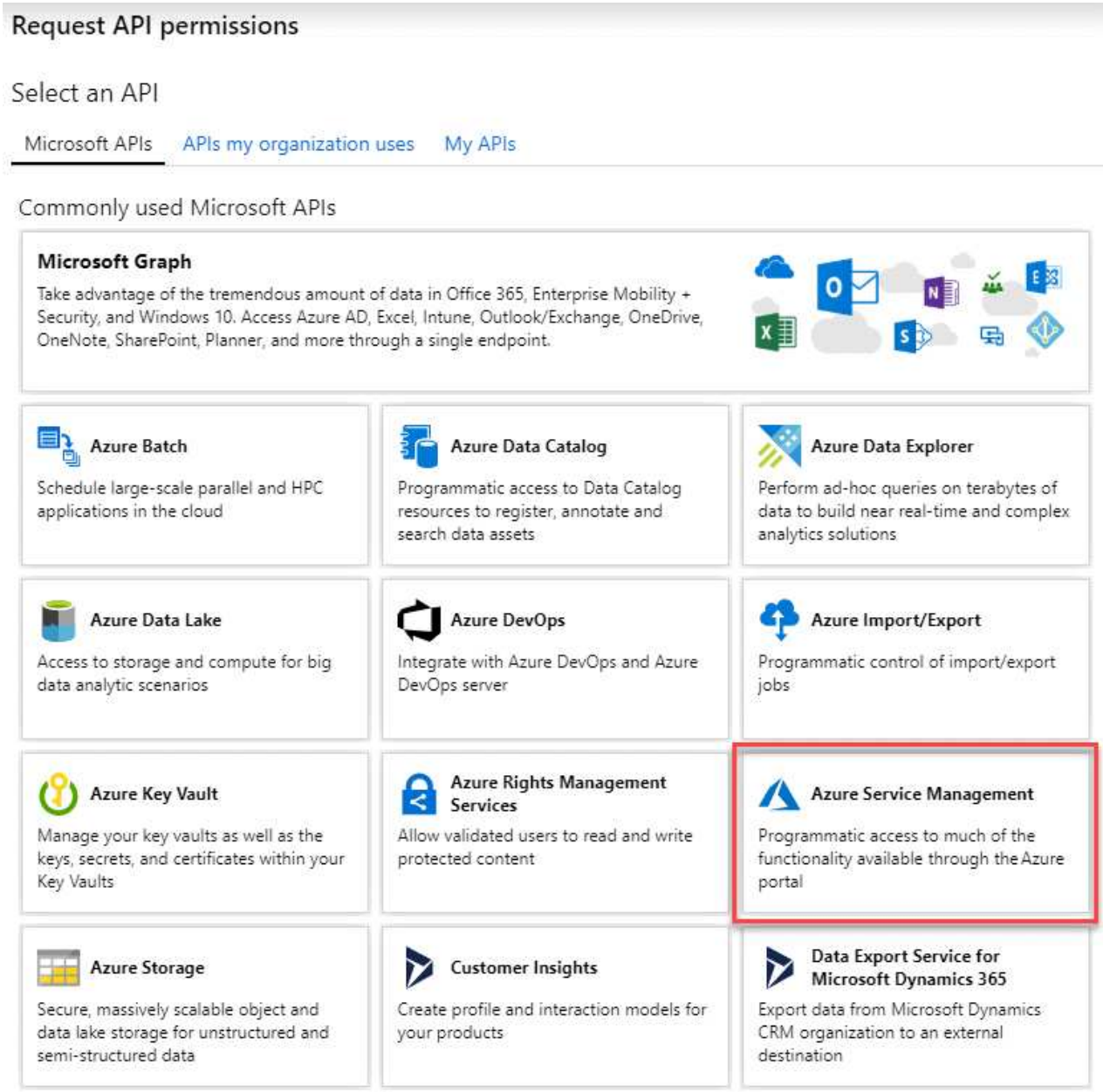
6. Fare clic su **Rivedi + assegna**.

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

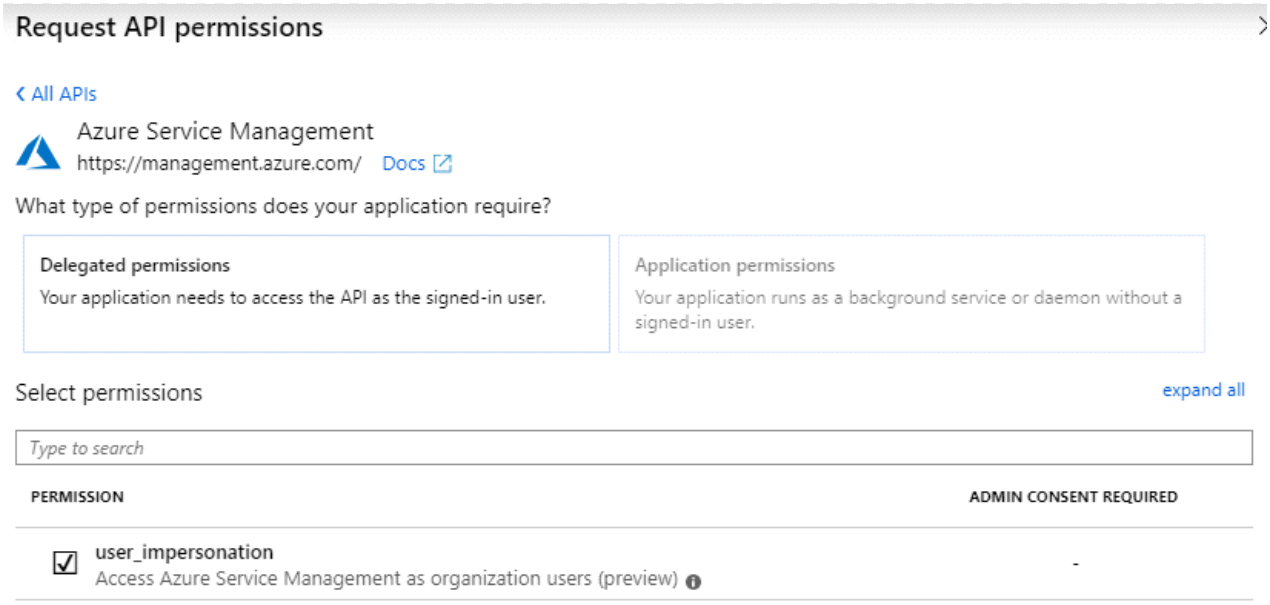
   Se si desidera gestire le risorse in più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. Ad esempio, BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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**.

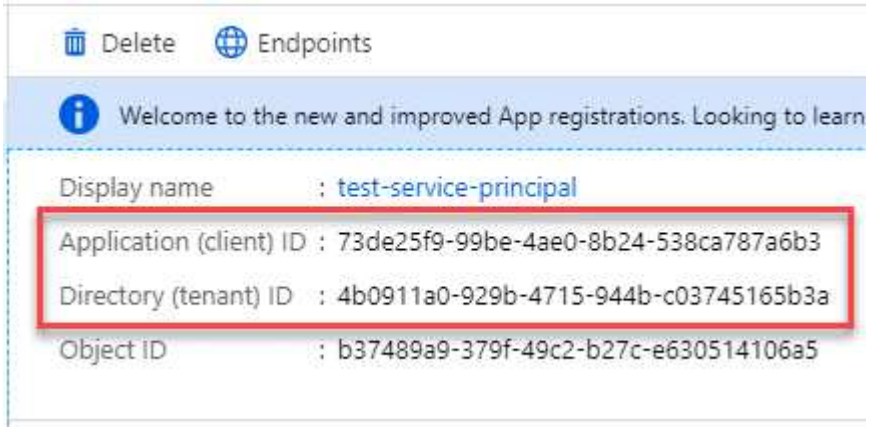


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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.

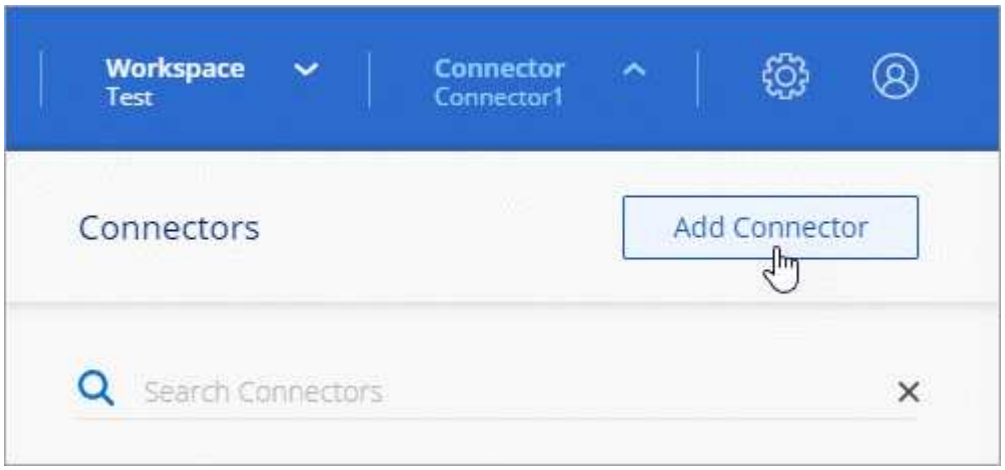
  "Scopri di più sulla connessione a una macchina virtuale Linux in Azure"

- 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.

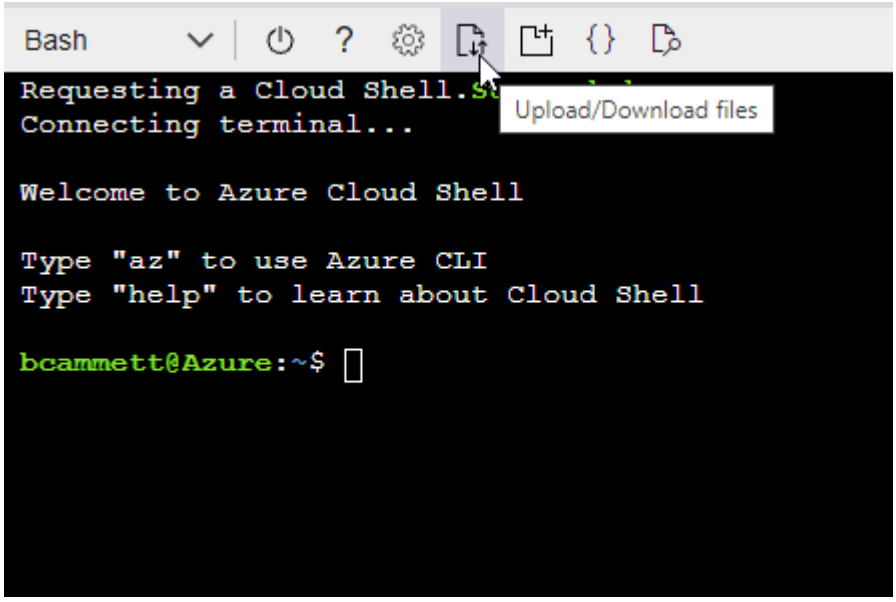
   Esempio

   ```
   "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

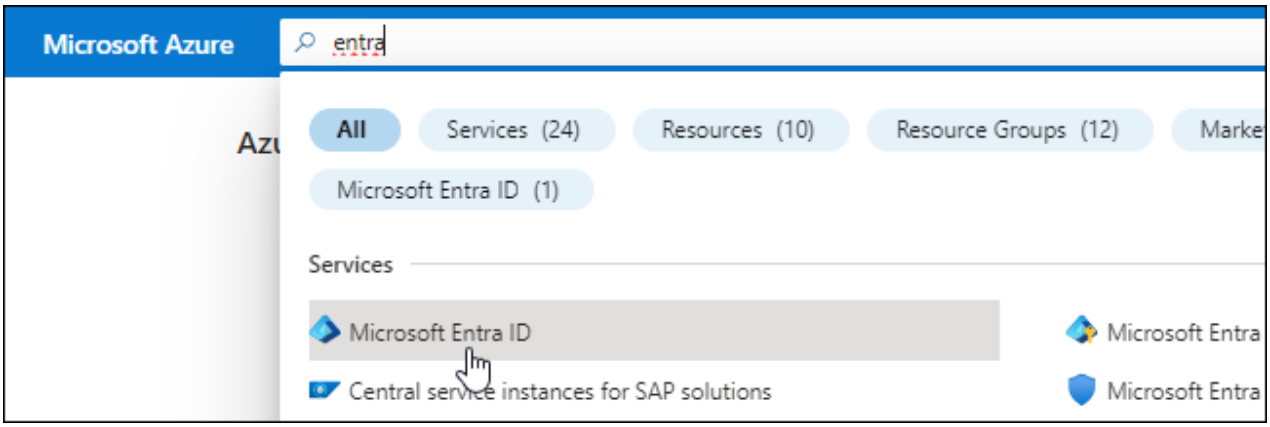
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP.

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.

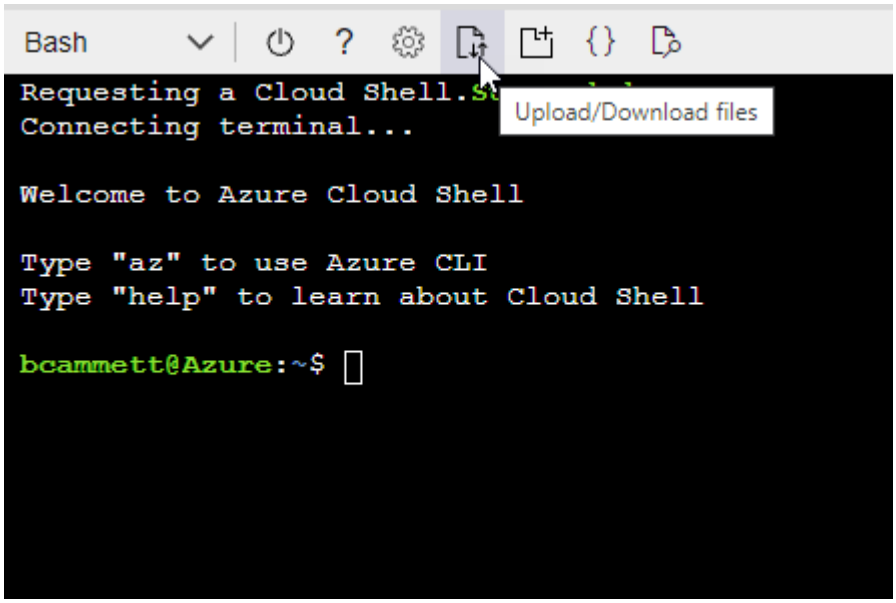
   Esempio

```
"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
```

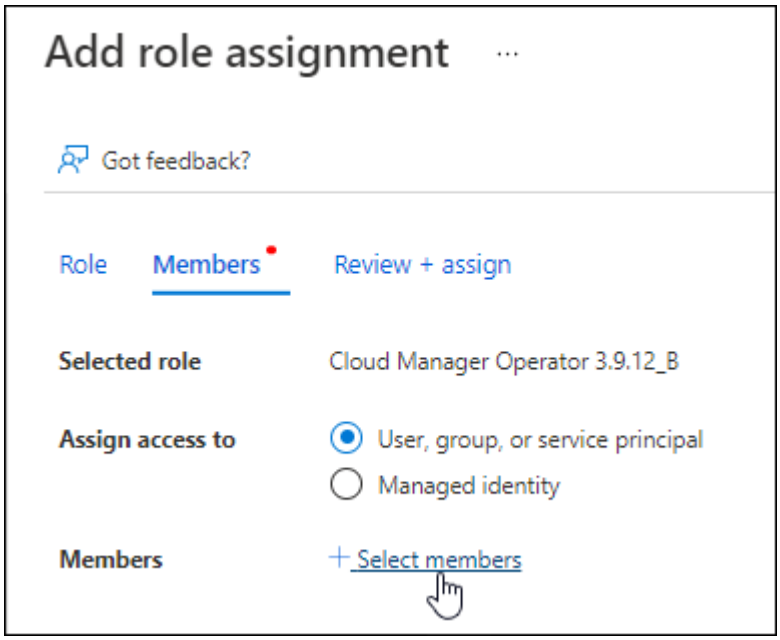
   A questo punto, dovrebbe essere disponibile un ruolo personalizzato denominato BlueXP

Operator che è possibile assegnare alla macchina virtuale Connector.

2. Assegnare l'applicazione al ruolo:

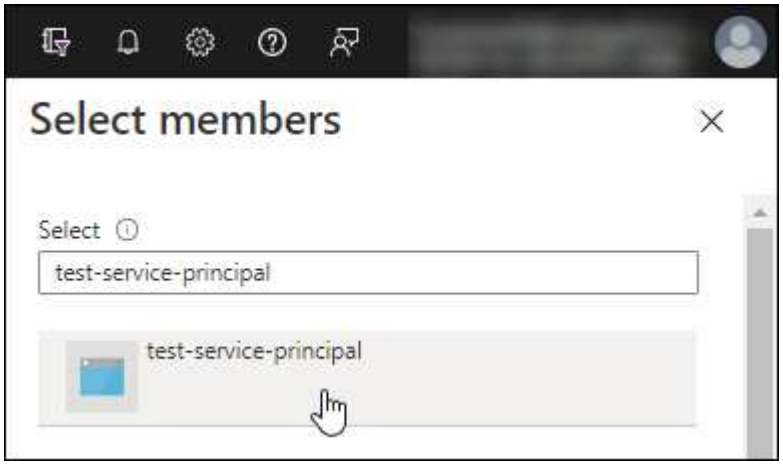
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

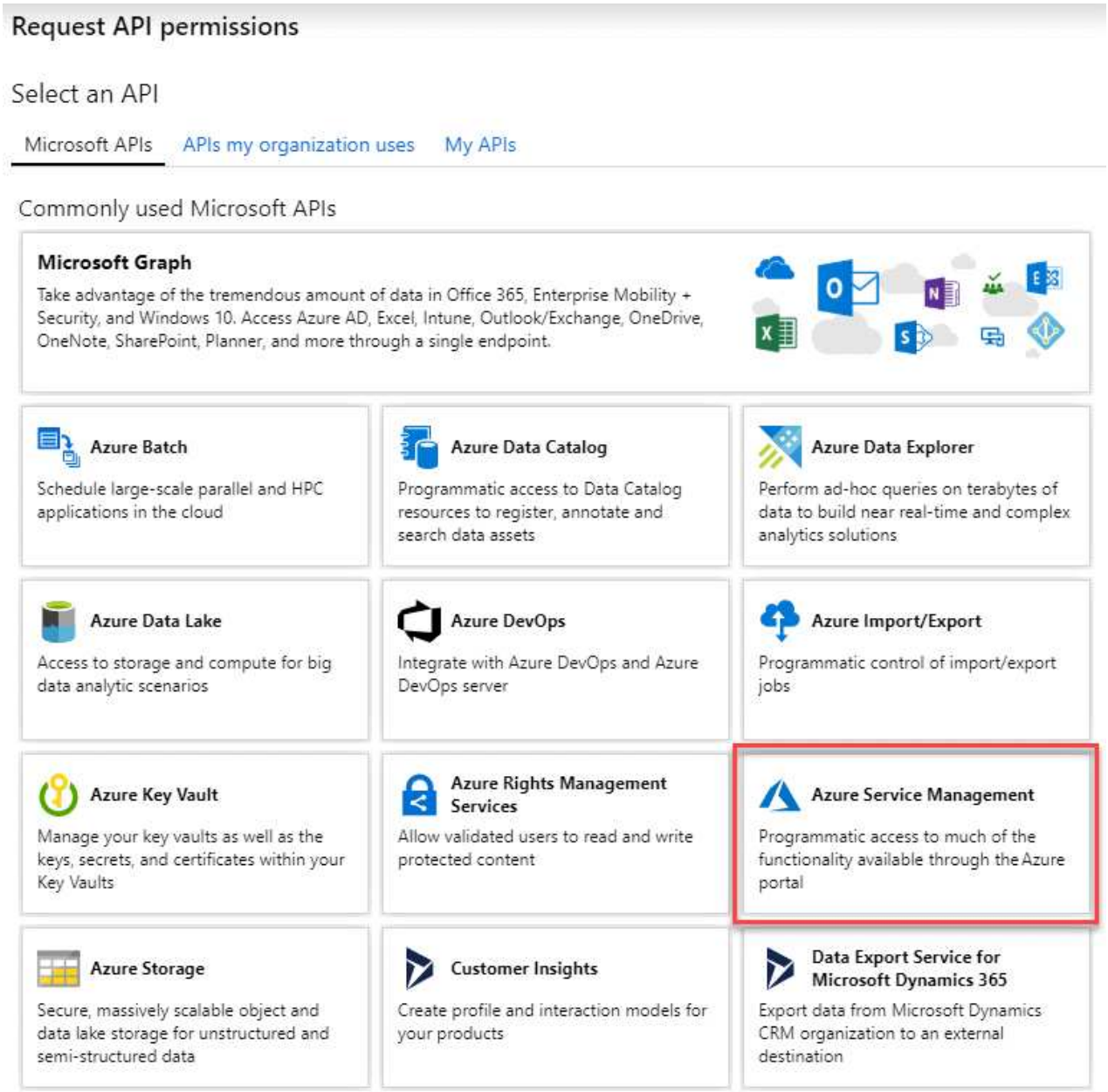
f. Selezionare **Rivedi + assegna**.

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

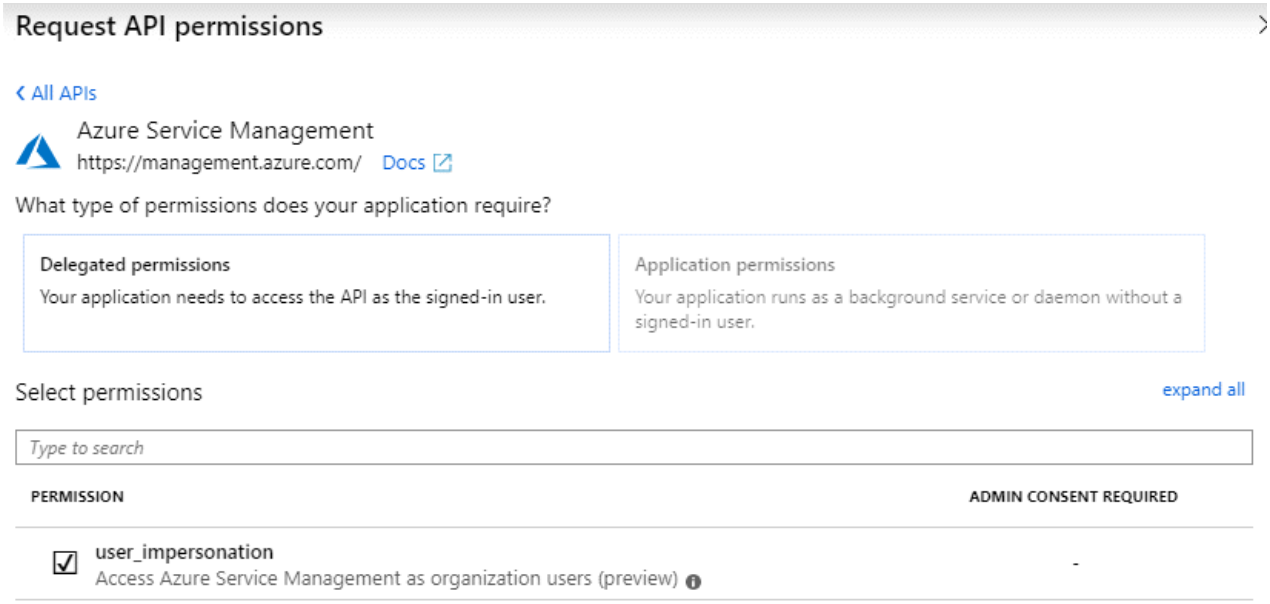
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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**.

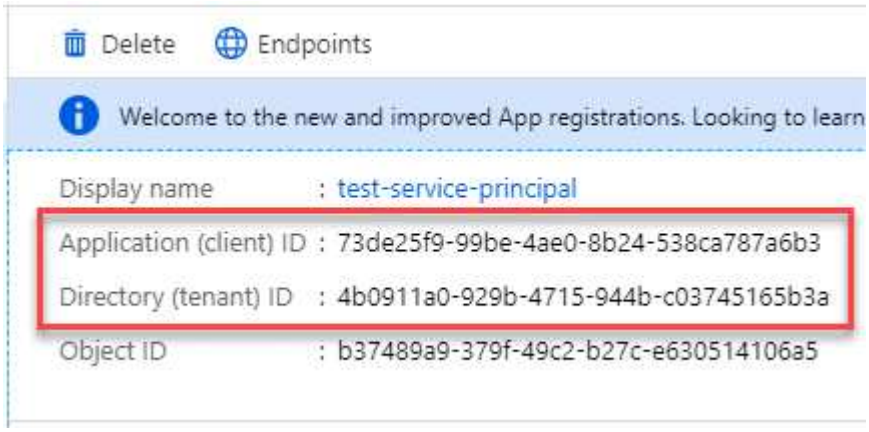


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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.

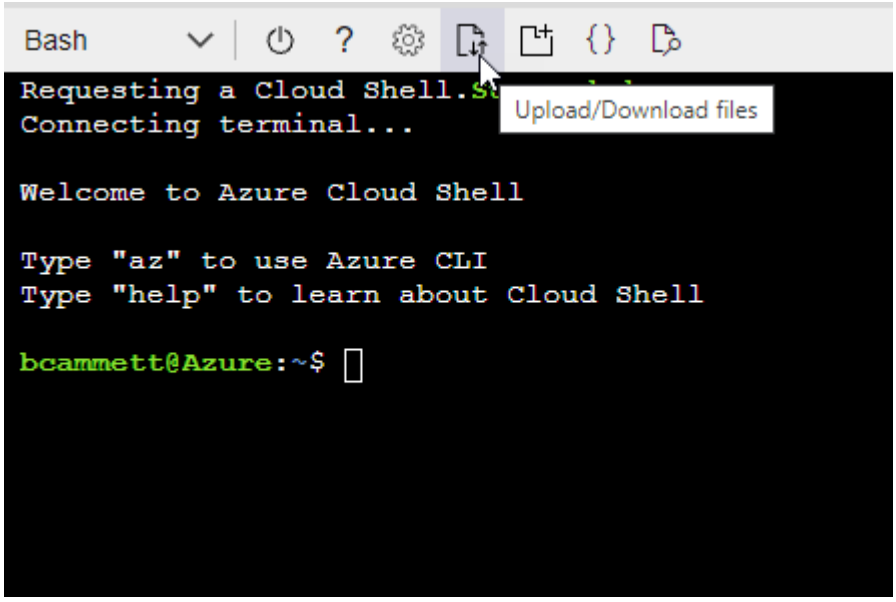
   Esempio

   ```
   "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

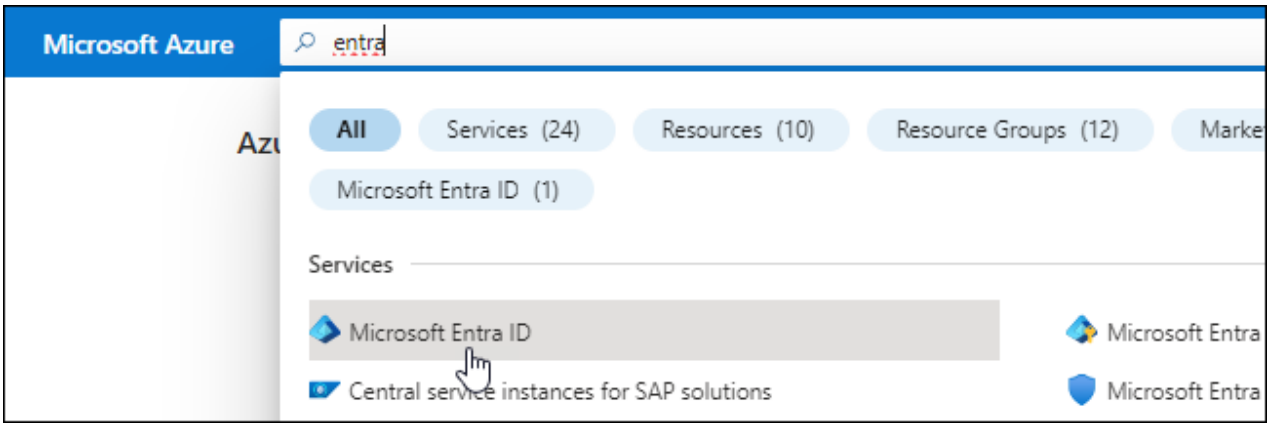
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP.

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.

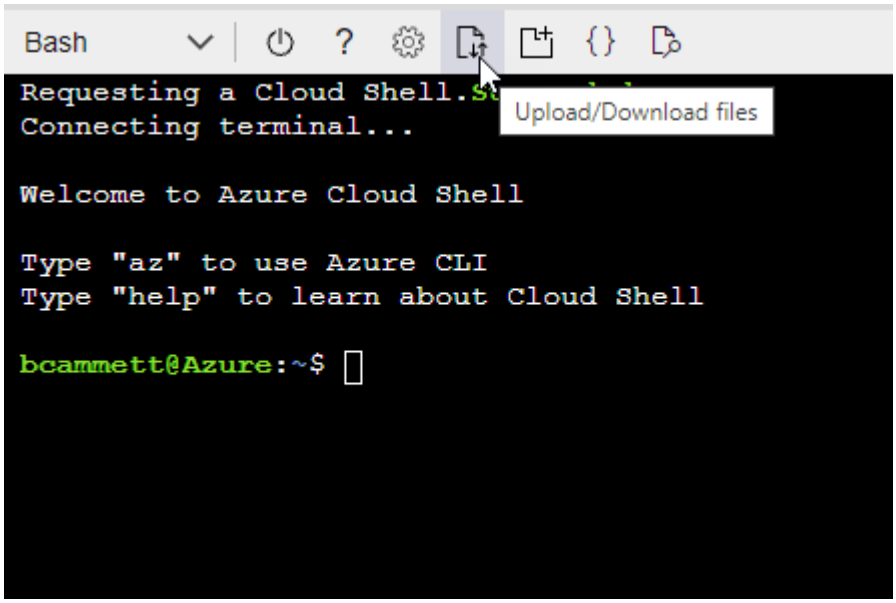
   Esempio

```
"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
```

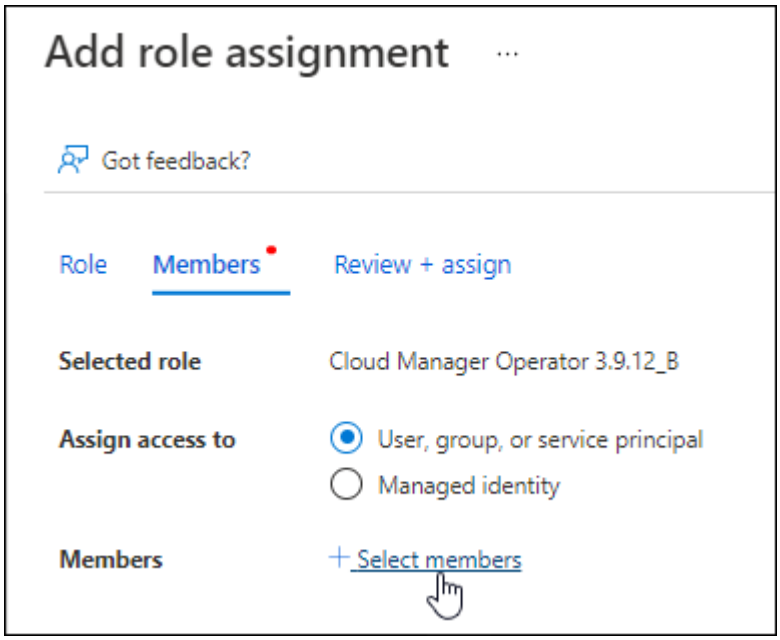
   A questo punto, dovrebbe essere disponibile un ruolo personalizzato denominato BlueXP

Operator che è possibile assegnare alla macchina virtuale Connector.

2. Assegnare l'applicazione al ruolo:

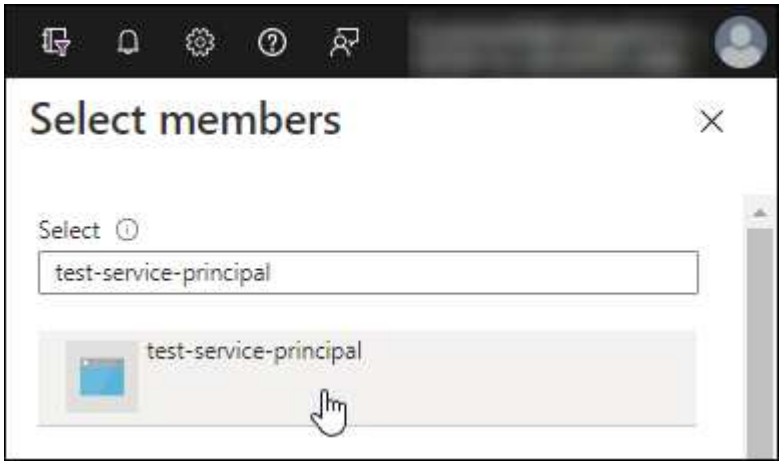
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

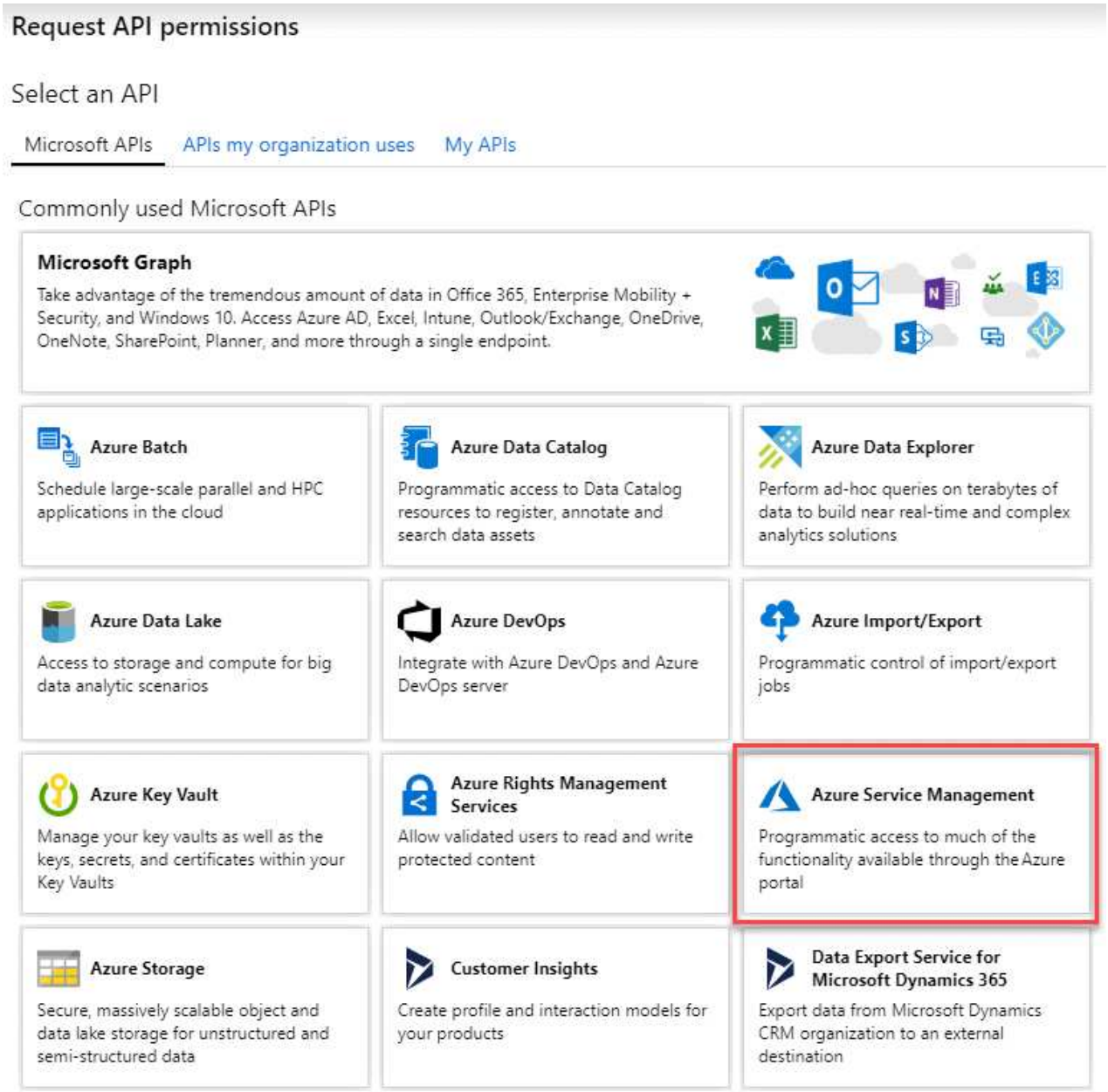
f. Selezionare **Rivedi + assegna**.

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

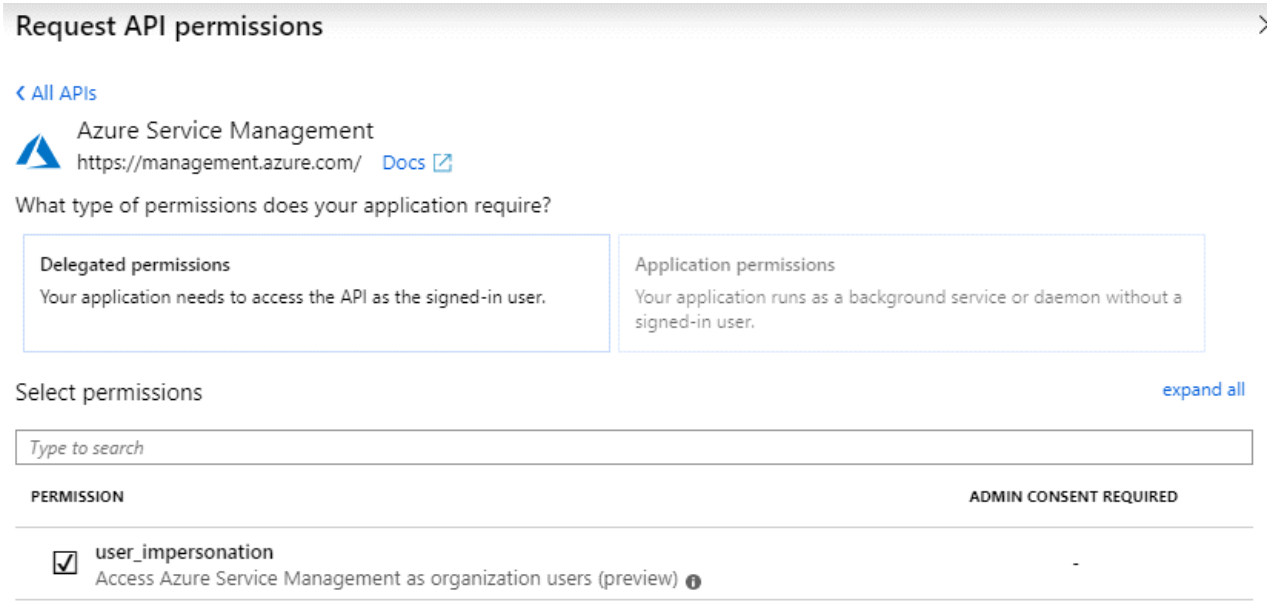
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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**.

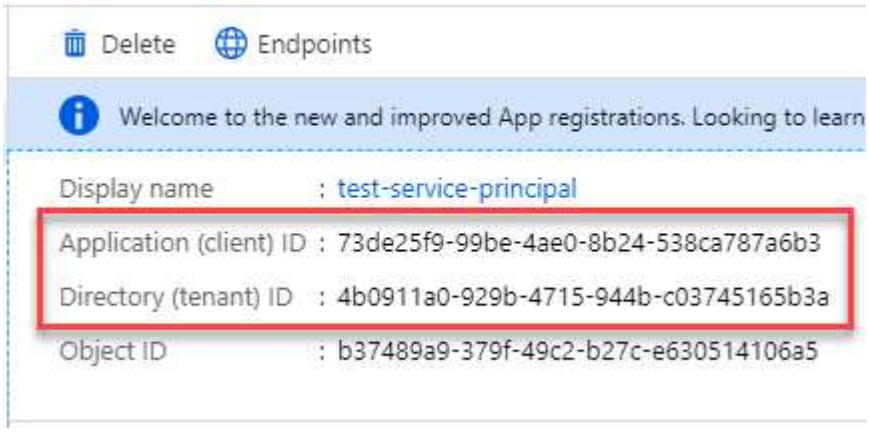


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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:

```yaml
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

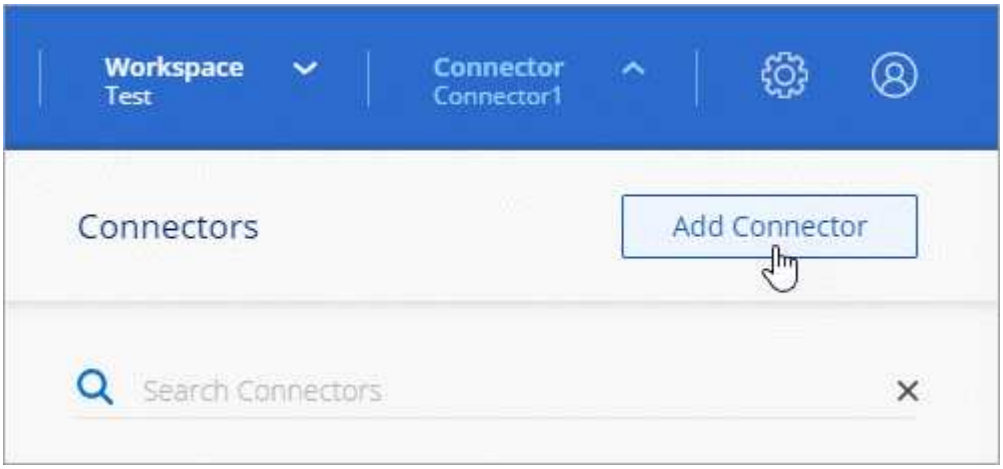
Prima di iniziare

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

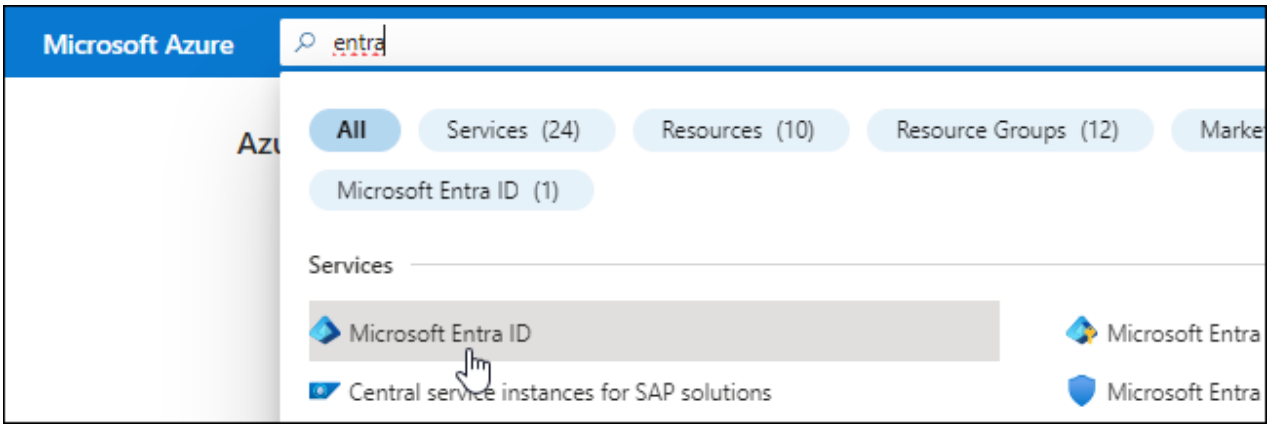
Quando il connettore è installato on-premise, devi fornire ad BlueXP le autorizzazioni di Azure, configurando un'identità di servizio in Microsoft Entra ID e ottenendo le credenziali di Azure di cui BlueXP ha bisogno.

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.

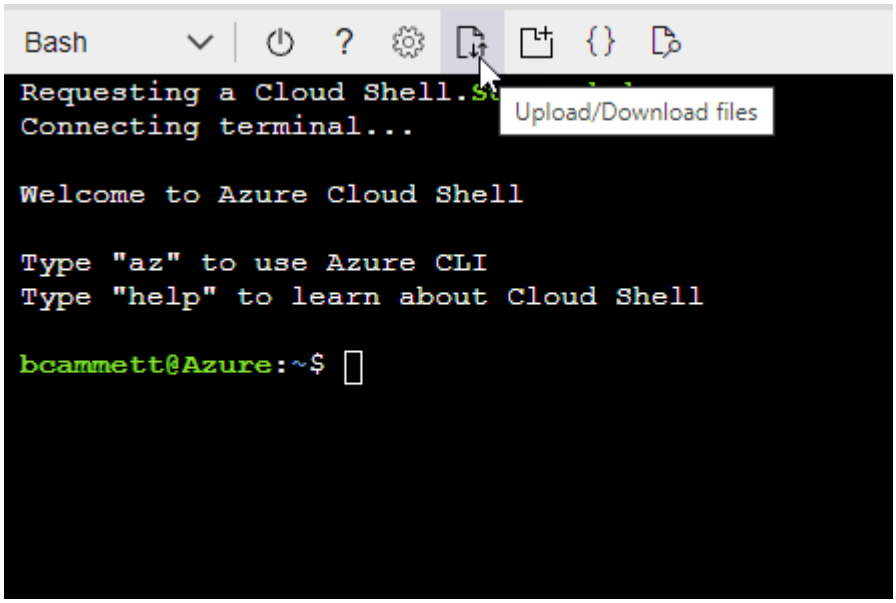
      Esempio

      ```
      "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:

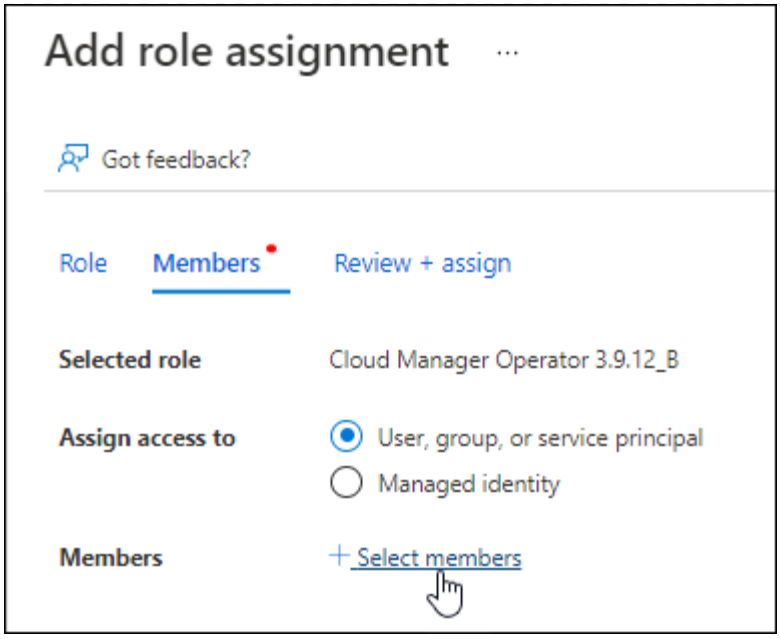
```
az role definition create --role-definition
Connector_Policy.json
```

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:

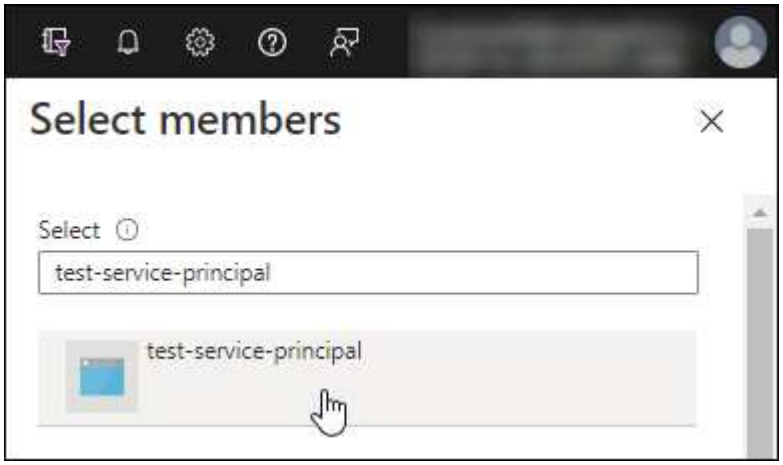
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

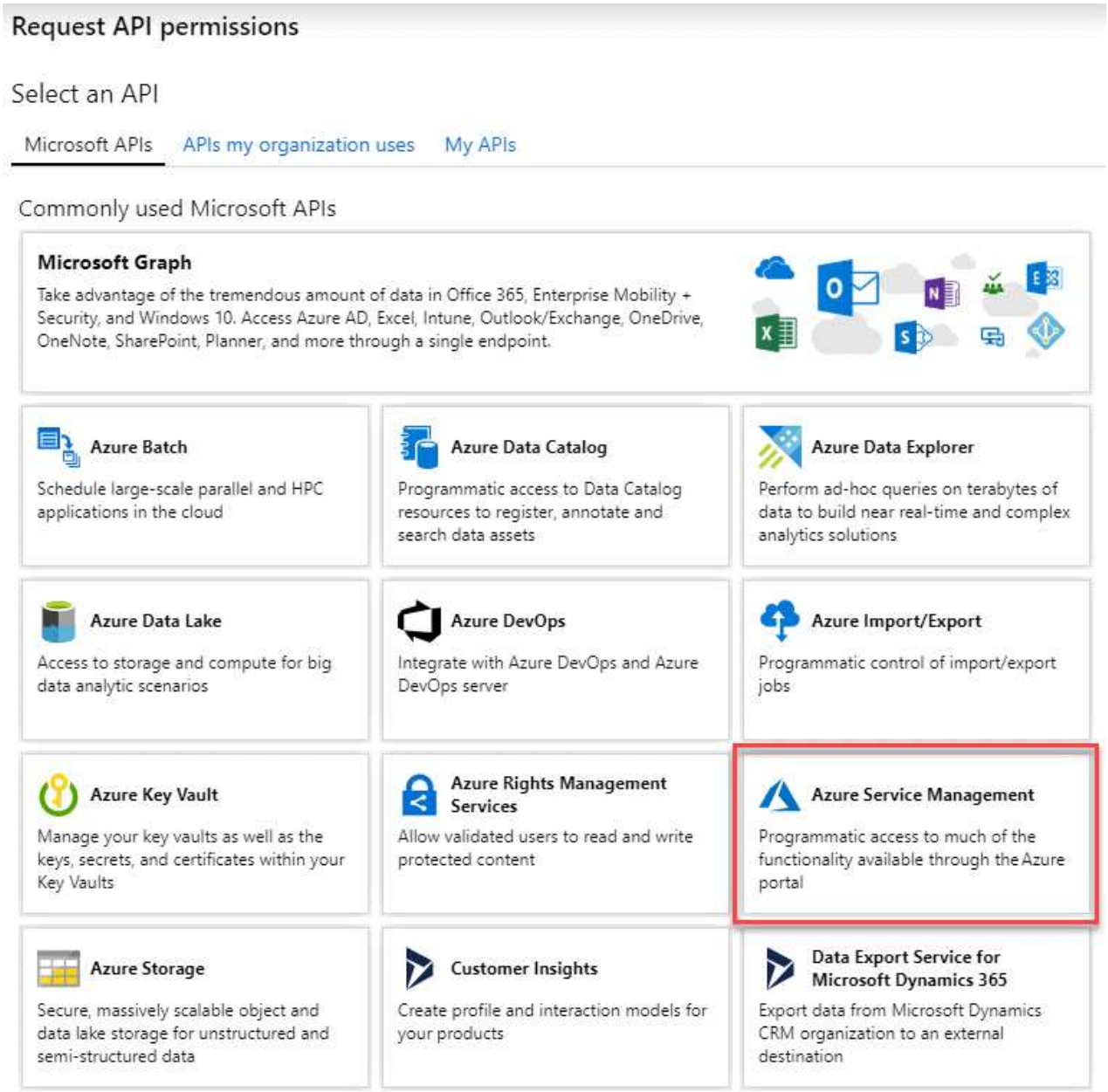
L'entità del servizio dispone ora delle autorizzazioni Azure necessarie per implementare il connettore.

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.

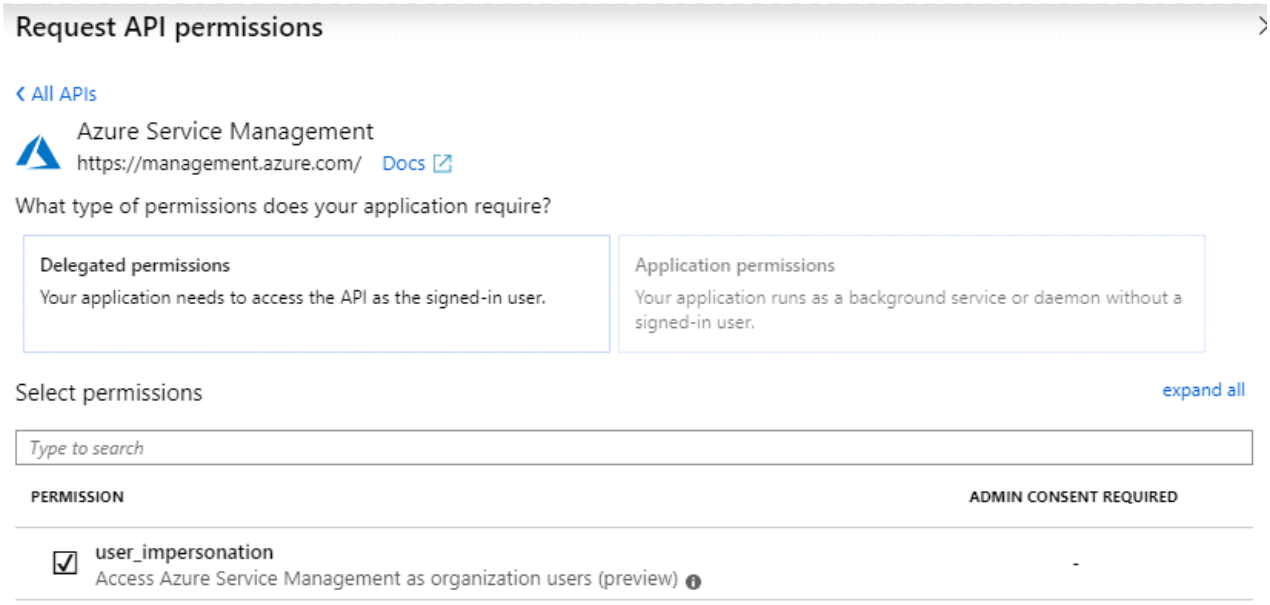
Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

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**.

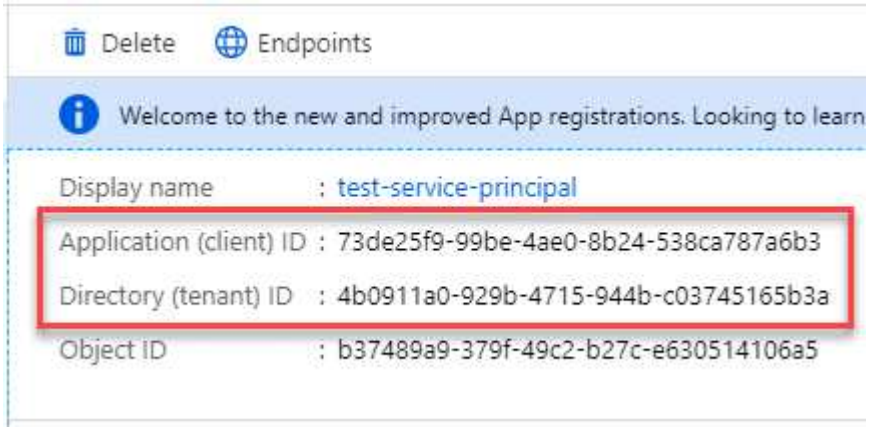


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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

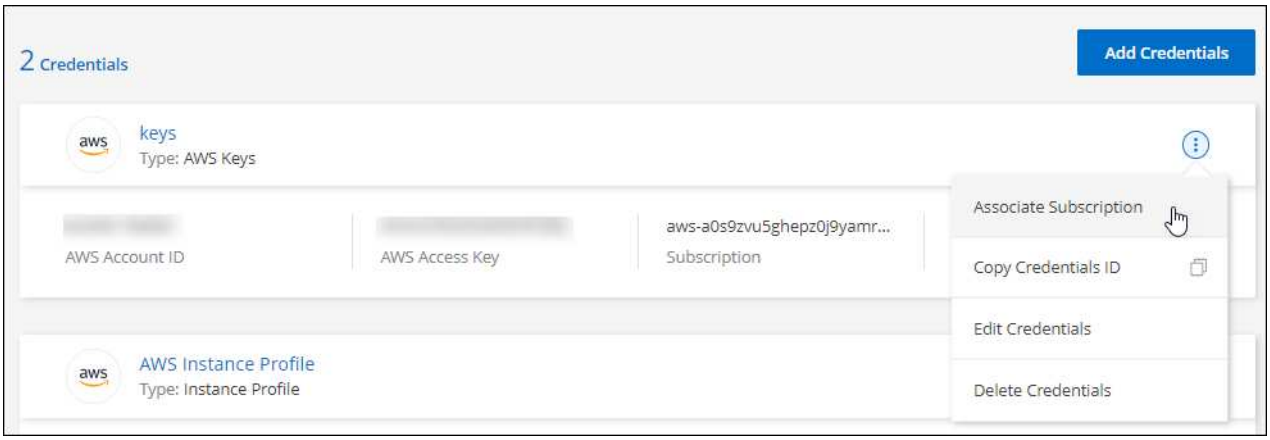
L'iscrizione a BlueXP implica l'associazione di un abbonamento Marketplace alle credenziali cloud associate a un connettore. Se hai seguito il flusso di lavoro "Get Started with standard mode" (inizia con la modalità standard), dovresti già disporre di un connettore. Per ulteriori informazioni, consulta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

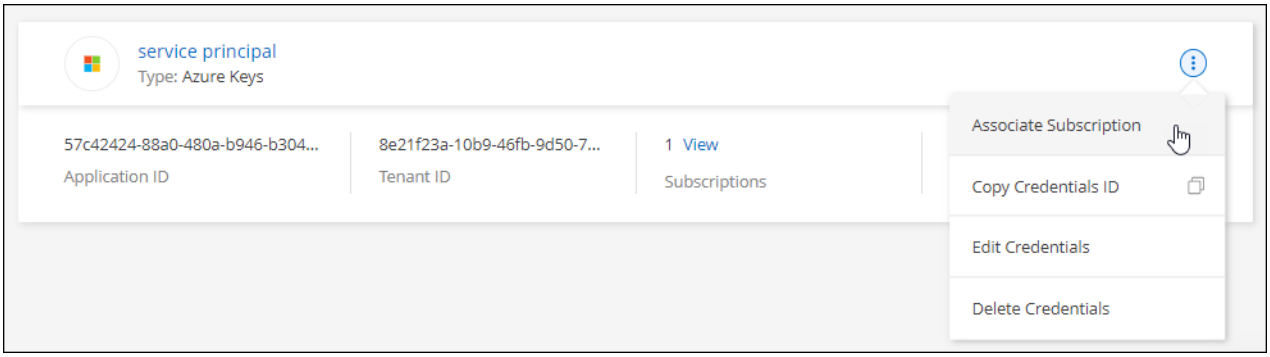
Iscriviti a BlueXP dal marketplace AWS

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**.

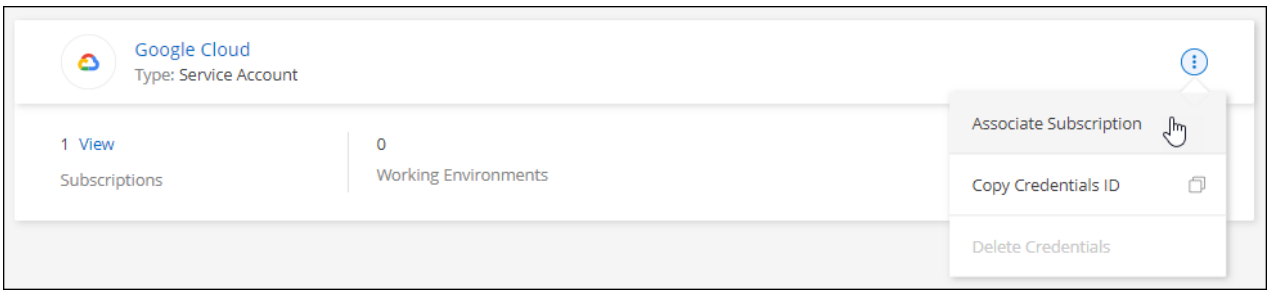
        Il seguente video mostra i passaggi per iscriversi a Azure Marketplace:

Iscriviti a BlueXP da Azure Marketplace

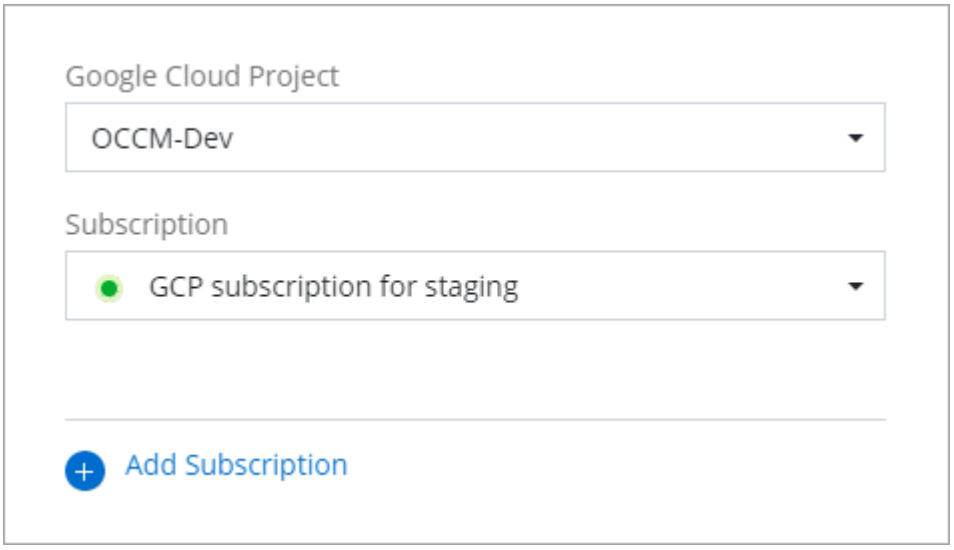
Google Cloud

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**.



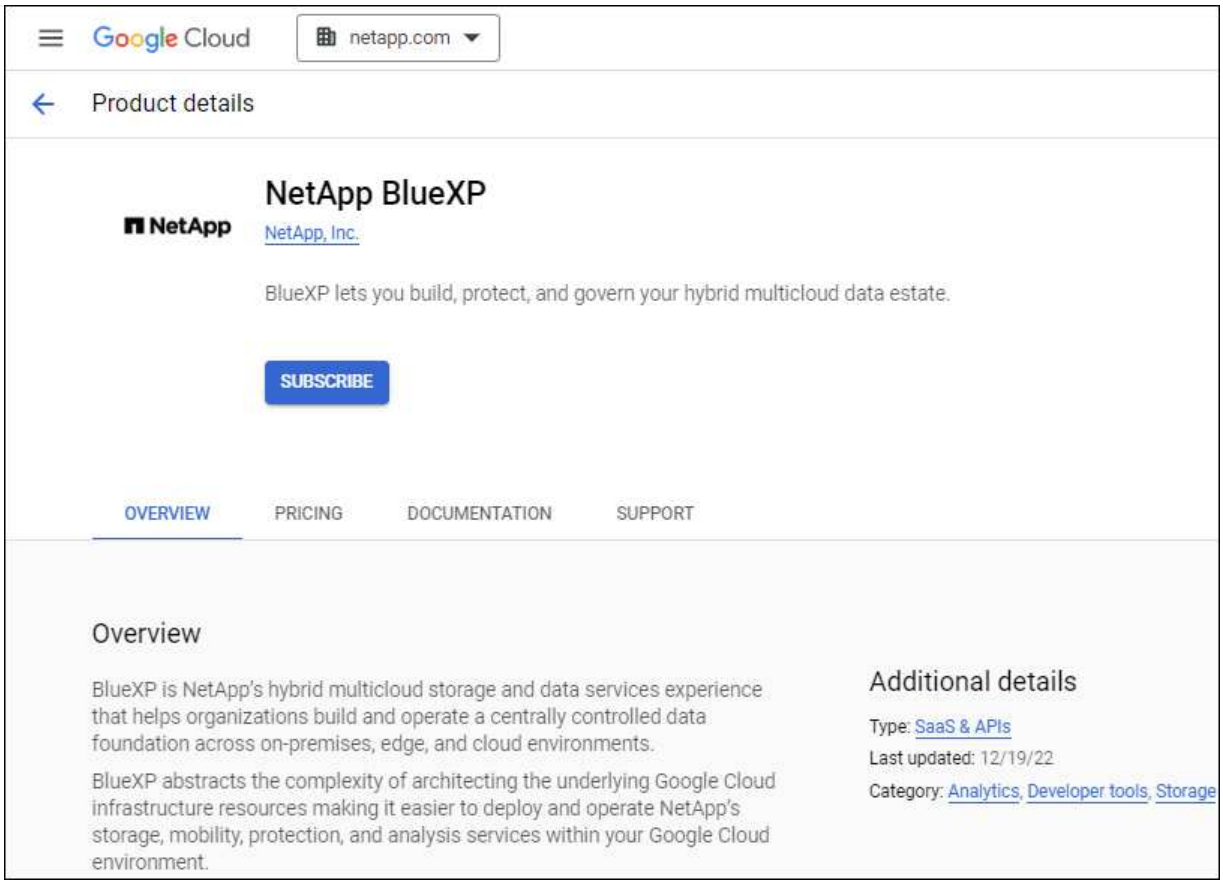
3. Per associare le credenziali a un abbonamento esistente, selezionare un progetto e un abbonamento Google Cloud dall'elenco a discesa, quindi selezionare **Associa**.



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**.

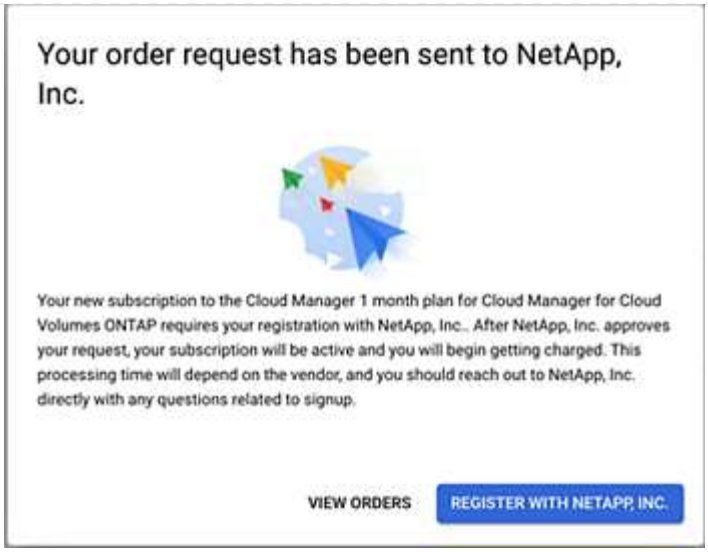
c. Selezionare l'account di fatturazione appropriato e accettare i termini e le condizioni.

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.

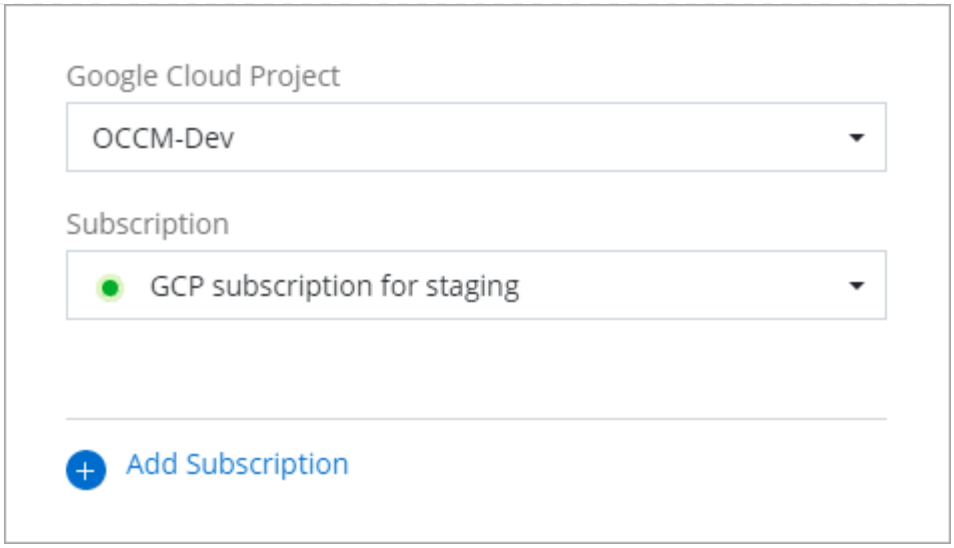
Per tutti gli altri account, è necessario associare manualmente l'abbonamento ripetendo questa procedura.

- 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

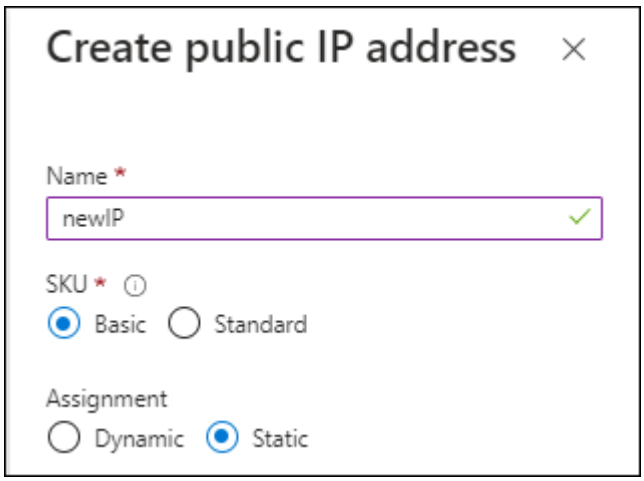
La posizione di rete in cui si implementa il connettore deve disporre di una connessione Internet in uscita. Il connettore richiede l'accesso a Internet in uscita per contattare i seguenti endpoint al fine di gestire risorse e processi all'interno dell'ambiente di cloud pubblico.

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.

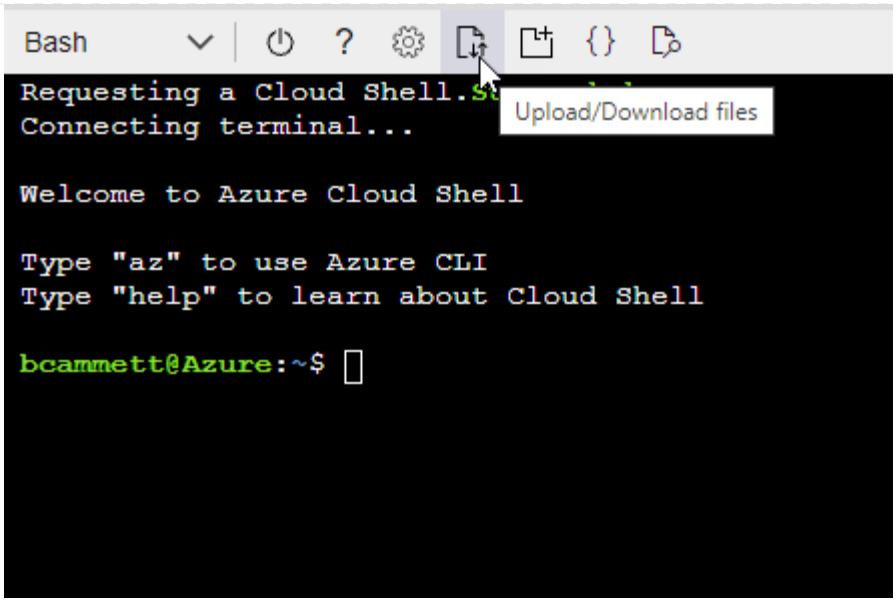
   Esempio

   ```
   "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

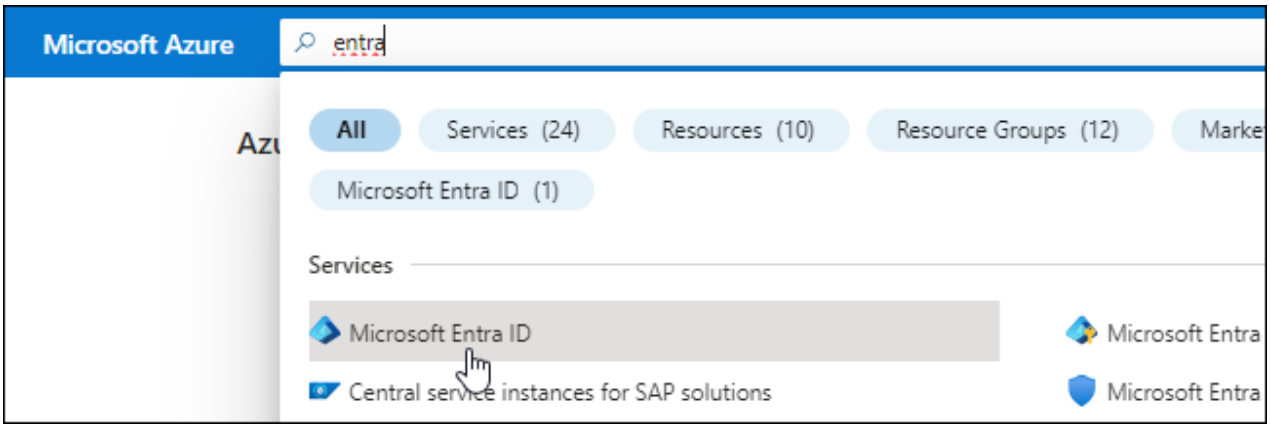
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP. È necessario fornire queste credenziali a BlueXP dopo aver installato il connettore e configurato BlueXP.

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.

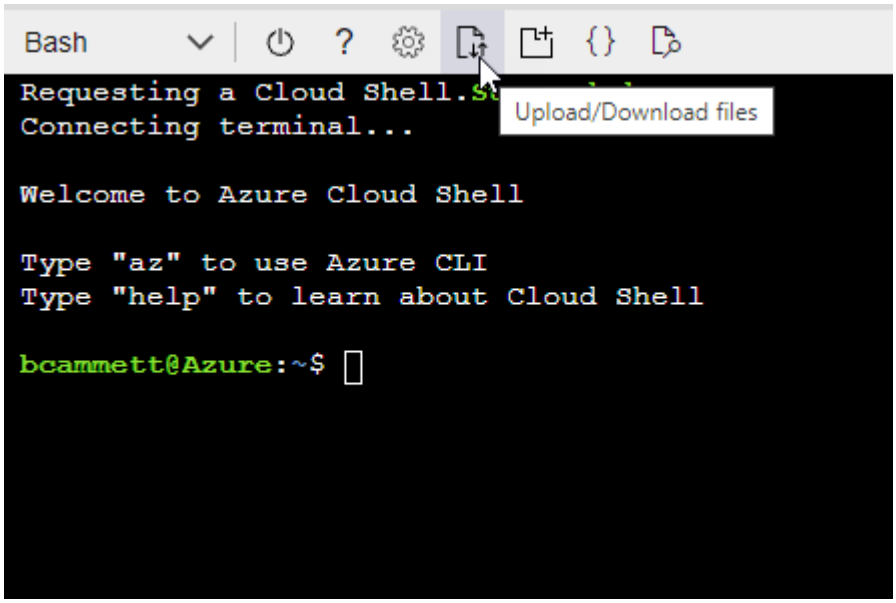
      Esempio

      ```
      "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:

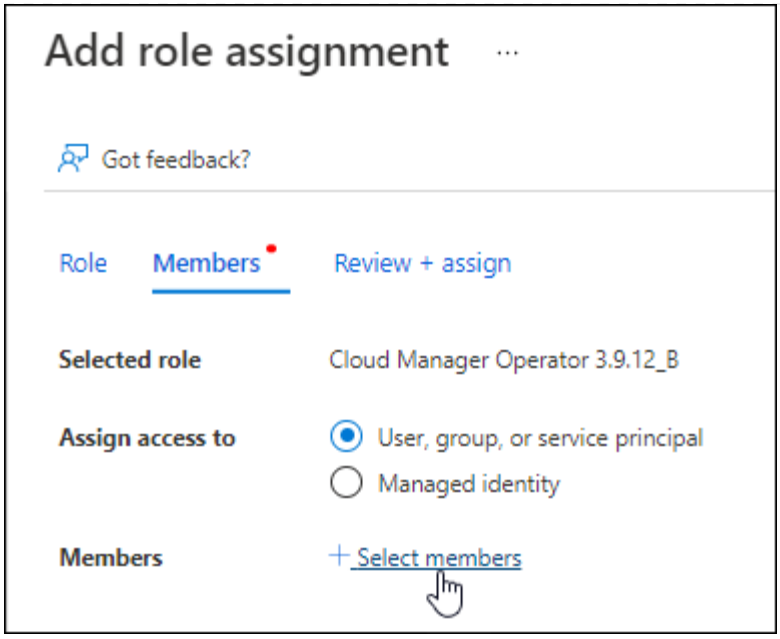
```
az role definition create --role-definition
Connector_Policy.json
```

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:

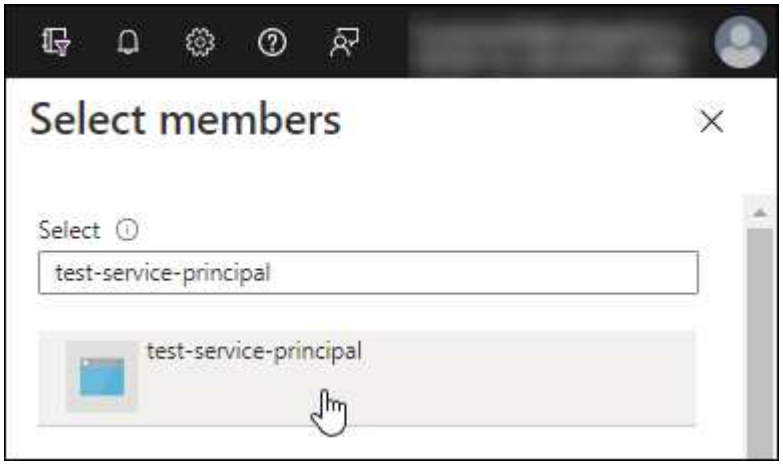
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

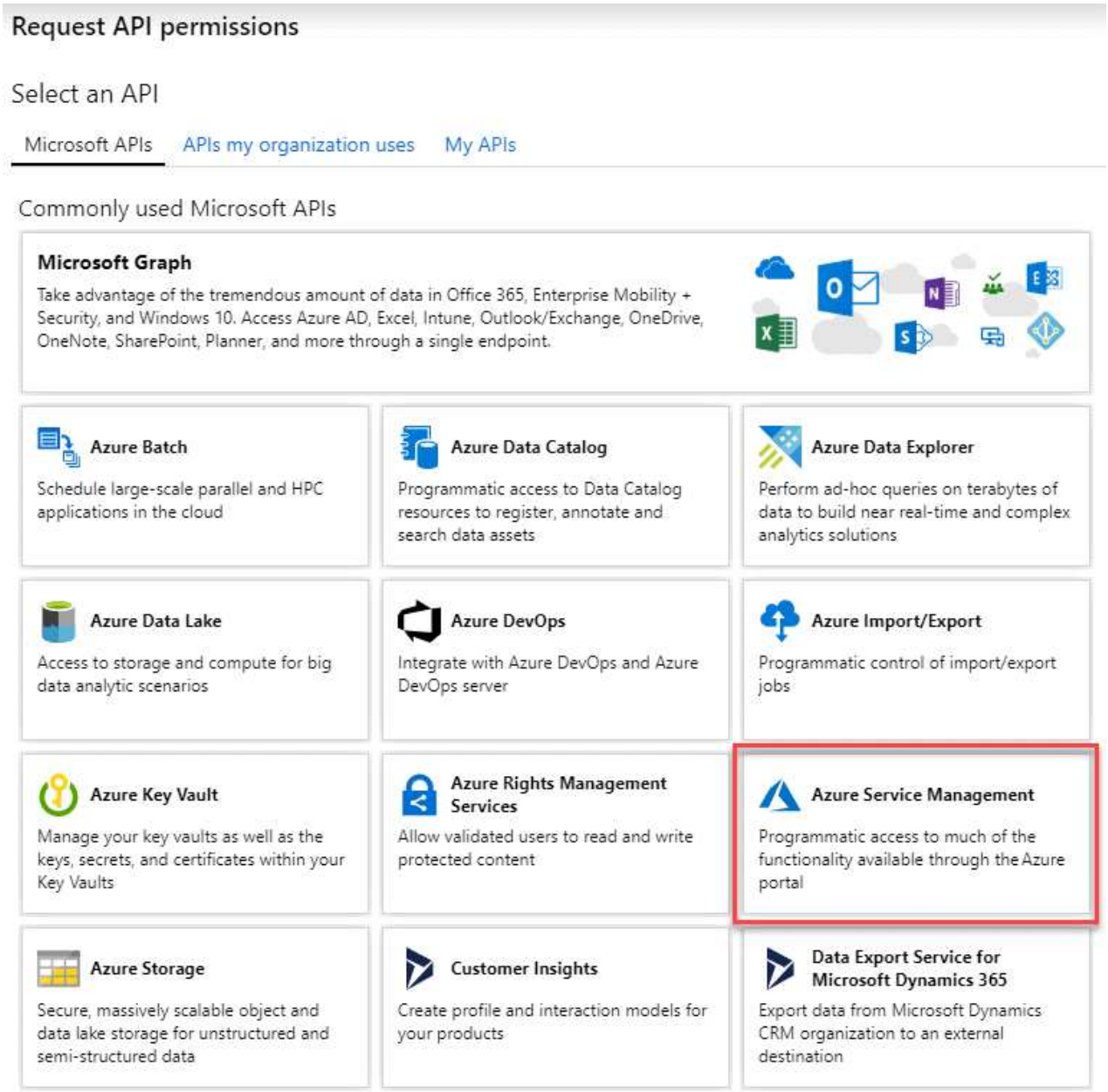
L'entità del servizio dispone ora delle autorizzazioni Azure necessarie per implementare il connettore.

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.

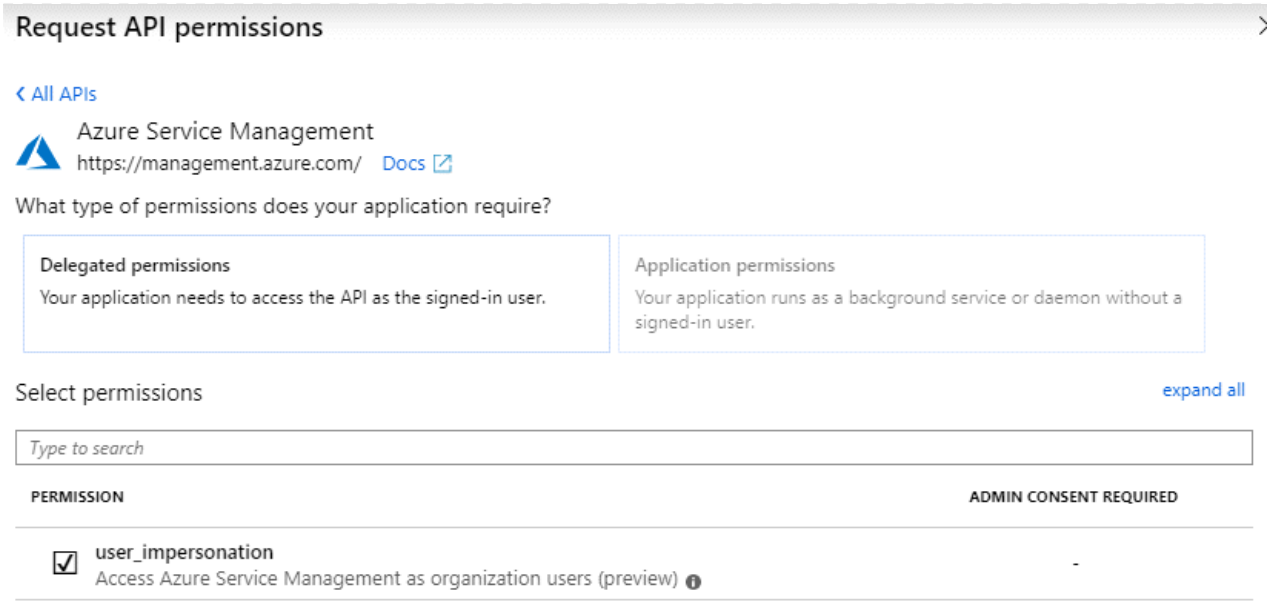
Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

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**.

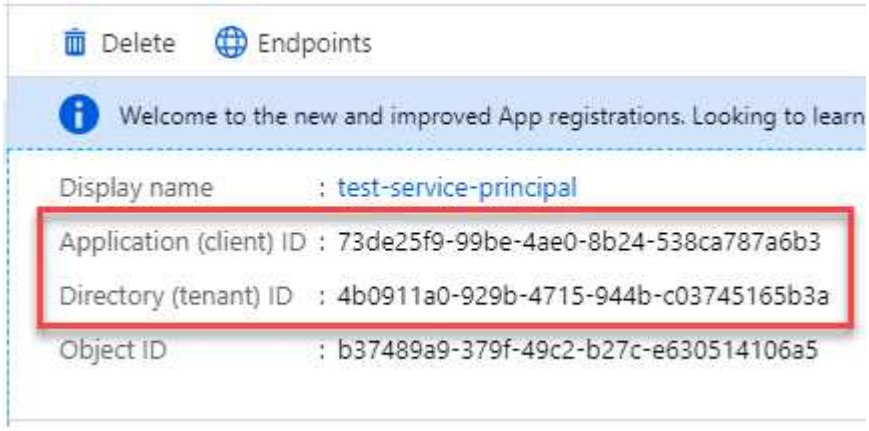


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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"

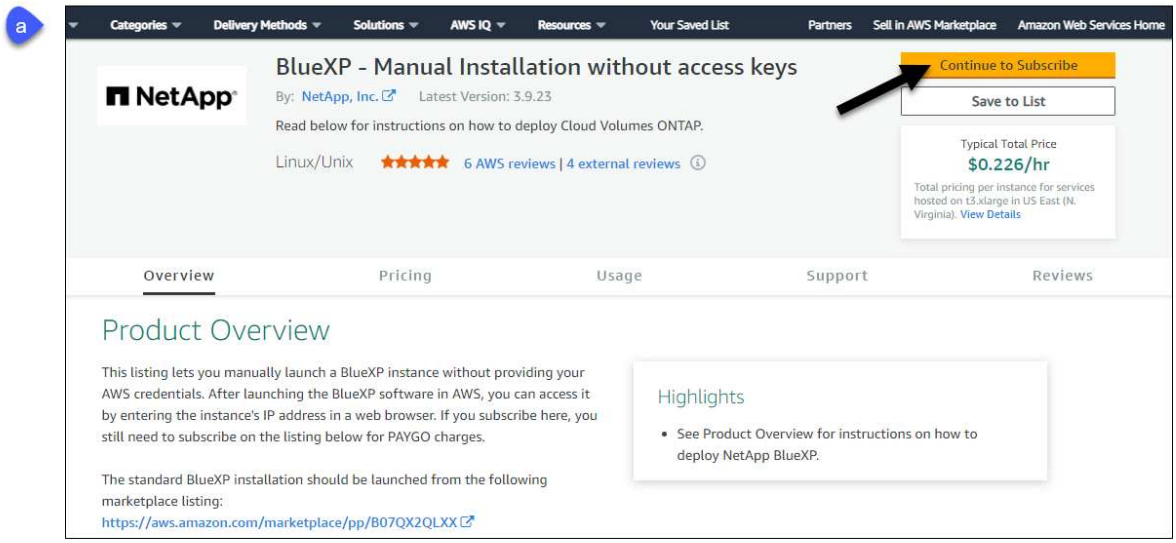
- Autorizzazioni per iscriversi e annullare l'iscrizione da AWS Marketplace per l'utente IAM.
- Comprensione dei requisiti di CPU e RAM per l'istanza.

  "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"

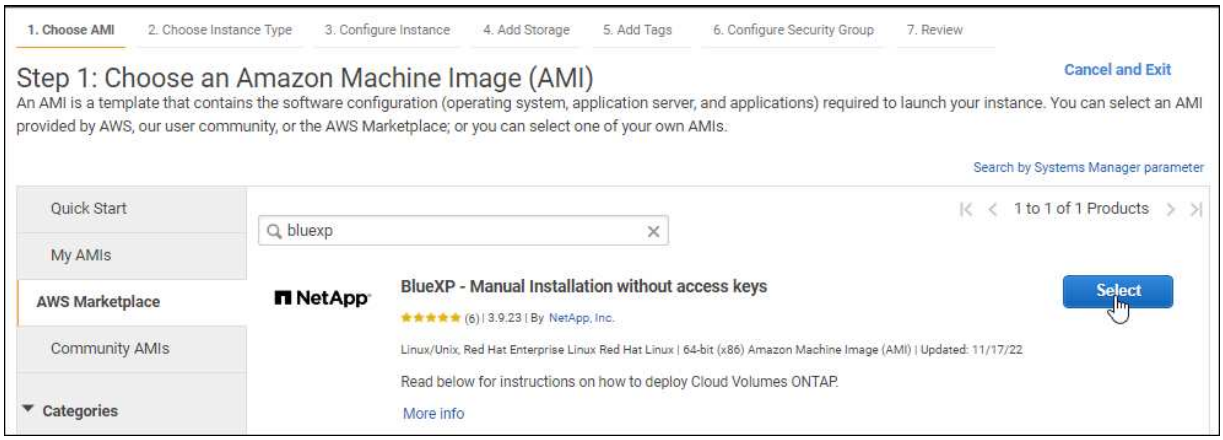
- Un ruolo IAM con un criterio allegato che include le autorizzazioni richieste per il connettore.

  "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.

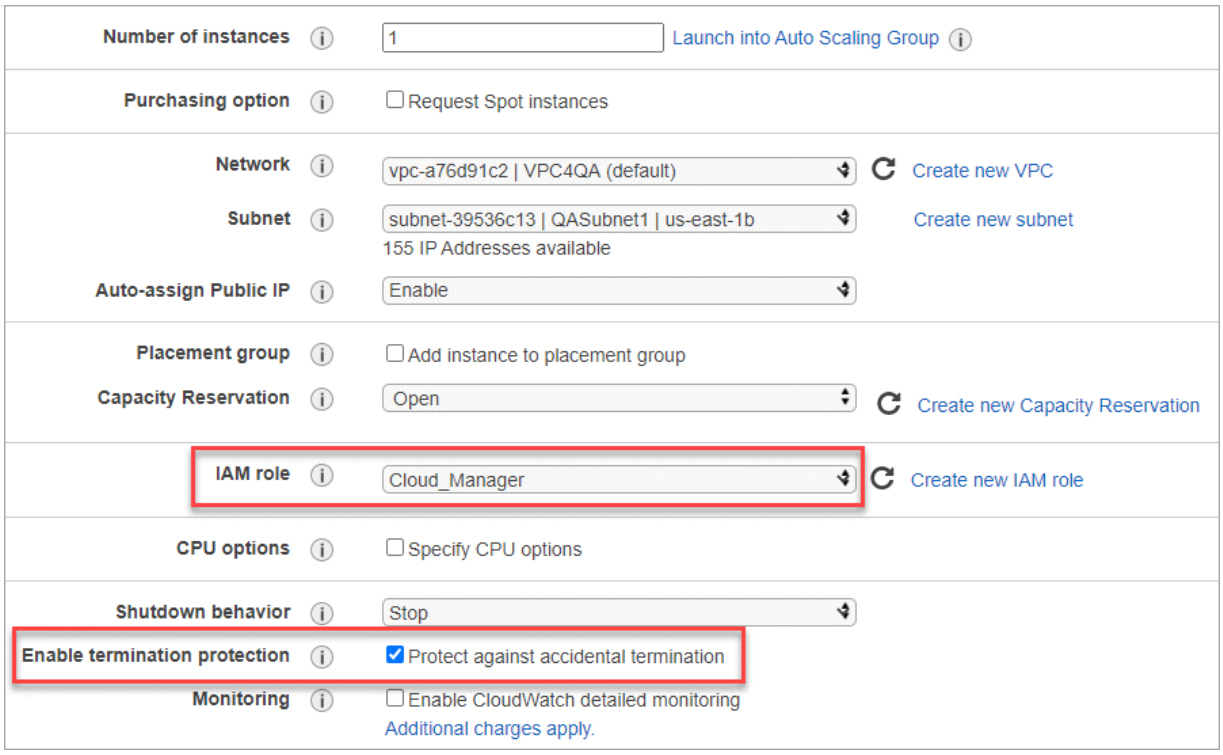


   d. Selezionare **continua**.

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

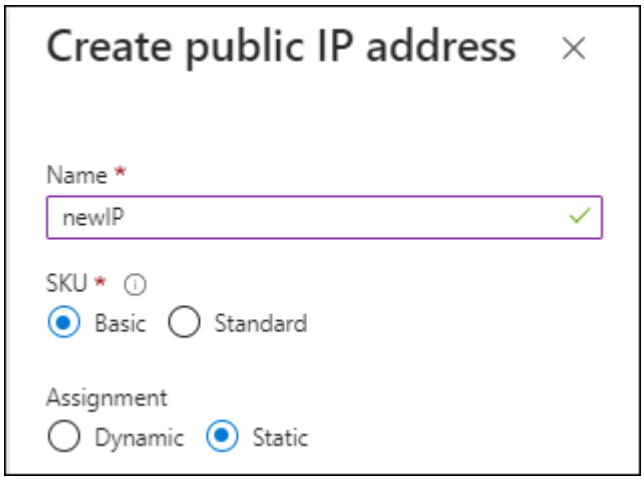
1. Accedere alla pagina NetApp Connector VM in Azure Marketplace.
   - "Pagina di Azure Marketplace per le regioni commerciali"

- "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:

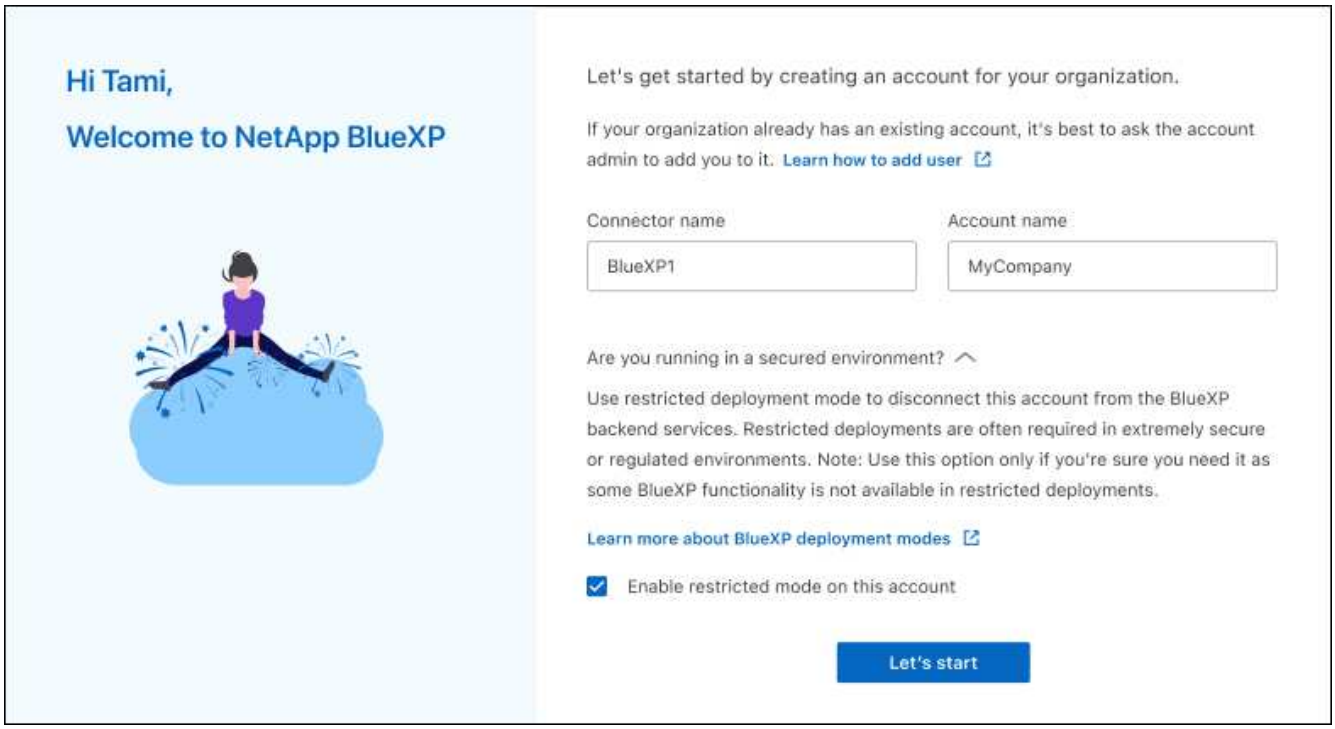
   a. Inserire un nome per il connettore.
   b. Immettere un nome per un nuovo account BlueXP o selezionare un account esistente.

      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

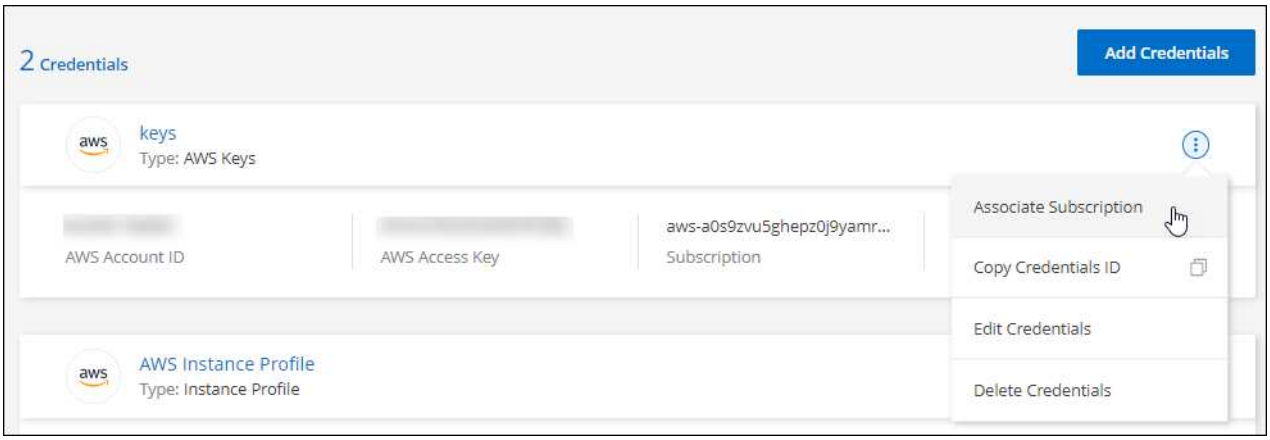
L'iscrizione a BlueXP implica l'associazione di un abbonamento Marketplace alle credenziali cloud associate a un connettore. Se hai seguito il flusso di lavoro "Get Started with Restricted mode" (inizia con la modalità limitata), dovresti già disporre di un connettore. Per ulteriori informazioni, consulta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

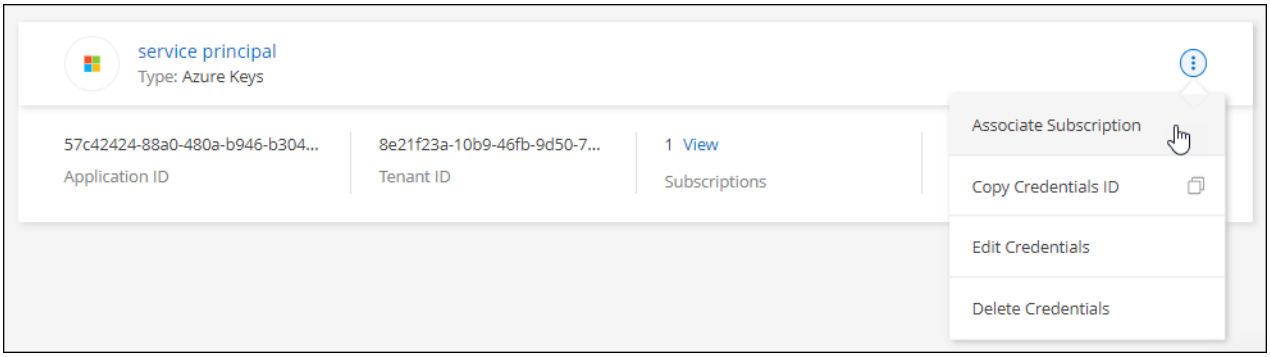
Iscriviti a BlueXP dal marketplace AWS

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**.

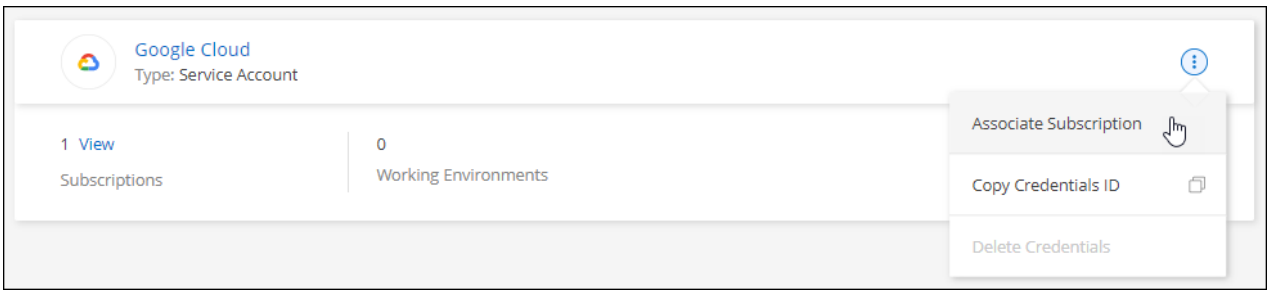
        Il seguente video mostra i passaggi per iscriversi a Azure Marketplace:

Iscriviti a BlueXP da Azure Marketplace

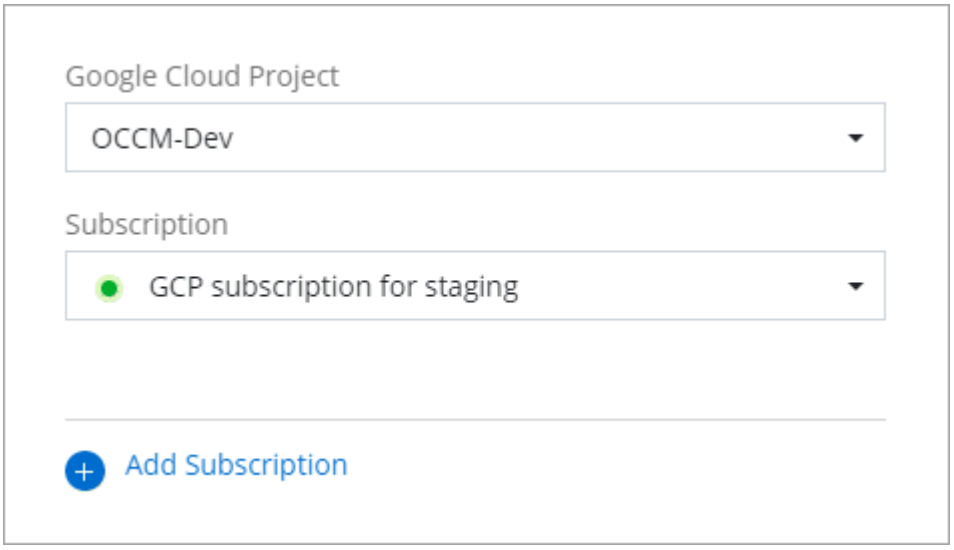
Google Cloud

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**.



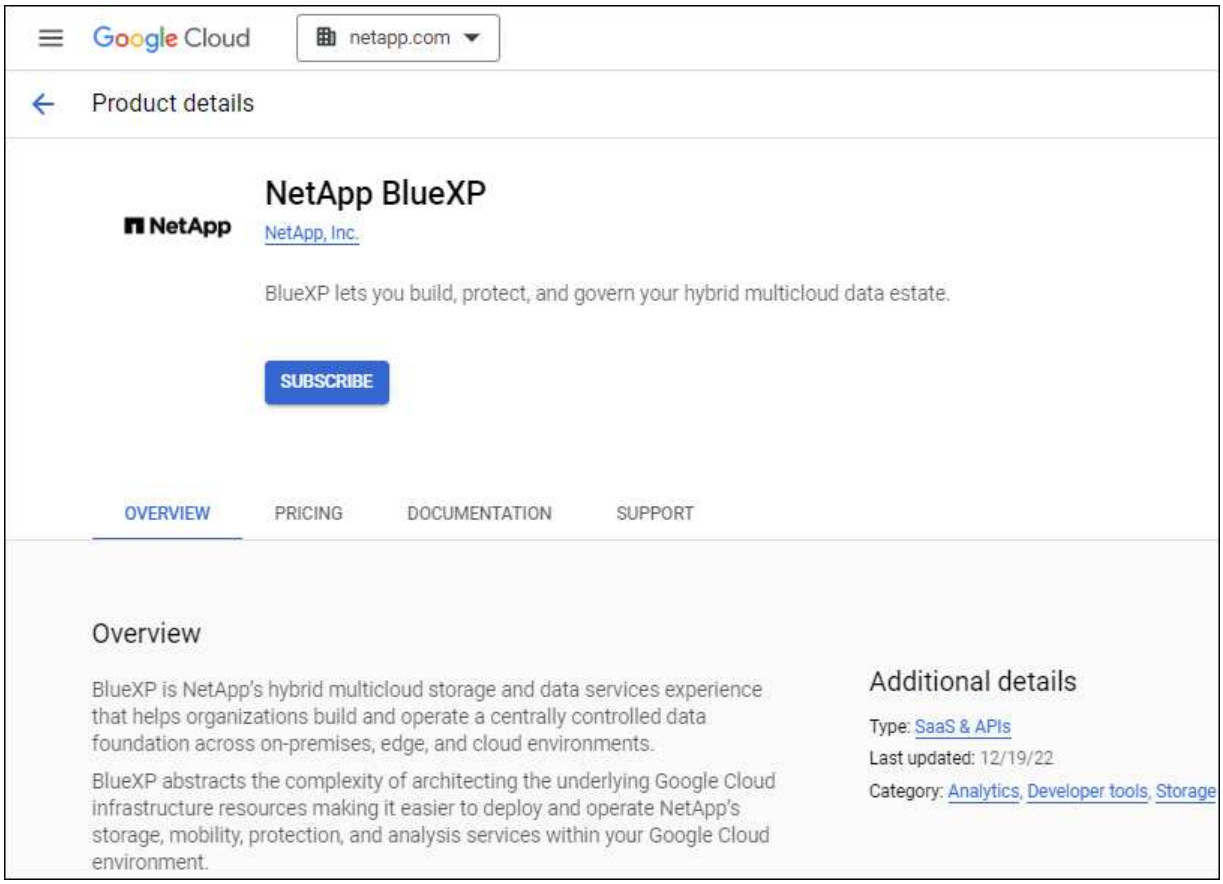
3. Per associare le credenziali a un abbonamento esistente, selezionare un progetto e un abbonamento Google Cloud dall'elenco a discesa, quindi selezionare **Associa**.



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**.

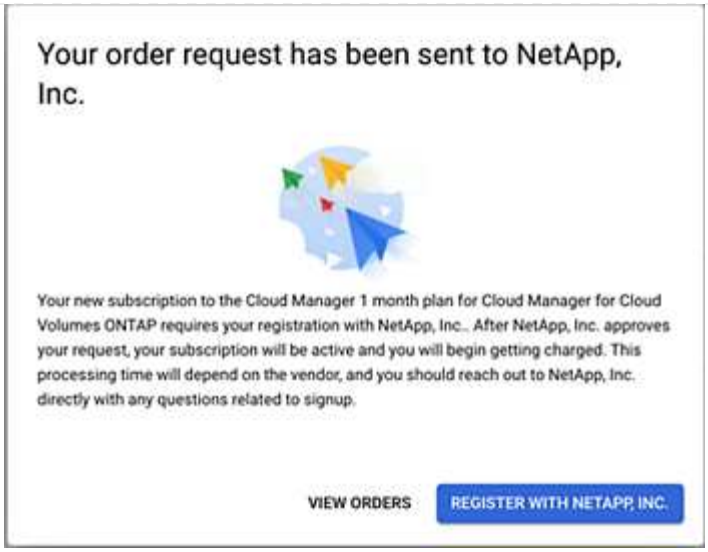
c. Selezionare l'account di fatturazione appropriato e accettare i termini e le condizioni.

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.

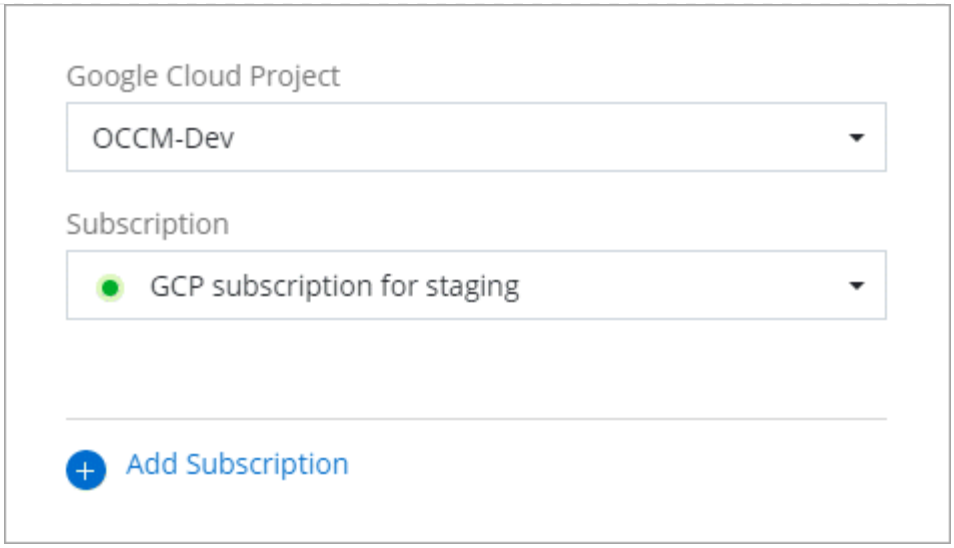
Per tutti gli altri account, è necessario associare manualmente l'abbonamento ripetendo questa procedura.

- 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

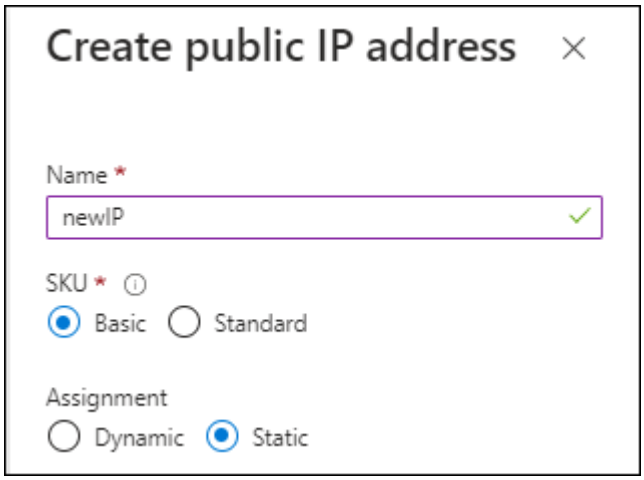
Il connettore contatta i seguenti endpoint per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

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.

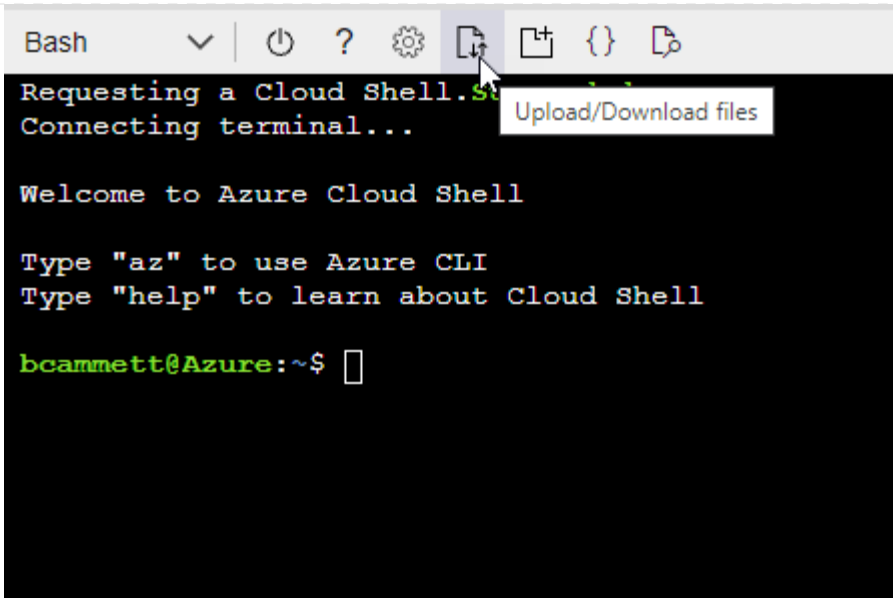
   Esempio

   ```
   "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

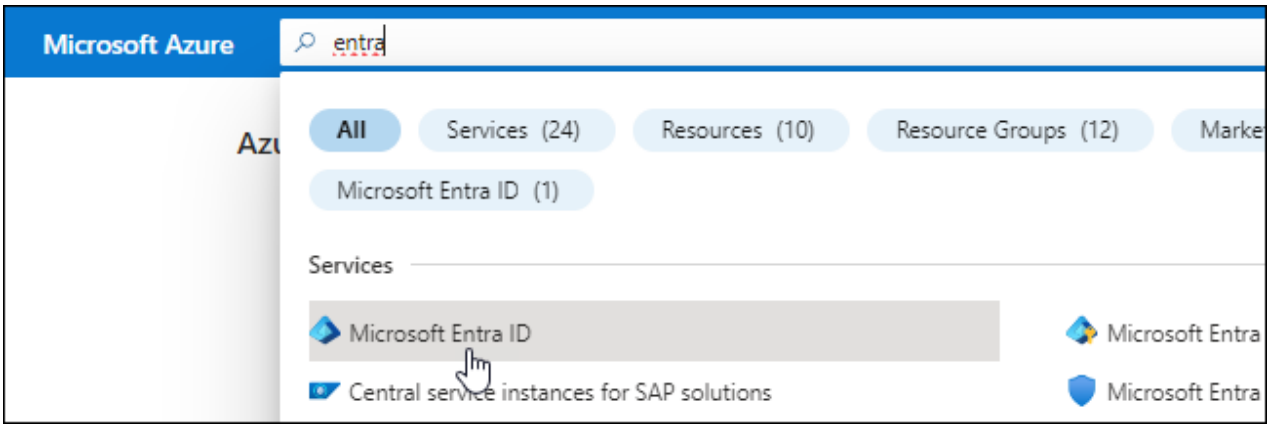
Creare e configurare un'entità di servizio in Microsoft Entra ID e ottenere le credenziali di Azure necessarie per BlueXP. È necessario fornire queste credenziali a BlueXP dopo aver installato il connettore e configurato BlueXP.

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.

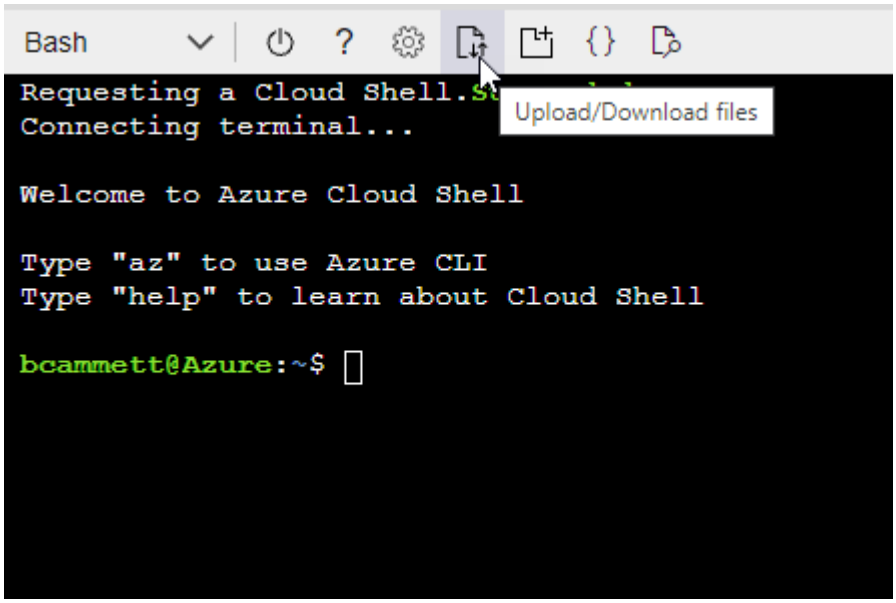
      Esempio

      ```
      "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:

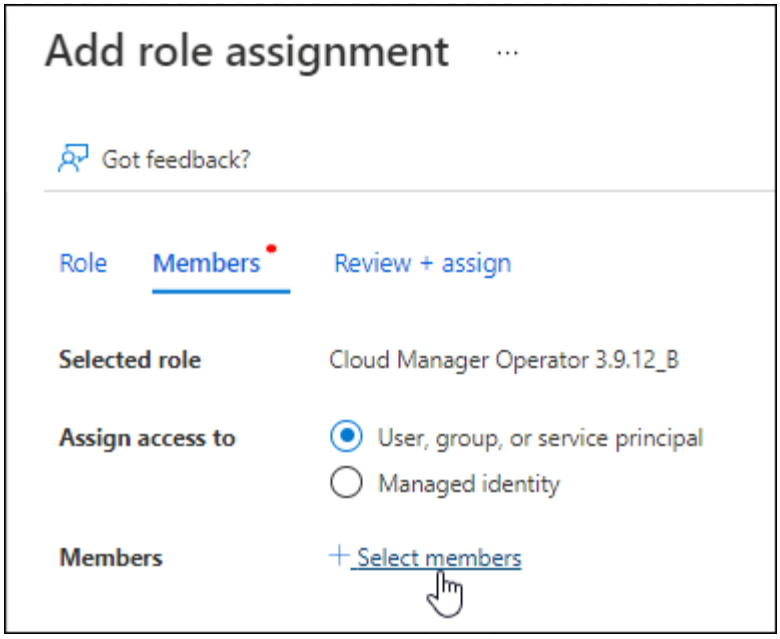
```
az role definition create --role-definition
Connector_Policy.json
```

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:

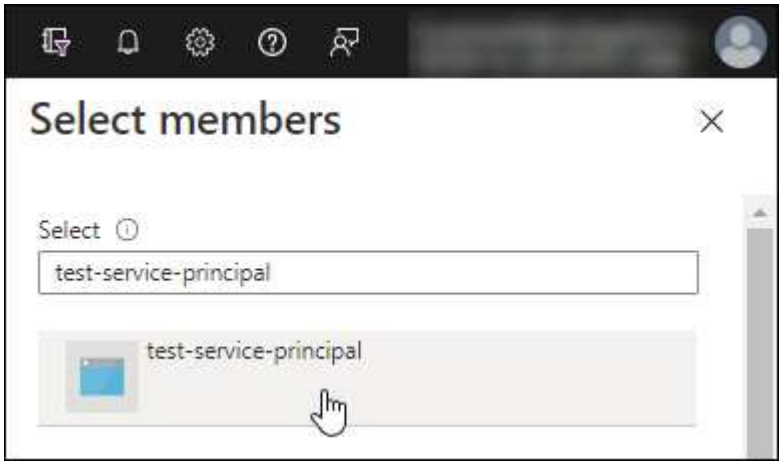
   a. Dal portale Azure, aprire il servizio **Subscriptions**.
   b. Selezionare l'abbonamento.
   c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.
   d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.
   e. Nella scheda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

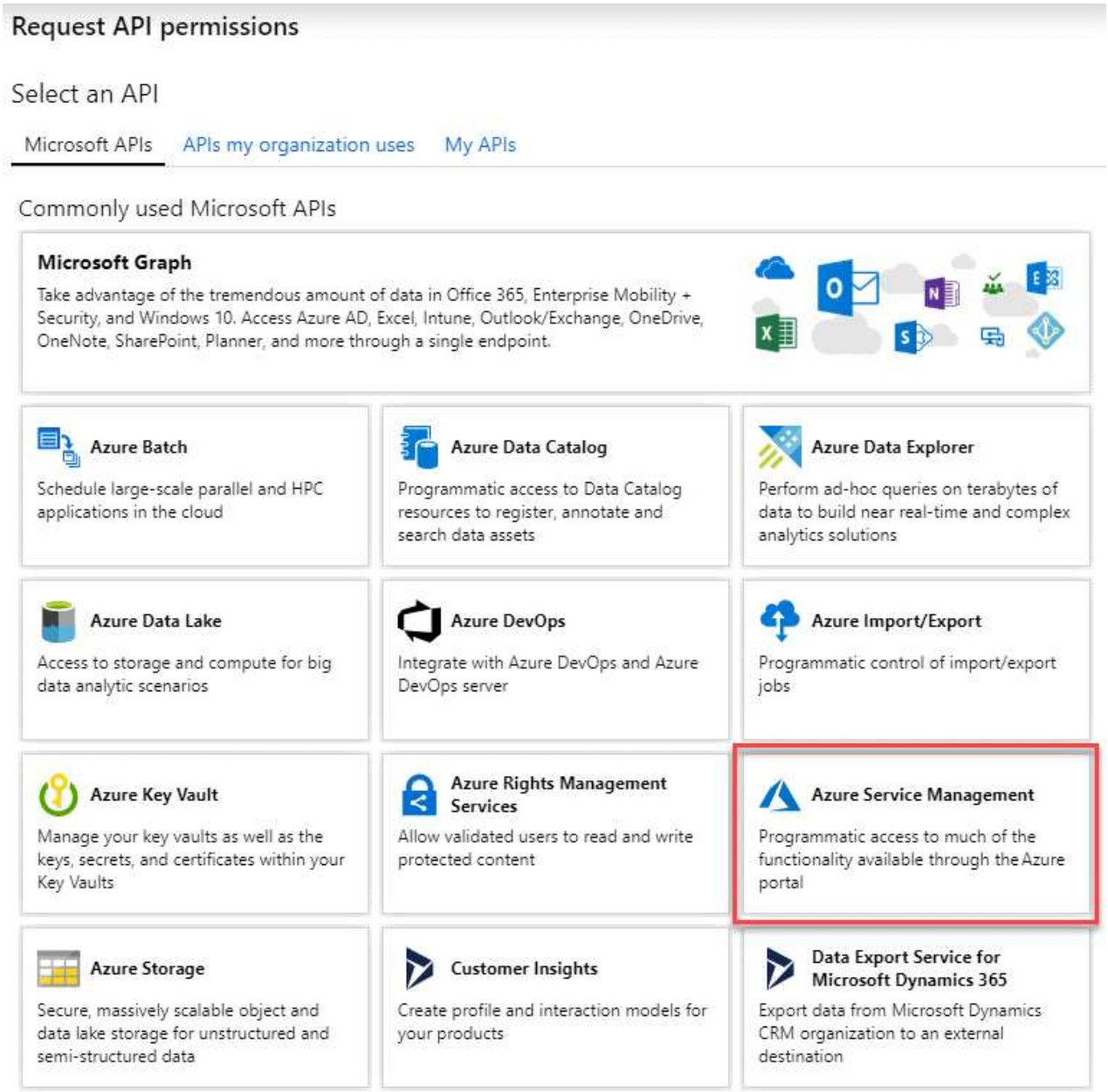
L'entità del servizio dispone ora delle autorizzazioni Azure necessarie per implementare il connettore.

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.

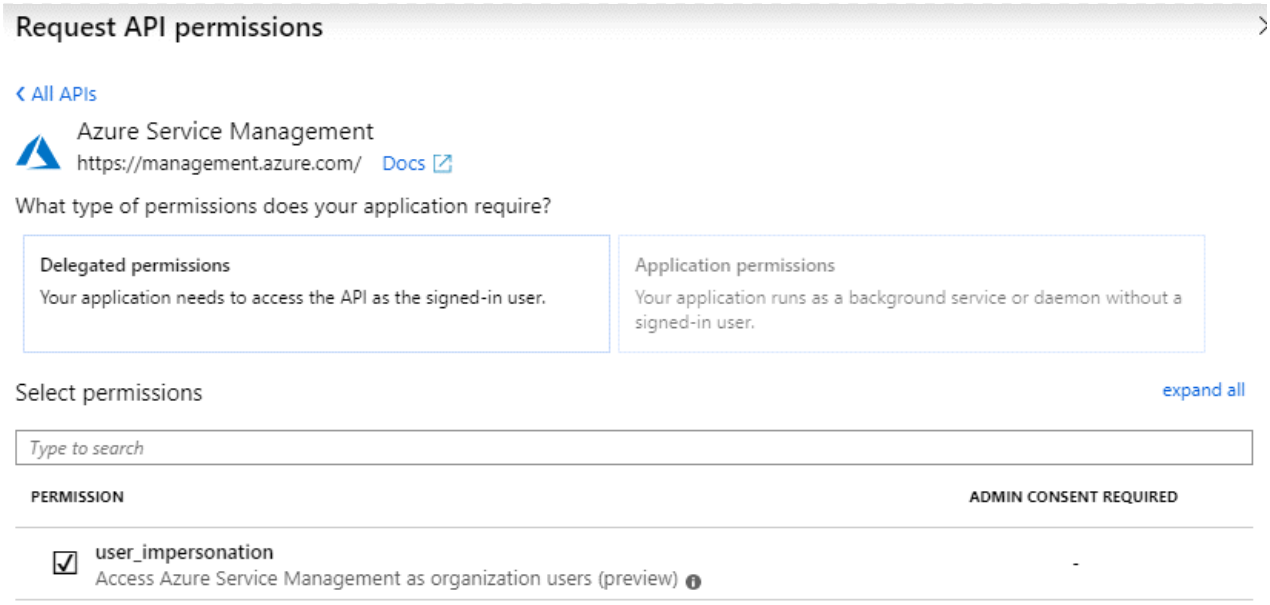
Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

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**.

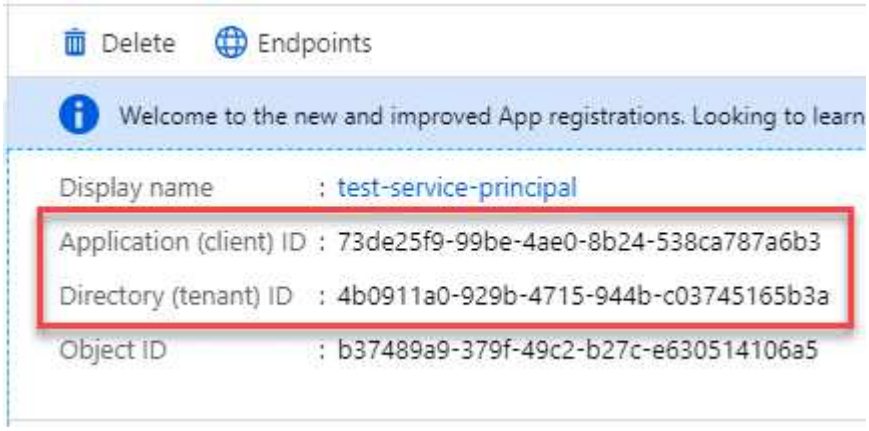


4. Selezionare **Access Azure Service Management as organization users** (accesso a Azure Service Management come utenti dell'organizzazione), quindi selezionare **Add permissions** (Aggiungi autorizzazioni).



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.

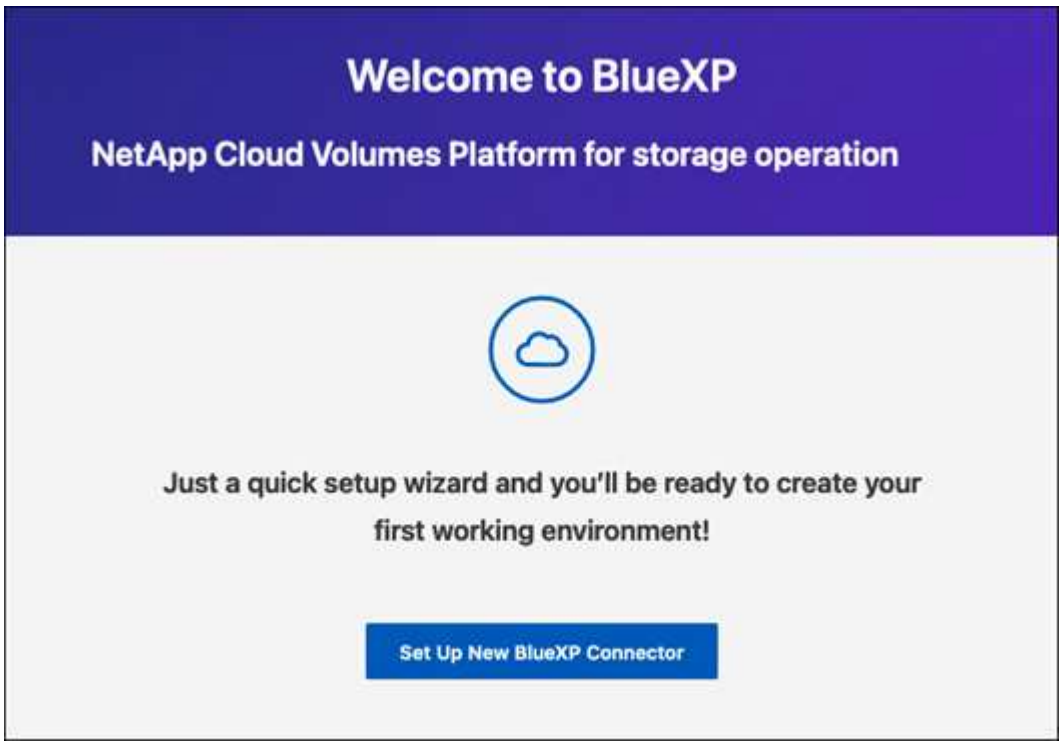
Fase 2: Configurare BlueXP

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

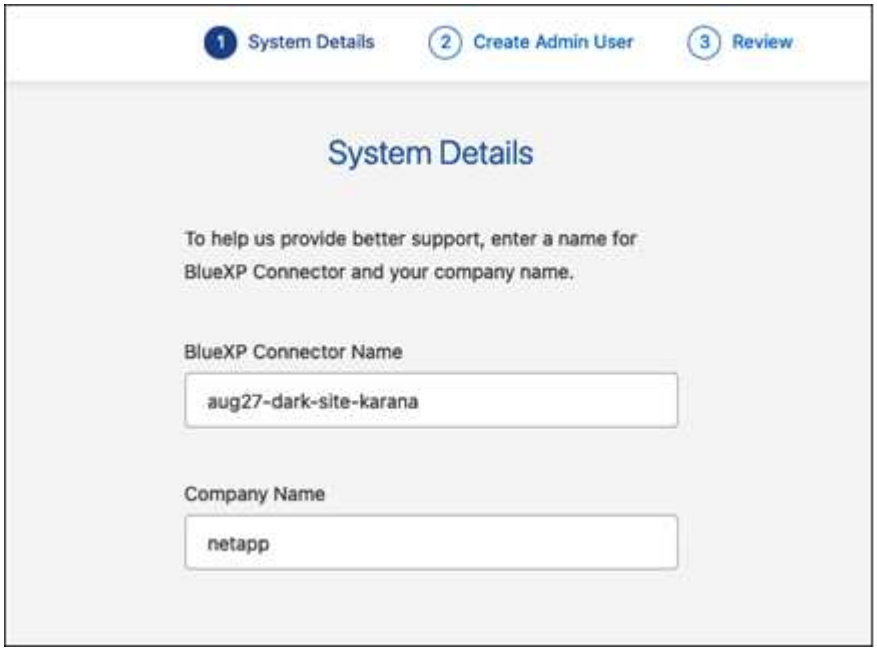
Fasi

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.

Amministrare BlueXP

Utilizzo della federazione delle identità con BlueXP

Identity Federation abilita il single sign-on con BlueXP, in modo che gli utenti possano accedere utilizzando le credenziali della tua identità aziendale. Per iniziare, scopri come funziona la federazione delle identità con BlueXP e consulta una panoramica del processo di installazione.

Federazione di identità con credenziali NSS

Se si utilizzano le credenziali NetApp Support Site (NSS) per accedere a BlueXP, non seguire le istruzioni riportate in questa pagina per configurare la federazione delle identità. Si consiglia di eseguire le seguenti operazioni:

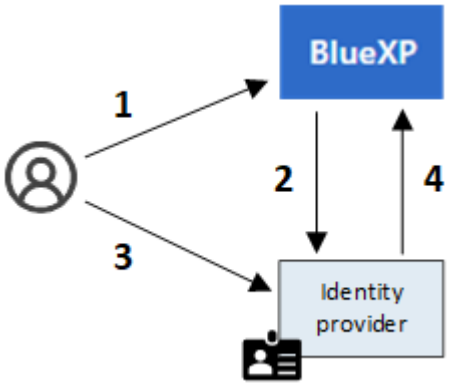
- Scaricare e completare il "Modulo di richiesta della Federazione NetApp"
- Inviare il modulo all'indirizzo e-mail specificato nel modulo

Il team di gestione delle identità e degli accessi di NetApp esaminerà la tua richiesta.

Come funziona la federazione delle identità

L'impostazione della federazione delle identità crea una connessione trust tra il provider di servizi di autenticazione (auth0) di BlueXP e il provider di gestione delle identità.

La seguente immagine mostra il funzionamento della federazione di identità con BlueXP:



1. Un utente inserisce il proprio indirizzo e-mail nella pagina di accesso di BlueXP.
2. BlueXP identifica che il dominio di posta elettronica fa parte di una connessione federata e invia la richiesta di autenticazione al provider di identità utilizzando la connessione trusted.

   Quando si imposta una connessione federata, BlueXP utilizza sempre tale connessione federata per l'autenticazione.

3. L'utente esegue l'autenticazione utilizzando le credenziali della directory aziendale.
4. Il provider di identità autentica l'identità dell'utente e l'utente ha effettuato l'accesso a BlueXP.

Identity Federation utilizza standard aperti, come Security Assertion Markup Language 2.0 (SAML) e OpenID

Connect (OIDC).

Provider di identità supportati

BlueXP supporta i seguenti provider di identità:

- Provider di identità SAML (Security Assertion Markup Language)
- ID Microsoft Entra
- Active Directory Federation Services (ADFS)
- PingFederate

BlueXP supporta solo SSO avviato da service provider (SP-Initiated). SSO avviato dal provider di identità (avviato da IdP) non supportato.

Panoramica del processo di installazione

Prima di impostare una connessione tra BlueXP e il provider di gestione delle identità, è necessario comprendere i passaggi necessari per prepararsi di conseguenza.

Questi passaggi sono specifici per gli utenti che accedono a BlueXP utilizzando un login cloud NetApp. Se si utilizzano le credenziali NSS per accedere a BlueXP, Scopri come configurare la federazione delle identità con le credenziali NSS.

Provider di identità SAML

Ad alto livello, la configurazione di una connessione federata tra BlueXP e un provider di identità SAML include i seguenti passaggi:

Fase	Completato da	Descrizione
1	Amministratore di Active Directory (ad)	Configura il tuo provider di identità SAML per abilitare la federazione delle identità con BlueXP. Visualizza le istruzioni per il tuo provider di identità SAML: • "ADFS" • "OKTA" • "OneLogin" • "PingFederate" • "Salesforce" • "Siteminder" • "SSOCircle" Se il provider di identità non compare nell'elenco precedente, "seguire queste istruzioni generiche" Non completare i passaggi che descrivono come creare una connessione in auth0. La connessione verrà creata nel passaggio successivo.
2	Amministratore di BlueXP	Accedere alla "Pagina NetApp Federation Setup" E creare la connessione con BlueXP. Per completare questo passaggio, è necessario ottenere quanto segue dall'amministratore ad in merito al provider di identità: • URL di accesso • Un certificato di firma X509 (formato PEM o CER) • URL di disconnessione (opzionale) Dopo aver creato la connessione utilizzando queste informazioni, la pagina Federation Setup elenca i parametri che è possibile inviare all'amministratore di ad per completare la configurazione nel passaggio successivo. Prendere nota della data di scadenza del certificato. È necessario tornare alla pagina Federation Setup e aggiornare il certificato *prima* che scada. Questa è la tua responsabilità. BlueXP non tiene traccia della data di scadenza. È meglio collaborare con il tuo team ad per ricevere avvisi puntuali.
3	AD admin	Completare la configurazione sul provider di identità utilizzando i parametri mostrati nella pagina Federation Setup (impostazione federazione) al termine del passaggio 2.

Fase	Completato da	Descrizione
4	Amministratore di BlueXP	Verificare e attivare la connessione da "Pagina NetApp Federation Setup" Si noti che la pagina viene aggiornata tra il test della connessione e l'abilitazione della connessione.

ID Microsoft Entra

A un livello elevato, la configurazione di una connessione federata tra BlueXP e Microsoft Entra ID include i seguenti passaggi:

Fase	Completato da	Descrizione
1	AD admin	Configurare Microsoft Entra ID per abilitare la federazione delle identità con BlueXP. "Visualizzare le istruzioni per la registrazione dell'applicazione con Microsoft Entra ID" Non completare i passaggi che descrivono come creare una connessione in auth0. La connessione verrà creata nel passaggio successivo.
2	Amministratore di BlueXP	Accedere alla "Pagina NetApp Federation Setup" E creare la connessione con BlueXP. Per completare questo passaggio, è necessario ottenere quanto segue dall'amministratore di ad: • ID client • Valore segreto del client • Dominio Microsoft Entra ID Dopo aver creato la connessione utilizzando queste informazioni, la pagina Federation Setup elenca i parametri che è possibile inviare all'amministratore di ad per completare la configurazione nel passaggio successivo. Prendere nota della data di scadenza della chiave segreta. È necessario tornare alla pagina Federation Setup e aggiornare il certificato *prima* che scada. Questa è la tua responsabilità. BlueXP non tiene traccia della data di scadenza. È meglio collaborare con il tuo team ad per ricevere avvisi puntuali.
3	AD admin	Completare la configurazione in Microsoft Entra ID utilizzando i parametri mostrati nella pagina impostazione Federazione dopo aver completato il passaggio 2.

Fase	Completato da	Descrizione
4	Amministratore di BlueXP	Verificare e attivare la connessione da "Pagina NetApp Federation Setup" Si noti che la pagina viene aggiornata tra il test della connessione e l'abilitazione della connessione.

ADFS

Ad alto livello, la configurazione di una connessione federata tra BlueXP e ADFS include i seguenti passaggi:

Fase	Completato da	Descrizione
1	AD admin	Configurare il server ADFS per abilitare la federazione delle identità con BlueXP. "Visualizza le istruzioni per la configurazione del server ADFS con auth0"
2	Amministratore di BlueXP	Accedere alla "Pagina NetApp Federation Setup" E creare la connessione con BlueXP. Per completare questo passaggio, è necessario ottenere quanto segue dall'amministratore ad: L'URL del server ADFS o il file di metadati della federazione. Dopo aver creato la connessione utilizzando queste informazioni, la pagina Federation Setup elenca i parametri che è possibile inviare all'amministratore di ad per completare la configurazione nel passaggio successivo. Prendere nota della data di scadenza del certificato. È necessario tornare alla pagina Federation Setup e aggiornare il certificato *prima* che scada. Questa è la tua responsabilità. BlueXP non tiene traccia della data di scadenza. È meglio collaborare con il tuo team ad per ricevere avvisi puntuali.
3	AD admin	Completare la configurazione sul server ADFS utilizzando i parametri mostrati nella pagina Federation Setup (impostazione federazione) al termine del passaggio 2.
4	Amministratore di BlueXP	Verificare e attivare la connessione da "Pagina NetApp Federation Setup" Si noti che la pagina viene aggiornata tra il test della connessione e l'abilitazione della connessione.

PingFederate

Ad alto livello, la configurazione di una connessione federata tra BlueXP e un server PingFederate include i seguenti passaggi:

Fase	Completato da	Descrizione
1	AD admin	Configurare il server PingFederate per abilitare la federazione delle identità con BlueXP. "Visualizza le istruzioni per la creazione di una connessione" Non completare i passaggi che descrivono come creare una connessione in auth0. La connessione verrà creata nel passaggio successivo.
2	Amministratore di BlueXP	Accedere alla "Pagina NetApp Federation Setup" E creare la connessione con BlueXP. Per completare questo passaggio, è necessario ottenere quanto segue dall'amministratore di ad: • URL del server PingFederate • Un certificato di firma X509 (formato PEM o CER) Dopo aver creato la connessione utilizzando queste informazioni, la pagina Federation Setup elenca i parametri che è possibile inviare all'amministratore di ad per completare la configurazione nel passaggio successivo. Prendere nota della data di scadenza del certificato. È necessario tornare alla pagina Federation Setup e aggiornare il certificato *prima* che scada. Questa è la tua responsabilità. BlueXP non tiene traccia della data di scadenza. È meglio collaborare con il tuo team ad per ricevere avvisi puntuali.
3	AD admin	Completare la configurazione sul server PingFederate utilizzando i parametri mostrati nella pagina Federation Setup (impostazione federazione) al termine del passaggio 2.
4	Amministratore di BlueXP	Verificare e attivare la connessione da "Pagina NetApp Federation Setup" Si noti che la pagina viene aggiornata tra il test della connessione e l'abilitazione della connessione.

Aggiornamento di una connessione federated

Dopo che l'amministratore di BlueXP ha attivato una connessione, l'amministratore può aggiornare la connessione in qualsiasi momento da "Pagina NetApp Federation Setup"

Ad esempio, potrebbe essere necessario aggiornare la connessione caricando un nuovo certificato.

L'amministratore di BlueXP che ha creato la connessione è l'unico utente autorizzato che può aggiornare la connessione. Se desideri aggiungere altri amministratori, contatta il supporto NetApp.

BlueXP

Gestisci il tuo account BlueXP

Quando si crea un account BlueXP, questo include solo un singolo utente amministratore e un'area di lavoro. È possibile gestire l'account in base alle esigenze dell'organizzazione aggiungendo utenti, creando account di servizio per scopi di automazione, aggiungendo aree di lavoro e altro ancora.

"Scopri come funzionano gli account BlueXP".

Gestisci il tuo account con l'API tenancy

Se si desidera gestire le impostazioni dell'account inviando richieste API, è necessario utilizzare l'API *tenancy*. Questa API è diversa dall'API BlueXP, utilizzata per creare e gestire gli ambienti di lavoro Cloud Volumes ONTAP.

"Visualizzare gli endpoint per l'API tenancy"

Creare e gestire gli utenti

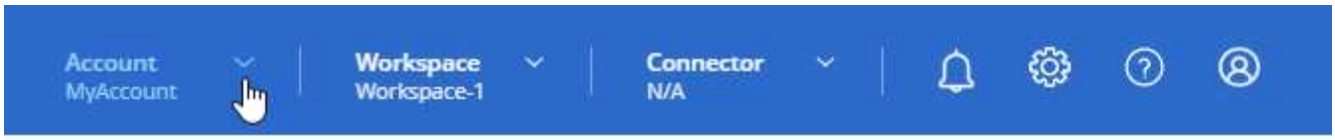
L'utente dell'account può accedere e gestire le risorse in aree di lavoro specifiche.

Aggiungere utenti

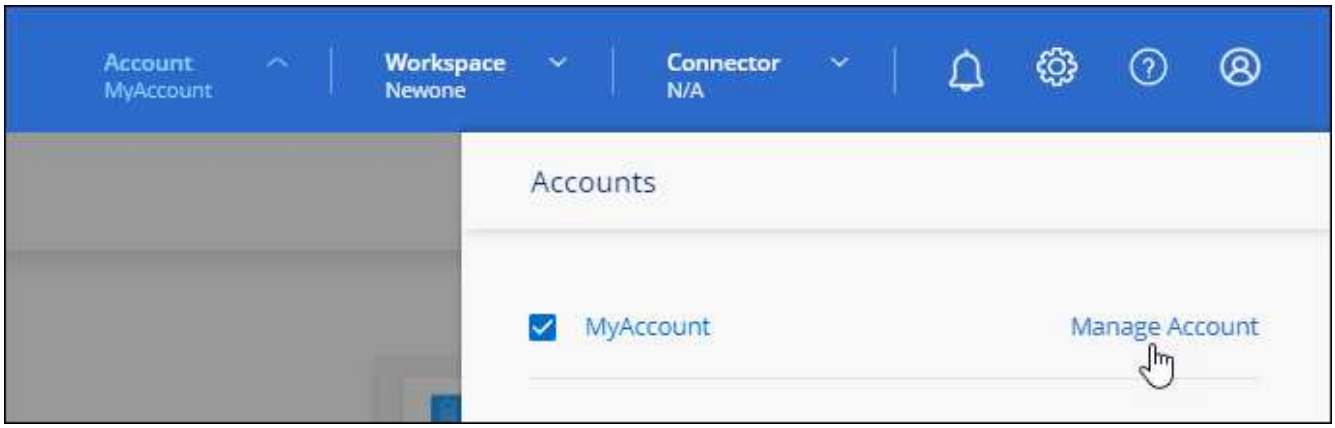
Associare gli utenti al proprio account BlueXP in modo che possano creare e gestire ambienti di lavoro in BlueXP.

Fasi

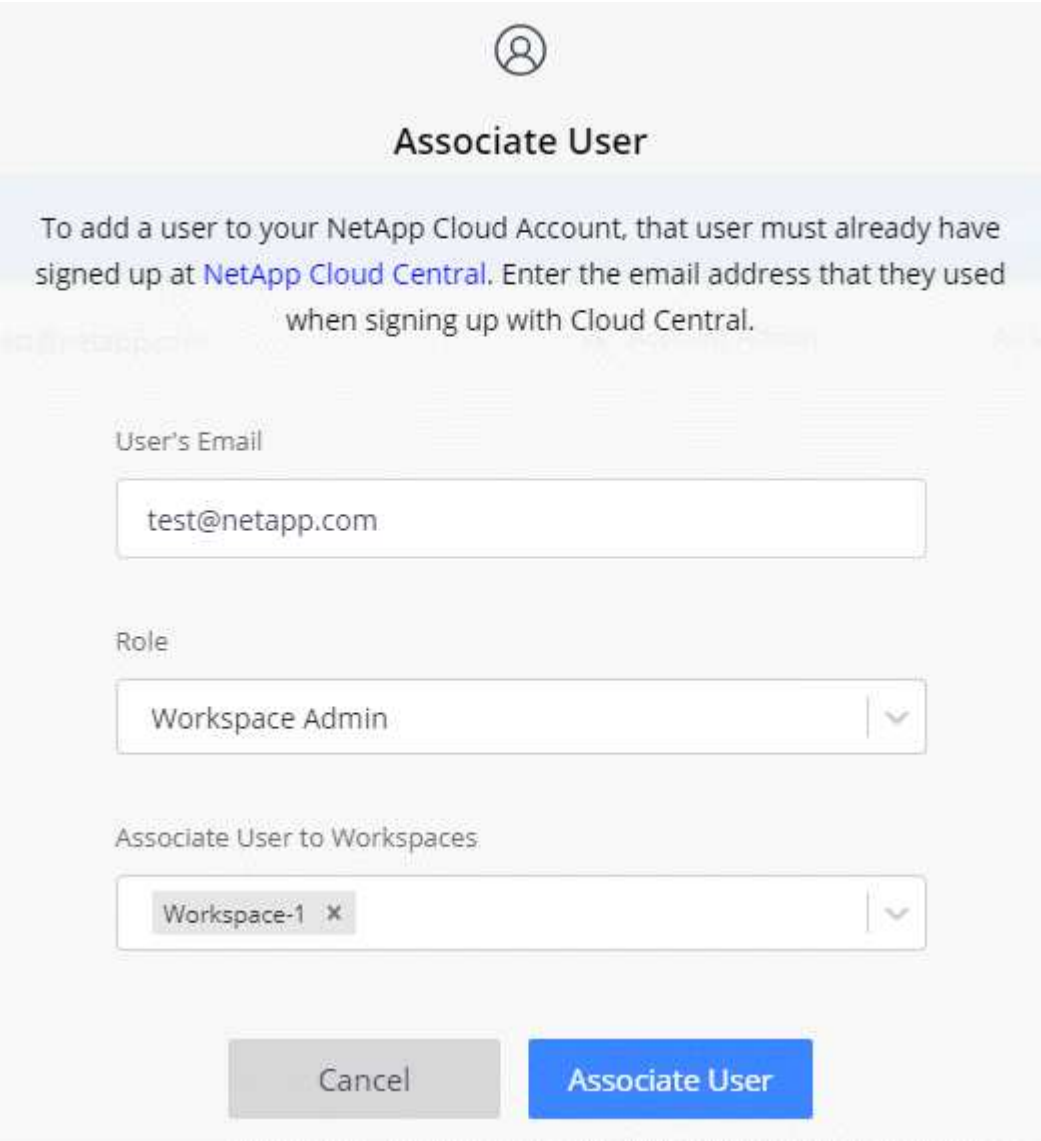
1. Se l'utente non l'ha già fatto, chiedere all'utente di accedere a. "Sito Web di NetApp BlueXP" e iscriverti.
2. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account**.



3. Selezionare **Manage account** (Gestisci account) accanto all'account attualmente selezionato.



4. Dalla scheda Members (membri), selezionare **associate User** (Associa utente).
5. Inserire l'indirizzo e-mail dell'utente e selezionare un ruolo per l'utente:
   - **Account Admin**: Può eseguire qualsiasi azione in BlueXP.
   - **Workspace Admin**: Consente di creare e gestire le risorse nelle aree di lavoro assegnate.
   - **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.
6. Se si seleziona Workspace Admin (Amministratore area di lavoro) o Compliance Viewer (Visualizzatore conformità), selezionare una o più aree di lavoro da associare all'utente.



7. Selezionare **Associa**.

Risultato

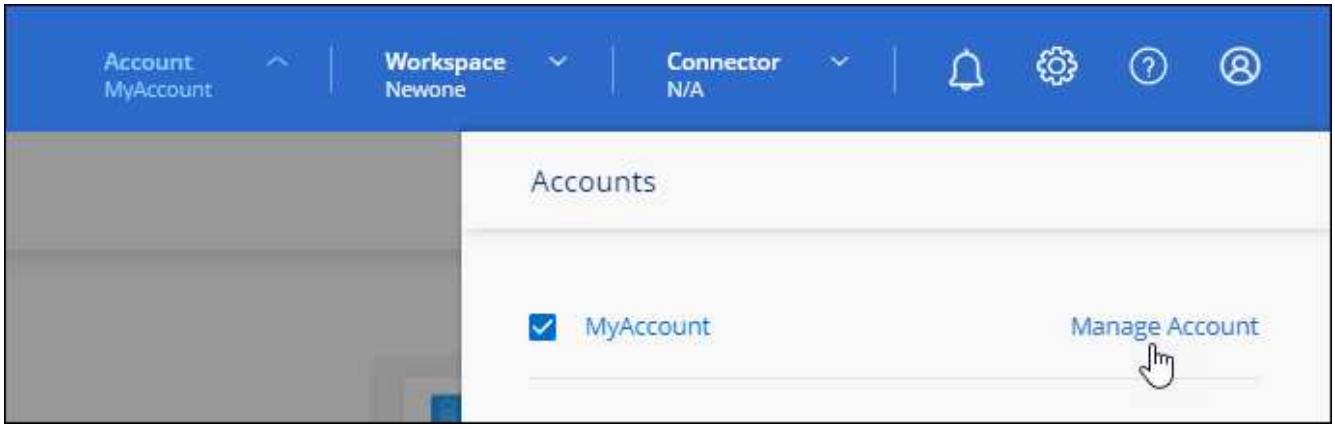
L'utente deve ricevere un'e-mail da NetApp BlueXP intitolata "account Association". L'e-mail include le informazioni necessarie per accedere a BlueXP.

Rimuovere gli utenti

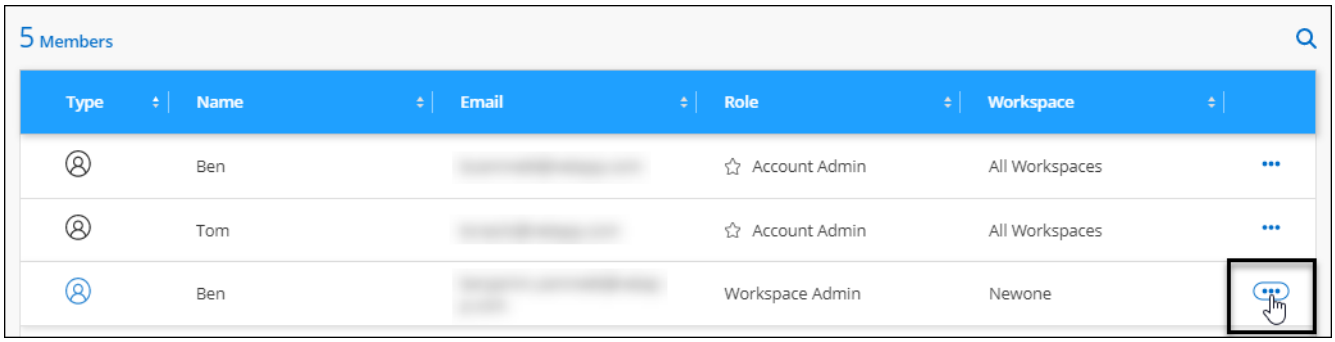
La disassociazione di un utente lo rende in modo che non possa più accedere alle risorse in un account BlueXP.

Fasi

1. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account** e selezionare **Gestisci account**.



2. Dalla scheda membri, selezionare il menu delle azioni nella riga corrispondente all'utente.



3. Selezionare **dissocia utente** e selezionare **dissocia** per confermare.

Risultato

L'utente non può più accedere alle risorse di questo account BlueXP.

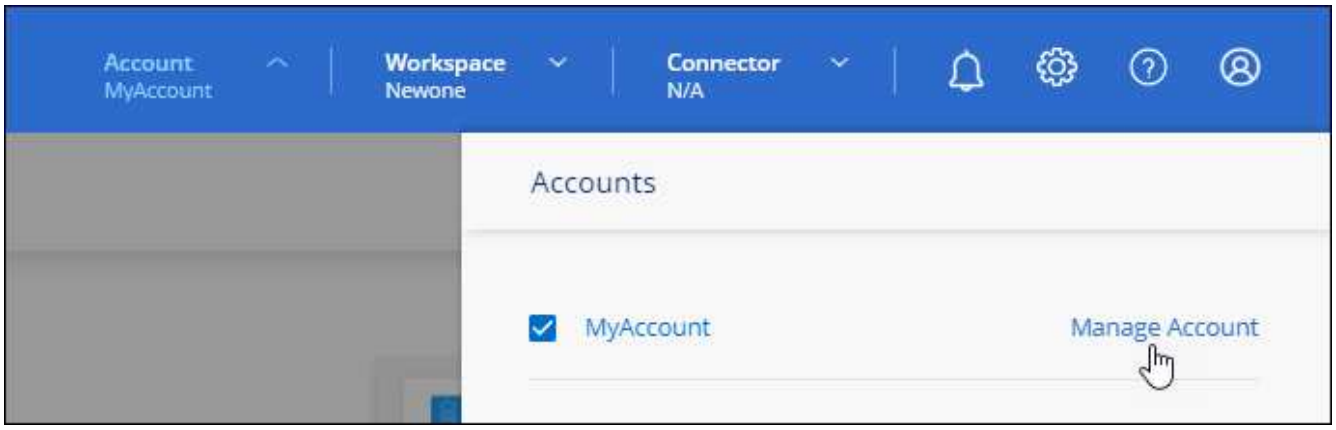
Gestire le aree di lavoro di un amministratore dell'area di lavoro

È possibile associare e disassociare gli amministratori Workspace alle aree di lavoro in qualsiasi momento. L'associazione dell'utente consente di creare e visualizzare gli ambienti di lavoro in tale area di lavoro.

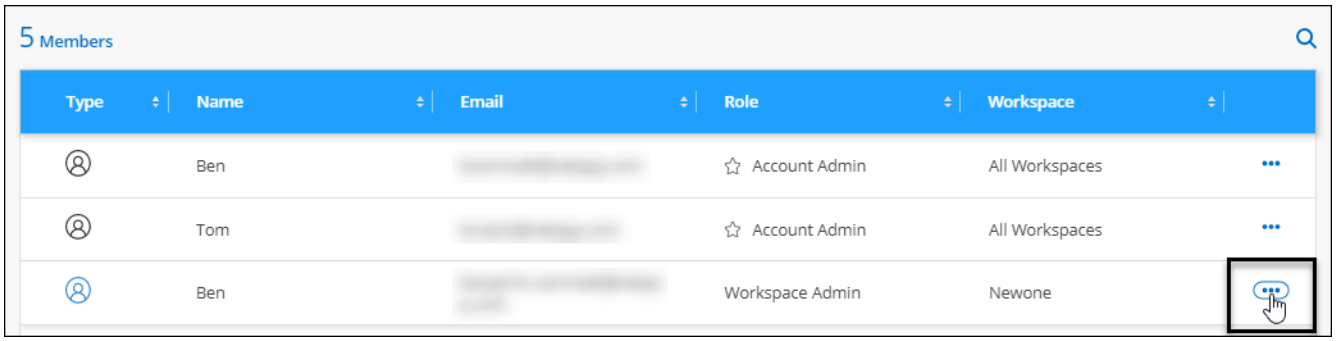
> Inoltre, è necessario associare il connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano accedervi da BlueXP. "Scopri come gestire le aree di lavoro di un connettore".

Fasi

1. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account** e selezionare **Gestisci account**.



2. Dalla scheda membri, selezionare il menu delle azioni nella riga corrispondente all'utente.



3. Selezionare **Gestisci aree di lavoro**.
4. Selezionare le aree di lavoro da associare all'utente e selezionare **Apply** (Applica).

Risultato

L'utente può ora accedere a tali aree di lavoro da BlueXP, purché il connettore sia stato associato anche alle aree di lavoro.

Creare e gestire gli account di servizio

Un account di servizio agisce come un "utente" che può effettuare chiamate API autorizzate a BlueXP per scopi di automazione. In questo modo è più semplice gestire l'automazione, poiché non è necessario creare script di automazione basati sull'account utente di una persona reale che può lasciare l'azienda in qualsiasi momento.

È possibile assegnare le autorizzazioni a un account di servizio assegnandolo un ruolo, proprio come qualsiasi altro utente BlueXP. È inoltre possibile associare l'account del servizio a aree di lavoro specifiche per controllare gli ambienti di lavoro (risorse) a cui il servizio può accedere.

Quando si crea l'account del servizio, BlueXP consente di copiare o scaricare un ID client e un segreto client per l'account del servizio. Questa coppia di chiavi viene utilizzata per l'autenticazione con BlueXP.

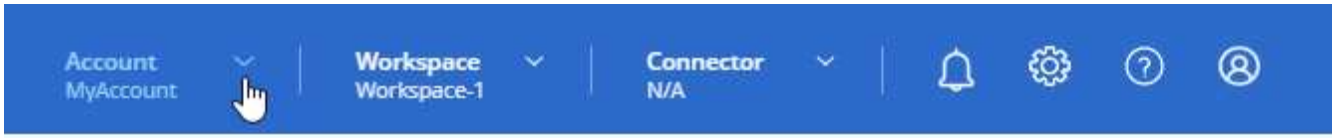
Tenere presente che non è necessario un token di aggiornamento per le operazioni API quando si utilizza un account di servizio. "Informazioni sui token di aggiornamento"

Creare un account di servizio

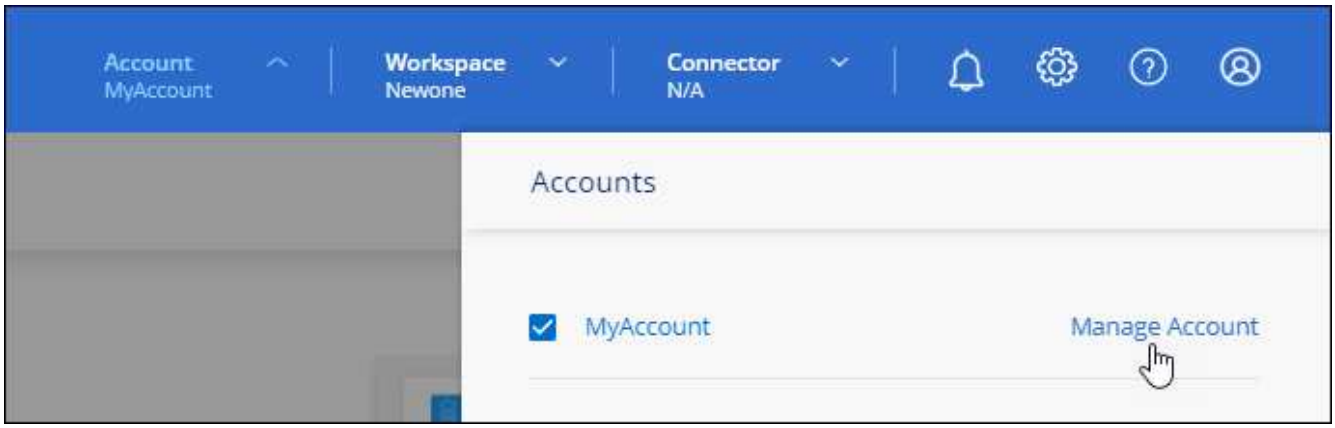
Creare tutti gli account di servizio necessari per gestire le risorse negli ambienti di lavoro.

Fasi

1. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account**.



2. Selezionare **Manage account** (Gestisci account) accanto all'account attualmente selezionato.



3. Dalla scheda membri, selezionare **Crea account di servizio**.
4. Inserire un nome e selezionare un ruolo. Se si sceglie un ruolo diverso da account Admin, scegliere lo spazio di lavoro da associare a questo account di servizio.
5. Selezionare **Crea**.
6. Copiare o scaricare l'ID client e il segreto client.

   Il segreto del client è visibile una sola volta e non viene memorizzato da BlueXP. Copia o scarica il segreto e conservalo in modo sicuro.

7. Selezionare **Chiudi**.

Ottenere un token bearer per un account di servizio

Per effettuare chiamate API a "API di tenancy", è necessario ottenere un token bearer per un account di servizio.

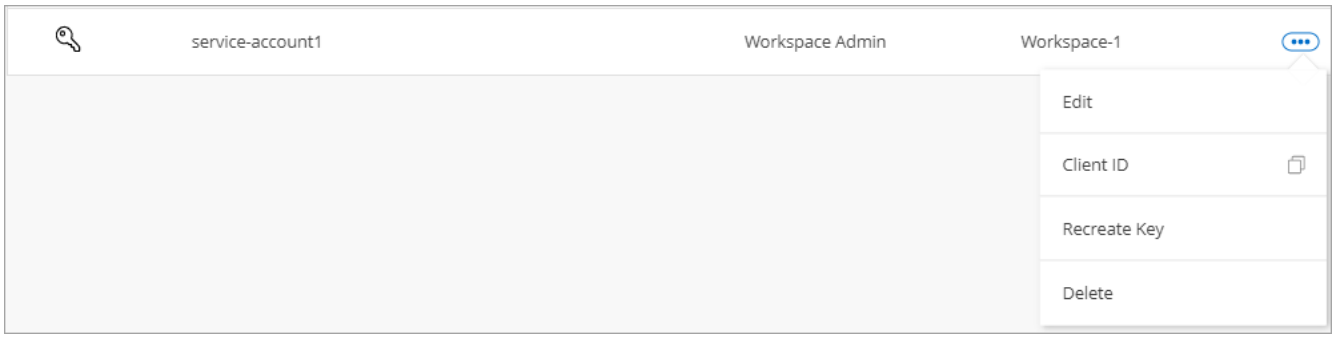
"Scopri come creare un token dell'account di servizio"

Copiare l'ID client

È possibile copiare l'ID client di un account di servizio in qualsiasi momento.

Fasi

1. Dalla scheda membri, selezionare il menu delle azioni nella riga corrispondente all'account del servizio.



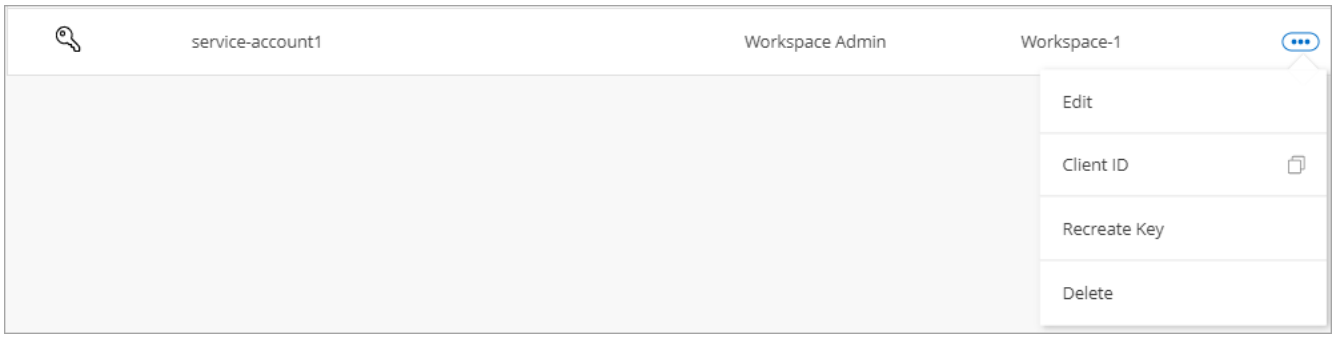
2. Selezionare **ID client**.
3. L'ID viene copiato negli Appunti.

Ricreare le chiavi

Ricreando la chiave si elimina la chiave esistente per questo account di servizio e si crea una nuova chiave. Non sarà possibile utilizzare la chiave precedente.

Fasi

1. Dalla scheda membri, selezionare il menu delle azioni nella riga corrispondente all'account del servizio.



2. Selezionare **Ricrea chiave**.
3. Selezionare **ricrea** per confermare.
4. Copiare o scaricare l'ID client e il segreto client.

   Il segreto del client è visibile una sola volta e non viene memorizzato da BlueXP. Copia o scarica il segreto e conservalo in modo sicuro.

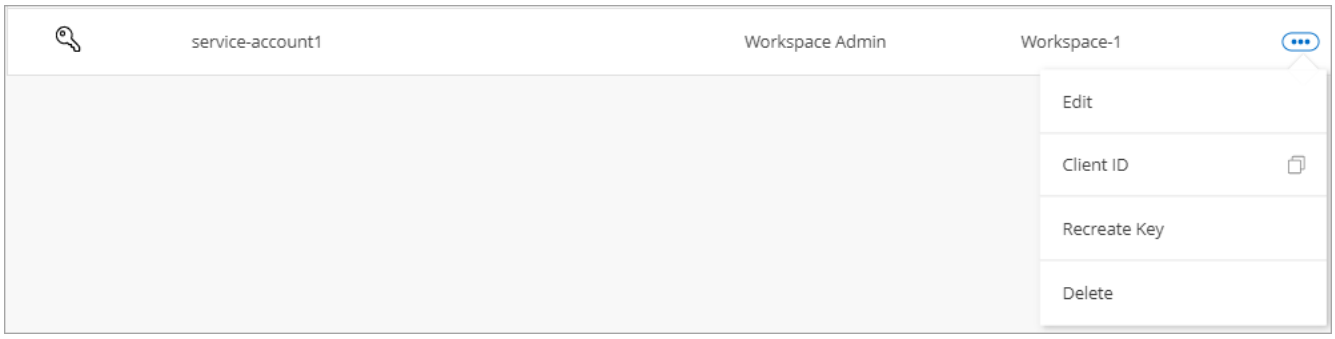
5. Selezionare **Chiudi**.

Eliminare un account di servizio

Eliminare un account di servizio se non è più necessario utilizzarlo.

Fasi

1. Dalla scheda membri, selezionare il menu delle azioni nella riga corrispondente all'account del servizio.



2. Selezionare **Delete** (Elimina).
3. Selezionare di nuovo **Delete** per confermare.

Gestire le aree di lavoro

Gestisci le tue aree di lavoro creando, rinominando ed eliminando le aree di lavoro. Nota: Non è possibile eliminare un'area di lavoro se contiene risorse. Deve essere vuoto.

Fasi

1. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account** e selezionare **Gestisci account**.
2. Selezionare **Workspaces**.
3. Scegliere una delle seguenti opzioni:
   - Selezionare **Add New Workspace** (Aggiungi nuova area di lavoro) per creare una nuova area di lavoro.
   - Selezionare **Rinomina** per rinominare l'area di lavoro.
   - Selezionare **Delete** (Elimina) per eliminare l'area di lavoro.

   Se è stata creata una nuova area di lavoro, è necessario aggiungere anche il connettore a tale area di lavoro. Se non si aggiunge il connettore, gli amministratori dell'area di lavoro non possono accedere alle risorse presenti nell'area di lavoro. Per ulteriori informazioni, fare riferimento alla sezione seguente.

Gestire le aree di lavoro di un connettore

È necessario associare il connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano accedervi da BlueXP.

Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in BlueXP per impostazione predefinita.

"Scopri di più su utenti, aree di lavoro e connettori".

Fasi

1. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account** e selezionare **Gestisci account**.
2. Selezionare **Connector**.
3. Selezionare **Manage Workspaces** (Gestisci aree di lavoro) per il connettore che si desidera associare.
4. Selezionare le aree di lavoro da associare al connettore e selezionare **Apply** (Applica).

Modificare il nome dell'account

Cambia il nome del tuo account in qualsiasi momento per modificarlo in qualcosa di significativo per te.

Fasi

1. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account** e selezionare **Gestisci account**.
2. Nella scheda **Panoramica**, selezionare l'icona di modifica accanto al nome dell'account.
3. Digitare un nuovo nome account e selezionare **Salva**.

Consenti anteprime private

Consenti anteprime private nel tuo account per accedere ai nuovi servizi resi disponibili come anteprima in BlueXP.

I servizi nell'anteprima privata non sono garantiti per comportarsi come previsto e potrebbero sostenere interruzioni e non avere funzionalità.

Fasi

1. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account** e selezionare **Gestisci account**.
2. Nella scheda **Panoramica**, attivare l'impostazione **Consenti anteprima privata**.

Consentire servizi di terze parti

Consentire ai servizi di terze parti presenti nell'account di accedere ai servizi di terze parti disponibili in BlueXP. I servizi di terze parti sono servizi cloud simili ai servizi offerti da NetApp, ma sono gestiti e supportati da aziende di terze parti.

Fasi

1. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account** e selezionare **Gestisci account**.
2. Nella scheda **Panoramica**, attivare l'impostazione **Consenti servizi di terze parti**.

Monitorare le operazioni nell'account

È possibile monitorare lo stato delle operazioni eseguite da BlueXP per verificare l'eventuale presenza di problemi da risolvere. È possibile visualizzare lo stato nel Centro notifiche, nella Timeline o inviare notifiche all'e-mail.

La seguente tabella fornisce un confronto tra il Centro notifiche e la cronologia, in modo da poter capire cosa offre ciascuno di essi.

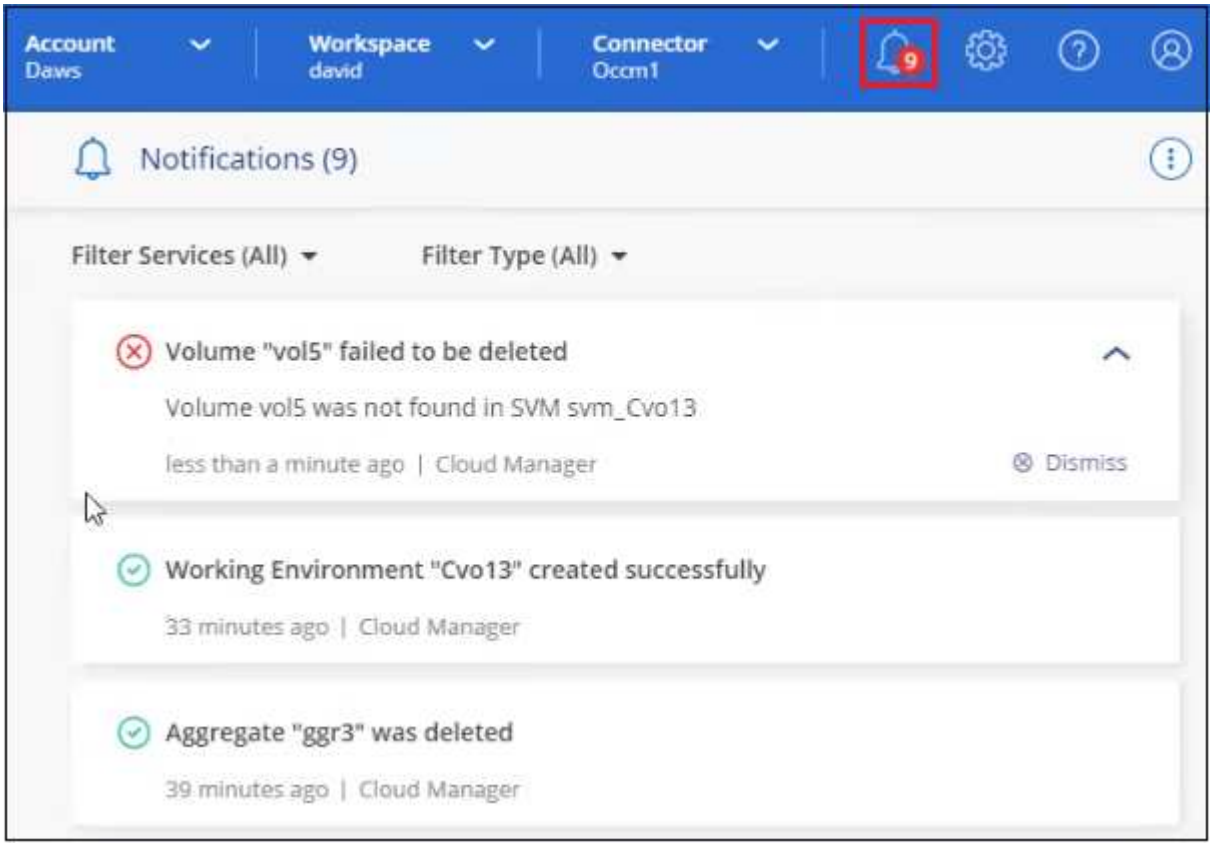
Centro notifiche	Tempistiche
Mostra lo stato di alto livello per eventi e azioni	Fornisce informazioni dettagliate su ciascun evento o azione per ulteriori indagini
Mostra lo stato della sessione di accesso corrente (le informazioni non vengono visualizzate nel Centro notifiche dopo la disconnessione)	Mantiene lo stato dell'ultimo mese
Mostra solo le azioni avviate nell'interfaccia utente	Mostra tutte le azioni dell'interfaccia utente o delle API
Mostra le azioni avviate dall'utente	Mostra tutte le azioni, avviate dall'utente o dal sistema

Centro notifiche	Tempistiche
Filtra i risultati in base all'importanza	Filtra per servizio, azione, utente, stato e altro ancora
Consente di inviare notifiche via email agli utenti account e ad altri utenti	Nessuna funzionalità di posta elettronica

Monitorare le attività utilizzando il Centro notifiche

Le notifiche tengono traccia dell'avanzamento delle operazioni avviate in BlueXP per verificare se l'operazione è stata eseguita correttamente. Consentono di visualizzare lo stato di molte azioni BlueXP avviate durante la sessione di accesso corrente. Attualmente non tutti i servizi BlueXP riportano informazioni nel Centro notifiche.

È possibile visualizzare le notifiche selezionando il campanello di notifica () nella barra dei menu. Il colore della piccola bolla nella campana indica la notifica di livello di severità più elevato attiva. Quindi, se vedi una bolla rossa, significa che c'è un'importante notifica che dovresti guardare.



È inoltre possibile configurare BlueXP in modo che invii determinati tipi di notifiche via email, in modo da essere informato di importanti attività del sistema anche quando non si è connessi al sistema. I messaggi di posta elettronica possono essere inviati a tutti gli utenti che fanno parte del tuo account BlueXP o a qualsiasi altro destinatario che deve essere a conoscenza di determinati tipi di attività del sistema. Scopri come consente di impostare le notifiche e-mail.

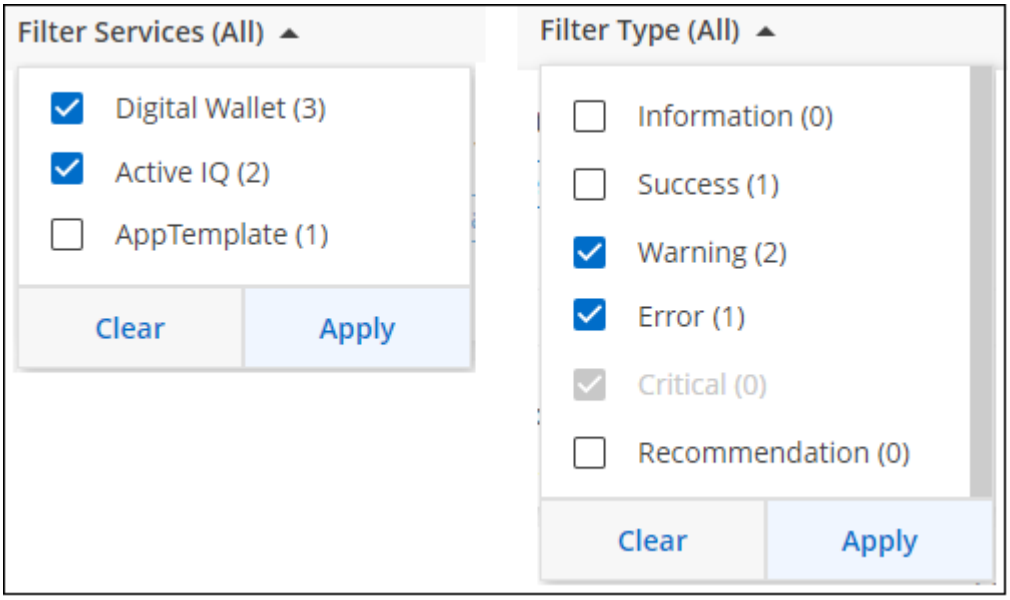
Tipi di notifica

Le notifiche sono classificate nelle seguenti categorie:

Tipo di notifica	Descrizione
Critico	Si è verificato un problema che potrebbe causare un'interruzione del servizio se non viene intrapresa immediatamente un'azione correttiva.
Errore	Un'azione o un processo terminano con un errore o potrebbero portare a un errore se non viene intrapresa un'azione correttiva.
Attenzione	Un problema di cui è necessario essere a conoscenza per assicurarsi che non raggiunga la severità critica. Le notifiche di questo livello di gravità non causano interruzioni del servizio e potrebbero non essere necessarie azioni correttive immediate.
Consiglio	Un consiglio di sistema per intraprendere un'azione per migliorare il sistema o un determinato servizio; ad esempio: Risparmio sui costi, suggerimenti per nuovi servizi, configurazione di sicurezza consigliata, ecc.
Informazioni	Messaggio che fornisce informazioni aggiuntive su un'azione o un processo.
Successo	Un'azione o un processo sono stati completati correttamente.

Filtra le notifiche

Per impostazione predefinita, tutte le notifiche attive vengono visualizzate nel Centro notifiche. È possibile filtrare le notifiche visualizzate in modo da visualizzare solo quelle importanti per l'utente. È possibile filtrare in base al "Servizio" BlueXP e alla notifica "tipo".



Ad esempio, se si desidera visualizzare solo le notifiche di "errore" e "Avviso" per le operazioni BlueXP, selezionare queste voci e verranno visualizzati solo i tipi di notifica.

Consente di chiudere le notifiche

Se non è più necessario visualizzarle, puoi rimuovere le notifiche dalla pagina. È possibile chiudere tutte le notifiche contemporaneamente oppure ignorare singole notifiche.

Per chiudere tutte le notifiche, nel Centro notifiche selezionare ⋮ E selezionare **Chiudi tutto**.

Per chiudere le singole notifiche, posizionare il cursore del mouse sulla notifica e selezionare **Dismiss** (Chiudi).

Consente di impostare le notifiche e-mail

È possibile inviare tramite e-mail tipi specifici di notifiche in modo da essere informati di importanti attività del sistema anche quando non si è connessi a BlueXP. I messaggi di posta elettronica possono essere inviati a tutti gli utenti che fanno parte del tuo account BlueXP o a qualsiasi altro destinatario che deve essere a conoscenza di determinati tipi di attività del sistema.

- Al momento, le notifiche vengono inviate via email per i seguenti servizi e funzionalità di BlueXP: Connettore, Digital Wallet di BlueXP, copia e sincronizzazione di BlueXP, backup e recovery di BlueXP, tiering di BlueXP e report di migrazione di BlueXP. Ulteriori servizi verranno aggiunti nelle versioni future.
- L'invio di notifiche e-mail non è supportato quando il connettore viene installato in un sito senza accesso a Internet.

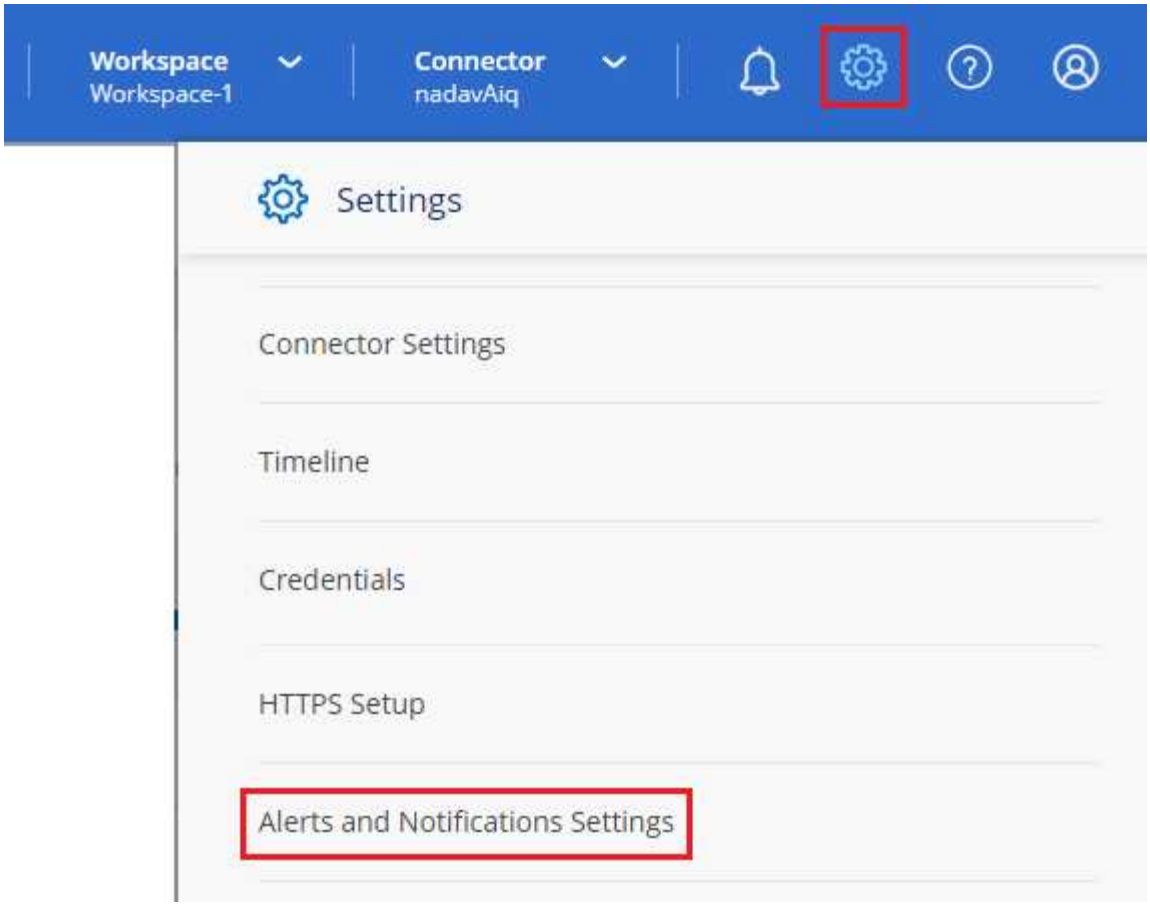
I filtri impostati nel Centro notifiche non determinano i tipi di notifiche che verranno inviate tramite e-mail. Per impostazione predefinita, gli account Admins di BlueXP riceveranno e-mail per tutte le notifiche "critiche" e "consigliate". Queste notifiche si applicano a tutti i servizi: Non è possibile scegliere di ricevere notifiche solo per alcuni servizi, ad esempio Connectors o BlueXP backup e recovery.

Tutti gli altri utenti e destinatari sono configurati per non ricevere alcuna email di notifica, pertanto dovrai configurare le impostazioni di notifica per eventuali utenti aggiuntivi.

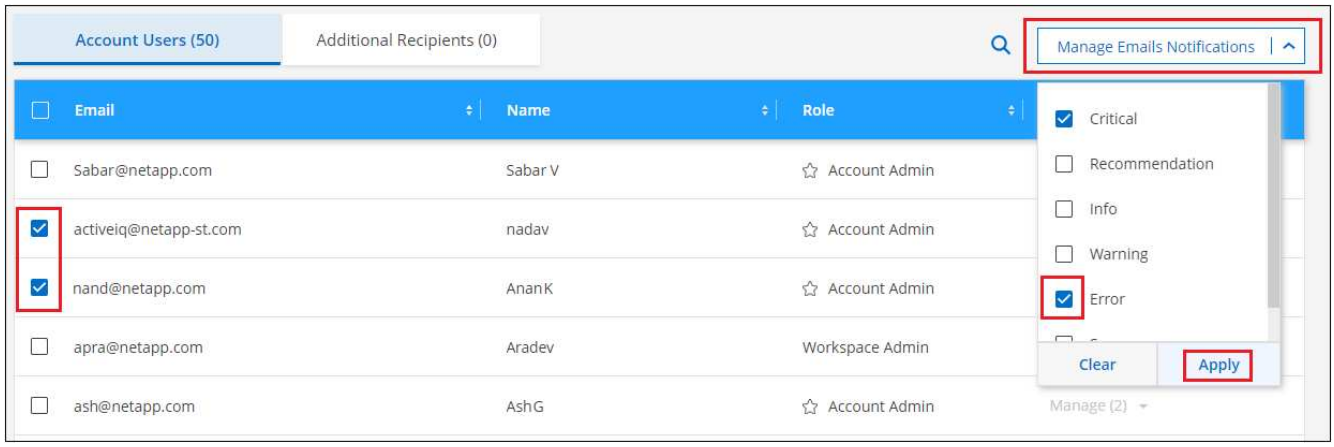
Per personalizzare le impostazioni delle notifiche, è necessario essere un amministratore dell'account.

Fasi

1. Dalla barra dei menu di BlueXP, selezionare **Impostazioni > Impostazioni avvisi e notifiche**.



2. Selezionare uno o più utenti dalla scheda *account Users* o dalla scheda *Additional Recipients* e scegliere il tipo di notifica da inviare:
   - Per apportare modifiche a un singolo utente, selezionare il menu nella colonna Notifiche dell'utente, selezionare i tipi di notifica da inviare e selezionare **Applica**.
   - Per apportare modifiche a più utenti, selezionare la casella corrispondente a ciascun utente, selezionare **Gestisci notifiche e-mail**, selezionare i tipi di notifiche da inviare e selezionare **Applica**.



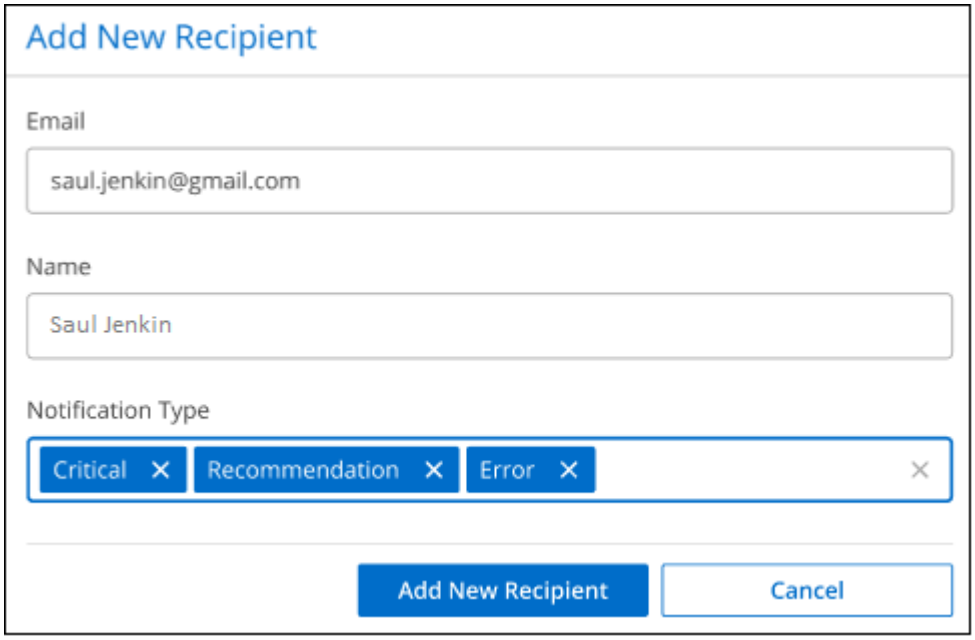
Aggiungere altri destinatari di posta elettronica

Gli utenti visualizzati nella scheda *account Users* vengono popolati automaticamente dagli utenti dell'account BlueXP (dal "Pagina Manage account (Gestisci account)"). È possibile aggiungere indirizzi e-mail nella scheda *destinatari aggiuntivi* per altre persone o gruppi che non hanno accesso a BlueXP, ma che devono essere

avvisati di determinati tipi di avvisi e notifiche.

Fasi

1. Dalla pagina Impostazioni avvisi e notifiche, selezionare **Aggiungi nuovi destinatari**.



2. Immettere il nome, l'indirizzo e-mail e selezionare i tipi di notifica che il destinatario riceverà, quindi selezionare **Aggiungi nuovo destinatario**.

Controllare l'attività dell'utente nell'account

La cronologia di BlueXP mostra le azioni che gli utenti hanno completato per gestire l'account. Ciò include azioni di gestione come l'associazione di utenti, la creazione di aree di lavoro, la creazione di connettori e altro ancora.

Controllare la cronologia può essere utile se è necessario identificare chi ha eseguito un'azione specifica o se è necessario identificare lo stato di un'azione.

Fasi

1. Dalla barra dei menu di BlueXP, selezionare **Impostazioni > Timeline**.
2. Nella sezione filtri, selezionare **Servizio**, attivare **locazione** e selezionare **Applica**.

Risultato

La cronologia viene aggiornata per mostrare le azioni di gestione dell'account.

Creare un altro account BlueXP

Quando ti iscrivi a BlueXP, ti viene richiesto di creare un account per la tua organizzazione. Questo account potrebbe essere tutto ciò di cui hai bisogno, ma se la tua azienda richiede più account, dovrai creare altri account utilizzando l'API tenancy.

Utilizzare la seguente chiamata API per creare un account BlueXP aggiuntivo:

POST `/tenancy/account/{accountName}`

Se si desidera attivare la modalità limitata, è necessario includere quanto segue nel corpo della richiesta:

```
{
  "isSaasDisabled": true
}
```

> Non è possibile modificare l'impostazione della modalità limitata 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. Deve essere impostato al momento della creazione dell'account.

"Scopri come utilizzare questa chiamata API"

Link correlati

- "Scopri di più sugli account BlueXP"
- "Scopri le modalità di implementazione di BlueXP"

Ruoli utente

I ruoli Amministratore account, Amministratore area di lavoro, Visualizzatore conformità e Amministratore SnapCenter forniscono autorizzazioni specifiche agli utenti. È possibile assegnare uno di questi ruoli quando si associa un nuovo utente all'account BlueXP.

Il ruolo Compliance Viewer è riservato all'accesso in sola lettura alla classificazione BlueXP.

Attività	Amministratore account	Amministratore dello spazio di lavoro	Compliance Viewer	Amministratore SnapCenter
Gestire gli ambienti di lavoro	Sì	Sì	No	No
Abilitare i servizi negli ambienti di lavoro	Sì	Sì	No	No
Rimuovere gli ambienti di lavoro da un'area di lavoro	Sì	Sì	No	No
Eliminare gli ambienti di lavoro	Sì	Sì	No	No
Visualizzare lo stato della replica dei dati	Sì	Sì	No	No
Visualizza la timeline	Sì	Sì	No	No
Passare da un'area di lavoro all'altra	Sì	Sì	Sì	No
Visualizzare i risultati della scansione di classificazione BlueXP	Sì	Sì	Sì	No

Attività	Amministratore account	Amministratore dello spazio di lavoro	Compliance Viewer	Amministratore SnapCenter
Ricevere il report Cloud Volumes ONTAP	Sì	No	No	No
Creare connettori	Sì	No	No	No
Gestire gli account BlueXP	Sì	No	No	No
Gestire le credenziali	Sì	No	No	No
Modificare le impostazioni di BlueXP	Sì	No	No	No
Visualizza e gestisci la dashboard di supporto	Sì	No	No	No
Installare un certificato HTTPS	Sì	No	No	No

Link correlati

- "Impostazione di aree di lavoro e utenti nell'account BlueXP"
- "Gestione delle aree di lavoro e degli utenti nell'account BlueXP"

Connettori

Individuare l'ID di sistema di un connettore

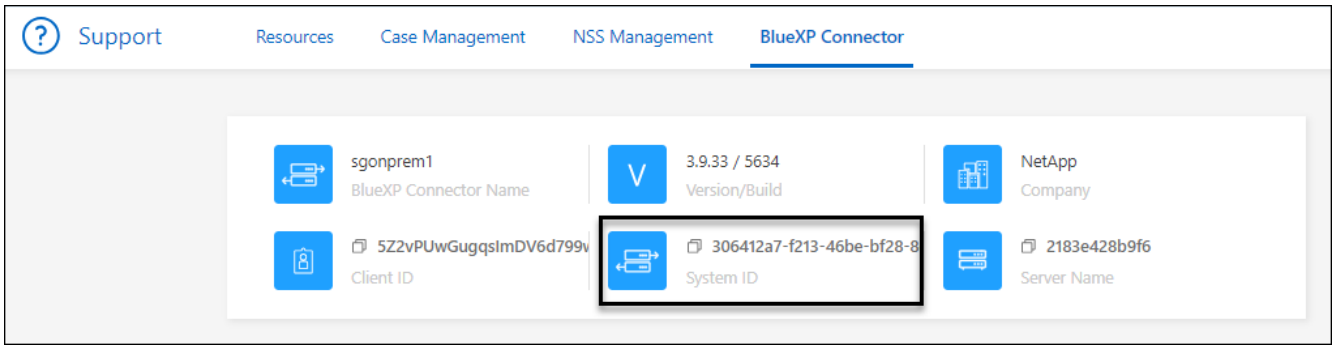
Per iniziare, il rappresentante NetApp potrebbe richiedere l'ID di sistema del connettore. L'ID viene generalmente utilizzato a scopo di licensing e troubleshooting.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida.
2. Selezionare **supporto > connettore BlueXP**.

   L'ID del sistema viene visualizzato nella parte superiore della pagina.

   Esempio



Gestire i connettori esistenti

Dopo aver creato un connettore, potrebbe essere necessario gestirlo ogni tanto. Ad esempio, se si dispone di più connettori, è possibile passare da un connettore all'altro. In alternativa, potrebbe essere necessario aggiornare manualmente il connettore quando si utilizza BlueXP in modalità privata.

"Scopri come funzionano i connettori".

> Il connettore include un'interfaccia utente locale, accessibile dall'host del connettore. Questa interfaccia utente è fornita per i clienti che utilizzano BlueXP in modalità limitata o privata. Quando si utilizza BlueXP in modalità standard, è necessario accedere all'interfaccia utente da "Console SaaS BlueXP"
>
> "Scopri le modalità di implementazione di BlueXP".

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".

Tipo di macchina virtuale o istanza

Se hai creato un connettore direttamente da BlueXP, BlueXP ha implementato un'istanza di macchina virtuale nel cloud provider utilizzando una configurazione predefinita. Dopo aver creato il connettore, non si dovrebbe passare a un'istanza VM più piccola con meno CPU o RAM.

I requisiti della CPU e della RAM sono i seguenti:

CPU
: 4 core o 4 vCPU

RAM
: 14 GB

"Informazioni sulla configurazione predefinita del connettore".

Visualizzare la versione di un connettore

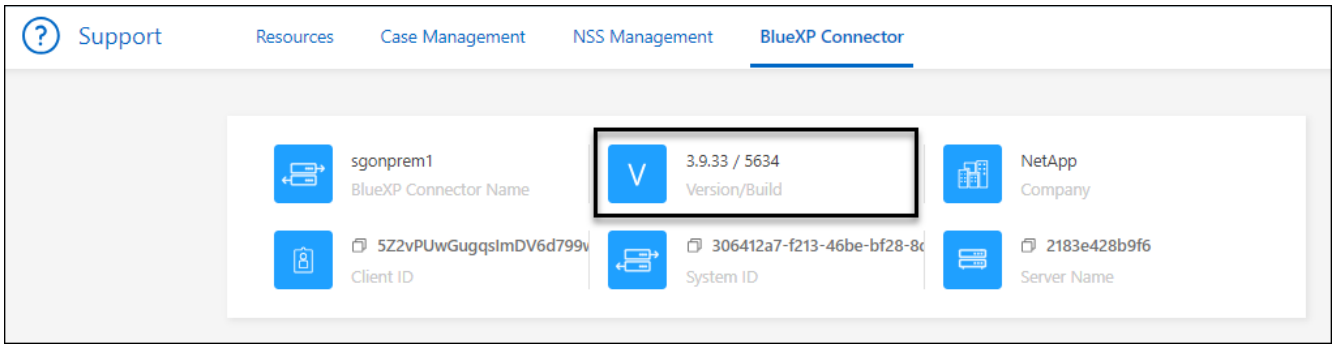
È possibile visualizzare la versione del connettore per verificare che il connettore sia stato aggiornato automaticamente alla versione più recente o perché è necessario condividerlo con il rappresentante NetApp.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida.

2. Selezionare **supporto > connettore BlueXP**.

   La versione viene visualizzata nella parte superiore della pagina.



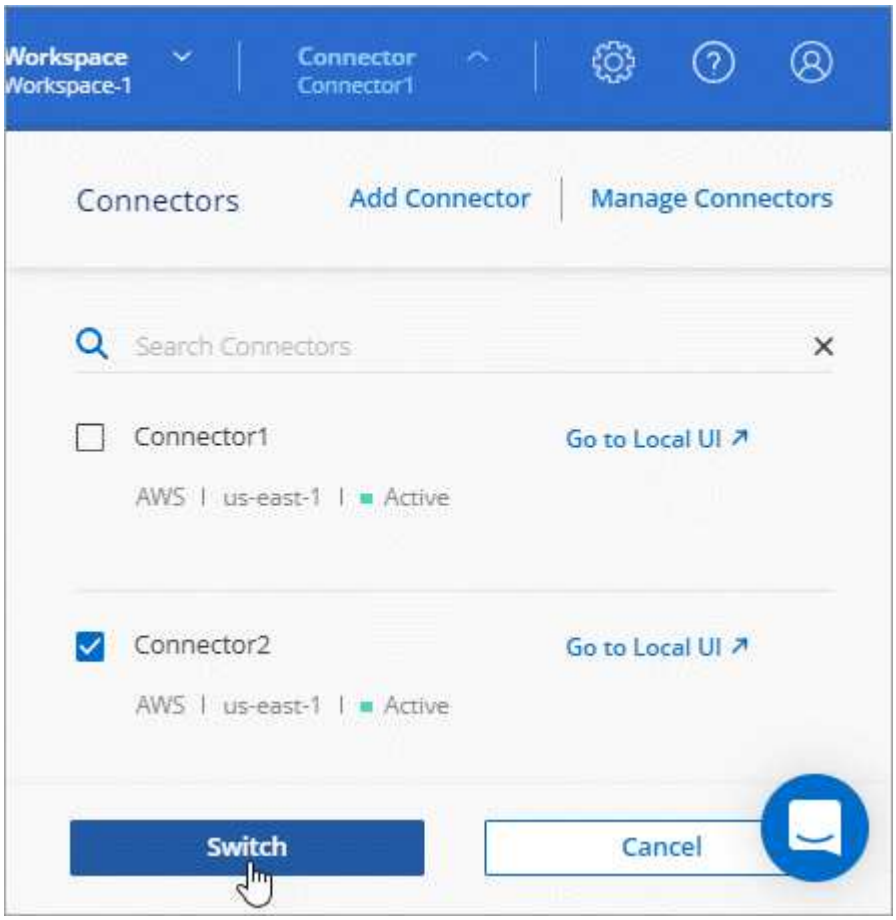
Passare da un connettore all'altro

Se si dispone di più connettori, è possibile passare da un connettore all'altro per visualizzare gli ambienti di lavoro associati a uno specifico connettore.

Ad esempio, supponiamo di lavorare in un ambiente multi-cloud. In AWS potrebbe essere presente un connettore e in Google Cloud un altro connettore. Per gestire i sistemi Cloud Volumes ONTAP in esecuzione in tali cloud, è necessario passare da un connettore all'altro.

Fase

1. Selezionare l'elenco a discesa **Connector**, selezionare un altro connettore, quindi **Switch**.



Risultato

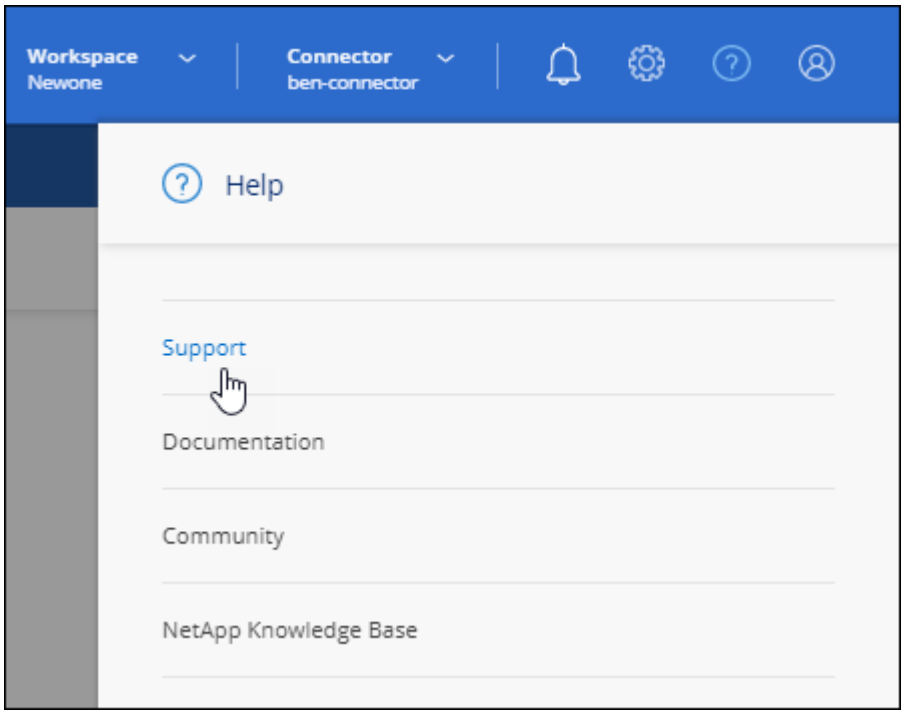
BlueXP aggiorna e mostra gli ambienti di lavoro associati al connettore selezionato.

Scaricare o inviare un messaggio AutoSupport

In caso di problemi, il personale NetApp potrebbe richiedere di inviare un messaggio AutoSupport al supporto NetApp per la risoluzione dei problemi.

Fasi

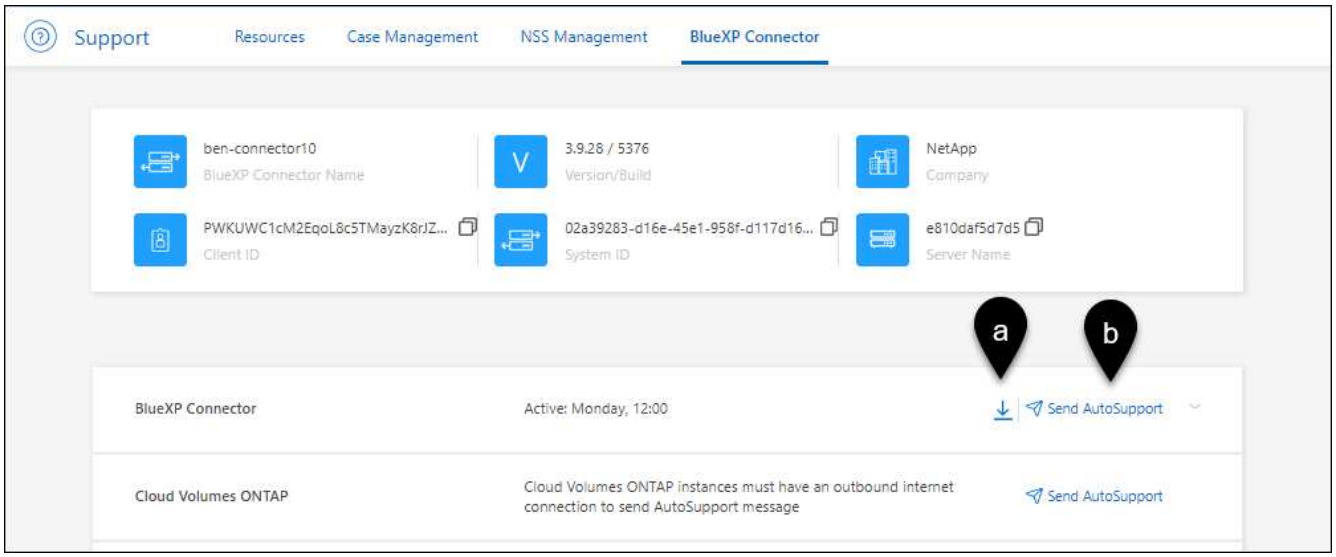
1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Selezionare **BlueXP Connector**.
3. A seconda della modalità di invio delle informazioni al supporto NetApp, scegliere una delle seguenti opzioni:

   a. Selezionare l'opzione per scaricare il messaggio AutoSupport sul computer locale. Puoi quindi inviarla al supporto NetApp utilizzando un metodo preferito.

   b. Selezionare **Send AutoSupport** (Invia messaggio) per inviare direttamente il messaggio al supporto NetApp.



Connettersi alla macchina virtuale Linux

Per connettersi alla macchina virtuale Linux su cui viene eseguito il connettore, è possibile utilizzare le opzioni di connettività disponibili presso il provider di servizi cloud.

AWS

Quando è stata creata l'istanza del connettore in AWS, sono stati forniti una chiave di accesso AWS e una chiave segreta. È possibile utilizzare questa coppia di chiavi per SSH all'istanza. Il nome utente per l'istanza EC2 Linux è ubuntu (per i connettori creati prima di maggio 2023, il nome utente era EC2-user).

"AWS Docs (documenti AWS): Connettersi all'istanza di Linux"

Azure

Quando è stata creata la Connector VM in Azure, è stato specificato un nome utente e si è scelto di autenticarsi con una password o una chiave pubblica SSH. Utilizzare il metodo di autenticazione scelto per la connessione alla macchina virtuale.

"Azure Docs: SSH nella macchina virtuale"

Google Cloud

Non è possibile specificare un metodo di autenticazione quando si crea un connettore in Google Cloud. Tuttavia, è possibile connettersi all'istanza di Linux VM utilizzando Google Cloud Console o Google Cloud CLI (gcloud).

"Google Cloud Docs: Connessione a macchine virtuali Linux"

Richiedi l'utilizzo di IMDSv2 sulle istanze di Amazon EC2

A partire da marzo 2024, BlueXP ora supporta Amazon EC2 Instance Metadata Service versione 2 (IMDSv2) con connettore e Cloud Volumes ONTAP (incluso il mediatore per le implementazioni ha). Nella maggior parte dei casi, IMDSv2 viene configurato automaticamente sulle nuove istanze EC2. IMDSv1 è stato abilitato prima di marzo 2024. Se richiesto dai criteri di protezione, potrebbe essere necessario configurare manualmente IMDSv2 sulle istanze EC2.

A proposito di questa attività

IMDSv2 fornisce una maggiore protezione contro le vulnerabilità. "Scopri di più su IMDSv2 dal blog sulla

sicurezza AWS"

Il servizio IMDS (Instance Metadata Service) viene attivato come segue nelle istanze EC2:

- Per implementazioni di nuovi connettori da BlueXP o che utilizzano "Script di terraform", IMDSv2 è attivato per impostazione predefinita nell'istanza EC2.
- Se si avvia una nuova istanza EC2 in AWS e quindi si installa manualmente il software del connettore, anche IMDSv2 viene attivato per impostazione predefinita.
- Se si avvia il connettore da AWS Marketplace, IMDSv1 viene attivato per impostazione predefinita. È possibile configurare manualmente IMDSv2 sull'istanza EC2.
- Per i connettori esistenti, IMDSv1 è ancora supportato, ma è possibile configurare manualmente IMDSv2 sull'istanza EC2, se si preferisce.
- Per Cloud Volumes ONTAP, IMDSv1 è attivato per impostazione predefinita sulle istanze nuove ed esistenti. Se si preferisce, è possibile configurare manualmente IMDSv2 sulle istanze EC2.

Prima di iniziare

- La versione del connettore deve essere 3.9.38 o successiva.
- Cloud Volumes ONTAP deve eseguire una delle seguenti versioni:
  - 9.12.1 P2 (o qualsiasi patch successivo)
  - 9.13.0 P4 (o qualsiasi patch successivo)
  - 9.13.1 o qualsiasi versione successiva a questa release
- Questa modifica richiede il riavvio delle istanze di Cloud Volumes ONTAP.

A proposito di questa attività

Questi passaggi richiedono l'utilizzo dell'interfaccia a riga di comando di AWS, perché devi modificare il limite del nodo di risposta su 3.

Fasi

1. Richiedere l'uso di IMDSv2 sull'istanza del connettore:

   a. Connettersi alla macchina virtuale Linux per il connettore.

      Quando è stata creata l'istanza del connettore in AWS, sono stati forniti una chiave di accesso AWS e una chiave segreta. È possibile utilizzare questa coppia di chiavi per SSH all'istanza. Il nome utente per l'istanza EC2 Linux è ubuntu (per i connettori creati prima di maggio 2023, il nome utente era EC2-user).

      "AWS Docs (documenti AWS): Connettersi all'istanza di Linux"

   b. Installa l'interfaccia a riga di comando di AWS.

      "Documentazione AWS: Installa o effettua l'aggiornamento alla versione più recente della CLI AWS"

   c. Utilizzare `aws ec2 modify-instance-metadata-options` Comando per richiedere l'uso di IMDSv2 e per modificare il limite di risposta PUT hop a 3.

      Esempio

```
aws ec2 modify-instance-metadata-options \
    --instance-id <instance-id> \
    --http-put-response-hop-limit 3 \
    --http-tokens required \
    --http-endpoint enabled
```

> Il `http-tokens` Set di parametri IMDSv2 su richiesto. Quando `http-tokens` è obbligatorio, è necessario impostare anche `http-endpoint` su attivato.

2. Richiedi l'utilizzo di IMDSv2 sulle istanze di Cloud Volumes ONTAP:
   a. Accedere alla "Console Amazon EC2"
   b. Dal riquadro di navigazione, selezionare **istanze**.
   c. Selezionare un'istanza di Cloud Volumes ONTAP.
   d. Selezionare **azioni > Impostazioni istanza > Modifica opzioni metadati istanza**.
   e. Nella finestra di dialogo **Modifica opzioni metadati istanza**, selezionare quanto segue:
      - Per **Servizio metadati istanza**, selezionare **Abilita**.
      - Per **IMDSv2**, selezionare **richiesto**.
      - Selezionare **Salva**.
   f. Ripetere questi passaggi per altre istanze di Cloud Volumes ONTAP, incluso il mediatore ha.
   g. "Arrestare e avviare le istanze di Cloud Volumes ONTAP"

Risultato

L'istanza del connettore e le istanze di Cloud Volumes ONTAP sono ora configurate per l'utilizzo di IMDSv2.

Aggiornare il connettore quando si utilizza la modalità privata

Se si utilizza BlueXP in modalità privata, è possibile aggiornare il connettore quando è disponibile una versione più recente dal NetApp Support Site.

Il connettore deve essere riavviato durante il processo di aggiornamento, in modo che la console basata su Web non sia disponibile durante l'aggiornamento.

> 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.

Fasi

1. 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.

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

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

Dove <version> è la versione del connettore scaricato.

4. Eseguire lo script di installazione:

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

Dove <version> è la versione del connettore scaricato.

5. Una volta completato l'aggiornamento, è possibile verificare la versione del connettore accedendo a **Guida > supporto tecnico > connettore**.

Modificare l'indirizzo IP di un connettore

Se necessario per la tua azienda, puoi modificare l'indirizzo IP interno e l'indirizzo IP pubblico dell'istanza del connettore assegnata automaticamente dal tuo cloud provider.

Fasi

1. Seguire le istruzioni del provider cloud per modificare l'indirizzo IP locale o l'indirizzo IP pubblico (o entrambi) per l'istanza del connettore.
2. Se è stato modificato l'indirizzo IP pubblico ed è necessario connettersi all'interfaccia utente locale in esecuzione sul connettore, riavviare l'istanza del connettore per registrare il nuovo indirizzo IP con BlueXP.
3. Se è stato modificato l'indirizzo IP privato, aggiornare la posizione di backup per i file di configurazione Cloud Volumes ONTAP in modo che i backup vengano inviati al nuovo indirizzo IP privato sul connettore.

   Sarà necessario aggiornare la posizione di backup per ciascun sistema Cloud Volumes ONTAP.

   a. Eseguire il seguente comando dall'interfaccia CLI di Cloud Volumes ONTAP per visualizzare la destinazione di backup corrente:

   ```
   system configuration backup show
   ```

   b. Eseguire il seguente comando per aggiornare l'indirizzo IP della destinazione di backup:

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

Modificare gli URI di un connettore

Aggiungere e rimuovere l'URI (Uniform Resource Identifier) per un connettore.

Fasi

1. Selezionare l'elenco a discesa **Connector** dall'intestazione BlueXP.
2. Selezionare **Gestisci connettori**.

3. Selezionare il menu delle azioni per un connettore e selezionare **Edit URI** (Modifica URI).
4. Aggiungere e rimuovere URI, quindi selezionare **Apply** (Applica).

Correggere gli errori di download quando si utilizza un gateway NAT Google Cloud

Il connettore scarica automaticamente gli aggiornamenti software per Cloud Volumes ONTAP. Il download potrebbe non riuscire se la configurazione utilizza un gateway Google Cloud NAT. È possibile correggere questo problema limitando il numero di parti in cui è divisa l'immagine software. Questa fase deve essere completata utilizzando l'API BlueXP.

Fase

1. Inviare una richiesta PUT a /occm/config con il seguente JSON come corpo:

   ```
   {
     "maxDownloadSessions": 32
   }
   ```

   Il valore per *maxDownloadSessions* può essere 1 o qualsiasi numero intero maggiore di 1. Se il valore è 1, l'immagine scaricata non verrà divisa.

   Si noti che 32 è un valore di esempio. Il valore da utilizzare dipende dalla configurazione NAT e dal numero di sessioni che è possibile avere contemporaneamente.

"Scopri di più sulla chiamata API /occm/config"

Rimuovere i connettori da BlueXP

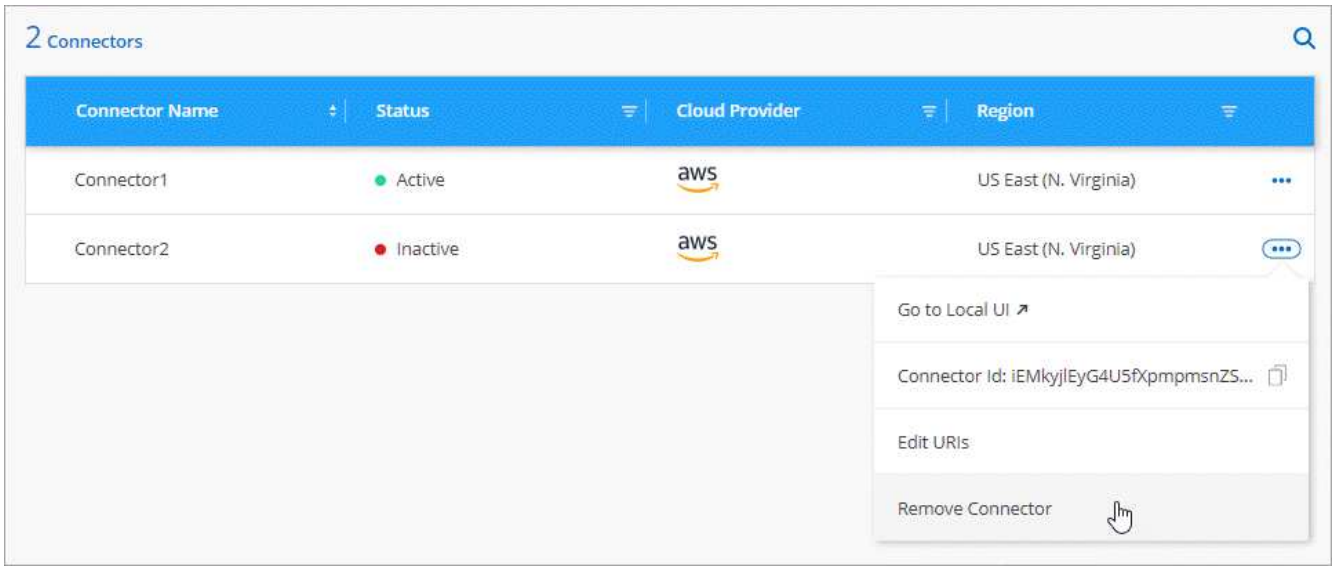
Se un connettore non è attivo, è possibile rimuoverlo dall'elenco dei connettori in BlueXP. Questa operazione può essere eseguita se la macchina virtuale Connector è stata eliminata o se il software Connector è stato disinstallato.

Tenere presente quanto segue per la rimozione di un connettore:

- Questa azione non elimina la macchina virtuale.
- Questa azione non può essere annullata - una volta rimosso un connettore da BlueXP, non è possibile aggiungerlo nuovamente.

Fasi

1. Selezionare l'elenco a discesa **Connector** dall'intestazione BlueXP.
2. Selezionare **Gestisci connettori**.
3. Selezionare il menu delle azioni per un connettore inattivo e selezionare **Remove Connector** (Rimuovi connettore).



4. Inserire il nome del connettore da confermare, quindi selezionare **Remove** (Rimuovi).

Risultato

BlueXP rimuove il connettore dai record.

Disinstallare il software Connector

Disinstallare il software Connector per risolvere i problemi o per rimuovere definitivamente il software dall'host. La procedura da seguire dipende dal fatto che il connettore sia stato installato su un host con accesso a Internet (modalità standard o limitata) o su un host in una rete che non dispone di accesso a Internet (modalità privata).

Disinstallare quando si utilizza la modalità standard o limitata

I passaggi riportati di seguito consentono di disinstallare il software del connettore quando si utilizza BlueXP in modalità standard o limitata.

Fasi

1. Connettersi alla macchina virtuale Linux per il connettore.
2. Eseguire lo script di disinstallazione dall'host Linux:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent esegue lo script senza richiedere conferma.

Disinstallare quando si utilizza la modalità privata

La procedura riportata di seguito consente di disinstallare il software del connettore quando si utilizza BlueXP in modalità privata in cui non è disponibile alcun accesso a Internet.

Fasi

1. Connettersi alla macchina virtuale Linux per il connettore.
2. Dall'host Linux, eseguire i seguenti comandi:

   ```
   ./opt/application/netapp/ds/cleanup.sh
   ```

```
rm -rf /opt/application/netapp/ds
```

Installare un certificato HTTPS per un accesso sicuro

Per impostazione predefinita, BlueXP utilizza un certificato autofirmato per l'accesso HTTPS alla console Web. Se richiesto dall'azienda, è possibile installare un certificato firmato da un'autorità di certificazione (CA), che fornisce una protezione migliore rispetto a un certificato autofirmato.

Prima di iniziare

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

Installare un certificato HTTPS

Installare un certificato firmato da una CA per un accesso sicuro.

Fasi

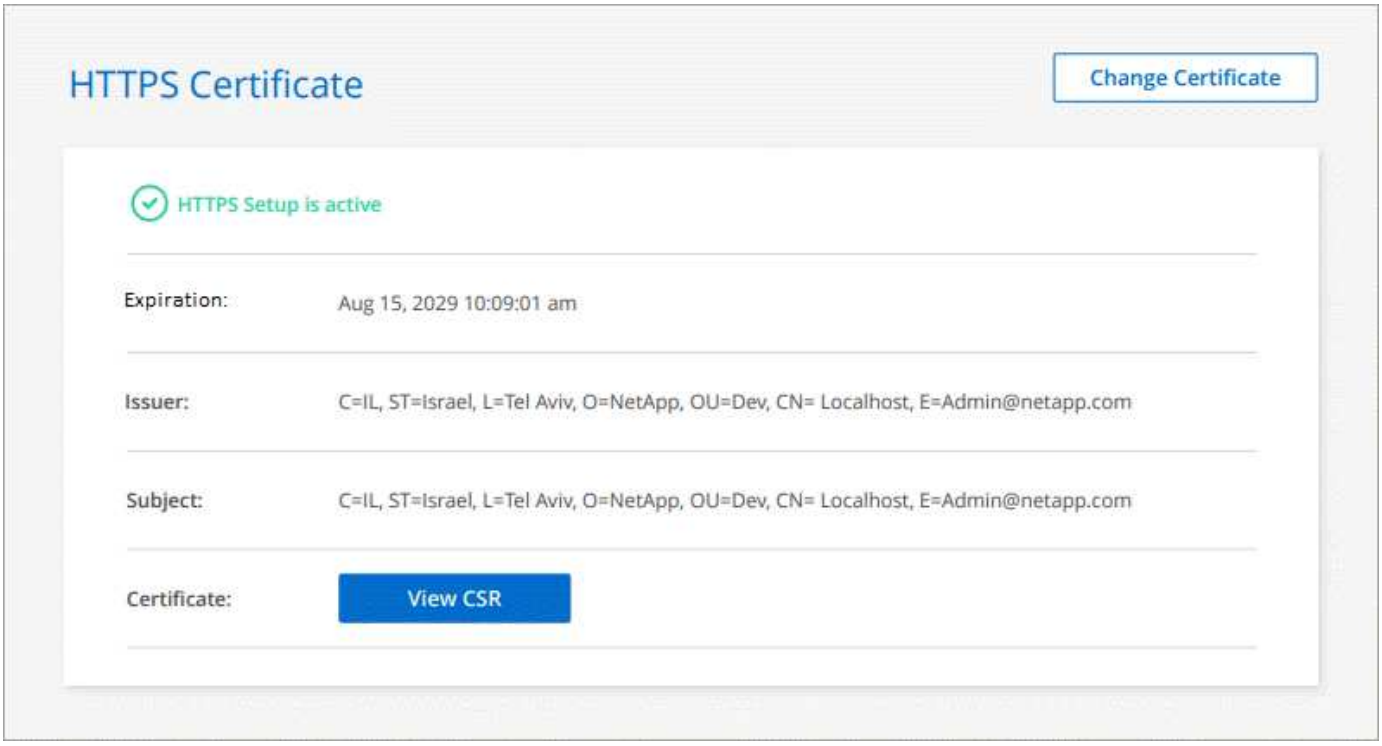
1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **impostazione HTTPS**.

2. Nella pagina HTTPS Setup (Configurazione HTTPS), installare un certificato generando una richiesta di firma del certificato (CSR) o installando il proprio certificato firmato dalla CA:

Opzione	Descrizione
Generare una CSR	a. Inserire il nome host o il DNS dell'host del connettore (il nome comune), quindi selezionare **generate CSR** (genera CSR). BlueXP visualizza una richiesta di firma del certificato. b. Utilizzare la CSR per inviare una richiesta di certificato SSL a una CA. Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64. c. Caricare il file del certificato e selezionare **Installa**.
Installare il proprio certificato firmato dalla CA	a. Selezionare **Installa certificato firmato dalla CA**. b. Caricare il file del certificato e la chiave privata, quindi selezionare **Installa**. Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64.

Risultato

BlueXP utilizza ora il certificato firmato dalla CA per fornire un accesso HTTPS sicuro. L'immagine seguente mostra un account BlueXP configurato per l'accesso sicuro:



Rinnovare il certificato BlueXP HTTPS

È necessario rinnovare il certificato HTTPS BlueXP prima della scadenza per garantire un accesso sicuro alla console BlueXP. Se il certificato non viene rinnovato prima della scadenza, viene visualizzato un avviso quando gli utenti accedono alla console Web utilizzando HTTPS.

Fasi

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

   Vengono visualizzati i dettagli del certificato BlueXP, inclusa la data di scadenza.

2. Selezionare **Cambia certificato** e seguire la procedura per generare una CSR o installare il proprio certificato firmato dalla CA.

Risultato

BlueXP utilizza il nuovo certificato firmato dalla CA per fornire un accesso HTTPS sicuro.

Configurare un connettore per l'utilizzo di un server proxy

Se le policy aziendali richiedono l'utilizzo di un server proxy per tutte le comunicazioni a Internet, è necessario configurare i connettori in modo che utilizzino tale server proxy. Se non è stato configurato un connettore per l'utilizzo di un server proxy durante l'installazione, è possibile configurare il connettore per l'utilizzo di tale server proxy in qualsiasi momento.

Se non è disponibile un indirizzo IP pubblico o un gateway NAT, la configurazione del connettore per l'utilizzo

di un server proxy fornisce l'accesso a Internet in uscita. Questo server proxy fornisce solo il connettore con una connessione in uscita. Non fornisce alcuna connettività per i sistemi Cloud Volumes ONTAP.

Se i sistemi Cloud Volumes ONTAP non dispongono di una connessione Internet in uscita per inviare messaggi AutoSupport, BlueXP configura automaticamente i sistemi Cloud Volumes ONTAP 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.

Configurazioni supportate

- BlueXP supporta HTTP e HTTPS.
- Il server proxy può trovarsi nel cloud o nella rete.
- BlueXP non supporta i server proxy trasparenti.

Attivare un proxy su un connettore

Quando si configura un connettore per l'utilizzo di un server proxy, il connettore e i sistemi Cloud Volumes ONTAP gestiti (inclusi i mediatori ha) utilizzano tutti il server proxy.

Si noti che questa operazione riavvia il connettore. Assicurarsi che il connettore non stia eseguendo alcuna operazione prima di procedere.

Fasi

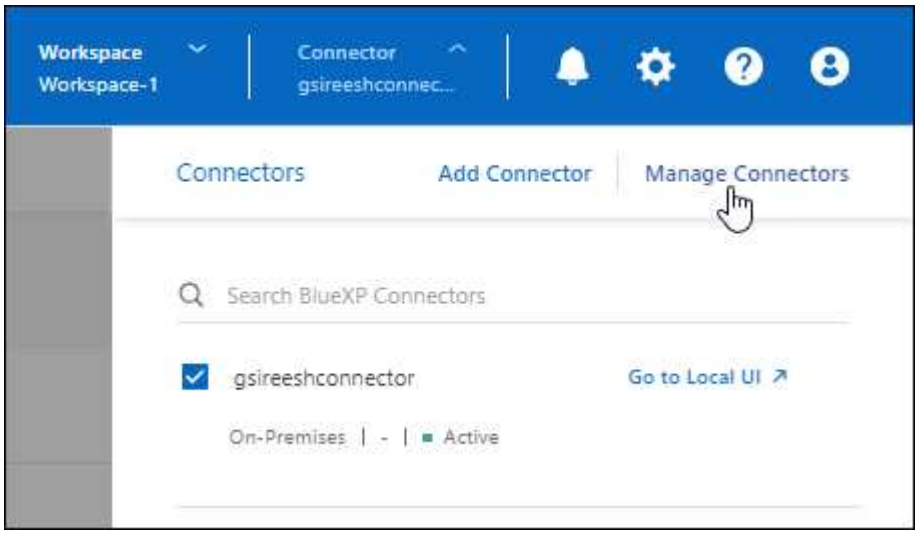
1. Accedere alla pagina **Modifica connettore BlueXP**.

   La navigazione dipende dall'utilizzo di BlueXP in modalità standard (accesso all'interfaccia BlueXP dal sito Web SaaS) o in modalità limitata o privata (accesso all'interfaccia BlueXP localmente dall'host del connettore).

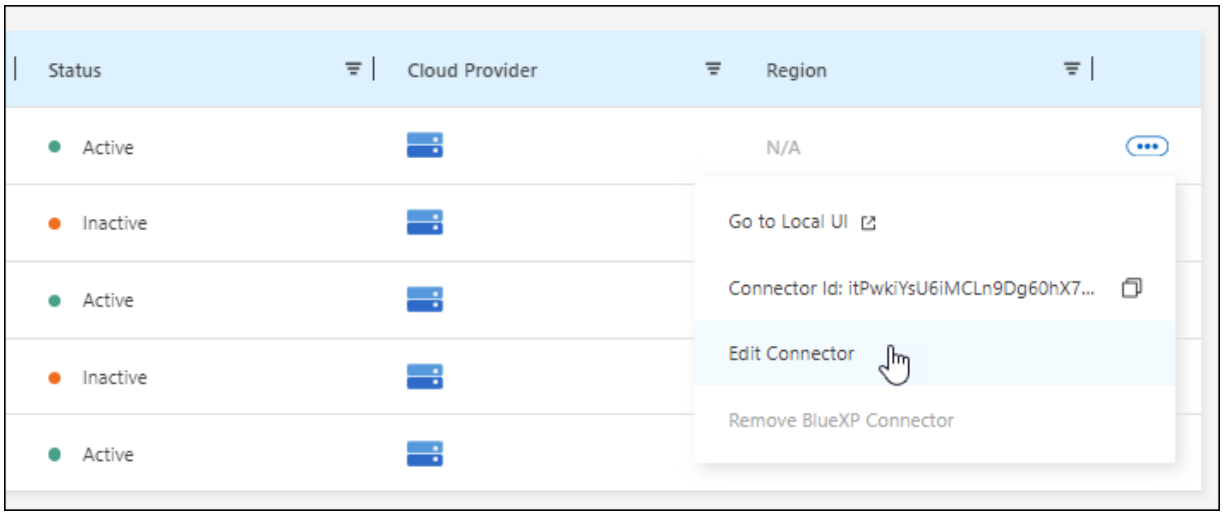
Modalità standard

a. Selezionare l'elenco a discesa **Connector** dall'intestazione BlueXP.

b. Selezionare **Gestisci connettori**.



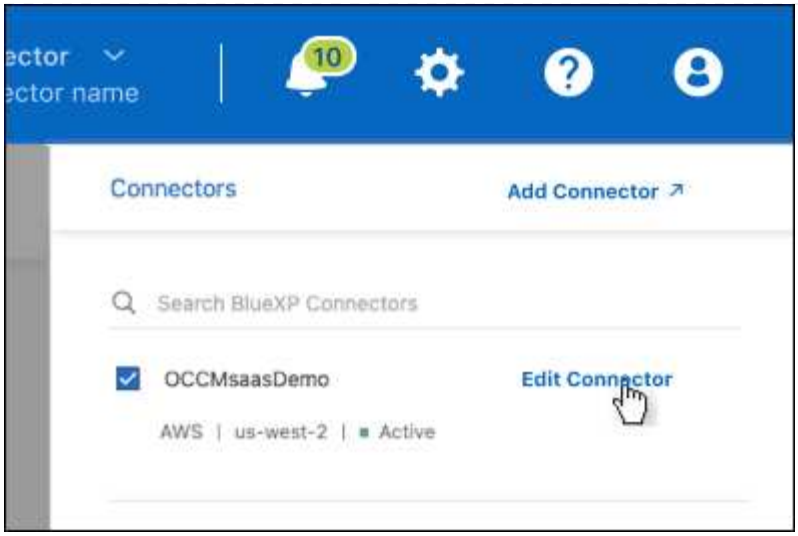
c. Selezionare il menu azione per un connettore e selezionare **Modifica connettore**.



Modalità limitata o privata

a. Selezionare l'elenco a discesa **Connector** dall'intestazione BlueXP.

b. Selezionare **Modifica connettore**.



2. Selezionare **Configurazione proxy HTTP**.
3. Configurare il proxy:
   a. Selezionare **Enable Proxy** (attiva proxy).
   b. Specificare il server utilizzando la sintassi http://address:port oppure https://address:port
   c. Specificare un nome utente e una password se è richiesta l'autenticazione di base per il server.

      Tenere presente quanto segue:

      - L'utente può essere un utente locale o un utente di dominio.
      - Per un utente di dominio, è necessario immettere il codice ASCII per \ come segue: Nome-dominio%92user-name

        Ad esempio: netapp%92proxy

      - BlueXP non supporta password che includono il carattere @.
   d. Selezionare **Salva**.

Abilitare il traffico API diretto

Se un connettore è stato configurato per l'utilizzo di un server proxy, è possibile attivare il traffico API diretto sul connettore per inviare chiamate API direttamente ai servizi del provider cloud senza passare attraverso il proxy. Questa opzione è supportata con i connettori eseguiti in AWS, Azure o Google Cloud.

Se è stato disattivato l'utilizzo dei collegamenti privati di Azure con Cloud Volumes ONTAP e si stanno utilizzando gli endpoint del servizio, è necessario attivare il traffico API diretto. In caso contrario, il traffico non verrà instradato correttamente.

"Scopri di più sull'utilizzo di un collegamento privato Azure o di endpoint di servizio con Cloud Volumes ONTAP"

Fasi

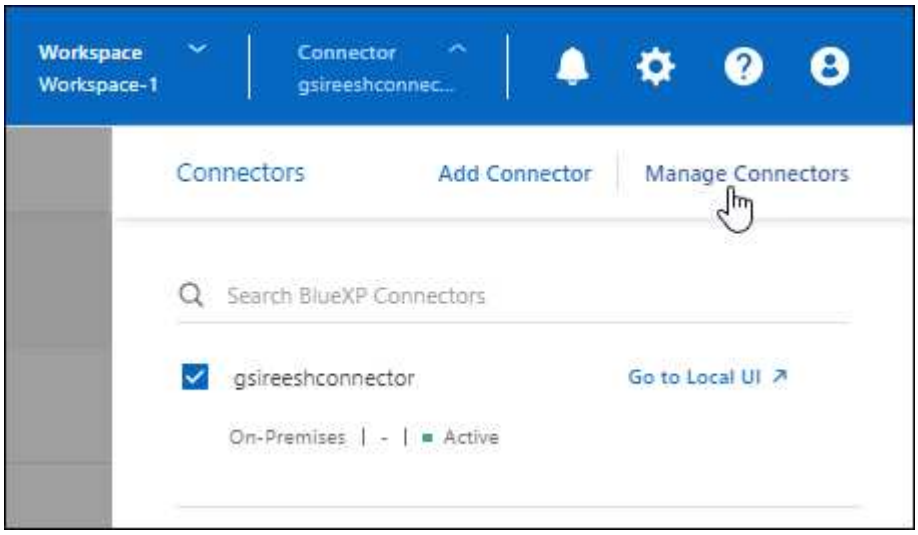
1. Accedere alla pagina **Modifica connettore BlueXP**:

La navigazione dipende dall’utilizzo di BlueXP in modalità standard (accesso all’interfaccia BlueXP dal sito Web SaaS) o in modalità limitata o privata (accesso all’interfaccia BlueXP localmente dall’host del connettore).

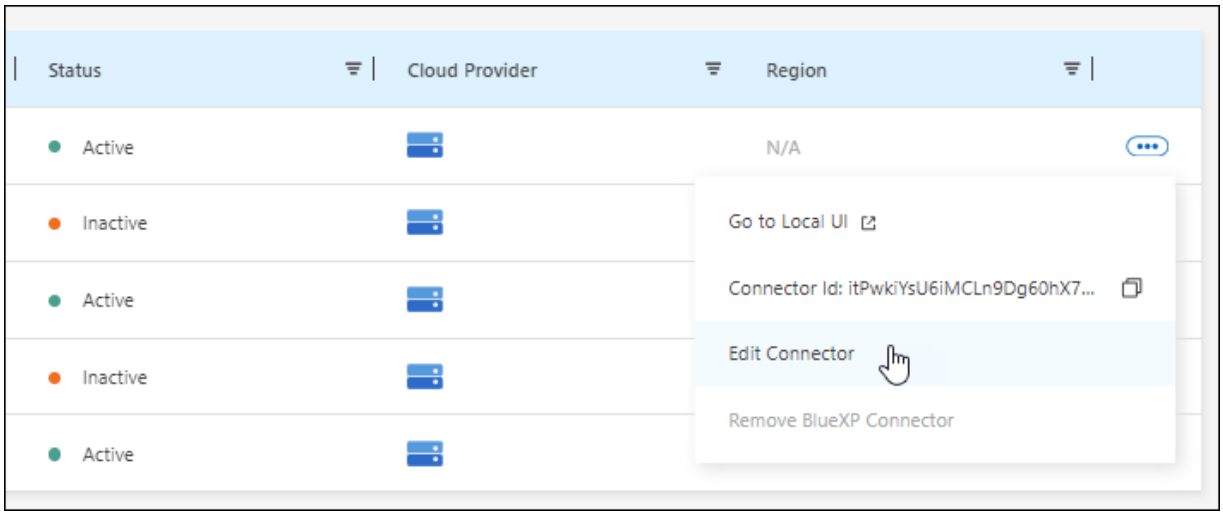
Modalità standard

a. Selezionare l'elenco a discesa **Connector** dall'intestazione BlueXP.

b. Selezionare **Gestisci connettori**.



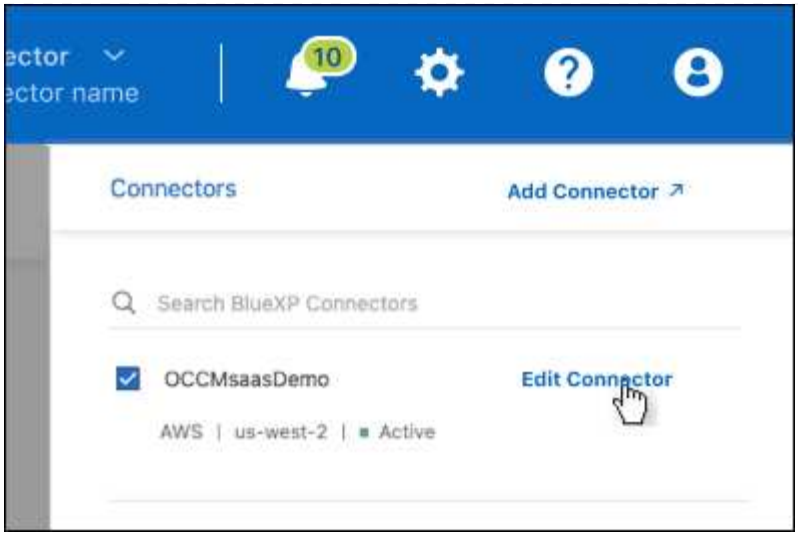
c. Selezionare il menu azione per un connettore e selezionare **Modifica connettore**.



Modalità limitata o privata

a. Selezionare l'elenco a discesa **Connector** dall'intestazione BlueXP.

b. Selezionare **Modifica connettore**.



2. Selezionare **Support Direct API Traffic**.
3. Selezionare la casella di controllo per attivare l'opzione, quindi selezionare **Salva**.

Configurazione predefinita per il connettore

Potrebbe essere necessario ottenere ulteriori informazioni sulla configurazione del connettore prima di implementarlo o se è necessario risolvere eventuali problemi.

Configurazione predefinita con accesso a Internet

I seguenti dettagli di configurazione si applicano se il connettore è stato implementato da BlueXP, dal mercato del cloud provider o se il connettore è stato installato manualmente su un host Linux on-premise con accesso a Internet.

Dettagli AWS

Se hai implementato il connettore da BlueXP o dal mercato del cloud provider, prendi nota di quanto segue:

- Il tipo di istanza EC2 è t3.xlarge.
- Il sistema operativo per l'immagine è Ubuntu 22,04 LTS.

  Il sistema operativo non include una GUI. Per accedere al sistema, è necessario utilizzare un terminale.

- Il nome utente per l'istanza EC2 Linux è ubuntu (per i connettori creati prima di maggio 2023, il nome utente era EC2-user).
- Il disco di sistema predefinito è un disco gp2 da 100 GiB.

Dettagli di Azure

Se hai implementato il connettore da BlueXP o dal mercato del cloud provider, prendi nota di quanto segue:

- Il tipo di macchina virtuale è DS3 v2.
- Il sistema operativo per l'immagine è Ubuntu 22,04 LTS.

  Il sistema operativo non include una GUI. Per accedere al sistema, è necessario utilizzare un terminale.

- Il disco di sistema predefinito è un disco SSD premium da 100 GiB.

Dettagli di Google Cloud

Se il connettore è stato implementato da BlueXP, tenere presente quanto segue:

- L'istanza della macchina virtuale è n2-standard-4.
- Il sistema operativo per l'immagine è Ubuntu 22,04 LTS.

  Il sistema operativo non include una GUI. Per accedere al sistema, è necessario utilizzare un terminale.

- Il disco di sistema predefinito è un disco persistente SSD da 100 GiB.

Cartella di installazione

La cartella di installazione del connettore si trova nella seguente posizione:

/opt/application/netapp/cloudmanager

File di log

I file di log sono contenuti nelle seguenti cartelle:

- /opt/application/netapp/cloudmanager/log
  oppure
- /opt/application/netapp/service-manager-2/logs (a partire dalle nuove installazioni 3.9.23)

  I log in queste cartelle forniscono dettagli sulle immagini del connettore e del docker.

- /opt/application/netapp/cloudmanager/docker_occm/data/log

  I log in questa cartella forniscono dettagli sui servizi cloud e sul servizio BlueXP in esecuzione sul connettore.

Servizio del connettore

- Il servizio BlueXP è denominato occm.
- Il servizio occm dipende dal servizio MySQL.

  Se il servizio MySQL non è attivo, anche il servizio occm è inattivo.

Porte

Il connettore utilizza le seguenti porte sull'host Linux:

- 80 per l'accesso HTTP
- 443 per l'accesso HTTPS

Configurazione predefinita senza accesso a Internet

La seguente configurazione si applica se il connettore è stato installato manualmente su un host Linux on-premise che non dispone di accesso a Internet. "Scopri di più su questa opzione di installazione".

- La cartella di installazione del connettore si trova nella seguente posizione:

  /opt/application/netapp/ds

- I file di log sono contenuti nelle seguenti cartelle:

  /var/lib/docker/volumes/ds_occmdata/_data/log

  I log in questa cartella forniscono dettagli sulle immagini del connettore e del docker.

- Tutti i servizi vengono eseguiti all'interno di container di tipo docker

  I servizi dipendono dal servizio di runtime di docker in esecuzione

- Il connettore utilizza le seguenti porte sull'host Linux:
  - 80 per l'accesso HTTP
  - 443 per l'accesso HTTPS

Credenziali e iscrizioni

AWS

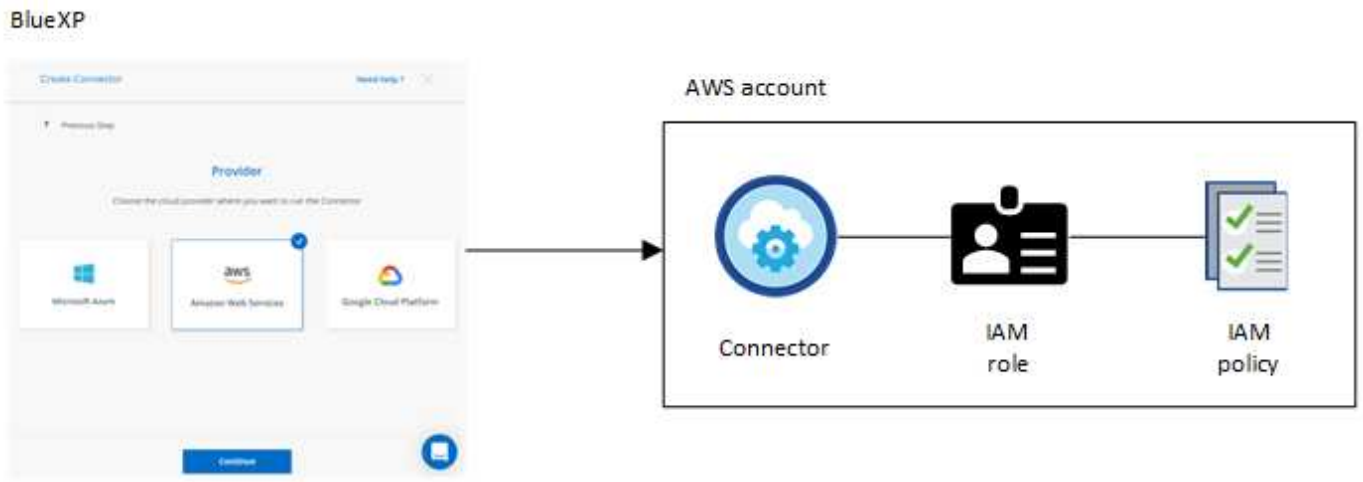
Scopri le credenziali e le autorizzazioni AWS

Scopri in che modo BlueXP usa le credenziali AWS per eseguire azioni per tuo conto e come tali credenziali sono associate alle iscrizioni al marketplace. La comprensione di questi dettagli può essere utile quando si gestiscono le credenziali per uno o più account AWS in BlueXP. Ad esempio, potrebbe essere utile sapere quando aggiungere ulteriori credenziali AWS a BlueXP.

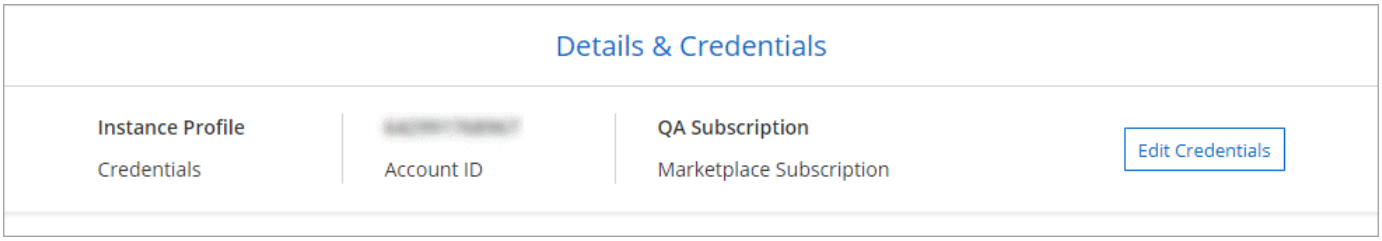
Credenziali AWS iniziali

Quando si implementa un connettore da BlueXP, è necessario fornire l'ARN di un ruolo IAM o le chiavi di accesso per un utente IAM. Il metodo di autenticazione utilizzato deve disporre delle autorizzazioni necessarie per implementare l'istanza del connettore in AWS. Le autorizzazioni richieste sono elencate nella "Policy di implementazione del connettore per AWS".

Quando BlueXP avvia l'istanza del connettore in AWS, crea un ruolo IAM e un profilo di istanza per l'istanza. Allega inoltre un criterio che fornisce al connettore le autorizzazioni per gestire risorse e processi all'interno di tale account AWS. "Analisi dell'utilizzo delle autorizzazioni da parte di BlueXP".



Se si crea un nuovo ambiente di lavoro per Cloud Volumes ONTAP, BlueXP seleziona queste credenziali AWS per impostazione predefinita:



È possibile implementare tutti i sistemi Cloud Volumes ONTAP utilizzando le credenziali AWS iniziali oppure aggiungere credenziali aggiuntive.

Credenziali AWS aggiuntive

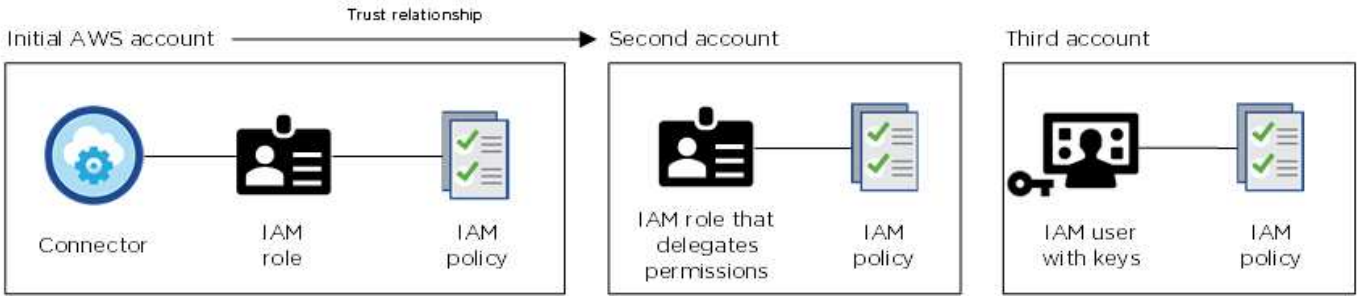
Esistono due modi per aggiungere ulteriori credenziali AWS:

- È possibile aggiungere le credenziali AWS a un connettore esistente
- È possibile aggiungere le credenziali AWS direttamente a BlueXP

Consulta le sezioni seguenti per ulteriori dettagli.

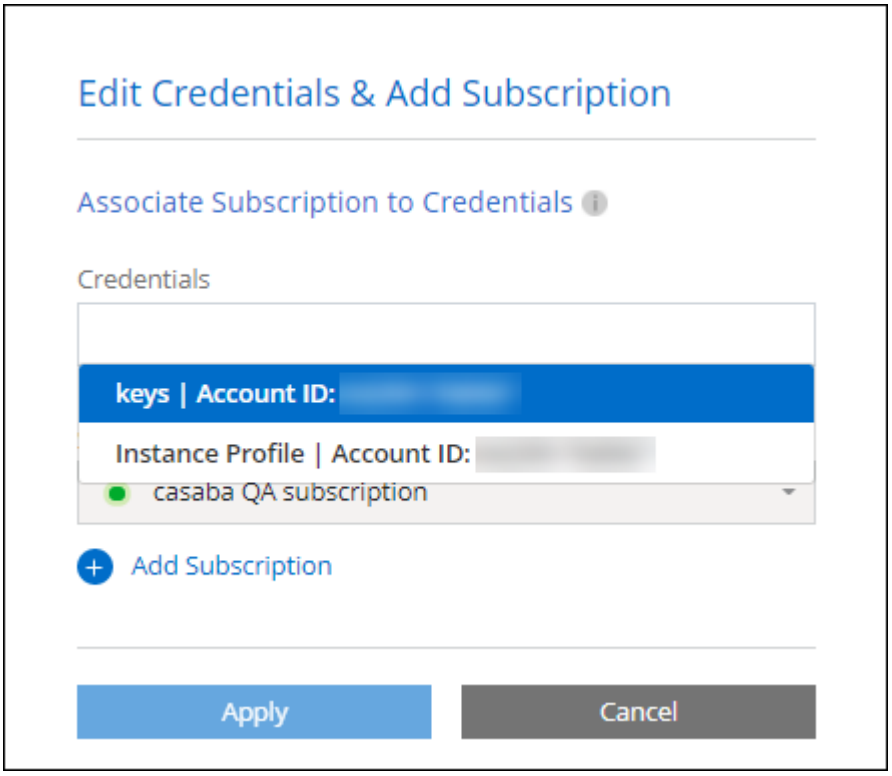
Aggiungere le credenziali AWS a un connettore esistente

Se vuoi utilizzare BlueXP con altri account AWS, puoi fornire le chiavi AWS per un utente IAM o l'ARN di un ruolo in un account attendibile. L'immagine seguente mostra due account aggiuntivi, uno che fornisce le autorizzazioni tramite un ruolo IAM in un account attendibile e l'altro tramite le chiavi AWS di un utente IAM:



Aggiungere quindi le credenziali dell'account a BlueXP specificando il nome risorsa Amazon (ARN) del ruolo IAM o le chiavi AWS per l'utente IAM.

Ad esempio, è possibile passare da una credenziale all'altra quando si crea un nuovo ambiente di lavoro Cloud Volumes ONTAP:



"Scopri come aggiungere le credenziali AWS a un connettore esistente."

Aggiungere le credenziali AWS direttamente a BlueXP

L'aggiunta di nuove credenziali AWS a BlueXP fornisce le autorizzazioni necessarie per creare e gestire un ambiente di lavoro FSX per ONTAP o per creare un connettore.

- "Scopri come aggiungere le credenziali AWS a BlueXP per Amazon FSX per ONTAP"
- "Scopri come aggiungere le credenziali AWS a BlueXP per la creazione di un connettore"

Credenziali e iscrizioni al marketplace

Le credenziali che Aggiungi a un connettore devono essere associate a un'iscrizione al marketplace AWS in modo che puoi pagare per Cloud Volumes ONTAP a una tariffa oraria (PAYGO) o tramite un contratto annuale e per utilizzare altri servizi BlueXP.

"Scopri come associare un abbonamento AWS".

Nota quanto segue sulle credenziali e le iscrizioni al marketplace di AWS:

- Puoi associare una sola iscrizione al marketplace di AWS a un set di credenziali AWS
- È possibile sostituire un abbonamento esistente al mercato con un nuovo abbonamento

FAQ

Le seguenti domande sono relative alle credenziali e agli abbonamenti.

Come si possono ruotare in modo sicuro le credenziali AWS?

Come descritto nelle sezioni precedenti, BlueXP ti consente di fornire le credenziali AWS in pochi modi: Un ruolo IAM associato all'istanza di connettore, assumendo un ruolo IAM in un account attendibile o fornendo chiavi di accesso AWS.

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

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

Posso modificare l'iscrizione al marketplace AWS per gli ambienti di lavoro Cloud Volumes ONTAP?

Sì, è possibile. Quando modifichi l'iscrizione al marketplace di AWS associata a un set di credenziali, tutti gli ambienti di lavoro Cloud Volumes ONTAP esistenti e nuovi verranno addebitati i costi del nuovo abbonamento.

"Scopri come associare un abbonamento AWS".

Posso aggiungere più credenziali AWS, ciascuna con diverse iscrizioni al marketplace?

Tutte le credenziali AWS che appartengono allo stesso account AWS saranno associate allo stesso abbonamento a AWS Marketplace.

Se disponi di più credenziali AWS appartenenti a diversi account AWS, tali credenziali possono essere associate alla stessa iscrizione di AWS Marketplace o a iscrizioni diverse.

Posso spostare gli ambienti di lavoro Cloud Volumes ONTAP esistenti su un account AWS diverso?

No, non è possibile spostare le risorse AWS associate al tuo ambiente di lavoro Cloud Volumes ONTAP su un account AWS diverso.

Come funzionano le credenziali per le implementazioni del marketplace e le implementazioni on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato per il connettore, fornito da BlueXP. È inoltre possibile implementare un connettore in AWS da AWS Marketplace ed è possibile installare manualmente il software del connettore sul proprio host Linux.

Se si utilizza Marketplace, le autorizzazioni vengono fornite nello stesso modo. È sufficiente creare e configurare manualmente il ruolo IAM, quindi fornire le autorizzazioni per eventuali account aggiuntivi.

Per le implementazioni on-premise, non è possibile impostare un ruolo IAM per il sistema BlueXP, ma è possibile fornire le autorizzazioni utilizzando le chiavi di accesso AWS.

Per informazioni su come impostare le autorizzazioni, fare riferimento alle seguenti pagine:

- Modalità standard
  - "Impostare le autorizzazioni per un'implementazione di AWS Marketplace"
  - "Impostare le autorizzazioni per le implementazioni on-premise"

- "Impostare le autorizzazioni per la modalità limitata"
- "Impostare le autorizzazioni per la modalità privata"

Gestisci le credenziali AWS e le iscrizioni al marketplace per BlueXP

Aggiungi e gestisci le credenziali AWS in modo che BlueXP disponga delle autorizzazioni necessarie per implementare e gestire le risorse cloud nei tuoi account AWS. Se si gestiscono più sottoscrizioni AWS Marketplace, è possibile assegnarle a diverse credenziali AWS dalla pagina credenziali.

Panoramica

È possibile aggiungere le credenziali AWS a un connettore esistente o direttamente a BlueXP:

- Aggiungere ulteriori credenziali AWS a un connettore esistente

  L'aggiunta di credenziali AWS a un connettore esistente fornisce le autorizzazioni necessarie per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Scopri come aggiungere le credenziali AWS a un connettore.

- Aggiungere le credenziali AWS a BlueXP per creare un connettore

  L'aggiunta di nuove credenziali AWS a BlueXP offre a BlueXP le autorizzazioni necessarie per creare un connettore. Scopri come aggiungere le credenziali AWS a BlueXP.

- Aggiungere le credenziali AWS a BlueXP per FSX per ONTAP

  L'aggiunta di nuove credenziali AWS a BlueXP offre a BlueXP le autorizzazioni necessarie per creare e gestire FSX per ONTAP. "Scopri come impostare le autorizzazioni per FSX per ONTAP"

Come ruotare le credenziali

BlueXP consente di fornire le credenziali AWS in diversi modi: Un ruolo IAM associato all'istanza del connettore, assumendo un ruolo IAM in un account attendibile o fornendo le chiavi di accesso AWS. "Scopri di più sulle credenziali e le autorizzazioni AWS".

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

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

Aggiungere credenziali aggiuntive a un connettore

Aggiungi credenziali AWS aggiuntive a un connettore in modo che disponga delle autorizzazioni necessarie per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. È possibile fornire l'ARN di un ruolo IAM in un altro account o fornire le chiavi di accesso AWS.

Se stai solo per iniziare a utilizzare BlueXP, "Scopri come BlueXP utilizza le credenziali e le autorizzazioni AWS".

Concedere le autorizzazioni

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

> Se è stato implementato un connettore da BlueXP, BlueXP ha aggiunto automaticamente le credenziali AWS per l'account in cui è stato implementato il connettore. Questo account iniziale non viene aggiunto se il connettore è stato implementato da AWS Marketplace o se il software del connettore è stato installato manualmente su un sistema esistente. "Scopri le credenziali e le autorizzazioni AWS".

Scelte

- Concedere le autorizzazioni assumendo un ruolo IAM in un altro account
- Concedere le autorizzazioni fornendo le chiavi AWS

Concedere le autorizzazioni assumendo un ruolo IAM in un altro account

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

Se il connettore è installato on-premise, non è possibile utilizzare questo metodo di autenticazione. È necessario utilizzare le chiavi AWS.

Fasi

1. Accedere alla console IAM nell'account di destinazione in cui si desidera fornire le autorizzazioni al connettore.
2. In Gestione accessi, selezionare **ruoli > Crea ruolo** e seguire i passaggi per creare il ruolo.

   Assicurarsi di effettuare le seguenti operazioni:

   - In **Trusted entity type**, selezionare **AWS account**.
   - Selezionare **un altro account AWS** e inserire l'ID dell'account in cui risiede l'istanza del connettore.
   - Creare i criteri richiesti copiando e incollando il contenuto di "I criteri IAM per il connettore".
3. Copiare l'ARN del ruolo IAM in modo da poterlo incollare in BlueXP in un secondo momento.

Risultato

L'account dispone ora delle autorizzazioni necessarie. È ora possibile aggiungere le credenziali a un connettore.

Concedere le autorizzazioni fornendo le chiavi AWS

Se si desidera fornire a BlueXP chiavi AWS per un utente IAM, è necessario concedere le autorizzazioni necessarie a tale utente. Il criterio IAM BlueXP definisce le azioni e le risorse AWS che BlueXP può utilizzare.

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

Fasi

1. Dalla console IAM, creare policy copiando e incollando il contenuto di "I criteri IAM per il connettore".

   "Documentazione AWS: Creazione di policy IAM"

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

Risultato

L'account dispone ora delle autorizzazioni necessarie. È ora possibile aggiungere le credenziali a un connettore.

Aggiungere le credenziali

Dopo aver fornito un account AWS con le autorizzazioni richieste, è possibile aggiungere le credenziali per tale account a un connettore esistente. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in quell'account utilizzando lo stesso connettore.

Prima di iniziare

Se hai appena creato queste credenziali nel tuo cloud provider, potrebbero essere necessari alcuni minuti prima che siano disponibili per l'utilizzo. Attendere alcuni minuti prima di aggiungere le credenziali a BlueXP.

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**.

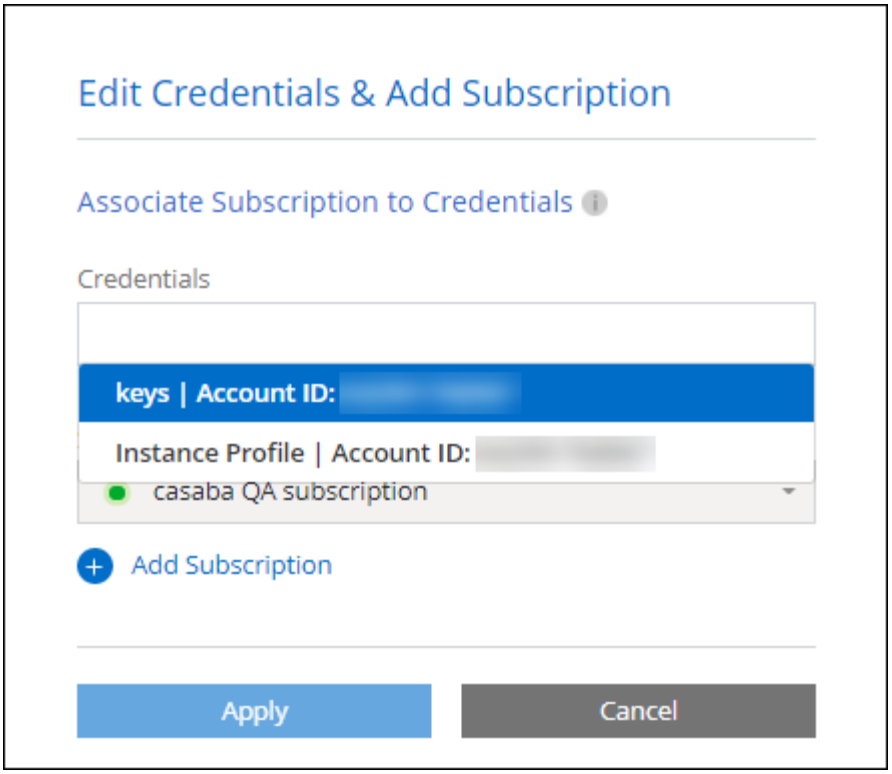
3. Nella pagina **credenziali account**, selezionare **Aggiungi credenziali** e seguire la procedura guidata.
   a. **Credentials Location**: Selezionare **Amazon Web Services > Connector**.
   b. **Definisci credenziali**: Fornire l'ARN (Amazon Resource Name) di un ruolo IAM attendibile oppure inserire 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.

      Per pagare i servizi BlueXP a una tariffa oraria (PAYGO) o con un contratto annuale, le credenziali AWS devono essere associate a un abbonamento AWS Marketplace.

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

Risultato

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



Aggiungere le credenziali a BlueXP per la creazione di un connettore

Aggiungere le credenziali AWS a BlueXP fornendo l'ARN di un ruolo IAM che assegna a BlueXP le autorizzazioni necessarie per creare un connettore. È possibile scegliere queste credenziali quando si crea un nuovo connettore.

Impostare il ruolo IAM

Impostare un ruolo IAM che consenta al layer BlueXP SaaS di assumere il ruolo.

Fasi

1. Accedere alla console IAM nell'account di destinazione.
2. In Gestione accessi, selezionare **ruoli > Crea ruolo** e seguire i passaggi per creare il ruolo.

   Assicurarsi di effettuare le seguenti operazioni:

   - In **Trusted entity type**, selezionare **AWS account**.
   - Selezionare **un altro account AWS** e inserire l'ID di BlueXP SaaS: 952013314444
   - Creare un criterio che includa le autorizzazioni necessarie per creare un connettore.
     - "Visualizzare le autorizzazioni necessarie per FSX per ONTAP"
     - "Visualizzare il criterio di implementazione del connettore"
3. Copiare l'ARN del ruolo IAM in modo da poterlo incollare in BlueXP nella fase successiva.

Risultato

Il ruolo IAM dispone ora delle autorizzazioni necessarie. Ora puoi aggiungerlo a BlueXP.

Aggiungere le credenziali

Dopo aver fornito al ruolo IAM le autorizzazioni richieste, aggiungere il ruolo ARN a BlueXP.

Prima di iniziare

Se hai appena creato il ruolo IAM, 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. Nella pagina **credenziali account**, selezionare **Aggiungi credenziali** e seguire la procedura guidata.
   a. **Posizione credenziali**: Selezionare **Amazon Web Services > BlueXP**.
   b. **Definisci credenziali**: Fornire l'ARN (Amazon Resource Name) del ruolo IAM.
   c. **Revisione**: Confermare i dettagli relativi alle nuove credenziali e selezionare **Aggiungi**.

Risultato

È ora possibile utilizzare le credenziali per creare un nuovo connettore.

Aggiungi credenziali a BlueXP per Amazon FSX per ONTAP

Per ulteriori informazioni, fare riferimento a. "Documentazione BlueXP per Amazon FSX per ONTAP"

Associare un abbonamento AWS

Dopo aver aggiunto le credenziali AWS a BlueXP, è possibile associare un abbonamento AWS Marketplace a tali credenziali. L'abbonamento consente di pagare Cloud Volumes ONTAP a una tariffa oraria (PAYGO) o utilizzando un contratto annuale e di utilizzare altri servizi BlueXP.

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

- Non hai associato un abbonamento quando inizialmente hai aggiunto le credenziali a BlueXP.
- Vuoi modificare l'iscrizione al marketplace AWS associata alle credenziali AWS.

  Sostituendo l'attuale sottoscrizione al marketplace con una nuova sottoscrizione, l'abbonamento al marketplace viene modificato per qualsiasi ambiente di lavoro Cloud Volumes ONTAP esistente e per tutti i nuovi ambienti di lavoro.

Prima di iniziare

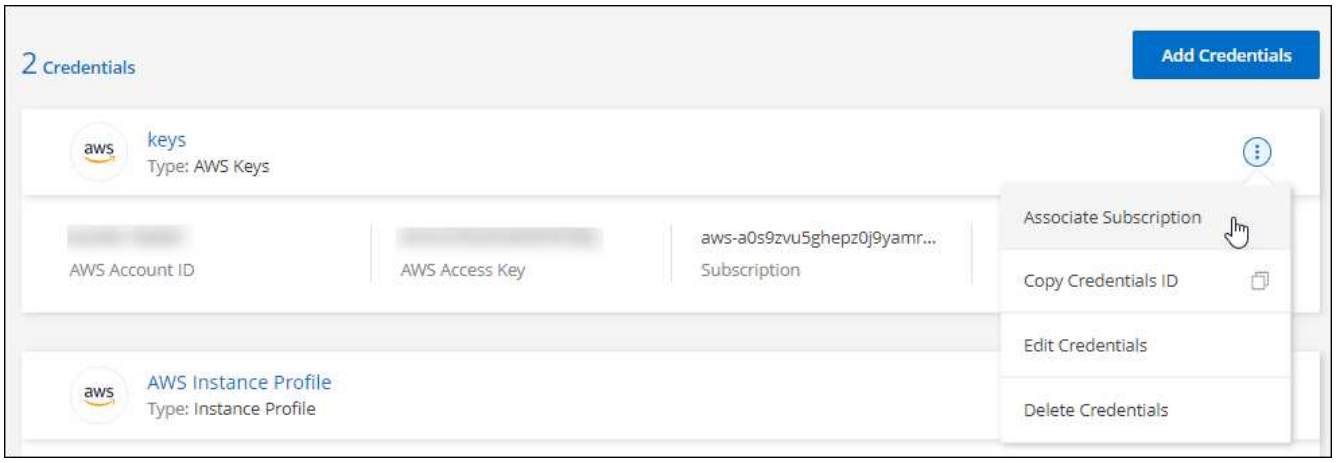
È necessario creare un connettore prima di poter modificare le impostazioni di BlueXP. "Scopri come creare un connettore".

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

Associa un abbonamento esistente al tuo account

Quando effettui l'iscrizione a BlueXP dal marketplace AWS, l'ultimo passaggio del processo consiste nell'associare l'iscrizione agli account BlueXP dal sito web BlueXP. Se non hai completato questo passaggio,

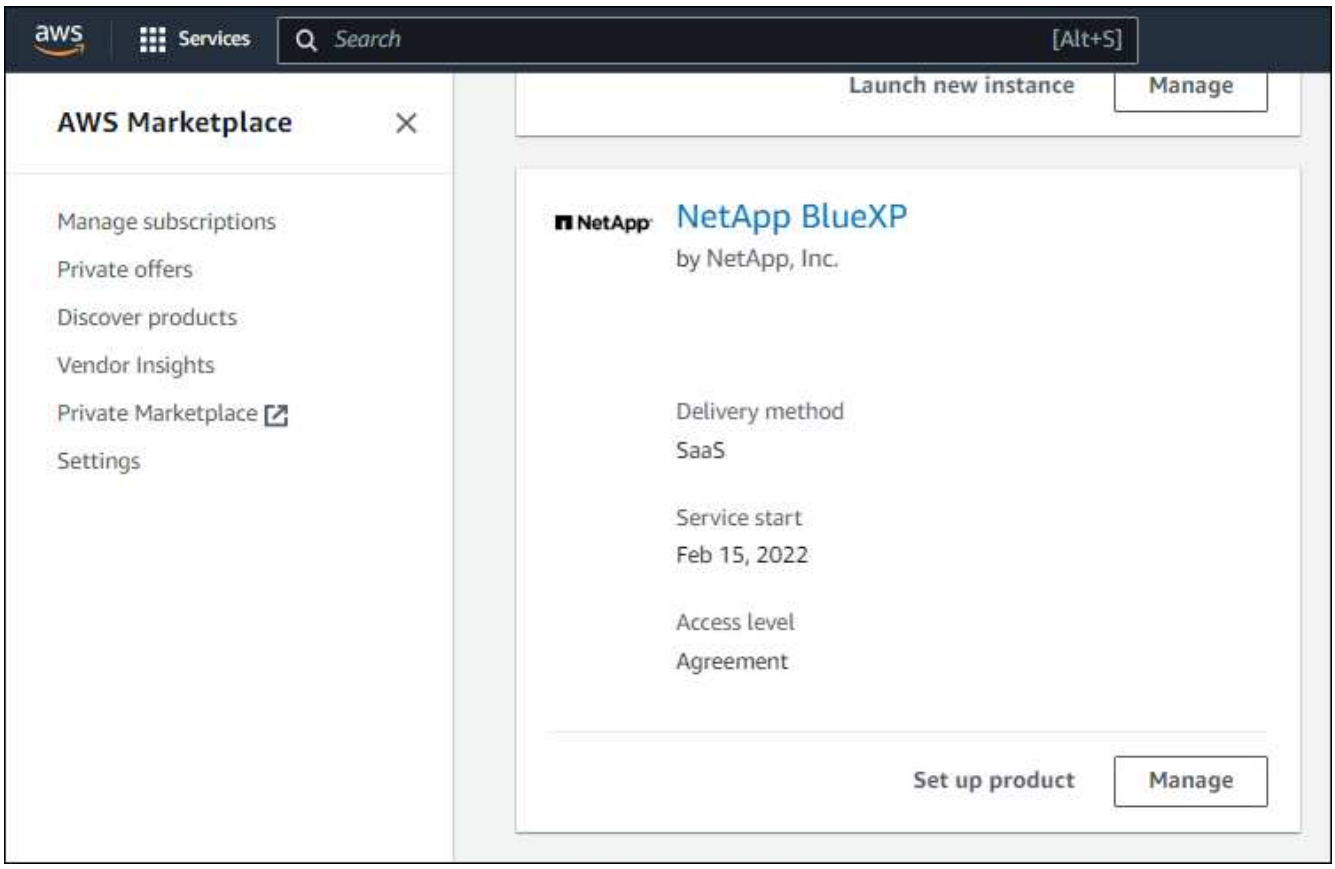
non puoi utilizzare l'abbonamento con il tuo account BlueXP.

Segui i passaggi riportati di seguito se ti sei abbonato a BlueXP da AWS Marketplace, ma non hai fatto la procedura per associare l'abbonamento all'account.

Fasi

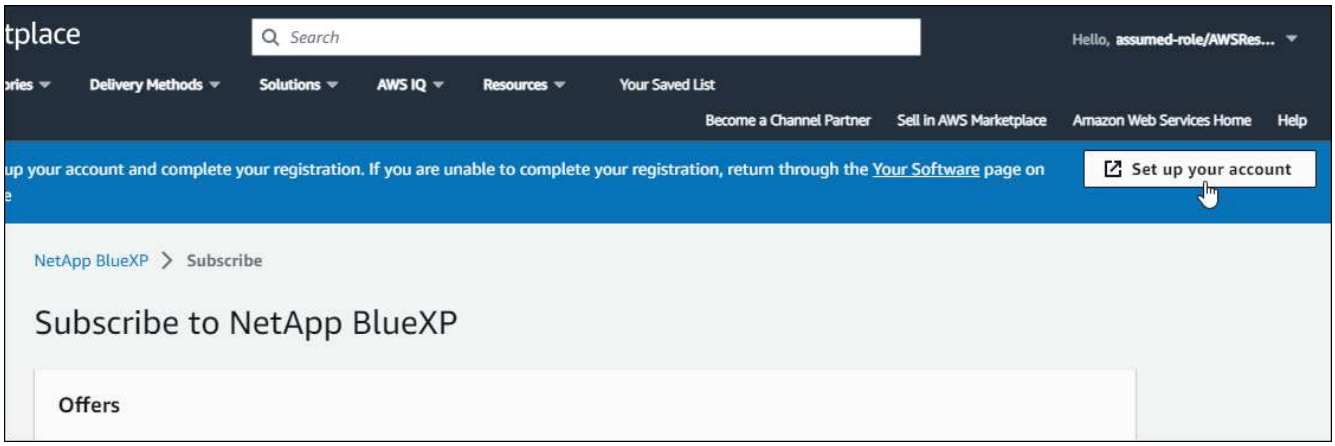
1. Accedi al Digital Wallet di BlueXP per confermare che non hai associato il tuo abbonamento all'account BlueXP.
   a. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
   b. Selezionare **Abbonamenti**.
   c. Verifica che il tuo abbonamento BlueXP non venga visualizzato.

      Verranno visualizzati solo gli abbonamenti associati all'account attualmente visualizzato. Se non vedi il tuo abbonamento, procedi con i passaggi seguenti.
2. Accedi alla console AWS e accedi a **sottoscrizioni al marketplace AWS**.
3. Trova l'iscrizione a NetApp BlueXP.



4. Selezionare **configura prodotto**.

   La pagina dell'offerta di sottoscrizione dovrebbe essere caricata in una nuova scheda o finestra del browser.
5. Selezionare **Configura account**.



La pagina **assegnazione abbonamento** su netapp.com dovrebbe essere caricata in una nuova scheda o finestra del browser.

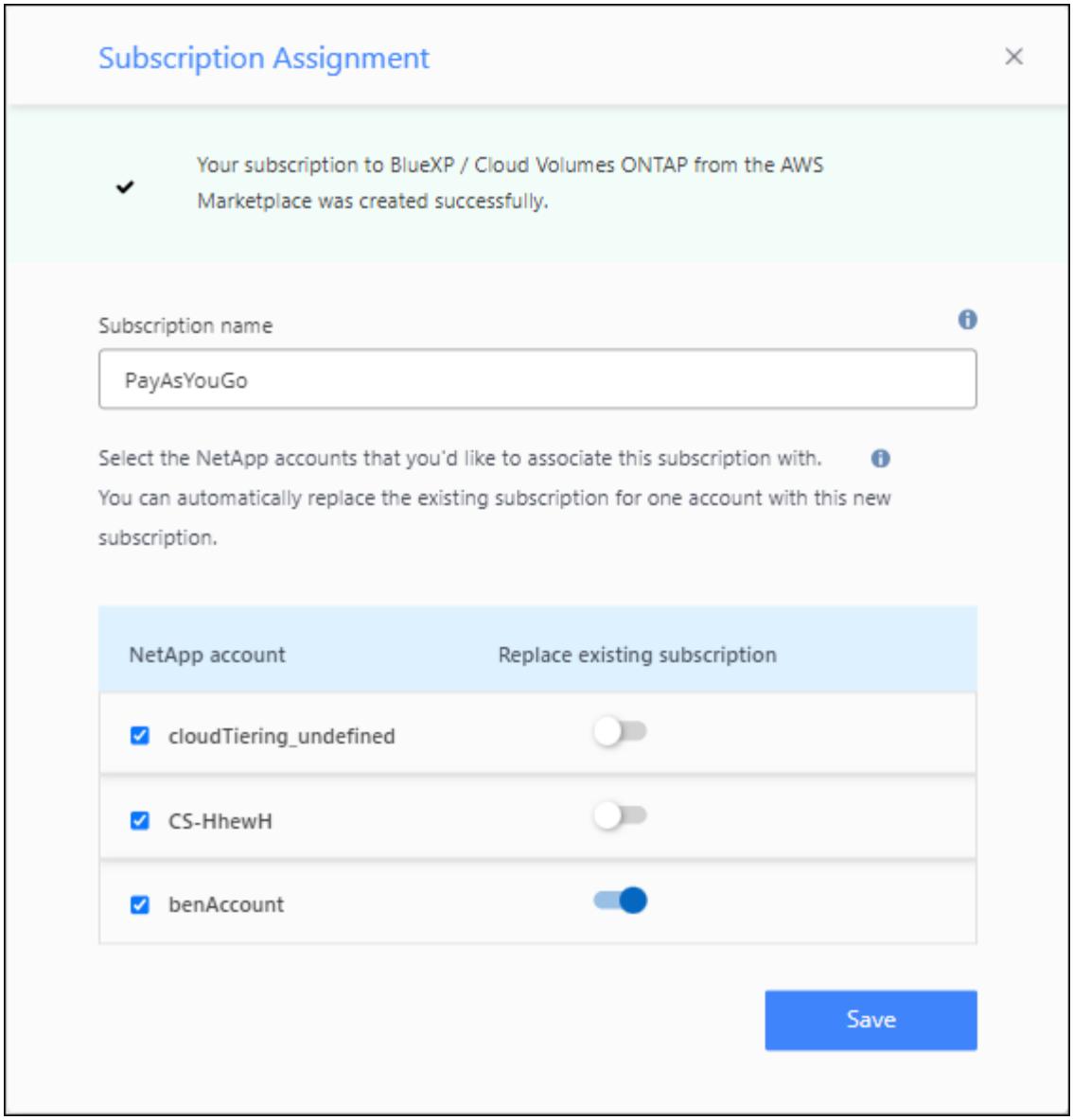
Nota: Potrebbe essere richiesto di accedere prima a BlueXP.

6. 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.

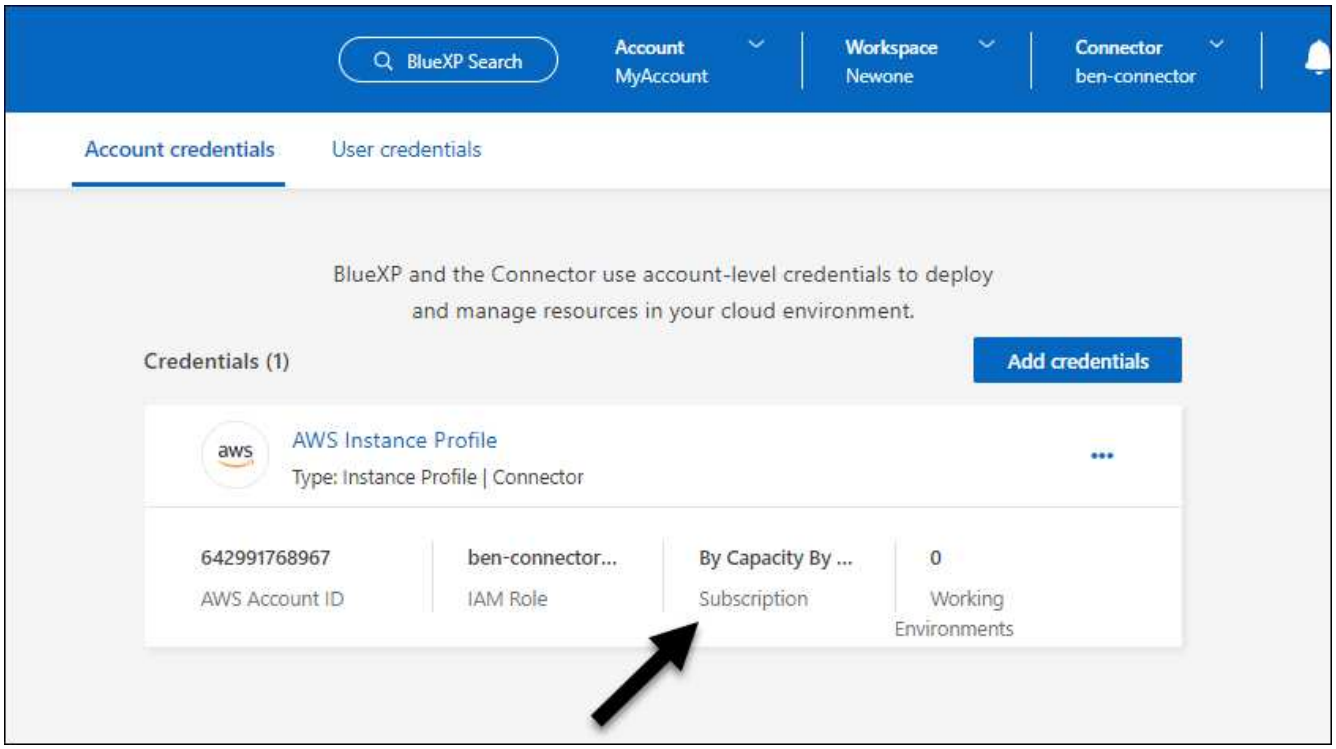
     BlueXP sostituisce l'abbonamento esistente per tutte le credenziali dell'account con questo nuovo abbonamento. Se un insieme di credenziali non è mai stato associato a un abbonamento, questo nuovo abbonamento non sarà associato a tali credenziali.

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



7. Accedi al Digital Wallet di BlueXP per verificare che l'iscrizione sia associata al tuo account BlueXP.
   a. Dal menu di navigazione di BlueXP, selezionare **Governance > Digital wallet**.
   b. Selezionare **Abbonamenti**.
   c. Verifica che venga visualizzato il tuo abbonamento BlueXP.
8. Verifica che l'iscrizione sia associata alle tue credenziali AWS.
   a. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.
   b. Nella pagina **credenziali dell'account**, verifica che l'abbonamento sia associato alle tue credenziali AWS.

      Ecco un esempio.



Modificare le credenziali

Modificare le credenziali AWS in BlueXP modificando il tipo di account (chiavi AWS o assumere il ruolo), modificando il nome o aggiornando le credenziali (le chiavi o il ruolo ARN).

> Non è possibile modificare le credenziali per un profilo di istanza associato a un'istanza del connettore.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.
2. Nella pagina **credenziali account**, selezionare il menu delle azioni per un set di credenziali, quindi selezionare **Modifica credenziali**.
3. Apportare le modifiche richieste, quindi selezionare **Applica**.

Eliminare le credenziali

Se non hai più bisogno di una serie di credenziali, puoi eliminarle da BlueXP. È possibile eliminare solo le credenziali non associate a un ambiente di lavoro.

> Non è possibile eliminare le credenziali per un profilo di istanza associato a un'istanza del connettore.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.
2. Nella pagina **credenziali account**, selezionare il menu delle azioni per un set di credenziali, quindi selezionare **Elimina credenziali**.

3. Selezionare **Delete** per confermare.

Azure

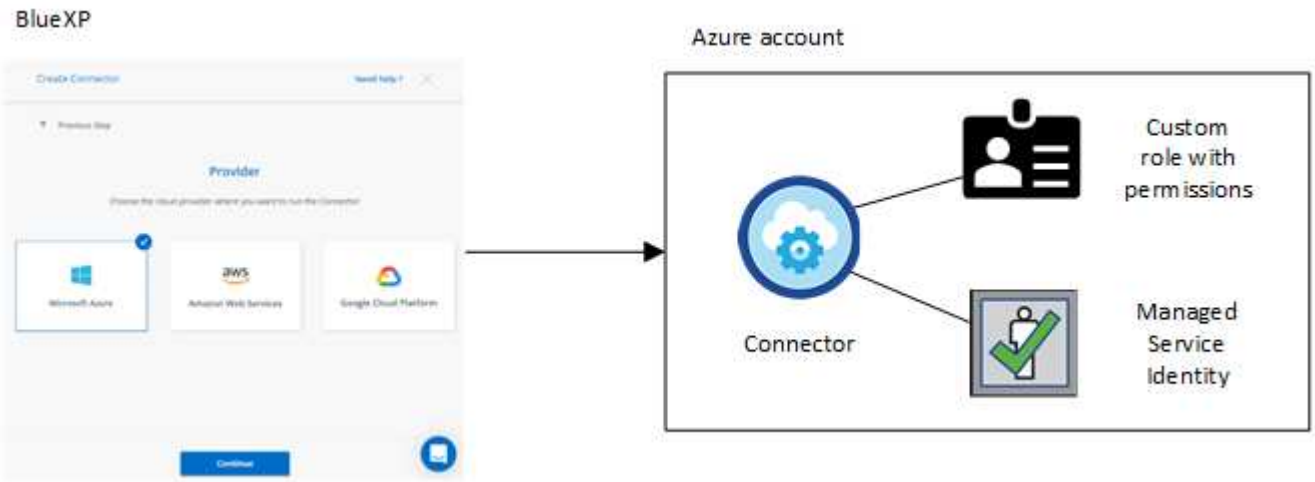
Scopri le credenziali e le autorizzazioni di Azure

Scopri in che modo BlueXP usa le credenziali di Azure per eseguire azioni per tuo conto e come tali credenziali sono associate alle iscrizioni al marketplace. La comprensione di questi dettagli può essere utile quando si gestiscono le credenziali per una o più sottoscrizioni Azure. Ad esempio, potrebbe essere utile sapere quando aggiungere ulteriori credenziali Azure a BlueXP.

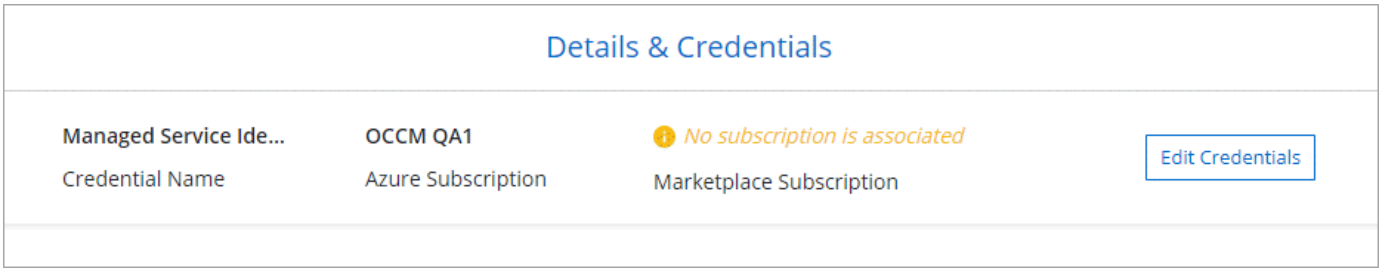
Credenziali iniziali di Azure

Quando si implementa un connettore da BlueXP, è necessario utilizzare un account Azure o un'entità di servizio che disponga delle autorizzazioni necessarie per implementare la macchina virtuale del connettore. Le autorizzazioni richieste sono elencate nella "Policy di implementazione del connettore per Azure".

Quando BlueXP implementa la macchina virtuale del connettore in Azure, abilita una "identità gestita assegnata dal sistema" sulla macchina virtuale, crea un ruolo personalizzato e lo assegna alla macchina virtuale. Il ruolo fornisce a BlueXP le autorizzazioni necessarie per gestire le risorse e i processi all'interno dell'abbonamento Azure. "Analisi dell'utilizzo delle autorizzazioni da parte di BlueXP".



Se si crea un nuovo ambiente di lavoro per Cloud Volumes ONTAP, BlueXP seleziona queste credenziali Azure per impostazione predefinita:



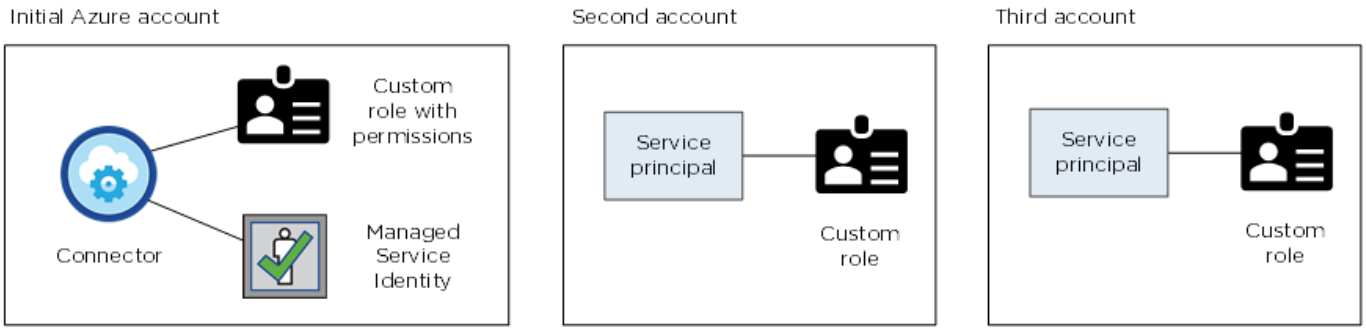
È possibile implementare tutti i sistemi Cloud Volumes ONTAP utilizzando le credenziali iniziali di Azure oppure aggiungere ulteriori credenziali.

Abbonamenti Azure aggiuntivi per un'identità gestita

L'identità gestita assegnata dal sistema alla macchina virtuale del connettore è associata all'abbonamento con cui è stato avviato il connettore. Se si desidera selezionare un abbonamento Azure diverso, è necessario "associare l'identità gestita a tali sottoscrizioni".

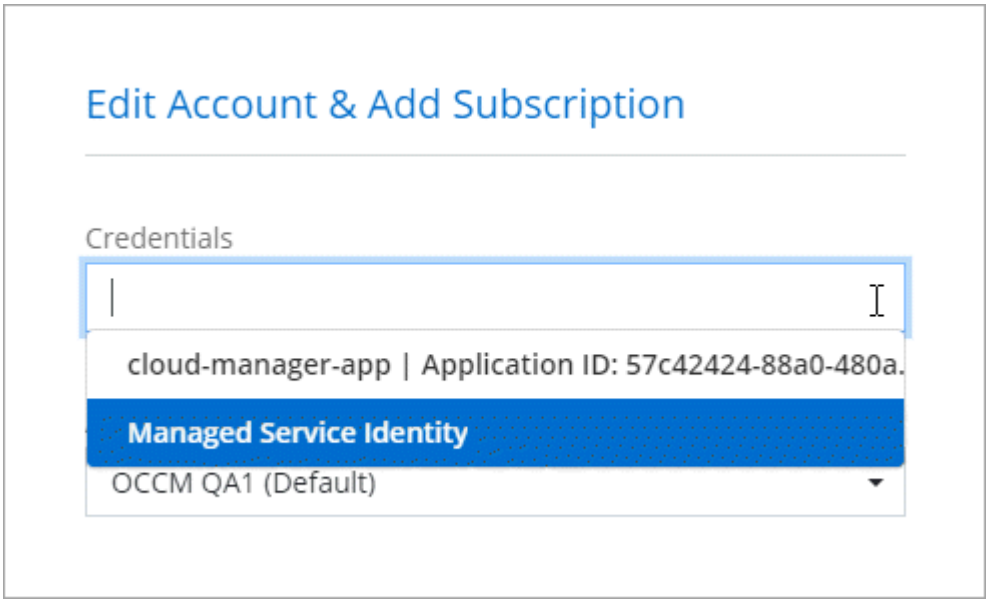
Credenziali Azure aggiuntive

Se si desidera utilizzare credenziali Azure diverse con BlueXP, è necessario concedere le autorizzazioni richieste da "Creazione e impostazione di un'entità di servizio in Microsoft Entra ID" Per ciascun account Azure. L'immagine seguente mostra due account aggiuntivi, ciascuno configurato con un'entità del servizio e un ruolo personalizzato che fornisce le autorizzazioni:



Allora "Aggiungere le credenziali dell'account a BlueXP" Fornendo dettagli sull'identità del servizio ad.

Ad esempio, è possibile passare da una credenziale all'altra quando si crea un nuovo ambiente di lavoro Cloud Volumes ONTAP:



Credenziali e iscrizioni al marketplace

Le credenziali che Aggiungi a un connettore devono essere associate a un'iscrizione ad Azure Marketplace in modo da poter pagare per Cloud Volumes ONTAP a una tariffa oraria (PAYGO) o tramite un contratto annuale e per utilizzare altri servizi BlueXP.

"Scopri come associare un abbonamento Azure".

Nota quanto segue sulle credenziali e le iscrizioni al marketplace di Azure:

- Puoi associare solo un'iscrizione ad Azure Marketplace a un set di credenziali Azure
- È possibile sostituire un abbonamento esistente al mercato con un nuovo abbonamento

FAQ

La seguente domanda riguarda le credenziali e gli abbonamenti.

Posso modificare l'iscrizione ad Azure Marketplace per gli ambienti di lavoro Cloud Volumes ONTAP?

Sì, è possibile. Quando modifichi l'abbonamento ad Azure Marketplace associato a un set di credenziali Azure, tutti gli ambienti di lavoro Cloud Volumes ONTAP esistenti e nuovi verranno addebitati sulla nuova iscrizione.

"Scopri come associare un abbonamento Azure".

Posso aggiungere più credenziali Azure, ciascuna con diverse iscrizioni al marketplace?

Tutte le credenziali di Azure che appartengono alla stessa iscrizione di Azure saranno associate alla stessa iscrizione di Azure Marketplace.

Se disponi di più credenziali Azure che appartengono a diverse iscrizioni ad Azure, queste possono essere associate alla stessa iscrizione ad Azure Marketplace o a diverse iscrizioni al marketplace.

Posso spostare gli ambienti di lavoro Cloud Volumes ONTAP esistenti in un'altra iscrizione ad Azure?

No, non è possibile spostare le risorse di Azure associate al tuo ambiente di lavoro Cloud Volumes ONTAP in un'altra sottoscrizione di Azure.

Come funzionano le credenziali per le implementazioni del marketplace e le implementazioni on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato per il connettore, fornito da BlueXP. È inoltre possibile implementare un connettore in Azure da Azure Marketplace e installare il software del connettore sul proprio host Linux.

Se si utilizza Marketplace, è possibile fornire autorizzazioni assegnando un ruolo personalizzato alla macchina virtuale del connettore e a un'identità gestita assegnata al sistema oppure è possibile utilizzare un'entità del servizio Microsoft Entra.

Per le implementazioni on-premise, non è possibile impostare un'identità gestita per il connettore, ma è possibile fornire le autorizzazioni utilizzando un'identità di servizio.

Per informazioni su come impostare le autorizzazioni, fare riferimento alle seguenti pagine:

- Modalità standard
  - "Impostare le autorizzazioni per un'implementazione di Azure Marketplace"
  - "Impostare le autorizzazioni per le implementazioni on-premise"
- "Impostare le autorizzazioni per la modalità limitata"
- "Impostare le autorizzazioni per la modalità privata"

Gestisci le credenziali di Azure e le iscrizioni al marketplace per BlueXP

Aggiungi e gestisci le credenziali Azure in modo che BlueXP disponga delle autorizzazioni necessarie per implementare e gestire le risorse cloud nelle tue sottoscrizioni Azure. Se si gestiscono più sottoscrizioni Azure Marketplace, è possibile assegnarle a diverse credenziali Azure dalla pagina credenziali.

Seguire la procedura riportata in questa pagina se si desidera utilizzare più credenziali Azure o più sottoscrizioni Azure Marketplace per Cloud Volumes ONTAP.

Panoramica

Esistono due modi per aggiungere ulteriori sottoscrizioni e credenziali Azure in BlueXP.

1. Associare ulteriori sottoscrizioni Azure all'identità gestita da Azure.
2. Se si desidera implementare Cloud Volumes ONTAP utilizzando credenziali Azure diverse, concedere le autorizzazioni Azure utilizzando un'entità del servizio e aggiungerne le credenziali a BlueXP.

Associare sottoscrizioni Azure aggiuntive a un'identità gestita

BlueXP consente di scegliere le credenziali Azure e l'abbonamento Azure in cui si desidera implementare Cloud Volumes ONTAP. Non è possibile selezionare un'altra sottoscrizione Azure per il profilo di identità gestita, a meno che non venga associato a. "identità gestita" con questi abbonamenti.

A proposito di questa attività

Un'identità gestita è "L'account Azure iniziale" Quando si implementa un connettore da BlueXP. Quando si implementa il connettore, BlueXP ha creato il ruolo di operatore BlueXP e lo ha assegnato alla macchina virtuale del connettore.

Fasi

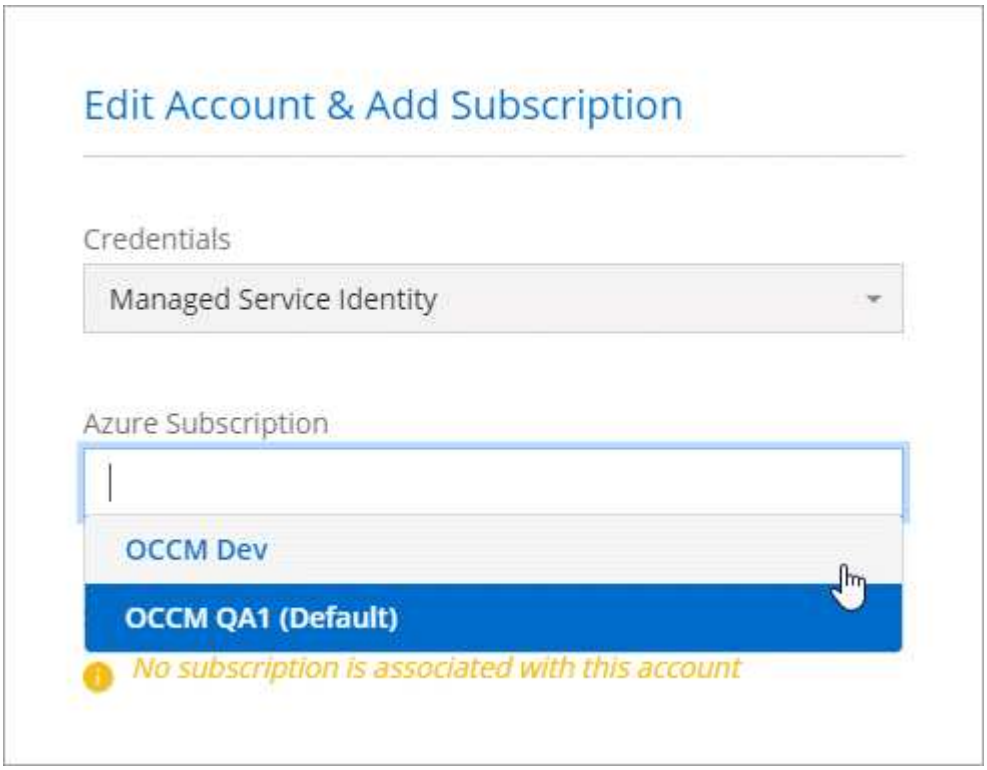
1. Accedere al portale Azure.
2. Aprire il servizio **Abbonamenti** e selezionare l'abbonamento in cui si desidera implementare Cloud Volumes ONTAP.
3. Selezionare **controllo di accesso (IAM)**.
   a. Selezionare **Aggiungi** > **Aggiungi assegnazione ruolo** e aggiungere le autorizzazioni:
      - Selezionare il ruolo **BlueXP Operator**.

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

      - Assegnare l'accesso a una **macchina virtuale**.
      - Selezionare l'abbonamento in cui è stata creata la macchina virtuale Connector.
      - Selezionare la macchina virtuale Connector.
      - Selezionare **Salva**.
4. Ripetere questa procedura per gli abbonamenti aggiuntivi.

Risultato

Quando crei un nuovo ambiente di lavoro, dovresti ora avere la possibilità di scegliere tra più sottoscrizioni Azure per il profilo di identità gestito.



Aggiungere ulteriori credenziali Azure a BlueXP

Quando si implementa un connettore da BlueXP, BlueXP abilita un'identità gestita assegnata dal sistema sulla macchina virtuale che dispone delle autorizzazioni necessarie. BlueXP seleziona queste credenziali Azure per impostazione predefinita quando si crea un nuovo ambiente di lavoro per Cloud Volumes ONTAP.

> Se il software Connector è stato installato manualmente su un sistema esistente, non viene aggiunto un set iniziale di credenziali. "Scopri le credenziali e le autorizzazioni di Azure".

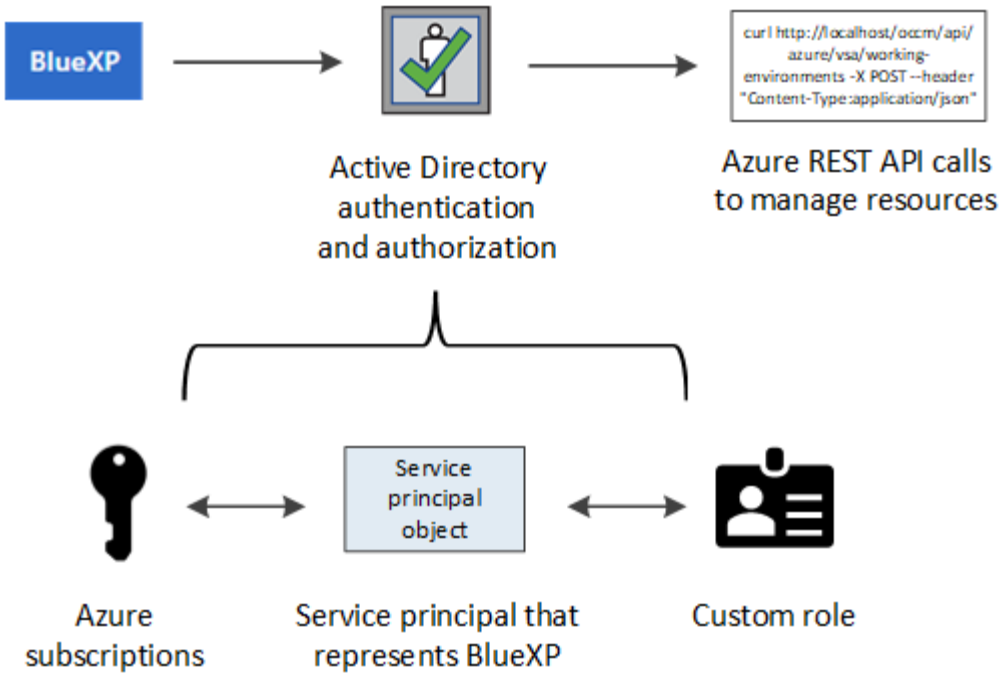
Se si desidera distribuire Cloud Volumes ONTAP utilizzando le credenziali *different* Azure, è necessario concedere le autorizzazioni richieste creando e impostando un'entità di servizio in Microsoft Entra ID per ogni account Azure. È quindi possibile aggiungere le nuove credenziali a BlueXP.

Concedere le autorizzazioni ad Azure utilizzando un'entità del servizio

BlueXP ha bisogno delle autorizzazioni per eseguire azioni in Azure. Puoi concedere le autorizzazioni richieste a un account Azure creando e impostando un'entità di servizio in Microsoft Entra ID e ottenendo le credenziali Azure necessarie per BlueXP.

A proposito di questa attività

L'immagine seguente mostra come BlueXP ottiene le autorizzazioni per eseguire operazioni in Azure. Un oggetto principale di servizio, legato a una o più sottoscrizioni di Azure, rappresenta BlueXP in Microsoft Entra ID e viene assegnato a un ruolo personalizzato che consente le autorizzazioni richieste.



Fasi

1. Creare un'applicazione Microsoft Entra.
2. Assegnare l'applicazione a un ruolo.
3. Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure.
4. Ottenere l'ID dell'applicazione e l'ID della directory.
5. Creare un client segreto.

Creare un'applicazione Microsoft Entra

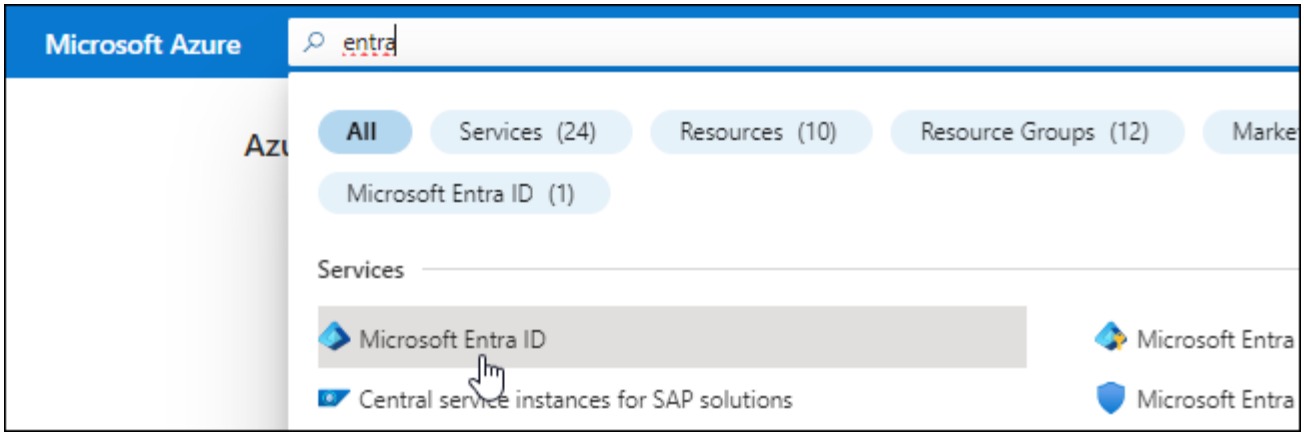
Creare un'applicazione e un'entità di servizio Microsoft Entra che BlueXP possa utilizzare per il role-based access control.

Fasi

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.

Risultato

Hai creato l'applicazione ad e il service principal.

Assegnare l'applicazione a un ruolo

È necessario associare l'entità del servizio a una o più sottoscrizioni Azure e assegnarle il ruolo personalizzato "operatore BlueXP" in modo che BlueXP disponga delle autorizzazioni in Azure.

Fasi

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.

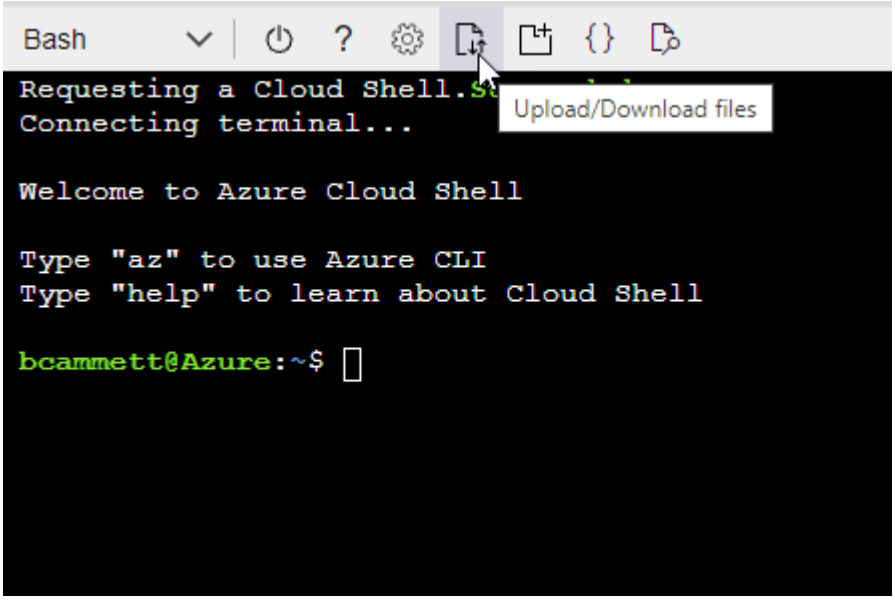
      Esempio

```
"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**.

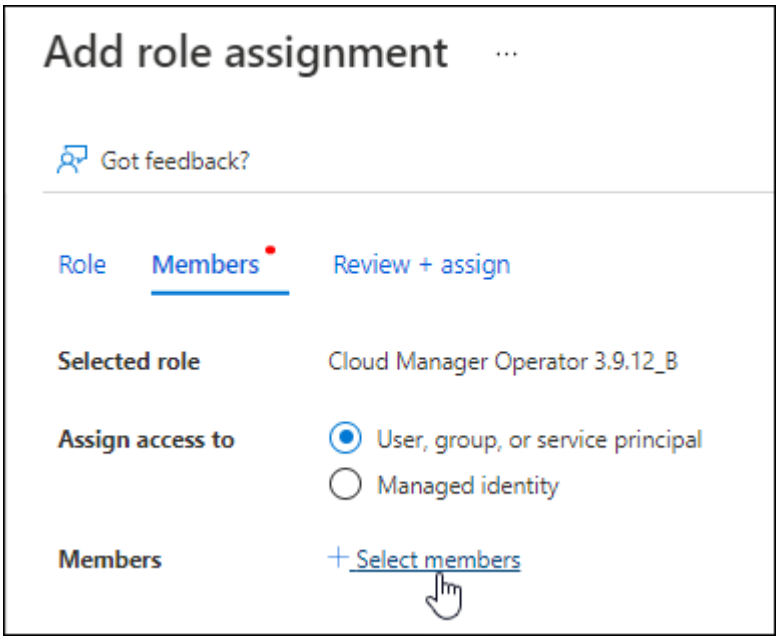
b. Selezionare l'abbonamento.

c. Selezionare **controllo di accesso (IAM) > Aggiungi > Aggiungi assegnazione ruolo**.

d. Nella scheda **ruolo**, selezionare il ruolo **operatore BlueXP** e selezionare **Avanti**.

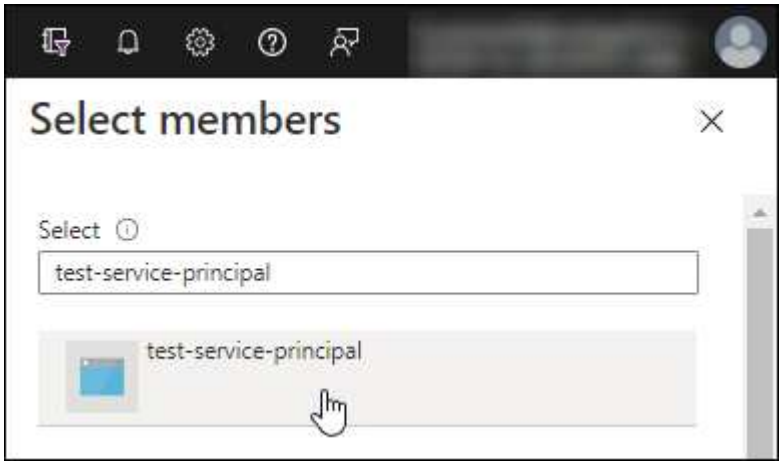
e. Nella scheda **membri**, completare la seguente procedura:

- 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.

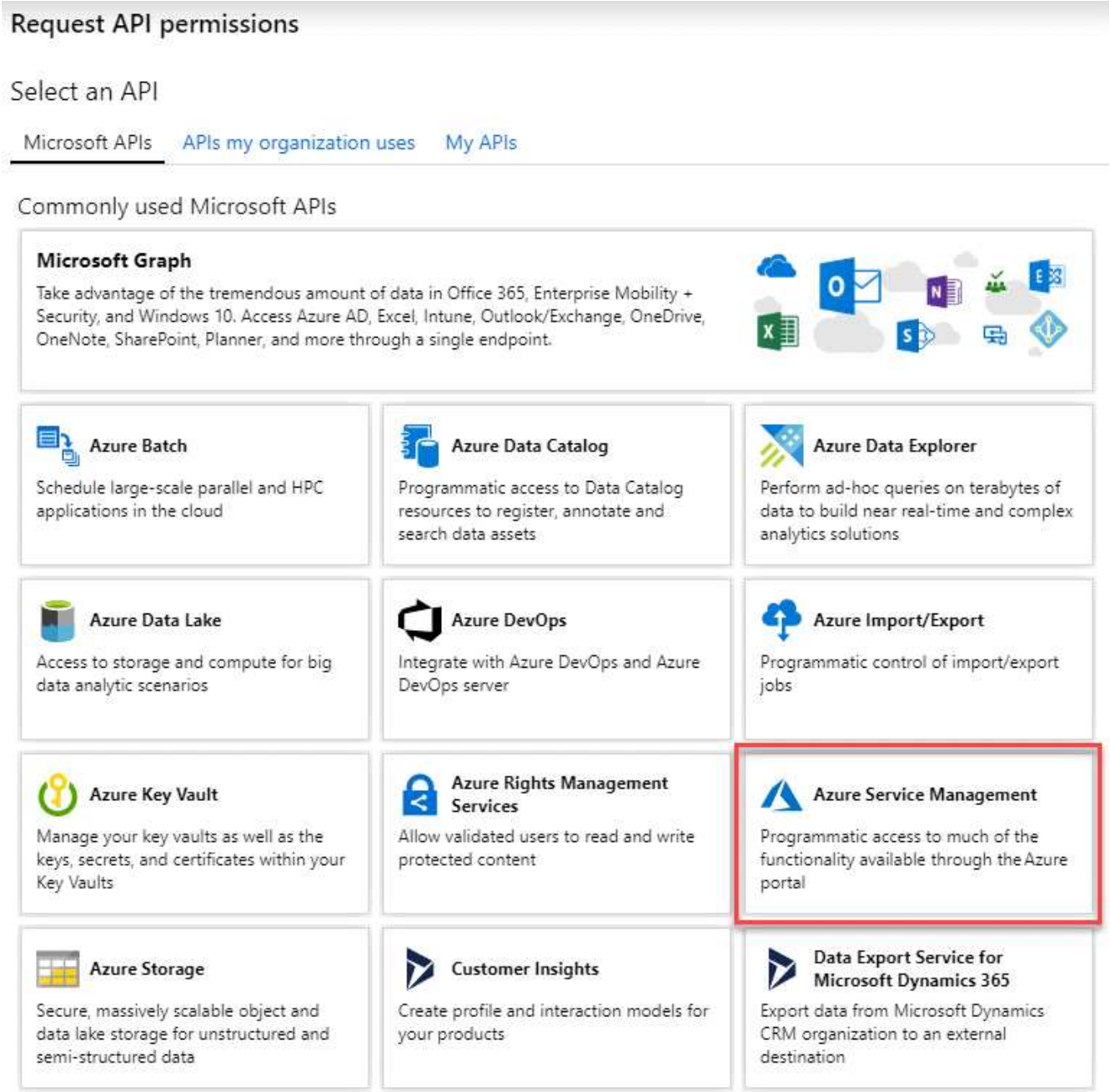
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. BlueXP consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure

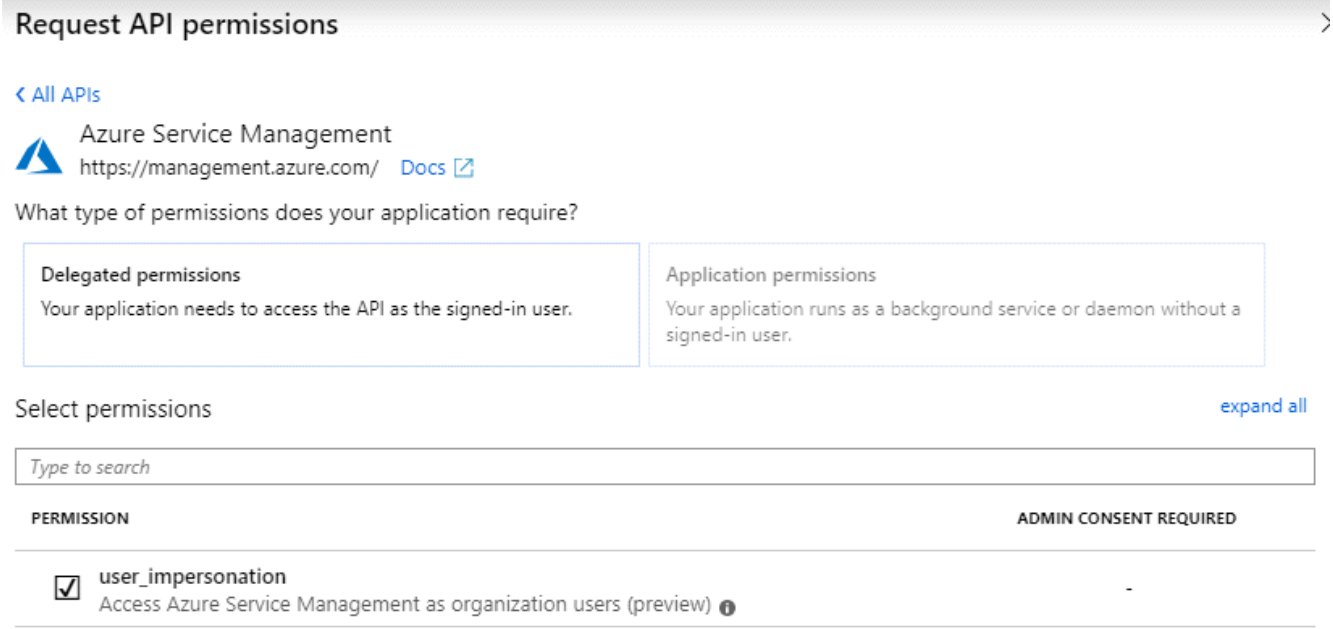
L'entità del servizio deve disporre delle autorizzazioni "API di gestione dei servizi Windows Azure".

Fasi

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).

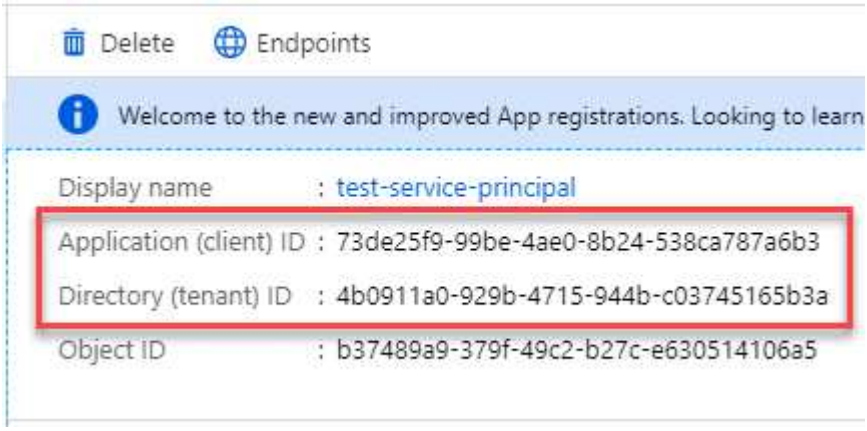


Ottenere l'ID dell'applicazione e l'ID della directory

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.

Fasi

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

Devi creare una password client e fornire a BlueXP il valore della password in modo che BlueXP possa utilizzarla per l'autenticazione con Microsoft Entra ID.

Fasi

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.

Aggiungere le credenziali a BlueXP

Dopo aver fornito un account Azure con le autorizzazioni richieste, è possibile aggiungere le credenziali per tale account a BlueXP. Il completamento di questo passaggio consente di avviare Cloud Volumes ONTAP utilizzando credenziali Azure diverse.

Prima di iniziare

Se hai appena creato queste credenziali nel tuo cloud provider, potrebbero essere necessari alcuni minuti prima che siano disponibili per l'utilizzo. Attendere alcuni minuti prima di aggiungere le credenziali a BlueXP.

Prima di iniziare

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

Fasi

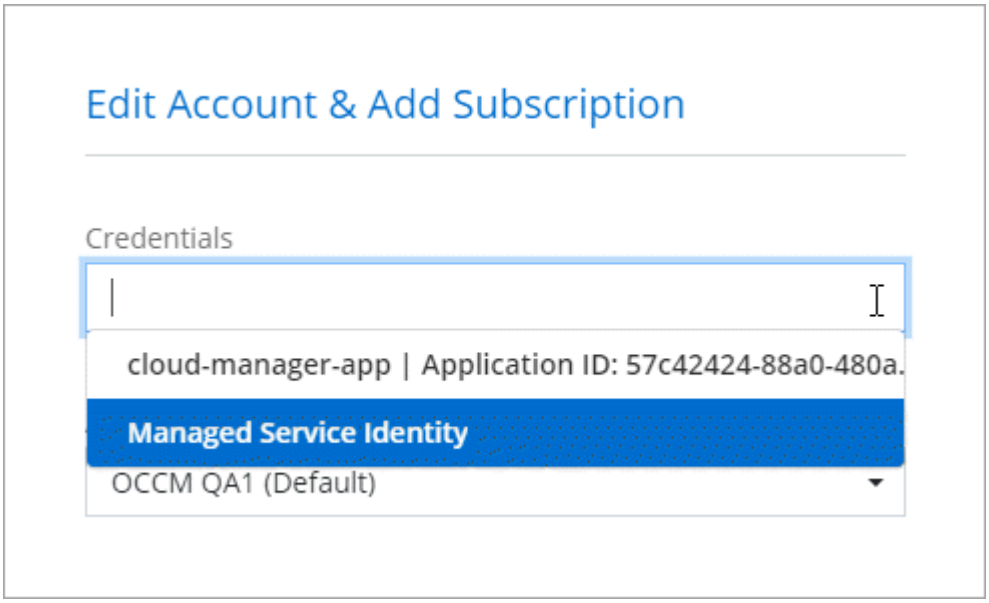
1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

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

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



Gestire le credenziali esistenti

Gestire le credenziali Azure già aggiunte a BlueXP associando un abbonamento Marketplace, modificando le credenziali ed eliminandole.

Associare un abbonamento a Azure Marketplace alle credenziali

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

Esistono due scenari in cui è possibile associare un abbonamento a Azure Marketplace dopo aver aggiunto le credenziali a BlueXP:

- Non hai associato un abbonamento quando inizialmente hai aggiunto le credenziali a BlueXP.
- Vuoi modificare l'iscrizione ad Azure Marketplace associata alle credenziali Azure.

  Sostituendo l'attuale sottoscrizione al marketplace con una nuova sottoscrizione, l'abbonamento al marketplace viene modificato per qualsiasi ambiente di lavoro Cloud Volumes ONTAP esistente e per tutti i nuovi ambienti di lavoro.

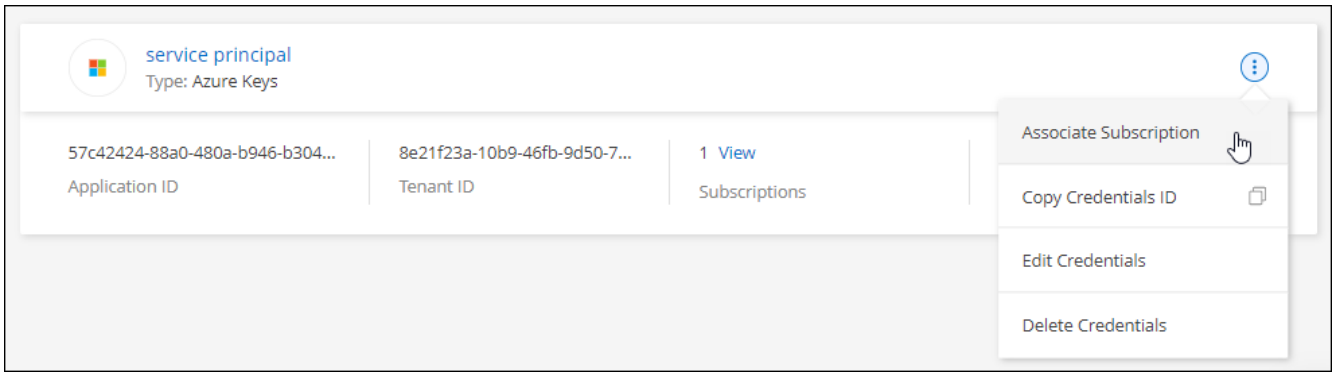
Prima di iniziare

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

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

Modificare le credenziali

Modificare le credenziali Azure in BlueXP modificando i dettagli relativi alle credenziali del servizio Azure. Ad esempio, potrebbe essere necessario aggiornare il segreto del client se è stato creato un nuovo segreto per l'applicazione principale del servizio.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.
2. Nella pagina **credenziali account**, selezionare il menu delle azioni per un set di credenziali, quindi selezionare **Modifica credenziali**.
3. Apportare le modifiche richieste, quindi selezionare **Applica**.

Eliminare le credenziali

Se non hai più bisogno di una serie di credenziali, puoi eliminarle da BlueXP. È possibile eliminare solo le credenziali non associate a un ambiente di lavoro.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.
2. Nella pagina **credenziali account**, selezionare il menu delle azioni per un set di credenziali, quindi selezionare **Elimina credenziali**.
3. Selezionare **Delete** per confermare.

Google Cloud

Scopri di più sui progetti e sulle autorizzazioni di Google Cloud

Scopri in che modo BlueXP usa le credenziali di Google Cloud per eseguire azioni per tuo conto e come tali credenziali sono associate alle iscrizioni al marketplace. Comprendere questi dettagli può essere utile quando si gestiscono le credenziali per uno o più progetti Google Cloud. Ad esempio, è possibile ottenere informazioni sull'account del servizio associato alla macchina virtuale del connettore.

Progetto e permessi per BlueXP

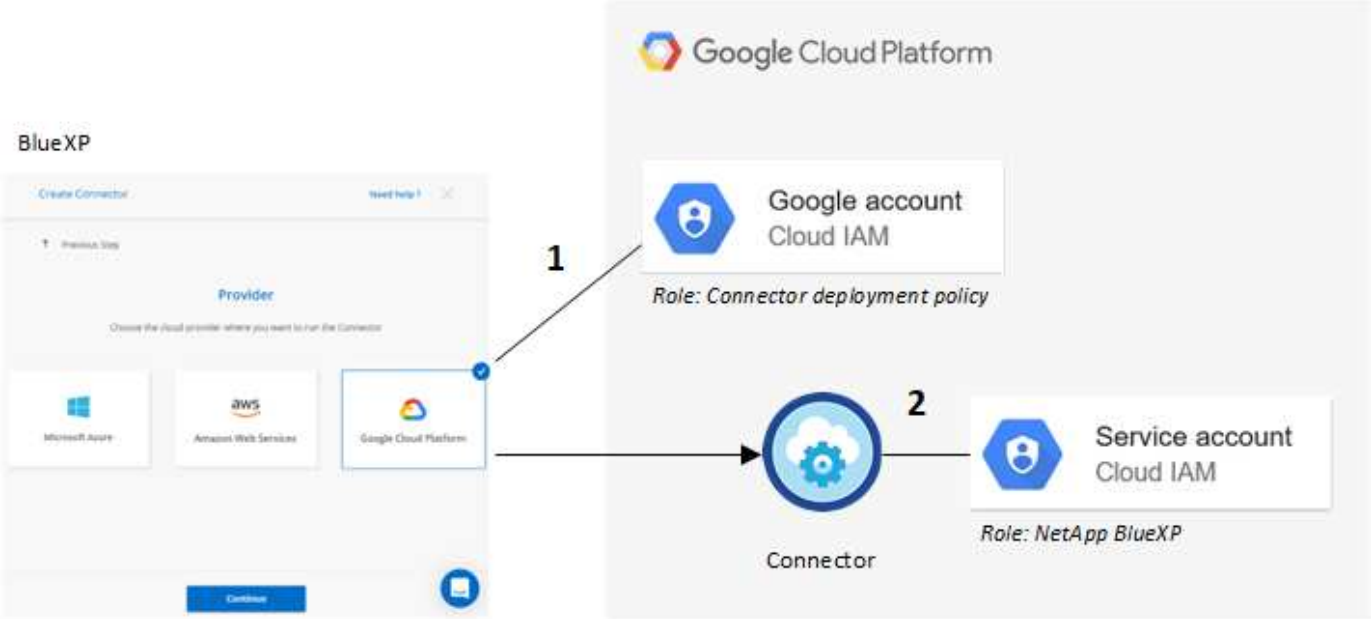
Prima di poter utilizzare BlueXP per gestire le risorse nel progetto Google Cloud, è necessario implementare un connettore. Il connettore non può essere in esecuzione in sede o in un altro cloud provider.

Prima di implementare un connettore direttamente da BlueXP, è necessario disporre di due set di autorizzazioni:

1. È necessario implementare un connettore utilizzando un account Google che disponga delle autorizzazioni per avviare l'istanza della macchina virtuale del connettore da BlueXP.
2. Quando si implementa il connettore, viene richiesto di selezionare un "account di servizio" Per l'istanza della macchina virtuale. BlueXP ottiene le autorizzazioni dall'account del servizio per creare e gestire i sistemi Cloud Volumes ONTAP, per gestire i backup utilizzando il backup e ripristino BlueXP e altro ancora.

Le autorizzazioni vengono fornite allegando un ruolo personalizzato all'account del servizio.

La seguente immagine mostra i requisiti di autorizzazione descritti nei numeri 1 e 2 precedenti:



Per informazioni su come impostare le autorizzazioni, fare riferimento alle seguenti pagine:

- "Impostare le autorizzazioni di Google Cloud per la modalità standard"
- "Impostare le autorizzazioni per la modalità limitata"
- "Impostare le autorizzazioni per la modalità privata"

Credenziali e iscrizioni al marketplace

Quando implementi un connettore in Google Cloud, BlueXP crea un set di credenziali predefinito per l'account del servizio Google Cloud nel progetto in cui risiede il connettore. Queste credenziali devono essere associate a un'iscrizione a Google Cloud Marketplace in modo da poter pagare per Cloud Volumes ONTAP a una tariffa oraria (PAYGO) e utilizzare altri servizi BlueXP.

"Scopri come associare un abbonamento a Google Cloud Marketplace".

Nota quanto segue riguardo le credenziali di Google Cloud e le iscrizioni al marketplace:

- A un connettore può essere associato un solo set di credenziali Google Cloud
- Puoi associare alle credenziali un solo abbonamento a Google Cloud Marketplace
- È possibile sostituire un abbonamento esistente al mercato con un nuovo abbonamento

Progetto per Cloud Volumes ONTAP

Cloud Volumes ONTAP può risiedere nello stesso progetto del connettore o in un progetto diverso. Per implementare Cloud Volumes ONTAP in un progetto diverso, è necessario prima aggiungere l'account e il ruolo del servizio Connector a tale progetto.

- "Scopri come configurare l'account di servizio"
- "Scopri come implementare Cloud Volumes ONTAP in Google Cloud e seleziona un progetto"

Gestire le credenziali e le sottoscrizioni di Google Cloud per BlueXP

È possibile gestire le credenziali Google Cloud associate all'istanza di Connector VM associando un abbonamento al marketplace e risolvendo i problemi del processo di abbonamento. Entrambe queste attività garantiscono che sia possibile utilizzare l'abbonamento al marketplace per pagare i servizi BlueXP.

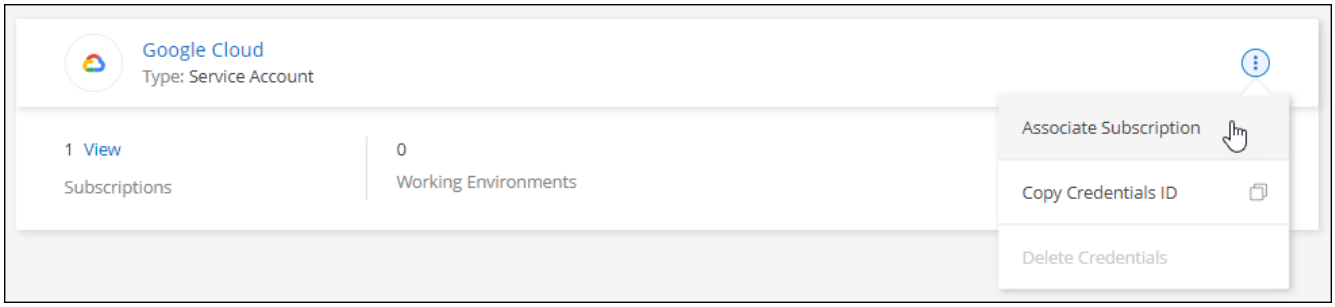
Associare un abbonamento Marketplace alle credenziali Google Cloud

Quando si implementa un connettore in Google Cloud, BlueXP crea un set predefinito di credenziali associate all'istanza della macchina virtuale del connettore. In qualsiasi momento, puoi modificare l'iscrizione di Google Cloud Marketplace associata a queste credenziali. L'abbonamento consente di creare un sistema Cloud Volumes ONTAP pay-as-you-go e di utilizzare altri servizi BlueXP.

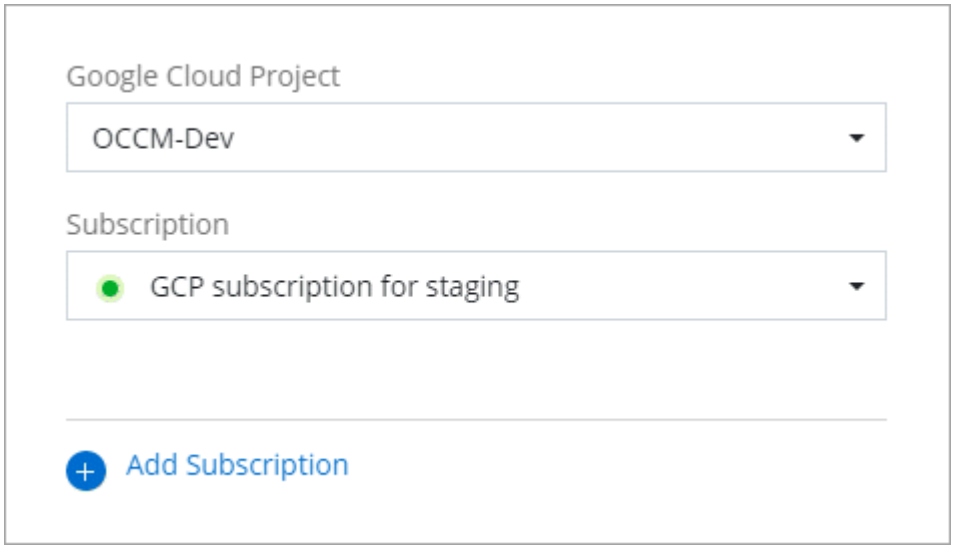
Sostituendo l'attuale sottoscrizione al marketplace con una nuova sottoscrizione, l'abbonamento al marketplace viene modificato per qualsiasi ambiente di lavoro Cloud Volumes ONTAP esistente e per tutti i nuovi ambienti di lavoro.

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**.



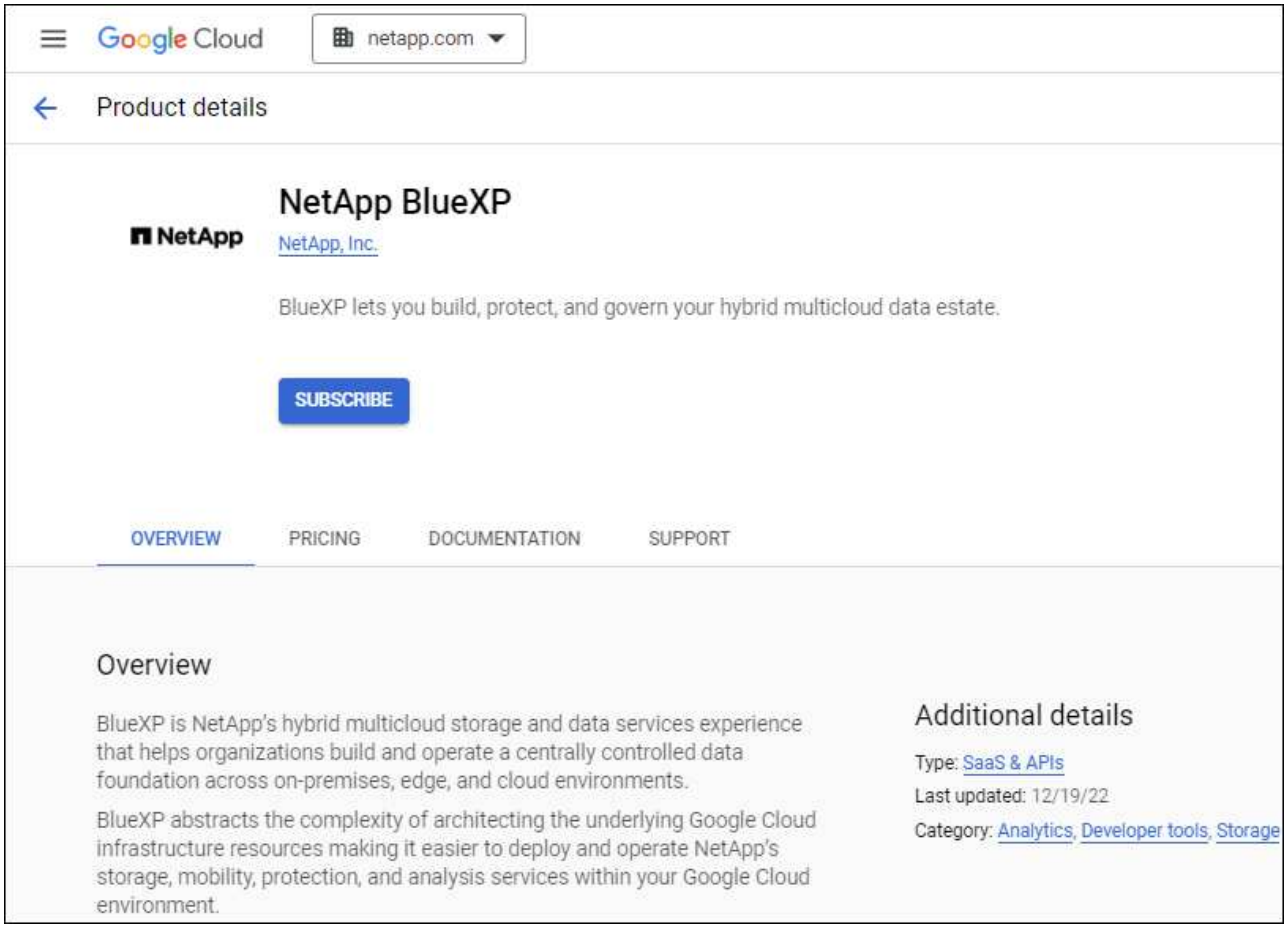
3. Per associare le credenziali a un abbonamento esistente, selezionare un progetto e un abbonamento Google Cloud dall'elenco a discesa, quindi selezionare **Associa**.



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**.

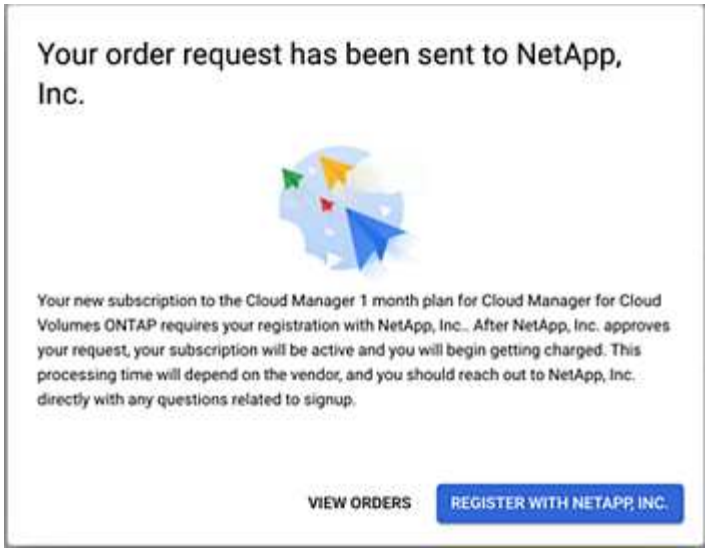
c. Selezionare l'account di fatturazione appropriato e accettare i termini e le condizioni.

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.

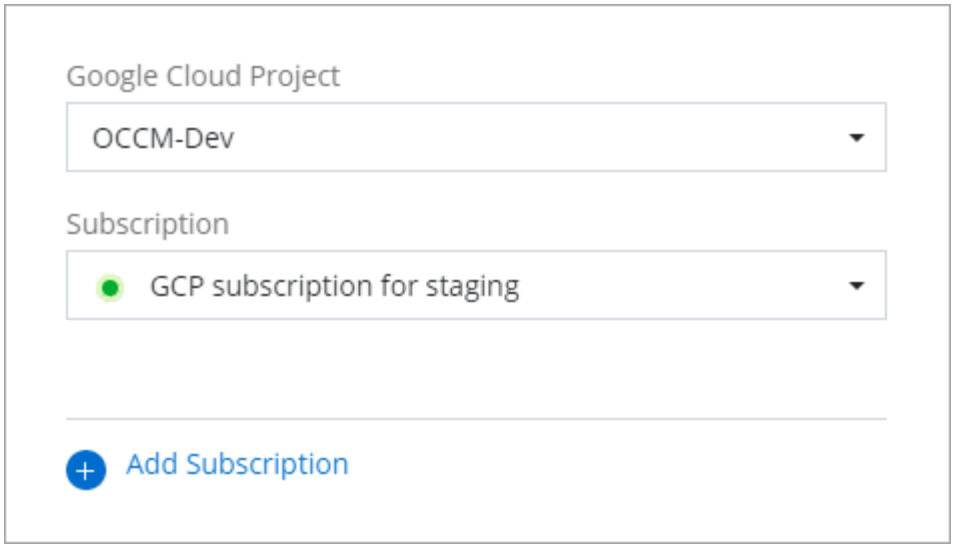
Per tutti gli altri account, è necessario associare manualmente l'abbonamento ripetendo questa procedura.

- 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.

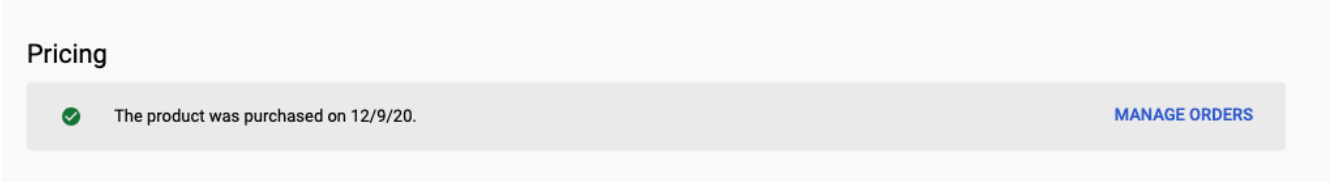


Risolvere i problemi relativi alla procedura di iscrizione a Marketplace

A volte, l'iscrizione a BlueXP tramite Google Cloud Marketplace può frammentarsi a causa di autorizzazioni errate o a causa del mancato reindirizzamento al sito Web BlueXP. In tal caso, attenersi alla procedura riportata di seguito per completare la procedura di iscrizione.

Fasi

1. Passare a. "Pagina NetApp BlueXP su Google Cloud Marketplace" per verificare lo stato dell'ordine. Se la pagina riporta **Gestisci su provider**, scorrere verso il basso e selezionare **Gestisci ordini**.



   - Se l'ordine mostra un segno di spunta verde e questo è inaspettato, qualcun altro dell'organizzazione che utilizza lo stesso account di fatturazione potrebbe essere già iscritto. In caso di imprevisti o se si richiedono i dettagli di questo abbonamento, contattare il team di vendita NetApp.

   - Se l'ordine mostra un orologio e lo stato **Pending**, torna alla pagina del marketplace e scegli **Manage on Provider** per completare il processo come descritto sopra.

Gestire le credenziali NSS associate a un account BlueXP

Associa un account del sito di supporto NetApp al tuo account BlueXP per abilitare i flussi di lavoro chiave per Cloud Volumes ONTAP. Queste credenziali NSS sono associate all'intero account BlueXP.

> BlueXP supporta anche l'associazione di un account NSS per utente BlueXP. "Scopri come gestire le credenziali a livello utente".

Panoramica

L'associazione delle credenziali NetApp Support Site con l'ID account BlueXP specifico è necessaria per attivare le seguenti attività in BlueXP:

- Implementazione di Cloud Volumes ONTAP con la propria licenza (BYOL)

  È necessario fornire l'account NSS in modo che BlueXP possa caricare la chiave di licenza e attivare l'abbonamento per il periodo di validità dell'acquisto. Sono inclusi gli aggiornamenti automatici per i rinnovi dei termini.

- Registrazione di sistemi Cloud Volumes ONTAP pay-as-you-go

  È necessario fornire l'account NSS per attivare il supporto per il sistema e accedere alle risorse di supporto tecnico di NetApp.

- Aggiornamento del software Cloud Volumes ONTAP alla versione più recente

Queste credenziali sono associate all'ID account BlueXP specifico. Gli utenti che appartengono all'account BlueXP possono accedere a queste credenziali da **Support > NSS Management**.

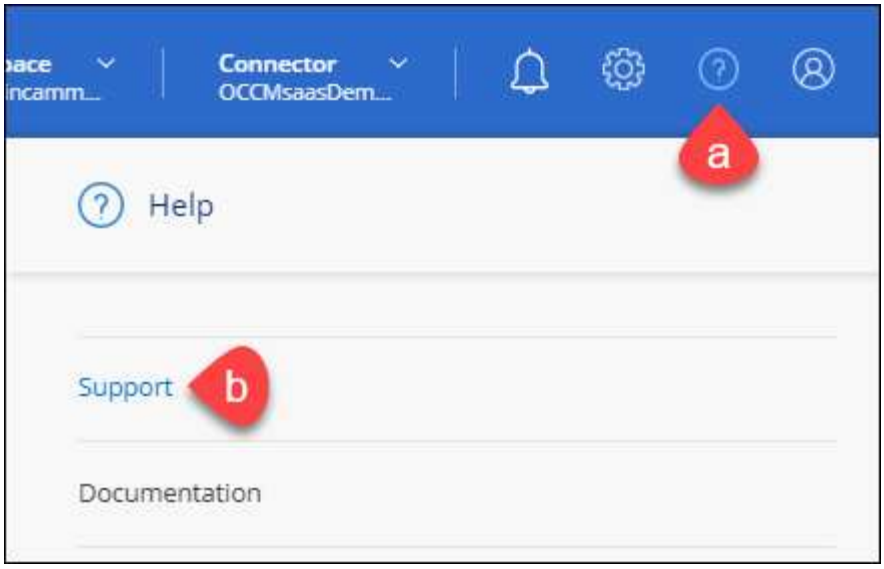
Aggiungi un account NSS

Support Dashboard consente di aggiungere e gestire gli account NetApp Support Site da utilizzare con BlueXP a livello di account BlueXP.

- Se disponi di un account a livello di cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o reseller, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

Fasi

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



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, selezionare **continua** per essere reindirizzato a una pagina di accesso Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e la licenza.

4. Nella pagina di accesso, fornire l'indirizzo e-mail e la password registrati del NetApp Support Site per eseguire il processo di autenticazione.

   Queste azioni consentono a BlueXP di utilizzare il tuo account NSS per download di licenze, verifica dell'aggiornamento software e registrazioni di supporto future.

   Tenere presente quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account guest o temporaneo). Puoi avere più account NSS a livello di cliente.
   - Se si tratta di un account di livello partner, può essere presente un solo account NSS. Se si tenta di aggiungere account NSS a livello di cliente ed esiste un account a livello di partner, viene visualizzato il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account, in quanto esistono già utenti NSS di tipo diverso."

   Lo stesso vale se si dispone di account NSS a livello di cliente preesistenti e si tenta di aggiungere un account a livello di partner.

   - Una volta effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che viene mappato all'e-mail. Nella pagina **NSS Management**, è possibile visualizzare l'e-mail da ••• menu.

   - Se è necessario aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Update Credentials** (Aggiorna credenziali) in ••• menu.

     Questa opzione richiede di effettuare nuovamente l'accesso. Il token per questi account scade dopo 90 giorni. Verrà inviata una notifica per avvisare l'utente.

Quali sono le prossime novità?

Gli utenti possono ora selezionare l'account durante la creazione di nuovi sistemi Cloud Volumes ONTAP e la registrazione di sistemi Cloud Volumes ONTAP esistenti.

- "Avvio di Cloud Volumes ONTAP in AWS"
- "Lancio di Cloud Volumes ONTAP in Azure"
- "Lancio di Cloud Volumes ONTAP in Google Cloud"
- "Registrazione di sistemi pay-as-you-go"

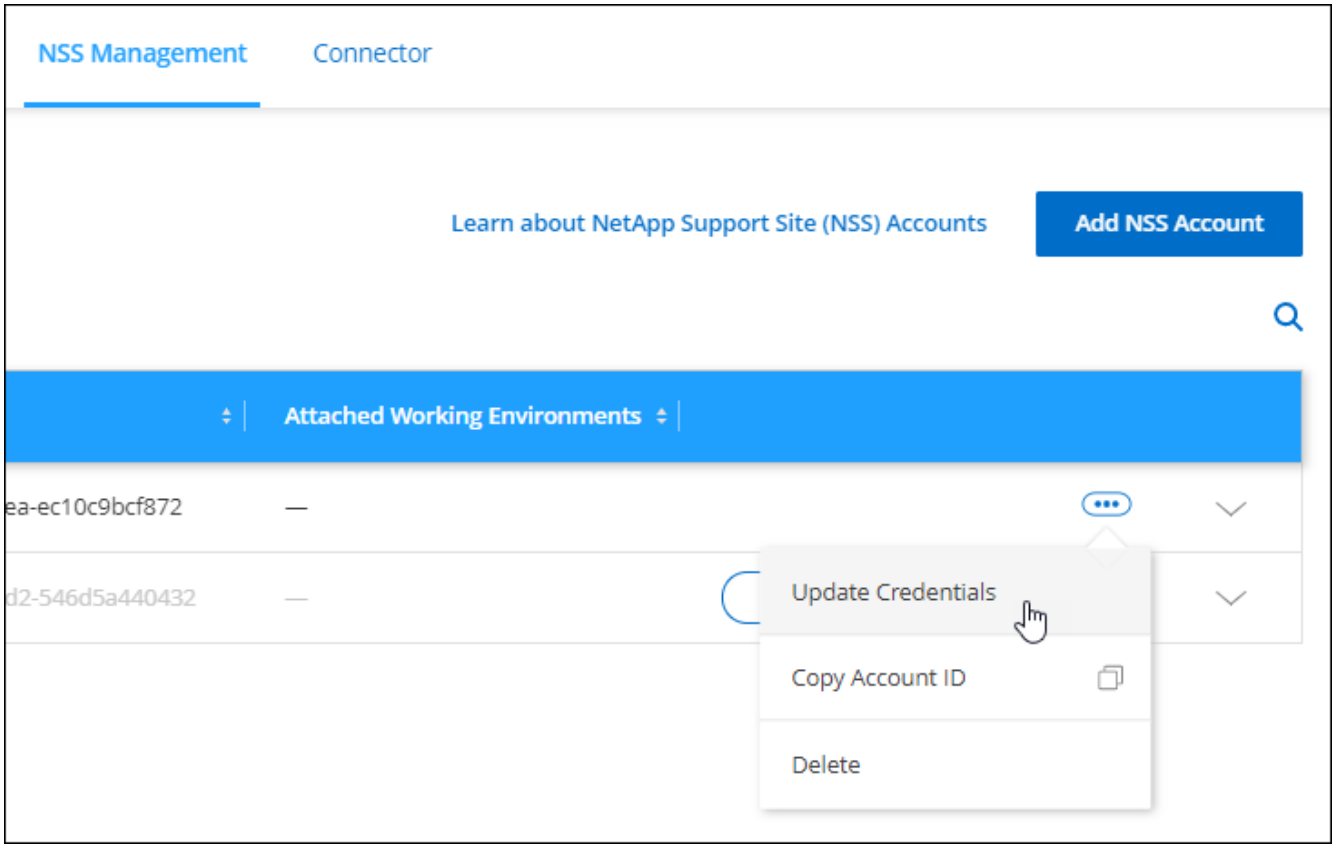
Aggiornare le credenziali NSS

Sarà necessario aggiornare le credenziali per gli account NSS in BlueXP quando si verifica una delle seguenti situazioni:

- Le credenziali dell'account vengono modificate
- Il token di refresh associato al tuo account scade dopo 3 mesi

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.
2. Selezionare **NSS Management**.
3. Per l'account NSS che si desidera aggiornare, selezionare ••• Quindi selezionare **Aggiorna credenziali**.



4. Quando richiesto, selezionare **continua** per essere reindirizzato a una pagina di accesso Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e la licenza.

5. Nella pagina di accesso, fornire l'indirizzo e-mail e la password registrati del NetApp Support Site per eseguire il processo di autenticazione.

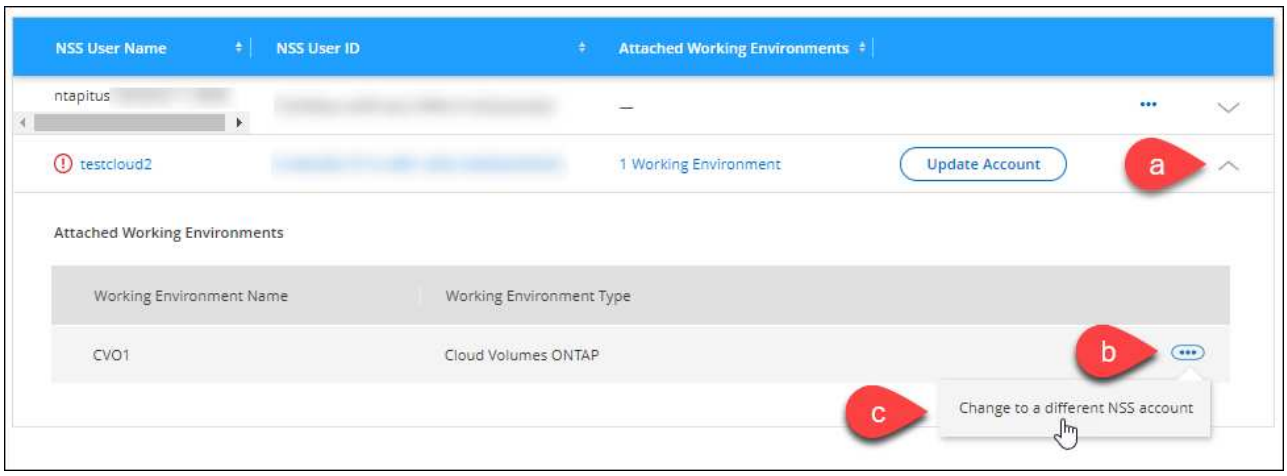
Collegare un ambiente di lavoro a un altro account NSS

Se l'organizzazione dispone di più account del sito di supporto NetApp, è possibile modificare l'account associato a un sistema Cloud Volumes ONTAP.

Questa funzione è supportata solo con gli account NSS configurati per l'utilizzo di Microsoft Entra ID adottato da NetApp per la gestione delle identità. Prima di utilizzare questa funzione, selezionare **Aggiungi account NSS** o **Aggiorna account**.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.
2. Selezionare **NSS Management**.
3. Per modificare l'account NSS, attenersi alla seguente procedura:
   a. Espandere la riga relativa all'account NetApp Support Site a cui è attualmente associato l'ambiente di lavoro.
   b. Per l'ambiente di lavoro per il quale si desidera modificare l'associazione, selezionare •••
   c. Selezionare **Cambia in un altro account NSS**.



   d. Selezionare l'account, quindi selezionare **Salva**.

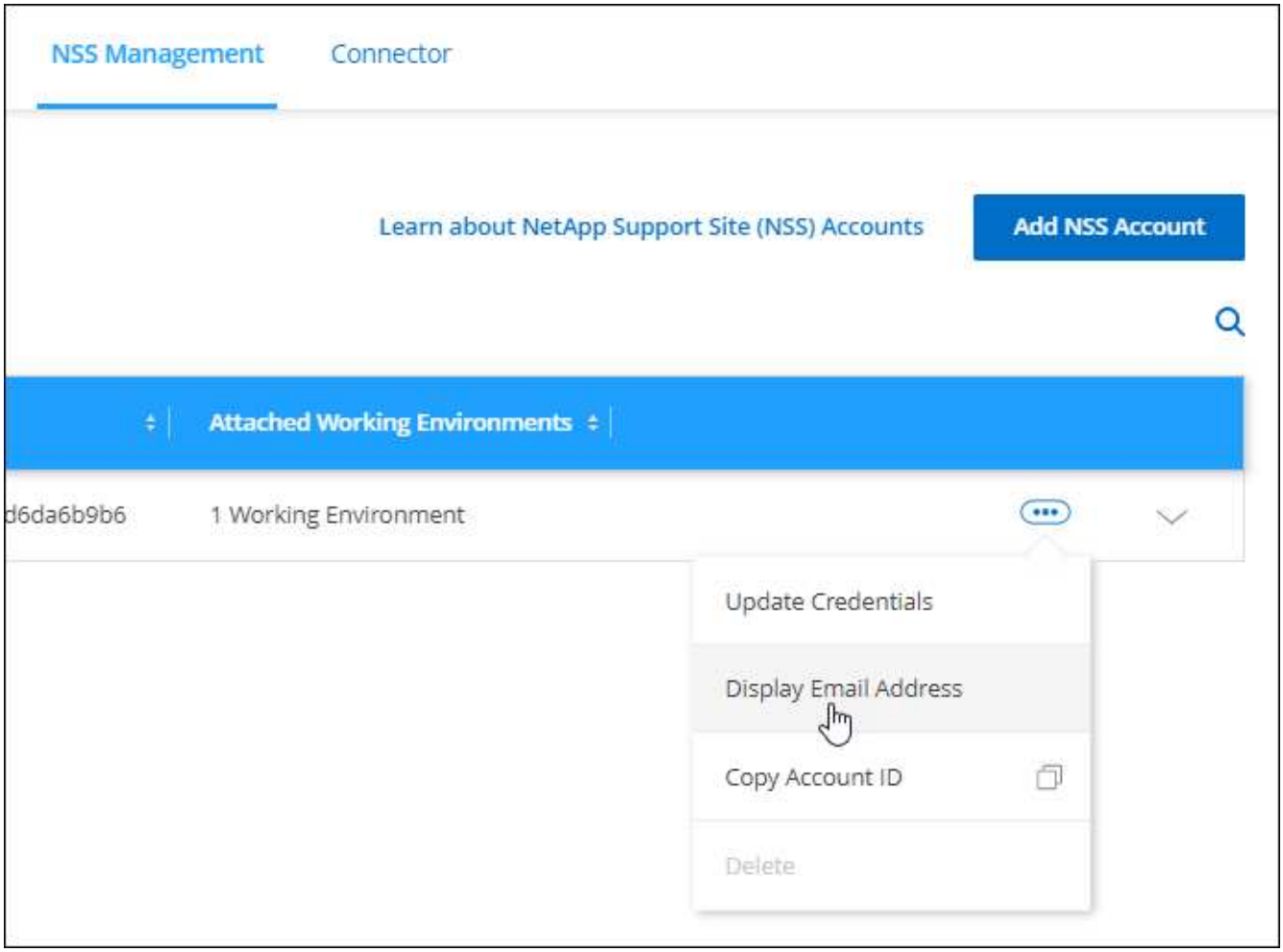
Visualizzare l'indirizzo e-mail di un account NSS

Ora che gli account del sito di supporto NetApp utilizzano l'Entra ID Microsoft per i servizi di autenticazione, il nome utente NSS visualizzato in BlueXP è in genere un identificatore generato da Microsoft Entra. Di conseguenza, potresti non conoscere immediatamente l'indirizzo e-mail associato a tale account. Tuttavia, BlueXP offre un'opzione per visualizzare l'indirizzo e-mail associato.

> Quando si accede alla pagina di gestione NSS, BlueXP genera un token per ciascun account nella tabella. Tale token include informazioni sull'indirizzo e-mail associato. Il token viene quindi rimosso quando si esce dalla pagina. Le informazioni non vengono mai memorizzate nella cache, il che contribuisce a proteggere la privacy dell'utente.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.
2. Selezionare **NSS Management**.
3. Per l'account NSS che si desidera aggiornare, selezionare ••• Quindi selezionare **Visualizza indirizzo e-mail**.



Risultato

BlueXP visualizza il nome utente del NetApp Support Site e l'indirizzo e-mail associato. È possibile utilizzare il pulsante di copia per copiare l'indirizzo e-mail.

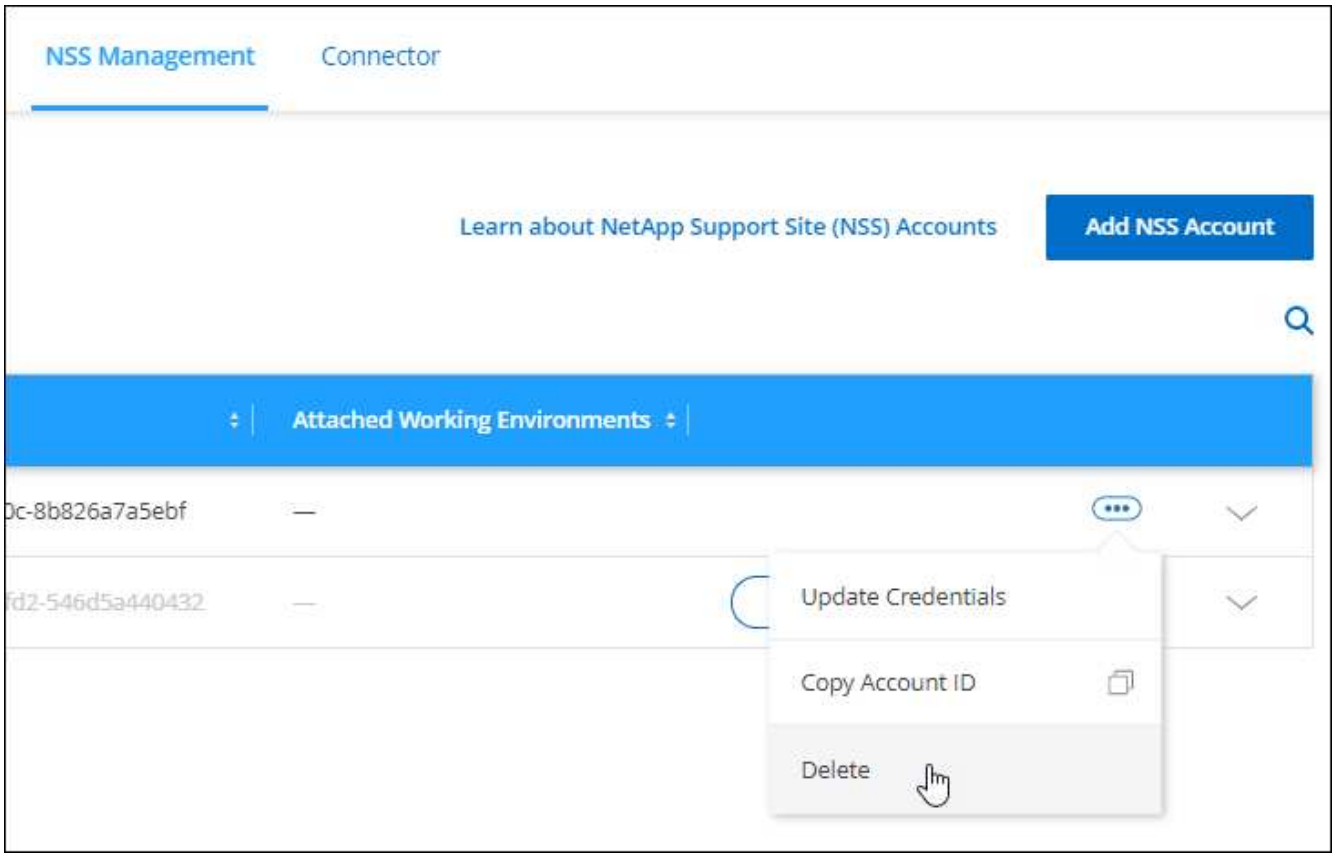
Rimuovere un account NSS

Eliminare gli account NSS che non si desidera più utilizzare con BlueXP.

Non puoi eliminare un account attualmente associato a un ambiente di lavoro Cloud Volumes ONTAP. Devi prima Collegare tali ambienti di lavoro a un account NSS diverso.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.
2. Selezionare **NSS Management**.
3. Per l'account NSS che si desidera eliminare, selezionare ••• Quindi selezionare **Delete** (Elimina).



4. Selezionare **Delete** per confermare.

Gestire le credenziali associate all'accesso a BlueXP

A seconda delle azioni intraprese in BlueXP, è possibile che siano associate le credenziali ONTAP e le credenziali del sito di supporto NetApp al proprio account di accesso utente BlueXP. È possibile visualizzare e gestire tali credenziali in BlueXP dopo averle associate. Ad esempio, se si modifica la password per queste credenziali, sarà necessario aggiornare la password in BlueXP.

Credenziali ONTAP

Quando si rileva direttamente un cluster ONTAP on-premise senza utilizzare un connettore, viene richiesto di immettere le credenziali ONTAP per il cluster. Queste credenziali vengono gestite a livello di utente, il che significa che non sono visualizzabili da altri utenti che effettuano l'accesso.

Credenziali NSS

Le credenziali NSS associate all'accesso a BlueXP consentono la registrazione del supporto, la gestione del caso e l'accesso a Digital Advisor.

- Quando si accede a **Support > Resources** e si effettua la registrazione per il supporto, viene richiesto di associare le credenziali NSS al proprio login BlueXP.

  Questa azione registra l'account BlueXP per il supporto e attiva i diritti di supporto. Solo un utente dell'account BlueXP deve associare un account del sito di supporto NetApp al proprio account di accesso BlueXP per registrarsi al supporto e attivare i diritti di supporto. Una volta completata questa operazione, la

pagina **risorse** mostra che il tuo account è registrato per il supporto.

"Scopri come registrarti per il supporto"

- Quando accedi a **Support > Case Management**, ti verrà richiesto di inserire le tue credenziali NSS, se non l'hai già fatto. Questa pagina consente di creare e gestire i casi di supporto associati all'account NSS e alla società.
- Quando si accede a Digital Advisor in BlueXP, viene richiesto di accedere a Digital Advisor inserendo le credenziali NSS.

Tenere presente quanto segue sull'account NSS associato all'accesso a BlueXP:

- L'account viene gestito a livello di utente, il che significa che non è visualizzabile da altri utenti che effettuano l'accesso.
- È possibile associare un solo account NSS a Digital Advisor e alla gestione dei casi di supporto, per utente.
- Se stai cercando di associare un account del sito di supporto NetApp a un ambiente di lavoro Cloud Volumes ONTAP, puoi scegliere solo tra gli account NSS aggiunti all'account BlueXP di cui sei membro.

  Le credenziali a livello di account NSS sono diverse dall'account NSS associato all'accesso a BlueXP. Le credenziali a livello di account NSS consentono di implementare Cloud Volumes ONTAP quando si porta la propria licenza (BYOL), registrare i sistemi PAYGO e aggiornare il software Cloud Volumes ONTAP.

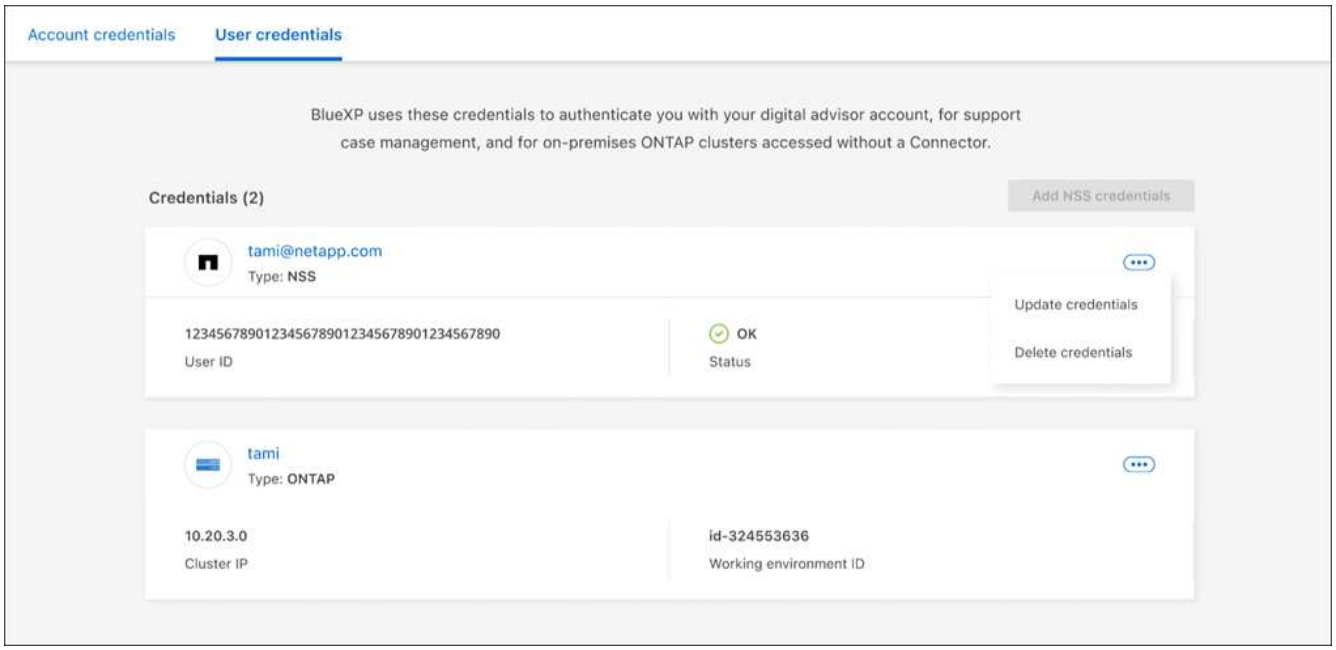
  "Scopri di più sull'utilizzo delle credenziali NSS con il tuo account BlueXP".

Gestire le credenziali utente

Gestire le credenziali utente aggiornando il nome utente e la password o eliminando le credenziali.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.
2. Selezionare **User Credentials** (credenziali utente).
3. Se non si dispone ancora di credenziali utente, selezionare **Aggiungi credenziali NSS** per aggiungere l'account NetApp Support Site.
4. Gestire le credenziali esistenti scegliendo le seguenti opzioni:
   - **Aggiorna credenziali**: Consente di aggiornare il nome utente e la password dell'account.
   - **Delete credentials** (Elimina credenziali): Consente di rimuovere l'account associato all'account utente BlueXP.



Risultato

BlueXP aggiorna le tue credenziali. Le modifiche verranno applicate quando si accede al cluster ONTAP, a Consulente digitale o alla pagina Gestione casi.

Riferimento

Permessi

Riepilogo delle autorizzazioni per BlueXP

Per utilizzare le funzionalità e i servizi di BlueXP, è necessario fornire le autorizzazioni in modo che BlueXP possa eseguire le operazioni nell'ambiente cloud. Utilizzare i collegamenti presenti in questa pagina per accedere rapidamente alle autorizzazioni necessarie in base all'obiettivo.

Autorizzazioni AWS

BlueXP richiede le autorizzazioni AWS per il connettore e per i singoli servizi.

Connettori

Obiettivo	Descrizione	Collegamento
Implementa il connettore da BlueXP	L'utente che crea un connettore da BlueXP ha bisogno di autorizzazioni specifiche per implementare l'istanza in AWS.	"Impostare le autorizzazioni AWS"
Fornire le autorizzazioni per il connettore	Quando BlueXP avvia il connettore, allega un criterio all'istanza che fornisce le autorizzazioni necessarie per gestire le risorse e i processi nell'account AWS. Devi impostare la policy da solo se avvii un connettore da AWS Marketplace, se installi manualmente il connettore o se vuoi "Aggiungere altre credenziali AWS a un connettore". Inoltre, è necessario assicurarsi che il criterio sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive.	"Autorizzazioni AWS per il connettore"

Backup e recovery

Obiettivo	Descrizione	Collegamento
Eseguire il backup dei cluster ONTAP on-premise su Amazon S3	Quando si attivano i backup sui volumi ONTAP, il backup e ripristino di BlueXP richiede di inserire una chiave di accesso e un segreto per un utente IAM che dispone di autorizzazioni specifiche.	"Impostare le autorizzazioni S3 per i backup"

Cloud Volumes ONTAP

Obiettivo	Descrizione	Collegamento
Fornire autorizzazioni per i nodi Cloud Volumes ONTAP	Un ruolo IAM deve essere associato a ciascun nodo Cloud Volumes ONTAP in AWS. Lo stesso vale per il mediatore ha. L'opzione predefinita è consentire a BlueXP di creare i ruoli IAM per te, ma puoi utilizzarne uno personalizzato durante la creazione dell'ambiente di lavoro.	"Scopri come impostare i ruoli IAM da solo"

Copia e sincronizzazione

Obiettivo	Descrizione	Collegamento
Implementa il broker dei dati in AWS	L'account utente AWS utilizzato per implementare il broker di dati deve disporre di autorizzazioni specifiche.	"Autorizzazioni necessarie per implementare il data broker in AWS"
Fornire le autorizzazioni per il broker di dati	Quando BlueXP copia e sincronizza implementa il data broker, crea un ruolo IAM per l'istanza del data broker. Se preferisci, puoi implementare il data broker utilizzando il tuo ruolo IAM.	"Requisiti per utilizzare il tuo ruolo IAM con il broker dei dati AWS"
Abilitare l'accesso AWS per un broker dei dati installato manualmente	Se utilizzi il broker di dati con un rapporto di sincronizzazione che include un bucket S3, devi preparare l'host Linux per l'accesso ad AWS. Quando installi il broker di dati, dovrai fornire le chiavi AWS a un utente IAM che dispone di accesso programmatico e autorizzazioni specifiche.	"Abilitazione dell'accesso ad AWS"

FSX per ONTAP

Obiettivo	Descrizione	Collegamento
Crea e gestisci FSX per ONTAP	Per creare o gestire un ambiente di lavoro Amazon FSX per NetApp ONTAP, devi aggiungere le credenziali AWS a BlueXP fornendo l'ARN di un ruolo IAM che conferisce ad BlueXP le autorizzazioni necessarie per creare l'ambiente di lavoro.	"Scopri come configurare le credenziali AWS per FSX"

Tiering

Obiettivo	Descrizione	Collegamento
Eseguire il Tier dei cluster ONTAP on-premise su Amazon S3	Quando si attiva il tiering BlueXP su AWS, la procedura guidata richiede di inserire una chiave di accesso e una chiave segreta. Queste credenziali vengono passate al cluster ONTAP in modo che ONTAP possa eseguire il Tier dei dati al bucket S3.	"Impostare le autorizzazioni S3 per il tiering"

Autorizzazioni Azure

BlueXP richiede le autorizzazioni di Azure per il connettore e per i singoli servizi.

Connettori

Obiettivo	Descrizione	Collegamento
Implementa il connettore da BlueXP	Quando si implementa un connettore da BlueXP, è necessario utilizzare un account Azure o un'entità di servizio che disponga delle autorizzazioni per implementare la macchina virtuale del connettore in Azure.	"Impostare le autorizzazioni Azure"
Fornire le autorizzazioni per il connettore	Quando BlueXP implementa la macchina virtuale del connettore in Azure, crea un ruolo personalizzato che fornisce le autorizzazioni necessarie per gestire le risorse e i processi all'interno dell'abbonamento Azure. È necessario impostare il ruolo personalizzato se si avvia un connettore dal mercato, se si installa manualmente il connettore o se si desidera "Aggiungere altre credenziali Azure a un connettore". Inoltre, è necessario assicurarsi che il criterio sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive.	"Autorizzazioni Azure per il connettore"

Copia e sincronizzazione

Obiettivo	Descrizione	Collegamento
Implementa il broker di dati in Azure	L'account utente Azure utilizzato per implementare il broker di dati deve disporre delle autorizzazioni richieste.	"Autorizzazioni necessarie per implementare il data broker in Azure"

Permessi Google Cloud

BlueXP richiede le autorizzazioni di Google Cloud per il connettore e per i singoli servizi.

Connettori

Obiettivo	Descrizione	Collegamento
Implementa il connettore da BlueXP	L'utente di Google Cloud che implementa un connettore di BlueXP ha bisogno di autorizzazioni specifiche per implementare il connettore in Google Cloud.	"Impostare le autorizzazioni per creare il connettore"
Fornire le autorizzazioni per il connettore	L'account di servizio per l'istanza di Connector VM deve disporre di autorizzazioni specifiche per le operazioni quotidiane. È necessario associare l'account del servizio al connettore durante la distribuzione. Inoltre, è necessario assicurarsi che il criterio sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive.	"Impostare le autorizzazioni per il connettore"

Backup e recovery

Obiettivo	Descrizione	Collegamento
Eseguire il backup di Cloud Volumes ONTAP su Google Cloud	Quando si utilizza il backup e ripristino di BlueXP per eseguire il backup di Cloud Volumes ONTAP, è necessario aggiungere autorizzazioni al connettore nei seguenti scenari: • Si desidera utilizzare la funzionalità di ricerca e ripristino • Si desidera utilizzare le chiavi di crittografia gestite dal cliente (CMEK)	• "Permessi per la funzionalità di ricerca Restore" • "Permessi per i CMEK"
Eseguire il backup dei cluster ONTAP on-premise su Google Cloud	Quando si utilizza il backup e ripristino di BlueXP per eseguire il backup dei cluster ONTAP on-premise, è necessario aggiungere le autorizzazioni al connettore per utilizzare la funzionalità di ricerca e ripristino.	"Permessi per la funzionalità di ricerca Restore"

Cloud Volumes Service per Google Cloud

Obiettivo	Descrizione	Collegamento
Scopri Cloud Volumes Service per Google Cloud	BlueXP deve accedere all'API di Cloud Volumes Service e disporre delle autorizzazioni necessarie tramite un account di servizio Google Cloud.	"Impostare un account di servizio"

Copia e sincronizzazione

Obiettivo	Descrizione	Collegamento
Implementa il broker dei dati in Google Cloud	Verifica che l'utente Google Cloud che implementa il broker di dati disponga delle autorizzazioni richieste.	"Autorizzazioni necessarie per implementare il data broker in Google Cloud"
Attiva l'accesso a Google Cloud per un broker dei dati installato manualmente	Se intendi utilizzare il data broker con una relazione di sincronizzazione che include un bucket di storage Google Cloud, devi preparare l'host Linux per l'accesso a Google Cloud. Quando si installa il data broker, è necessario fornire una chiave per un account di servizio che dispone di autorizzazioni specifiche.	"Abilitazione dell'accesso a Google Cloud"

Permessi StorageGRID

BlueXP richiede autorizzazioni StorageGRID per due servizi.

Backup e recovery

Obiettivo	Descrizione	Collegamento
Eseguire il backup dei cluster ONTAP on-premise su StorageGRID	Quando si prepara StorageGRID come destinazione di backup per i cluster ONTAP, il backup e ripristino di BlueXP richiede di inserire una chiave di accesso e un segreto per un utente IAM che dispone di autorizzazioni specifiche.	"Preparare StorageGRID come destinazione del backup"

Tiering

Obiettivo	Descrizione	Collegamento
Eseguire il Tier dei cluster ONTAP on-premise in StorageGRID	Quando si imposta il tiering BlueXP su StorageGRID, è necessario fornire il tiering BlueXP con una chiave di accesso S3 e una chiave segreta. BlueXP Tiering utilizza le chiavi per accedere ai bucket.	"Preparare il tiering a StorageGRID"

Autorizzazioni AWS per il connettore

Quando BlueXP avvia l'istanza del connettore in AWS, allega un criterio all'istanza che fornisce al connettore le autorizzazioni per gestire le risorse e i processi all'interno di tale account AWS. Il connettore utilizza le autorizzazioni per effettuare chiamate API a diversi servizi AWS, tra cui EC2, S3, CloudFormation, IAM, Il servizio di gestione delle chiavi (KMS) e molto altro ancora.

Policy IAM

Le policy IAM disponibili di seguito forniscono le autorizzazioni necessarie a un connettore per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico in base alla tua regione AWS.

Tenere presente quanto segue:

- Se si crea un connettore in una regione AWS standard direttamente da BlueXP, BlueXP applica automaticamente i criteri al connettore. In questo caso, non è necessario eseguire alcuna operazione.
- È necessario impostare autonomamente i criteri se si implementa il connettore da AWS Marketplace, se si installa manualmente il connettore su un host Linux o se si desidera aggiungere ulteriori credenziali AWS a BlueXP.
- Inoltre, è necessario assicurarsi che i criteri siano aggiornati quando vengono aggiunte nuove autorizzazioni nelle release successive.
- Se necessario, è possibile limitare le policy IAM utilizzando il modulo IAM `Condition` elemento. "Documentazione AWS: Elemento Condition"
- Per visualizzare istruzioni dettagliate sull'utilizzo di questi criteri, fare riferimento alle seguenti pagine:
  - "Impostare le autorizzazioni per un'implementazione di AWS Marketplace"
  - "Impostare le autorizzazioni per le implementazioni on-premise"
  - "Impostare le autorizzazioni per la modalità limitata"
  - "Impostare le autorizzazioni per la modalità privata"

Selezionare la propria regione per visualizzare le policy richieste:

Regioni standard

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.

Il primo criterio fornisce le autorizzazioni per i seguenti servizi:

- Discovery bucket Amazon S3
- Backup e recovery
- Classificazione
- Cloud Volumes ONTAP
- FSX per ONTAP
- Tiering

Il secondo criterio fornisce le autorizzazioni per i seguenti servizi:

- Caching edge
- Kubernetes

Policy n. 1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeTags",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:CreatePlacementGroup",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
```

```
                "ec2:UnassignPrivateIpAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteRoute",
                "ec2:DeletePlacementGroup",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumesModifications",
                "ec2:ModifyVolume",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "cloudformation:DeleteStack",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:ListInstanceProfiles",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:GetRolePolicy",
                "iam:GetRole",
                "sts:DecodeAuthorizationMessage",
                "sts:AssumeRole",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:PutObject",
                "s3:ListAllMyBuckets",
                "s3:GetObject",
```

```
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
```

```
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
```

```
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
```

```
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
    ]
```

```
}
```

Policy n. 2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeRegions",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "K8sServicePolicy"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudwatch:GetMetricStatistics",
                "cloudformation:ListStacks"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "GFCservicePolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GFCInstance": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "tag:getResources",
                "tag:getTagKeys",
                "tag:getTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "tagServicePolicy"
        }
    ]
}
```

Regioni di GovCloud (USA)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListInstanceProfiles",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "ec2:ModifyVolumeAttribute",
                "sts:DecodeAuthorizationMessage",
                "ec2:DescribeImages",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstances",
                "iam:PassRole",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:DeleteVolume",
                "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:CreateSnapshot",
                "ec2:DeleteSnapshot",
```

```
                "ec2:DescribeSnapshots",
                "ec2:StopInstances",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:CreateBucket",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
```

```
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
```

```
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Regioni segrete

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Regioni più segrete

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Modalità di utilizzo delle autorizzazioni AWS

Le sezioni seguenti descrivono come utilizzare le autorizzazioni per ciascun servizio BlueXP. Queste informazioni possono essere utili se le policy aziendali impongono che le autorizzazioni vengano fornite solo se necessario.

Amazon FSX per ONTAP

Il connettore effettua le seguenti richieste API per gestire Amazon FSX per ONTAP:

- ec2:DescripbeInstances
- ec2:DescripbeInstanceStatus
- ec2:DescripbeInstanceAttribute
- ec2:DescripteRouteTable
- ec2:DescripteImages
- ec2:CreateTag
- ec2:DescripteVolumes
- ec2:DescripteSecurityGroups
- ec2:DescripteNetworkInterfaces
- ec2:DescripteSubnet

- ec2:DescripteVpcs
- ec2:DescripbeDhcpOptions
- ec2:DescripteSnapshot
- ec2:DescripteKeyPairs
- ec2:DescripteRegions
- ec2:DescripteTag
- ec2:DescripteIamInstanceProfileAssociations
- ec2:DescripteReservedInstancesOfferings
- ec2:DescripteVpcEndpoint
- ec2:DescripteVpcs
- ec2:DescripteVolumesModificazioni
- ec2:DescriptePlacementGroups
- Km: Elenco*
- Km:descrivere*
- Km: CreateGrant
- Km:ListAlias
- fsx:descrivere*
- fsx: Elenco*

Discovery bucket Amazon S3

Il connettore effettua la seguente richiesta API per scoprire i bucket Amazon S3:

s3:GetEncryptionConfiguration

Backup e recovery

Il connettore effettua le seguenti richieste API per gestire i backup in Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBucket
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- Km: Elenco*
- Km:descrivere*

- s3:GetObject
- ec2:DescripteVpcEndpoint
- Km:ListAlias
- s3:PutEncryptionConfiguration

Il connettore effettua le seguenti richieste API quando si utilizza il metodo Search & Restore per ripristinare volumi e file:

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecution
- athena: GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- Incolla: CreateDatabase
- Incolla: CreateTable
- Incolla: BatchDeletePartition

Il connettore esegue le seguenti richieste API quando si utilizza la protezione DataLock e ransomware per i backup dei volumi:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging

- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Il connettore effettua le seguenti richieste API se si utilizza un account AWS diverso per i backup Cloud Volumes ONTAP rispetto a quello utilizzato per i volumi di origine:

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

Classificazione

Il connettore effettua le seguenti richieste API per implementare l'istanza di classificazione BlueXP:

- ec2:DescripbeInstances
- ec2:DescripbeInstanceStatus
- ec2:RunInstances
- ec2:installazioni terminate
- ec2:CreateTag
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:DescripteSecurityGroups
- ec2:CreateNetworkInterface

- ec2:DescripteNetworkInterfaces
- ec2:DeleteNetworkInterface
- ec2:DescripteSubnet
- ec2:DescripteVpcs
- ec2:CreateSnapshot
- ec2:DescripteRegions
- Cloud formation: CreateStack
- Cloud formation:DeleteStack
- Cloudformation:DescripteStack
- Cloudformation:DescripbeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescripteIamInstanceProfileAssociations

Il connettore effettua le seguenti richieste API per eseguire la scansione dei bucket S3 quando si utilizza la classificazione BlueXP:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescripteIamInstanceProfileAssociations
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyBucket
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam: GetRole
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:PutObject
- sts: AssumeRole

Cloud Volumes ONTAP

Il connettore effettua le seguenti richieste API per implementare e gestire Cloud Volumes ONTAP in AWS.

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Creare e gestire i ruoli IAM e i profili di istanza per le istanze di Cloud Volumes ONTAP	iam:ListInstanceProfiles	Sì	Sì	No
	iam: CreateRole	Sì	No	No
	iam: DeleteRole	No	Sì	Sì
	iam:PutRolePolicy	Sì	No	No
	iam:CreateInstanceProfile	Sì	No	No
	iam:DeleteRolePolicy	No	Sì	Sì
	iam:AddRoleToInstanceProfile	Sì	No	No
	iam:RemoveRoleFromInstanceProfile	No	Sì	Sì
	iam:DeleteInstanceProfile	No	Sì	Sì
	iam: PassRole	Sì	No	No
	ec2:AssociateIamInstanceProfile	Sì	Sì	No
	ec2:DescripteIamInstanceProfileAssociations	Sì	Sì	No
	ec2:DisassociateIamInstanceProfile	No	Sì	No
Decodificare i messaggi di stato dell'autorizzazione	sts:DecodeAuthorizationMessage	Sì	Sì	No
Descrivere le immagini specificate (Amis) disponibili per l'account	ec2:DescripteImages	Sì	Sì	No
Descrivere le tabelle di percorso in un VPC (richiesto solo per le coppie ha)	ec2:DescripteRouteTable	Sì	No	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Arrestare, avviare e monitorare le istanze	ec2:StartInstances	Sì	Sì	No
	ec2:StopInstances	Sì	Sì	No
	ec2:DescripbeInstances	Sì	Sì	No
	ec2:DescripbeInstanceStatus	Sì	Sì	No
	ec2:RunInstances	Sì	No	No
	ec2:installazioni terminate	No	No	Sì
	ec2:ModifyInstanceAttribute	No	Sì	No
Verificare che la rete avanzata sia abilitata per i tipi di istanze supportati	ec2:DescripbeInstanceAttribute	No	Sì	No
Contrassegnare le risorse con i tag "WorkingEnvironment" e "WorkingEnvironmentId" utilizzati per la manutenzione e l'allocazione dei costi	ec2:CreateTag	Sì	Sì	No
Gestire i volumi EBS utilizzati da Cloud Volumes ONTAP come storage back-end	ec2:CreateVolume	Sì	Sì	No
	ec2:DescripteVolumes	Sì	Sì	Sì
	ec2:ModifyVolumeAttribute	No	Sì	Sì
	ec2:AttachVolume	Sì	Sì	No
	ec2:DeleteVolume	No	Sì	Sì
	ec2:DetachVolume	No	Sì	Sì

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Creare e gestire gruppi di sicurezza per Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Sì	No	No
	ec2:DeleteSecurityGroup	No	Sì	Sì
	ec2:DescripteSecurityGroups	Sì	Sì	Sì
	ec2:RevokeSecurityGroupErgress	Sì	No	No
	ec2:AuthorizeSecurityGroupErgress	Sì	No	No
	ec2:AuthorizeSecurityGroupIngress	Sì	No	No
	ec2:RevokeSecurityGroupIngress	Sì	Sì	No
Creare e gestire le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione	ec2:CreateNetworkInterface	Sì	No	No
	ec2:DescripteNetworkInterfaces	Sì	Sì	No
	ec2:DeleteNetworkInterface	No	Sì	Sì
	ec2:ModifyNetworkInterfaceAttribute	No	Sì	No
Ottenere l'elenco delle subnet di destinazione e dei gruppi di protezione	ec2:DescripteSubnet	Sì	Sì	No
	ec2:DescripteVpcs	Sì	Sì	No
Ottenere i server DNS e il nome di dominio predefinito per le istanze di Cloud Volumes ONTAP	ec2:DescripbeDhcpOptions	Sì	No	No
Snapshot dei volumi EBS per Cloud Volumes ONTAP	ec2:CreateSnapshot	Sì	Sì	No
	ec2:DeleteSnapshot	No	Sì	Sì
	ec2:DescripteSnapshot	No	Sì	No
Acquisire la console Cloud Volumes ONTAP, che è allegata ai messaggi AutoSupport	ec2:GetConsoleOutput	Sì	Sì	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Ottieni l'elenco delle coppie di chiavi disponibili	ec2:DescripteKeyPairs	Sì	No	No
Ottieni l'elenco delle regioni AWS disponibili	ec2:DescripteRegions	Sì	Sì	No
Gestire i tag per le risorse associate alle istanze di Cloud Volumes ONTAP	ec2:DeleteMags	No	Sì	Sì
	ec2:DescripteTag	No	Sì	No
Creare e gestire gli stack per i modelli di AWS CloudFormation	Cloud formation: CreateStack	Sì	No	No
	Cloud formation:DeleteStack	Sì	No	No
	Cloudformation:DescripteStack	Sì	Sì	No
	Cloudformation:DescripbeStackEvents	Sì	No	No
	Cloud formation:ValidateTemplate	Sì	No	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Creare e gestire un bucket S3 che un sistema Cloud Volumes ONTAP utilizza come Tier di capacità per il tiering dei dati	s3:CreateBucket	Sì	Sì	No
	s3:Deletebucket	No	Sì	Sì
	s3:GetLifecycleConfiguration	No	Sì	No
	s3:PutLifecycleConfiguration	No	Sì	No
	s3:PutBucketTagging	No	Sì	No
	s3:ListBucketVersions	No	Sì	No
	s3:GetBucketPolicyStatus	No	Sì	No
	s3:GetBucketPublicAccessBlock	No	Sì	No
	s3:GetBucketAcl	No	Sì	No
	s3:GetBucketPolicy	No	Sì	No
	s3:PutBucketPublicAccessBlock	No	Sì	No
	s3:GetBucketTagging	No	Sì	No
	s3:GetBucketLocation	No	Sì	No
	s3:ListAllMyBucket	No	No	No
	s3:ListBucket	No	Sì	No
Abilitare la crittografia dei dati di Cloud Volumes ONTAP utilizzando il servizio di gestione delle chiavi AWS (KMS)	Km: Elenco*	Sì	Sì	No
	Kms: ReEncrypt*	Sì	No	No
	Km:descrivere*	Sì	Sì	No
	Km: CreateGrant	Sì	Sì	No
	Kms:GenerateDataKeyWithoutPlaintext	Sì	Sì	No
Creare e gestire un gruppo di posizionamento AWS Spread per due nodi ha e il mediatore in una singola AWS Availability zone	ec2:CreatePlacementGroup	Sì	No	No
	ec2:DeletePlacementGroup	No	Sì	Sì

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Creare report	fsx:descrivere*	No	Sì	No
	fsx: Elenco*	No	Sì	No
Crea e gestisci aggregati che supportano la funzionalità Amazon EBS Elastic Volumes	ec2:DescripteVolumesModificazioni	No	Sì	No
	ec2:ModifyVolume	No	Sì	No

Caching edge

Il connettore effettua le seguenti richieste API per implementare istanze di caching edge BlueXP durante l'implementazione:

- Cloudformation:DescripteStack
- Cloudwatch:GetMetricStatistics
- Cloudformation:ListStack

Kubernetes

Il connettore effettua le seguenti richieste API per rilevare e gestire i cluster Amazon EKS:

- ec2:DescripteRegions
- eks:ListClusters
- eks: DescripbeCluster
- iam:GetInstanceProfile

Registro delle modifiche

Man mano che le autorizzazioni vengono aggiunte e rimosse, le annoteremo nelle sezioni seguenti.

8 marzo 2024

La seguente autorizzazione è ora inclusa nel criterio del connettore:

EC2:DescribeAvailabilityZones

Questa autorizzazione è necessaria per una prossima release. Aggiorneremo le note di rilascio con ulteriori dettagli quando tale release sarà disponibile.

6 giugno 2023

Per Cloud Volumes ONTAP è ora richiesta la seguente autorizzazione:

Kms:GenerateDataKeyWithoutPlaintext

14 febbraio 2023

Per il tiering BlueXP è ora richiesta la seguente autorizzazione:

ec2:DescripteVpcEndpoint

Autorizzazioni Azure per il connettore

Quando BlueXP avvia la macchina virtuale del connettore in Azure, allega un ruolo personalizzato alla macchina virtuale che fornisce al connettore le autorizzazioni per gestire le risorse e i processi all'interno dell'abbonamento Azure. Il connettore utilizza le autorizzazioni per effettuare chiamate API a diversi servizi Azure.

Autorizzazioni di ruolo personalizzate

Il ruolo personalizzato mostrato di seguito fornisce le autorizzazioni necessarie a un connettore per gestire le risorse e i processi all'interno della rete Azure.

Quando si crea un connettore direttamente da BlueXP, BlueXP applica automaticamente questo ruolo personalizzato al connettore.

Se si implementa il connettore da Azure Marketplace o se si installa manualmente il connettore su un host Linux, sarà necessario impostare autonomamente il ruolo personalizzato.

Per visualizzare istruzioni dettagliate sull'utilizzo di questi criteri, fare riferimento alle seguenti pagine:

- "Impostare le autorizzazioni per un'implementazione di Azure Marketplace"
- "Impostare le autorizzazioni per le implementazioni on-premise"
- "Impostare le autorizzazioni per la modalità limitata"
- "Impostare le autorizzazioni per la modalità privata"

Inoltre, è necessario assicurarsi che il ruolo sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive.

```
{
    "Name": "BlueXP Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
                    "Microsoft.Compute/locations/vmSizes/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Compute/operations/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
```

```
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "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.Storage/checknameavailability/read",
                    "Microsoft.Storage/operations/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
```

```
"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",
```

```
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",

"Microsoft.ContainerService/managedClusters/listClusterUserCredential/acti
on",
                    "Microsoft.ContainerService/managedClusters/read",
                    "Microsoft.Synapse/workspaces/write",
                    "Microsoft.Synapse/workspaces/read",
                    "Microsoft.Synapse/workspaces/delete",
                    "Microsoft.Synapse/register/action",
```

```
                    "Microsoft.Synapse/checkNameAvailability/action",
                    "Microsoft.Synapse/workspaces/operationStatuses/read",
                    "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
                    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}
```

Modalità di utilizzo delle autorizzazioni Azure

Le sezioni seguenti descrivono come utilizzare le autorizzazioni per ciascun servizio BlueXP. Queste informazioni possono essere utili se le policy aziendali impongono che le autorizzazioni vengano fornite solo se necessario.

Azure NetApp Files

Il connettore esegue le seguenti richieste API quando si utilizza la classificazione BlueXP per eseguire la scansione dei dati Azure NetApp Files:

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccounts/capacityPools/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete

Backup e recovery

Il connettore effettua le seguenti richieste API per il backup e ripristino BlueXP:

- Microsoft.Storage/storageAccounts/listkeys/azione
- Microsoft.Storage/storageAccounts/Read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/Containers/Read
- Microsoft.Storage/storageAccountSas/action

- Microsoft.KeyVault/vault/Read
- Microsoft.KeyVault/vault/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources/subscriptions/locations/Read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/subscriptions/resourceGroups/Read
- Microsoft.Resources/subscriptions/resourcegroup/resources/Read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Authorization/locks/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/Deployments/delete
- Microsoft.ManagedIdentity/userAssistedIdentities/assign/action

Il connettore effettua le seguenti richieste API quando si utilizza la funzionalità di ricerca e ripristino:

- Microsoft.Synapse/aree di lavoro/scrittura
- Microsoft.Synapse/aree di lavoro/lettura
- Microsoft.Synapse/aree di lavoro/eliminazione
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/azione
- Microsoft.Synapse/workspaces/operationStatuses/Read
- Microsoft.Synapse/Workspaces/firewallRules/Read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/Read
- Microsoft.Synapse/Workspaces/privateEndpointConnectionsApproval/action

Classificazione

Il connettore crea le seguenti richieste API quando si utilizza la classificazione BlueXP.

Azione	Utilizzato per la configurazione?	Utilizzato per le operazioni quotidiane?
Microsoft.Compute/locations/operations/read	Sì	Sì
Microsoft.Compute/locations/vmSizes/read	Sì	Sì
Microsoft.Compute/operations/read	Sì	Sì
Microsoft.Compute/virtualMachines/instanceView/read	Sì	Sì
Microsoft.Compute/virtualMachines/powerOff/action	Sì	No
Microsoft.Compute/virtualMachines/read	Sì	Sì
Microsoft.Compute/virtualMachines/restart/action	Sì	No
Microsoft.Compute/virtualMachines/start/action	Sì	No
Microsoft.Compute/virtualMachines/vmSizes/read	No	Sì
Microsoft.Compute/virtualMachines/write	Sì	No
Microsoft.Compute/images/read	Sì	Sì
Microsoft.Compute/disks/delete	Sì	No
Microsoft.Compute/disks/read	Sì	Sì
Microsoft.Compute/disks/write	Sì	No
Microsoft.Storage/checknameAvailability/Read	Sì	Sì
Microsoft.Storage/Operations/Read	Sì	Sì
Microsoft.Storage/storageAccounts/listkeys/azione	Sì	No
Microsoft.Storage/storageAccounts/Read	Sì	Sì
Microsoft.Storage/storageAccounts/write	Sì	No
Microsoft.Storage/storageAccounts/blobServices/Containers/Read	Sì	Sì
Microsoft.Network/networkInterfaces/read	Sì	Sì
Microsoft.Network/networkInterfaces/write	Sì	No

Azione	Utilizzato per la configurazione?	Utilizzato per le operazioni quotidiane?
Microsoft.Network/networkInterfaces/join/action	Sì	No
Microsoft.Network/networkSecurityGroups/read	Sì	Sì
Microsoft.Network/networkSecurityGroups/write	Sì	No
Microsoft.Resources/subscriptions/locations/Read	Sì	Sì
Microsoft.Network/locations/operationResults/read	Sì	Sì
Microsoft.Network/locations/operations/read	Sì	Sì
Microsoft.Network/virtualNetworks/read	Sì	Sì
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Sì	Sì
Microsoft.Network/virtualNetworks/subnets/read	Sì	Sì
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Sì	Sì
Microsoft.Network/virtualNetworks/virtualMachines/read	Sì	Sì
Microsoft.Network/virtualNetworks/subnets/join/action	Sì	No
Microsoft.Network/virtualNetworks/subnets/write	Sì	No
Microsoft.Network/routeTables/join/action	Sì	No
Microsoft.Resources/Deployments/Operations/Read	Sì	Sì
Microsoft.Resources/Deployments/Read	Sì	Sì
Microsoft.Resources/Deployments/write	Sì	No
Microsoft.Resources/resources/Read	Sì	Sì
Microsoft.Resources/subscriptions/operationresults/Read	Sì	Sì
Microsoft.Resources/subscriptions/resourceGroups/delete	Sì	No

Azione	Utilizzato per la configurazione?	Utilizzato per le operazioni quotidiane?
Microsoft.Resources/subscriptions/resourceGroups/Read	Sì	Sì
Microsoft.Resources/subscriptions/resourcegroup/resources/Read	Sì	Sì
Microsoft.Resources/subscriptions/resourceGroups/write	Sì	No

Cloud Volumes ONTAP

Il connettore effettua le seguenti richieste API per implementare e gestire Cloud Volumes ONTAP in Azure.

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Creare e gestire macchine virtuali	Microsoft.Compute/locations/operations/read	Sì	Sì	No
	Microsoft.Compute/locations/vmSizes/read	Sì	Sì	No
	Microsoft.Resources/subscriptions/locations/Read	Sì	No	No
	Microsoft.Compute/operations/read	Sì	Sì	No
	Microsoft.Compute/virtualMachines/instanceView/read	Sì	Sì	No
	Microsoft.Compute/virtualMachines/powerOff/action	Sì	Sì	No
	Microsoft.Compute/virtualMachines/read	Sì	Sì	No
	Microsoft.Compute/virtualMachines/restart/action	Sì	Sì	No
	Microsoft.Compute/virtualMachines/start/action	Sì	Sì	No
	Microsoft.Compute/virtualMachines/deallocate/action	No	Sì	Sì
	Microsoft.Compute/virtualMachines/vmSizes/read	No	Sì	No
	Microsoft.Compute/virtualMachines/write	Sì	Sì	No
	Microsoft.Compute/virtualMachines/delete	Sì	Sì	Sì
	Microsoft.Resources/Deployments/delete	Sì	No	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Abilitare l'implementazione da un VHD	Microsoft.Compute/images/read	Sì	No	No
	Microsoft.Compute/images/write	Sì	No	No
Creare e gestire le interfacce di rete nella subnet di destinazione	Microsoft.Network/networkInterfaces/read	Sì	Sì	No
	Microsoft.Network/networkInterfaces/write	Sì	Sì	No
	Microsoft.Network/networkInterfaces/join/action	Sì	Sì	No
	Microsoft.Network/networkInterfaces/delete	Sì	Sì	No
Creare e gestire gruppi di sicurezza di rete	Microsoft.Network/networkSecurityGroups/read	Sì	Sì	No
	Microsoft.Network/networkSecurityGroups/write	Sì	Sì	No
	Microsoft.Network/networkSecurityGroups/join/action	Sì	No	No
	Microsoft.Network/networkSecurityGroups/delete	No	Sì	Sì

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Ottenere informazioni di rete relative alle regioni, al VNET di destinazione e alla subnet e aggiungere le macchine virtuali ai VNets	Microsoft.Network/locations/operationResults/read	Sì	Sì	No
	Microsoft.Network/locations/operations/read	Sì	Sì	No
	Microsoft.Network/virtualNetworks/read	Sì	No	No
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Sì	No	No
	Microsoft.Network/virtualNetworks/subnets/read	Sì	Sì	No
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Sì	Sì	No
	Microsoft.Network/virtualNetworks/virtualMachines/read	Sì	Sì	No
	Microsoft.Network/virtualNetworks/subnets/join/action	Sì	Sì	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Creare e gestire gruppi di risorse	Microsoft.Resources/Deployments/Operations/Read	Sì	Sì	No
	Microsoft.Resources/Deployments/Read	Sì	Sì	No
	Microsoft.Resources/Deployments/write	Sì	Sì	No
	Microsoft.Resources/resources/Read	Sì	Sì	No
	Microsoft.Resources/subscriptions/operationresults/Read	Sì	Sì	No
	Microsoft.Resources/subscriptions/resourceGroups/delete	Sì	Sì	Sì
	Microsoft.Resources/subscriptions/resourceGroups/Read	No	Sì	No
	Microsoft.Resources/subscriptions/resourcegroup/resources/Read	Sì	Sì	No
	Microsoft.Resources/subscriptions/resourceGroups/write	Sì	Sì	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Gestione di dischi e account storage Azure	Microsoft.Compute/disks/read	Sì	Sì	Sì
	Microsoft.Compute/disks/write	Sì	Sì	No
	Microsoft.Compute/disks/delete	Sì	Sì	Sì
	Microsoft.Storage/checknameAvailability/Read	Sì	Sì	No
	Microsoft.Storage/Operations/Read	Sì	Sì	No
	Microsoft.Storage/storageAccounts/listkeys/azione	Sì	Sì	No
	Microsoft.Storage/storageAccounts/Read	Sì	Sì	No
	Microsoft.Storage/storageAccounts/delete	No	Sì	Sì
	Microsoft.Storage/storageAccounts/write	Sì	Sì	No
	Microsoft.Storage/uses/Read	No	Sì	No
Abilitare i backup per lo storage Blob e la crittografia degli account di storage	Microsoft.Storage/storageAccounts/blobServices/Containers/Read	Sì	Sì	No
	Microsoft.KeyVault/vault/Read	Sì	Sì	No
	Microsoft.KeyVault/vault/accessPolicies/write	Sì	Sì	No
Abilitare gli endpoint del servizio VNET per il tiering dei dati	Microsoft.Network/virtualNetworks/subnets/write	Sì	Sì	No
	Microsoft.Network/routeTables/join/action	Sì	Sì	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Creare e gestire snapshot gestite da Azure	Microsoft.Compute/snapshots/write	Sì	Sì	No
	Microsoft.Compute/snapshots/read	Sì	Sì	No
	Microsoft.Compute/snapshots/delete	No	Sì	Sì
	Microsoft.Compute/disks/beginGetAccess/action	No	Sì	No
Creare e gestire set di disponibilità	Microsoft.Compute/availabilitySets/write	Sì	No	No
	Microsoft.Compute/availabilitySets/read	Sì	No	No
Implementazione programmatica dal mercato	Microsoft.MarketplaceOrdazione/offertypes/publisher/offers/plans/agreements/Read	Sì	No	No
	Microsoft.MarketplaceOrdazione/offertypes/publisher/offers/plans/agreements/write	Sì	Sì	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Gestire un bilanciamento del carico per le coppie ha	Microsoft.Network/loadBalancers/read	Sì	Sì	No
	Microsoft.Network/loadBalancers/write	Sì	No	No
	Microsoft.Network/loadBalancers/delete	No	Sì	Sì
	Microsoft.Network/loadBalancers/backendAddressPools/read	Sì	No	No
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Sì	No	No
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	Sì	Sì	No
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Sì	No	No
	Microsoft.Network/loadBalancers/probes/read	Sì	No	No
	Microsoft.Network/loadBalancers/probes/join/action	Sì	No	No
Abilitare la gestione dei blocchi sui dischi Azure	Microsoft.Authorization/locks/*	Sì	Sì	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Abilitare gli endpoint privati per le coppie ha in assenza di connettività all'esterno della subnet	Microsoft.Network/privateEndpoints/write	Sì	Sì	No
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Sì	No	No
	Microsoft.Storage/storageAccounts/privateEndpointConnections/Read	Sì	Sì	Sì
	Microsoft.Network/privateEndpoints/read	Sì	Sì	Sì
	Microsoft.Network/privateDnsZones/write	Sì	Sì	No
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Sì	Sì	No
	Microsoft.Network/virtualNetworks/join/action	Sì	Sì	No
	Microsoft.Network/privateDnsZones/A/write	Sì	Sì	No
	Microsoft.Network/privateDnsZones/read	Sì	Sì	No
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Sì	Sì	No
Necessario per alcune implementazioni di macchine virtuali, a seconda dell'hardware fisico sottostante	Microsoft.Resources/Deployments/OperationStatuses/Read	Sì	Sì	No
Rimuovere le risorse da un gruppo di risorse in caso di errore di implementazione o di eliminazione	Microsoft.Network/privateEndpoints/delete	Sì	Sì	No
	Microsoft.Compute/availabilitySets/delete	Sì	Sì	No

Scopo	Azione	Utilizzato per l'implementazione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Abilitare l'utilizzo di chiavi di crittografia gestite dal cliente quando si utilizza l'API	Microsoft.Compute/diskEncryptionSets/read	Sì	Sì	Sì
	Microsoft.Compute/diskEncryptionSets/write	Sì	Sì	No
	Microsoft.KeyVault/vault/implementazione/azione	Sì	No	No
	Microsoft.Compute/diskEncryptionSets/delete	Sì	Sì	Sì
Configurare un gruppo di sicurezza dell'applicazione per una coppia ha per isolare le NIC di interconnessione ha e di rete del cluster	Microsoft.Network/applicationSecurityGroups/write	No	Sì	No
	Microsoft.Network/applicationSecurityGroups/read	No	Sì	No
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	No	Sì	No
	Microsoft.Network/networkSecurityGroups/securityRules/write	Sì	Sì	No
	Microsoft.Network/applicationSecurityGroups/delete	No	Sì	Sì
	Microsoft.Network/networkSecurityGroups/securityRules/delete	No	Sì	Sì
Lettura, scrittura ed eliminazione dei tag associati alle risorse Cloud Volumes ONTAP	Microsoft.Resources/tags/Read	No	Sì	No
	Microsoft.Resources/tags/write	Sì	Sì	No
	Microsoft.Resources/tags/delete	Sì	No	No
Crittografare gli account storage durante la creazione	Microsoft.ManagedIdentity/userAssistedIdentities/assign/action	Sì	Sì	No

Caching edge

Il connettore effettua le seguenti richieste API quando si utilizza il caching edge BlueXP:

- Microsoft.Insights/metriche/lettura
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/Deployments/delete

Kubernetes

Il connettore effettua le seguenti richieste API per rilevare e gestire i cluster in esecuzione in Azure Kubernetes Service (AKS):

- Microsoft.Compute/virtualMachines/read
- Microsoft.Resources/subscriptions/locations/Read
- Microsoft.Resources/subscriptions/operationresults/Read
- Microsoft.Resources/subscriptions/resourceGroups/Read
- Microsoft.Resources/subscriptions/resourcegroup/resources/Read
- Microsoft.ContainerService/managedClusters/Read
- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action

Tiering

Il connettore crea le seguenti richieste API quando si imposta il tiering BlueXP.

- Microsoft.Storage/storageAccounts/listkeys/azione
- Microsoft.Resources/subscriptions/resourceGroups/Read
- Microsoft.Resources/subscriptions/locations/Read

Il connettore esegue le seguenti richieste API per le operazioni quotidiane.

- Microsoft.Storage/storageAccounts/blobServices/Containers/Read
- Microsoft.Storage/storageAccounts/managementPolicies/Read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/Read

Registro delle modifiche

Man mano che le autorizzazioni vengono aggiunte e rimosse, le annoteremo nelle sezioni seguenti.

5 dicembre 2023

Le seguenti autorizzazioni non sono più necessarie per il backup e recovery di BlueXP durante il backup dei dati dei volumi nell'storage Azure Blob:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

Queste autorizzazioni sono necessarie per altri servizi storage BlueXP, pertanto resteranno nel ruolo personalizzato del connettore se utilizzi tali servizi storage.

12 maggio 2023

Le seguenti autorizzazioni sono state aggiunte al criterio JSON perché sono necessarie per la gestione di Cloud Volumes ONTAP:

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

Le seguenti autorizzazioni sono state rimosse dal criterio JSON perché non sono più necessarie:

- Microsoft.Storage/storageAccounts/blobServices/container/write
- Microsoft.Network/publicIPAddresses/delete

23 marzo 2023

L'autorizzazione "Microsoft.Storage/storageAccounts/delete" non è più necessaria per la classificazione BlueXP.

Questa autorizzazione è ancora richiesta per Cloud Volumes ONTAP.

5 gennaio 2023

Al criterio JSON sono state aggiunte le seguenti autorizzazioni:

- Microsoft.Storage/storageAccountSas/action
- Microsoft.Synapse/Workspaces/privateEndpointConnectionsApproval/action

  Queste autorizzazioni sono necessarie per il backup e il ripristino di BlueXP.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  Questa autorizzazione è necessaria per l'implementazione di Cloud Volumes ONTAP.

Permessi Google Cloud per il connettore

BlueXP richiede autorizzazioni per eseguire azioni in Google Cloud. Queste autorizzazioni sono incluse in un ruolo personalizzato fornito da NetApp. È possibile

comprendere le funzioni di BlueXP con queste autorizzazioni.

Autorizzazioni dell'account di servizio

Il ruolo personalizzato mostrato di seguito fornisce le autorizzazioni necessarie a un connettore per gestire le risorse e i processi all'interno della rete Google Cloud.

È necessario applicare questo ruolo personalizzato a un account di servizio che viene collegato alla macchina virtuale del connettore.

- "Impostare le autorizzazioni di Google Cloud per la modalità standard"
- "Impostare le autorizzazioni per la modalità limitata"
- "Impostare le autorizzazioni per la modalità privata"

Inoltre, è necessario assicurarsi che il ruolo sia aggiornato quando vengono aggiunte nuove autorizzazioni nelle release successive.

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- 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.addAccessConfig
- compute.instances.attachDisk
```

```
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- 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
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

Modalità di utilizzo delle autorizzazioni Google Cloud

Azioni	Scopo
- compute.disks.create - Compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Per creare e gestire dischi per Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Per creare regole firewall per Cloud Volumes ONTAP.
- Compute.globalOperations.get	Per ottenere lo stato delle operazioni.

Azioni	Scopo
- compute.images.get - Compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Per ottenere immagini per istanze di macchine virtuali.
- compute.instances.attachDisk - compute.instances.detachDisk	Per collegare e scollegare i dischi a Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Per creare ed eliminare istanze di Cloud Volumes ONTAP VM.
- compute.instances.get	Per elencare le istanze di macchine virtuali.
- compute.instances.getSerialPortOutput	Per ottenere i log della console.
- compute.instances.list	Per recuperare l'elenco di istanze in una zona.
- compute.instances.setDeletionProtection	Per impostare la protezione di eliminazione sull'istanza.
- compute.instances.setLabels	Per aggiungere etichette.
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Per modificare il tipo di macchina per Cloud Volumes ONTAP.
- compute.instances.setMetadata	Per aggiungere metadati.
- compute.instances.setTags	Per aggiungere tag per le regole del firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Per avviare e arrestare Cloud Volumes ONTAP.
- Compute.machineTypes.get	Per ottenere il numero di core per controllare le qoutas.
- compute.projects.get	Per supportare progetti multipli.
- compute.snapshot.create - compute.snapshots.delete - compute.snapshot.get - compute.snapshot.list - compute.snapshots.setLabels	Per creare e gestire snapshot di dischi persistenti.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - Compute.zoneOperations.get - compute.zones.get - compute.zones.list	Per ottenere le informazioni di rete necessarie per creare una nuova istanza di macchina virtuale Cloud Volumes ONTAP.

Azioni	Scopo
- 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	Per implementare l'istanza della macchina virtuale Cloud Volumes ONTAP utilizzando Google Cloud Deployment Manager.
- Logging.logEntries.list - Logging.privateLogEntries.list	Per ottenere unità di log stack.
- resourcemanager.projects.get	Per supportare progetti multipli.
- storage.bucket.create - storage.buckets.delete - storage.bucket.get - storage.bucket.list - storage.bucket.update	Per creare e gestire un bucket di storage Google Cloud per il tiering dei dati.
- cloudkms.cryptoKeyVersions.useToEncrypt - Cloudkms.cryptKeys.get - Cloudkms.cryptKeys.list - Cloudkms.keyrings.list	Per utilizzare le chiavi di crittografia gestite dal cliente dal servizio di gestione delle chiavi cloud con Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list	Per impostare un account di servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud.
- compute.addresses.list	Recuperare gli indirizzi in una regione durante l'implementazione di una coppia ha.
- Compute.backendServices.create - Compute.regionBackendServices.create - Compute.regionBackendServices.get - Compute.regionBackendServices.list	Per configurare un servizio back-end per la distribuzione del traffico in una coppia ha.
- compute.networks.updatePolicy	Per applicare le regole del firewall ai VPC e alle subnet per una coppia ha.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	Per attivare la classificazione BlueXP.

Azioni	Scopo
- container.cluster.get - container.cluster.list	Per scoprire i cluster Kubernetes in esecuzione in Google Kubernetes Engine.
- compute.instanceGroups.get - compute.addresses.get - compute.instances.updateNetworkInterface	Per creare e gestire le VM di storage su coppie Cloud Volumes ONTAP ha.
- Monitoring.timeseries.list - Storage.bucket.getIamPolicy	Per scoprire informazioni sui bucket di storage di Google Cloud.
- Cloudkms.cryptKeys.get - Cloudkms.cryptKeys.getIamPolicy - Cloudkms.cryptKeys.list - cloudkms.cryptoKeys.setIamPolicy - Cloudkms.keyrings.get - Cloudkms.keyrings.getIamPolicy - Cloudkms.keyrings.list - cloudkms.keyRings.setIamPolicy	Per selezionare le proprie chiavi gestite dal cliente nella procedura guidata di attivazione del backup e ripristino BlueXP invece di utilizzare le chiavi di crittografia predefinite gestite da Google.

Registro delle modifiche

Man mano che le autorizzazioni vengono aggiunte e rimosse, le annoteremo nelle sezioni seguenti.

6 febbraio 2023

La seguente autorizzazione è stata aggiunta a questo criterio:

- compute.instances.updateNetworkInterface

Questa autorizzazione è richiesta per Cloud Volumes ONTAP.

27 gennaio 2023

Al criterio sono state aggiunte le seguenti autorizzazioni:

- Cloudkms.cryptKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- Cloudkms.keyrings.get
- Cloudkms.keyrings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Queste autorizzazioni sono necessarie per il backup e il ripristino di BlueXP.

Porte

Regole del gruppo di sicurezza del connettore in AWS

Il gruppo di sicurezza AWS per il connettore richiede regole sia in entrata che in uscita. BlueXP crea automaticamente questo gruppo di protezione quando si crea un connettore da BlueXP. È necessario impostare questo gruppo di protezione per tutte le altre opzioni

di installazione.

Regole in entrata

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host del connettore
HTTP	80	• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale • Utilizzato durante il processo di aggiornamento di Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale e le connessioni dall'istanza di classificazione BlueXP
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet per inviare messaggi AutoSupport al supporto NetApp. È necessario aprire manualmente questa porta dopo l'implementazione. "Scopri come il connettore viene utilizzato come proxy per i messaggi AutoSupport"
TCP	9060, 9061	Consente di abilitare e utilizzare la classificazione BlueXP e il backup e ripristino BlueXP nelle regioni governative.

Regole in uscita

Il gruppo di protezione predefinito per il connettore apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per il connettore include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	L'API chiama AWS, ONTAP, classificandosi BlueXP e inviando messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	Mediatore ONTAP ha	Comunicazione con il mediatore ONTAP ha
	TCP	8080	Classificazione BlueXP	Eseguire una verifica dell'istanza di classificazione BlueXP durante l'implementazione
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS di BlueXP

Regole del gruppo di sicurezza del connettore in Azure

Il gruppo di sicurezza Azure per il connettore richiede regole sia in entrata che in uscita. BlueXP crea automaticamente questo gruppo di protezione quando si crea un connettore da BlueXP. È necessario impostare questo gruppo di protezione per tutte le altre opzioni di installazione.

Regole in entrata

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host del connettore
HTTP	80	• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale • Utilizzato durante il processo di aggiornamento di Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale e le connessioni dall'istanza di classificazione BlueXP

Protocollo	Porta	Scopo
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet per inviare messaggi AutoSupport al supporto NetApp. È necessario aprire manualmente questa porta dopo l'implementazione. "Scopri come il connettore viene utilizzato come proxy per i messaggi AutoSupport"
TCP	9060, 9061	Consente di abilitare e utilizzare la classificazione BlueXP e il backup e ripristino BlueXP nelle regioni governative.

Regole in uscita

Il gruppo di protezione predefinito per il connettore apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per il connettore include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Le chiamate API ad Azure, a ONTAP, alla classificazione BlueXP e all'invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	8080	Classificazione BlueXP	Eseguire una verifica dell'istanza di classificazione BlueXP durante l'implementazione

Servizio	Protocollo	Porta	Destinazione	Scopo
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS di BlueXP

Regole del firewall connettore in Google Cloud

Le regole del firewall Google Cloud per il connettore richiedono regole sia in entrata che in uscita. BlueXP crea automaticamente questo gruppo di protezione quando si crea un connettore da BlueXP. È necessario impostare questo gruppo di protezione per tutte le altre opzioni di installazione.

Regole in entrata

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host del connettore
HTTP	80	• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale • Utilizzato durante il processo di aggiornamento di Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet per inviare messaggi AutoSupport al supporto NetApp. È necessario aprire manualmente questa porta dopo l'implementazione. "Scopri come il connettore viene utilizzato come proxy per i messaggi AutoSupport"

Regole in uscita

Le regole firewall predefinite per il connettore aprono tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Le regole firewall predefinite per il connettore includono le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

> L'indirizzo IP di origine è l'host del connettore.

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Le chiamate API a Google Cloud, a ONTAP, alla classificazione BlueXP e all'invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	8080	Classificazione BlueXP	Eseguire una verifica dell'istanza di classificazione BlueXP durante l'implementazione
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS di BlueXP

Porte per il connettore on-premise

Il connettore utilizza porte *inbound* se installato manualmente su un host Linux on-premise. Potrebbe essere necessario fare riferimento a queste porte per scopi di pianificazione.

Queste regole in entrata si applicano a tutti i modelli di implementazione BlueXP.

Protocollo	Porta	Scopo
HTTP	80	• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale • Utilizzato durante il processo di aggiornamento di Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale

Conoscenza e supporto

Registrati per ricevere assistenza

È necessaria la registrazione del supporto per ricevere supporto tecnico specifico per BlueXP e le relative soluzioni e servizi storage. È inoltre necessaria la registrazione del supporto per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP.

La registrazione per il supporto non attiva il supporto NetApp per un file service provider cloud. Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service per Google Cloud"

Panoramica sulla registrazione del supporto

Esistono due forme di registrazione per attivare i diritti di supporto:

- Registrazione dell'abbonamento al supporto per l'ID account BlueXP (il numero di serie a 20 cifre 960xxxxxxxxx nella pagina Support Resources di BlueXP).

  Questa funzione funge da unico ID di abbonamento al supporto per qualsiasi servizio all'interno di BlueXP. Ogni abbonamento al supporto a livello di account BlueXP deve essere registrato.

- Registrazione dei numeri di serie Cloud Volumes ONTAP associati a un abbonamento nel mercato del provider cloud (si tratta di numeri di serie 909201xxxxxxxx a 20 cifre).

  Questi numeri seriali sono comunemente denominati *numeri seriali PAYGO* e vengono generati da BlueXP al momento dell'implementazione di Cloud Volumes ONTAP.

La registrazione di entrambi i tipi di numeri di serie offre funzionalità come l'apertura di ticket di supporto e la generazione automatica dei casi. La registrazione viene completata aggiungendo account del sito di supporto NetApp a BlueXP come descritto di seguito.

Registrare l'account BlueXP per il supporto NetApp

Per registrarsi al supporto e attivare i diritti di supporto, un utente del proprio account BlueXP deve associare un account del sito di supporto NetApp al proprio account di accesso BlueXP. La modalità di registrazione al supporto NetApp dipende dal fatto che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

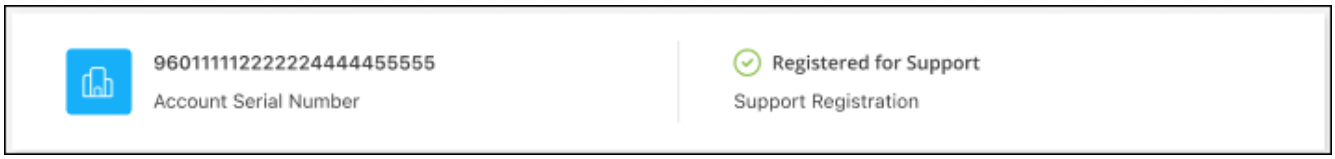
Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite BlueXP.

Fasi

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

2. Selezionare **User Credentials** (credenziali utente).
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp.
4. Per confermare che la procedura di registrazione è stata eseguita correttamente, selezionare l'icona Guida e selezionare **supporto**.

   La pagina **risorse** dovrebbe mostrare che il tuo account è registrato per il supporto.

   Si noti che gli altri utenti di BlueXP non visualizzeranno lo stesso stato di registrazione del supporto se non hanno associato un account del sito di supporto NetApp al proprio login BlueXP. Tuttavia, ciò non significa che il tuo account BlueXP non sia registrato per il supporto. Se un utente dell'account ha seguito questa procedura, l'account è stato registrato.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp con licenze e numeri di serie esistenti ma *no* account NSS, devi creare un account NSS e associarlo al tuo login BlueXP.

Fasi

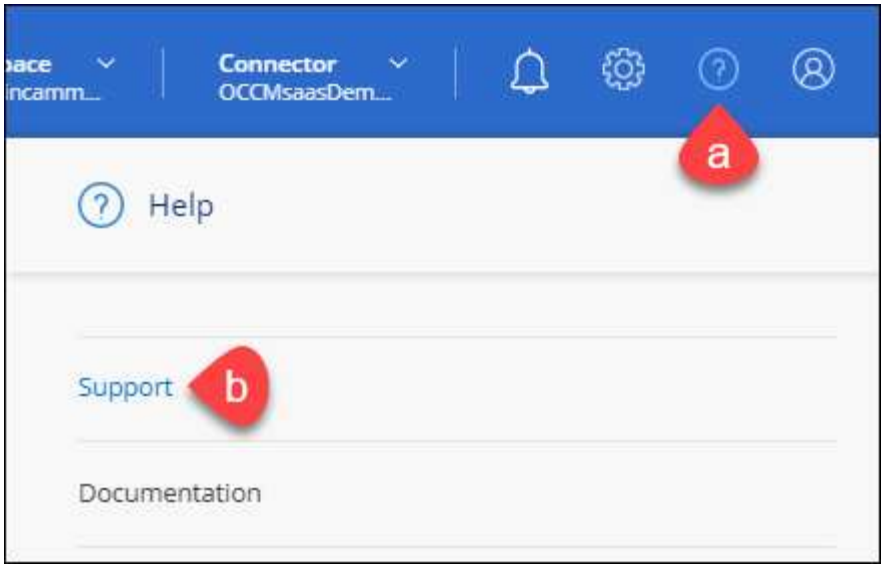
1. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account BlueXP (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.
2. Associare il nuovo account NSS al login BlueXP completando la procedura riportata sotto Cliente esistente con un account NSS.

Novità di NetApp

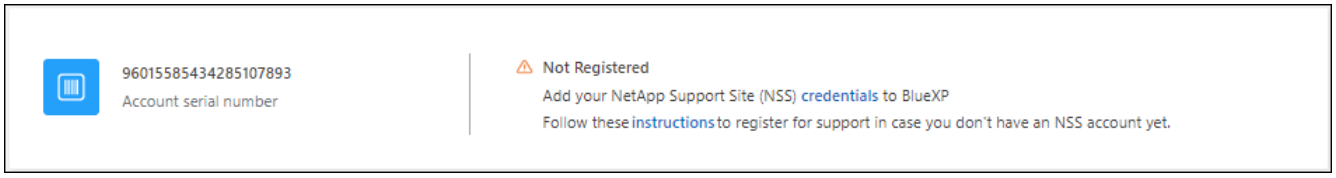
Se sei nuovo di NetApp e non disponi di un account NSS, segui i passaggi riportati di seguito.

Fasi

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



2. Individuare il numero di serie dell'ID account nella pagina Support Registration (registrazione supporto).



3. Selezionare "Sito per la registrazione del supporto NetApp" E selezionare **non sono un cliente NetApp registrato**.
4. Compilare i campi obbligatori (con asterischi rossi).
5. Nel campo **Product Line**, selezionare **Cloud Manager**, quindi selezionare il provider di fatturazione appropriato.
6. Copia il numero di serie del tuo account dal punto 2 precedente, completa il controllo di sicurezza, quindi conferma di aver letto la Global Data Privacy Policy di NetApp.

   Viene immediatamente inviata un'e-mail alla casella di posta fornita per finalizzare questa transazione sicura. Controllare le cartelle di spam se l'e-mail di convalida non arriva in pochi minuti.

7. Confermare l'azione dall'interno dell'e-mail.

   La conferma invia la tua richiesta a NetApp e ti consiglia di creare un account NetApp Support Site.

8. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.

Al termine

NetApp dovrebbe contattarti durante questo processo. Si tratta di un esercizio di assunzione per i nuovi utenti.

Una volta ottenuto l'account del sito di supporto NetApp, associare l'account al login BlueXP completando la procedura indicata in Cliente esistente con un account NSS.

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

Per attivare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP, è necessario associare le credenziali del sito di supporto NetApp all'account BlueXP:

- Registrazione dei sistemi Cloud Volumes ONTAP pay-as-you-go per il supporto

  È necessario fornire l'account NSS per attivare il supporto per il sistema e accedere alle risorse di supporto tecnico di NetApp.

- Implementazione di Cloud Volumes ONTAP con la propria licenza (BYOL)

  È necessario fornire l'account NSS in modo che BlueXP possa caricare la chiave di licenza e attivare l'abbonamento per il periodo di validità dell'acquisto. Sono inclusi gli aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP alla versione più recente

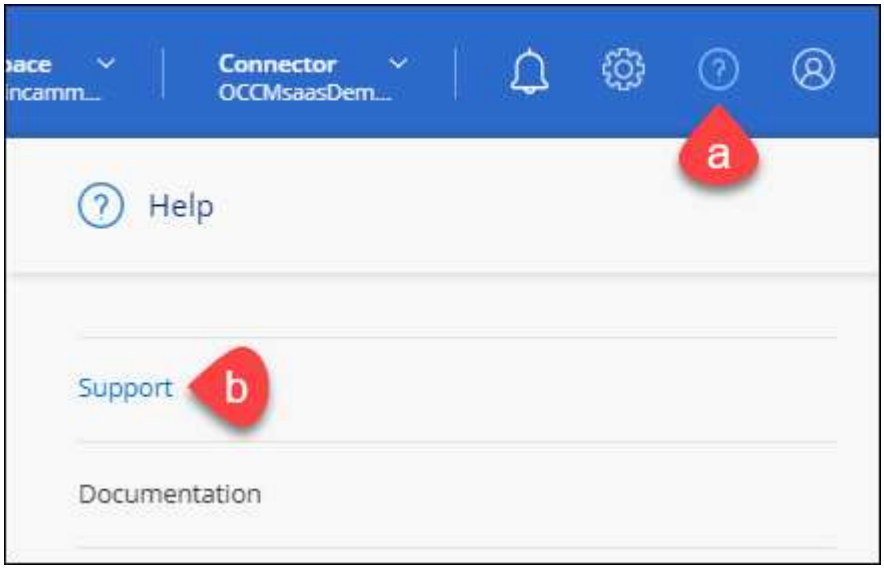
L'associazione delle credenziali NSS all'account BlueXP è diversa dall'account NSS associato a un account utente BlueXP.

Queste credenziali NSS sono associate all'ID account BlueXP specifico. Gli utenti che appartengono all'account BlueXP possono accedere a queste credenziali da **Support > NSS Management**.

- Se disponi di un account a livello di cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o reseller, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

Fasi

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



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, selezionare **continua** per essere reindirizzato a una pagina di accesso Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e la licenza.

4. Nella pagina di accesso, fornire l'indirizzo e-mail e la password registrati del NetApp Support Site per eseguire il processo di autenticazione.

   Queste azioni consentono a BlueXP di utilizzare il tuo account NSS per download di licenze, verifica dell'aggiornamento software e registrazioni di supporto future.

   Tenere presente quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account guest o temporaneo). Puoi avere più account NSS a livello di cliente.
   - Se si tratta di un account di livello partner, può essere presente un solo account NSS. Se si tenta di aggiungere account NSS a livello di cliente ed esiste un account a livello di partner, viene visualizzato il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account, in quanto esistono già utenti NSS di tipo diverso."

   Lo stesso vale se si dispone di account NSS a livello di cliente preesistenti e si tenta di aggiungere un account a livello di partner.

   - Una volta effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che viene mappato all'e-mail. Nella pagina **NSS Management**, è possibile visualizzare l'e-mail da ••• menu.

   - Se è necessario aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Update Credentials** (Aggiorna credenziali) in ••• menu.

     Questa opzione richiede di effettuare nuovamente l'accesso. Il token per questi account scade dopo 90 giorni. Verrà inviata una notifica per avvisare l'utente.

Richiedi assistenza

NetApp fornisce supporto per BlueXP e i suoi servizi cloud in diversi modi. Sono disponibili opzioni complete di supporto autonomo gratuito 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include il supporto tecnico remoto via web ticketing.

Ottieni supporto per un file service del cloud provider

Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service per Google Cloud"

Per ricevere supporto tecnico specifico di BlueXP e delle relative soluzioni e servizi storage, utilizza le opzioni di supporto descritte di seguito.

Utilizzare le opzioni di supporto automatico

Queste opzioni sono disponibili gratuitamente, 24 ore su 24, 7 giorni su 7:

- Documentazione

  La documentazione BlueXP attualmente visualizzata.

- "Knowledge base"

  Cercare nella Knowledge base di BlueXP articoli utili per la risoluzione dei problemi.

- "Community"

  Unisciti alla community BlueXP per seguire le discussioni in corso o crearne di nuove.

Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo l'attivazione del supporto.

Prima di iniziare

- Per utilizzare la funzione **creazione di un caso**, è necessario prima associare le credenziali del sito di supporto NetApp al login BlueXP. "Scopri come gestire le credenziali associate all'accesso a BlueXP".
- Se stai aprendo un caso per un sistema ONTAP con un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Nella pagina **risorse**, scegliere una delle opzioni disponibili in supporto tecnico:

   a. Selezionare **Chiamateci** se si desidera parlare con qualcuno al telefono. Viene visualizzata una pagina su netapp.com che elenca i numeri di telefono che è possibile chiamare.

   b. Selezionare **Crea un caso** per aprire un ticket con uno specialista del supporto NetApp:

      - **Servizio**: Selezionare il servizio a cui è associato il problema. Ad esempio, BlueXP quando si tratta di un problema di supporto tecnico relativo a flussi di lavoro o funzionalità all'interno del servizio.
      - **Ambiente di lavoro**: Se applicabile allo storage, selezionare **Cloud Volumes ONTAP** o **on-premise** e quindi l'ambiente di lavoro associato.

        L'elenco degli ambienti di lavoro rientra nell'ambito dell'account, dell'area di lavoro e del connettore BlueXP selezionato nel banner superiore del servizio.

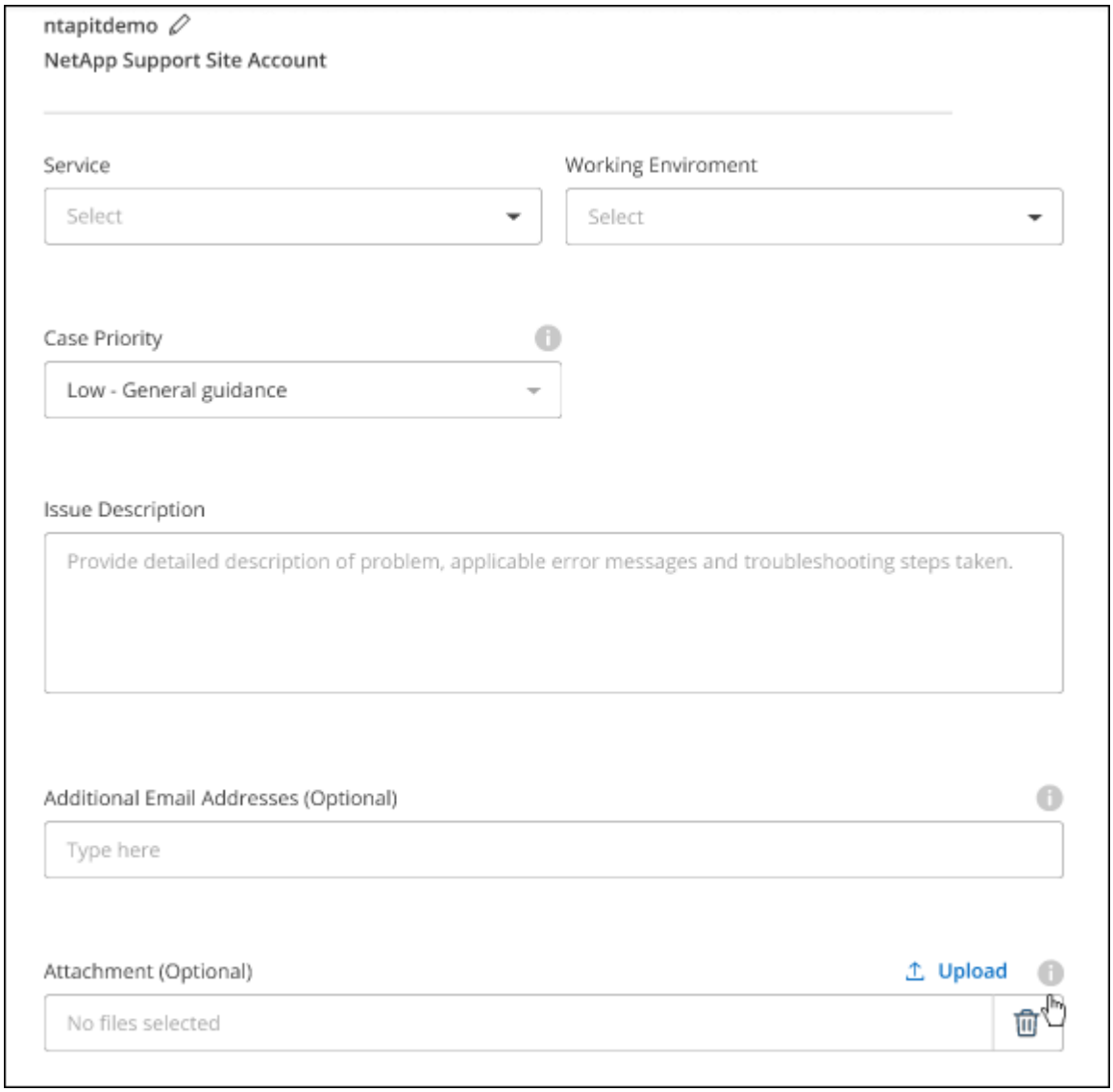
      - **Priorità caso**: Scegliere la priorità per il caso, che può essere bassa, Media, alta o critica.

        Per ulteriori informazioni su queste priorità, passare il mouse sull'icona delle informazioni accanto al nome del campo.

      - **Descrizione del problema**: Fornire una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o procedure di risoluzione dei problemi che sono state eseguite.
      - **Indirizzi e-mail aggiuntivi**: Inserisci indirizzi e-mail aggiuntivi se desideri informare qualcun altro del problema.

- **Allegato (opzionale)**: Carica fino a cinque allegati, uno alla volta.

  Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Al termine

Viene visualizzata una finestra a comparsa con il numero del caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei casi di supporto, selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "Crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzare i dettagli.

È possibile che venga visualizzato il seguente messaggio di errore quando si tenta di creare un caso:

"Non sei autorizzato a creare un caso per il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società di registrazione a cui è associato non sono la stessa società di registrazione per il numero di serie dell'account BlueXP (ad es. 960xxxx) o il numero di serie dell'ambiente di lavoro. È possibile richiedere assistenza utilizzando una delle seguenti opzioni:

- Utilizza la chat integrata nel prodotto
- Inviare un caso non tecnico all'indirizzo https://mysupport.netapp.com/site/help

Gestire i casi di supporto (anteprima)

È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente da BlueXP. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

La gestione del caso è disponibile come anteprima. Intendiamo perfezionare questa esperienza e aggiungere miglioramenti alle prossime release. Inviaci un feedback utilizzando la chat in-product.

Tenere presente quanto segue:

- La dashboard di gestione dei casi nella parte superiore della pagina offre due visualizzazioni:
  - La vista a sinistra mostra il totale dei casi aperti negli ultimi 3 mesi dall'account NSS dell'utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base all'account NSS dell'utente.

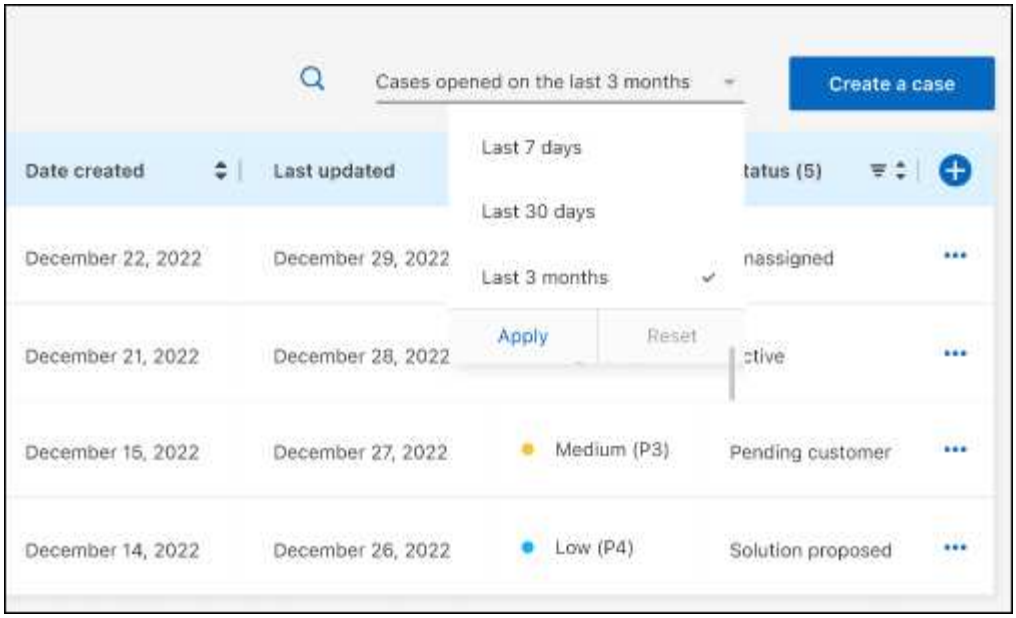
  I risultati della tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come priorità e Stato. Altre colonne offrono funzionalità di ordinamento.

  Per ulteriori informazioni, consulta la procedura riportata di seguito.
- A livello di caso, offriamo la possibilità di aggiornare le note del caso o chiudere un caso che non è già in stato chiuso o in attesa di chiusura.

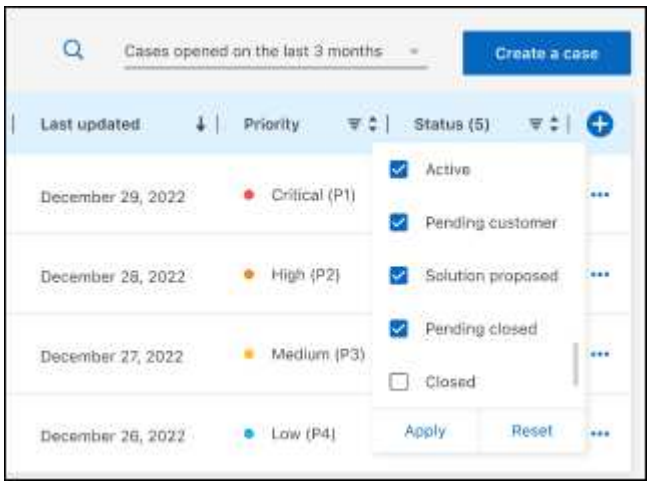
Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Selezionare **Gestione casi** e, se richiesto, aggiungere l'account NSS a BlueXP.

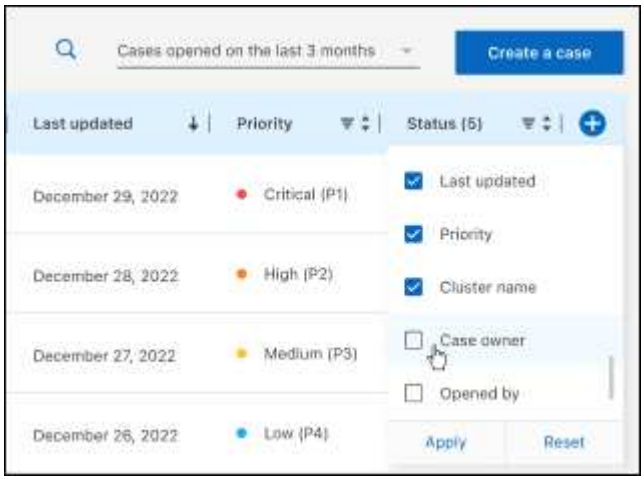
   La pagina **Gestione del caso** mostra i casi aperti relativi all'account NSS associato all'account utente BlueXP. Si tratta dello stesso account NSS visualizzato nella parte superiore della pagina **gestione NSS**.
3. Se si desidera, modificare le informazioni visualizzate nella tabella:
   - In **Organization's Cases** (casi dell'organizzazione), selezionare **View** (Visualizza) per visualizzare tutti i casi associati alla società.
   - Modificare l'intervallo di date scegliendo un intervallo di date esatto o scegliendo un intervallo di tempo diverso.



- Filtrare il contenuto delle colonne.



- Modificare le colonne visualizzate nella tabella selezionando e quindi scegliere le colonne che si desidera visualizzare.

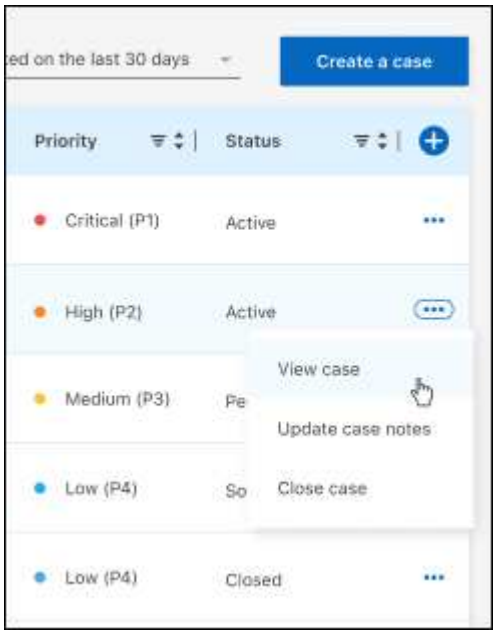


4. Gestire un caso esistente selezionando ••• e selezionando una delle opzioni disponibili:

   - **Visualizza caso**: Visualizza tutti i dettagli relativi a un caso specifico.
   - **Aggiorna note sul caso**: Fornisci ulteriori dettagli sul problema oppure seleziona **carica file** per allegare fino a un massimo di cinque file.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

   - **Chiudi caso**: Fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.



Note legali

Le note legali forniscono l’accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all’indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

"Avviso per BlueXP"