Connettori

Setup and administration

NetApp
April 26, 2024

Sommario

Connettori

Individuare l'ID di sistema di un connettore

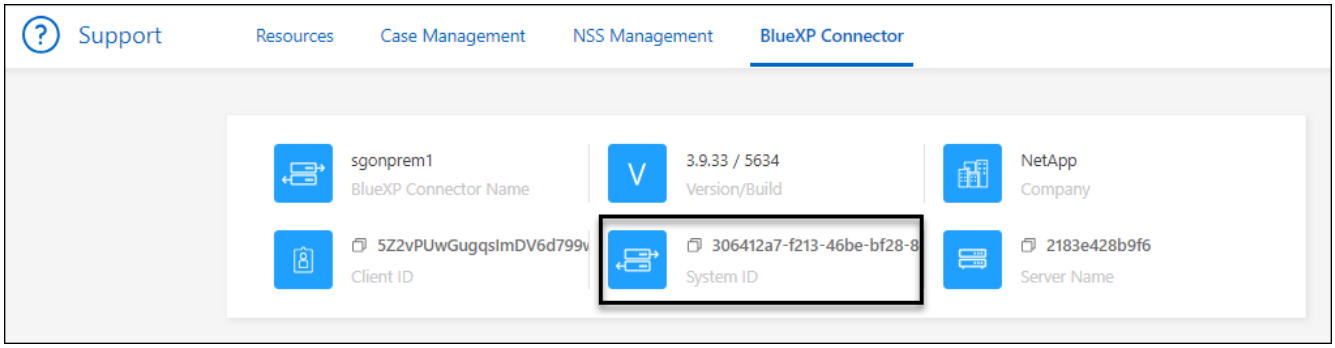
Per iniziare, il rappresentante NetApp potrebbe richiedere l'ID di sistema del connettore. L'ID viene generalmente utilizzato a scopo di licensing e troubleshooting.

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".

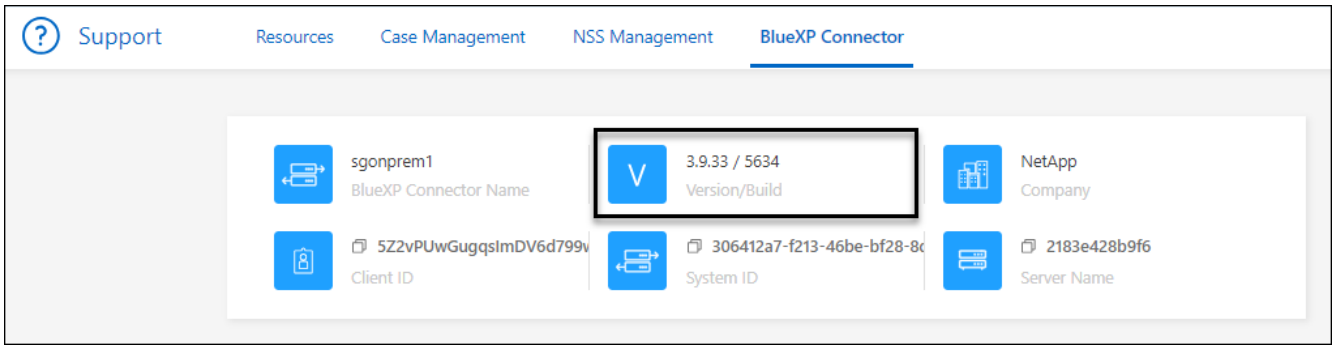
Visualizzare la versione di un connettore

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.



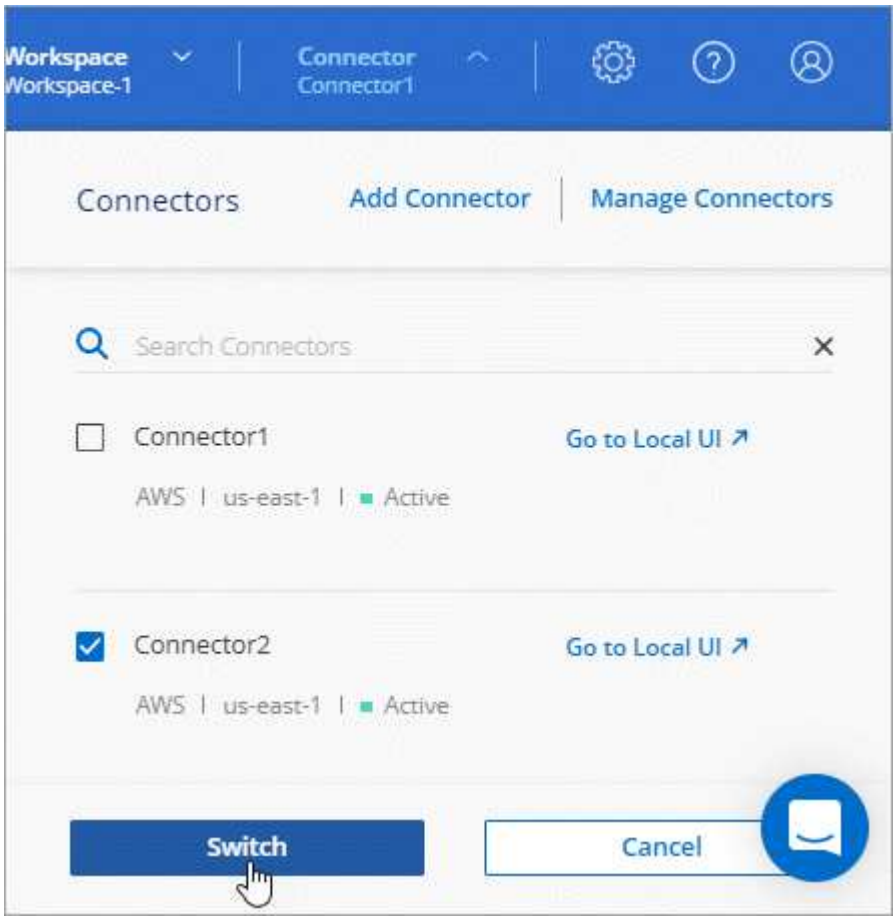
Passare da un connettore all'altro

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

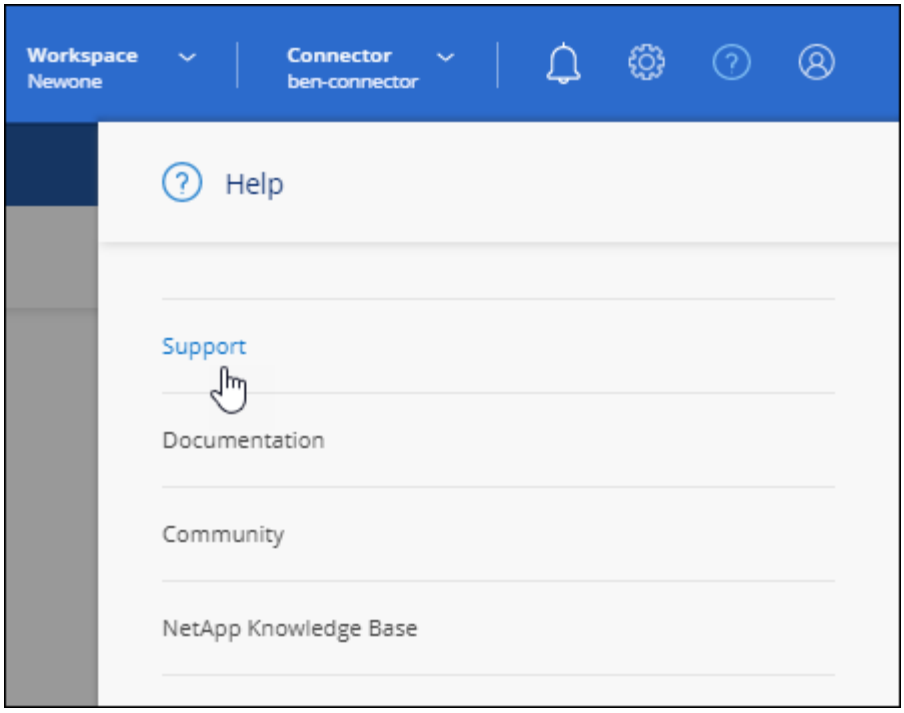
BlueXP aggiorna e mostra gli ambienti di lavoro associati al connettore selezionato.

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

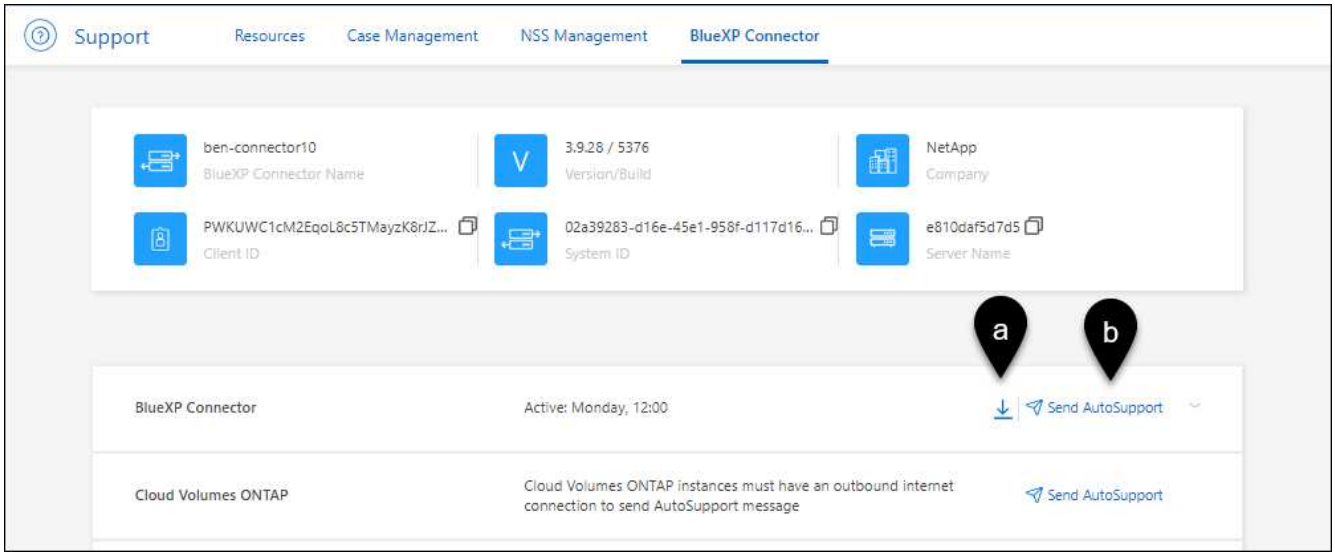
1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



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

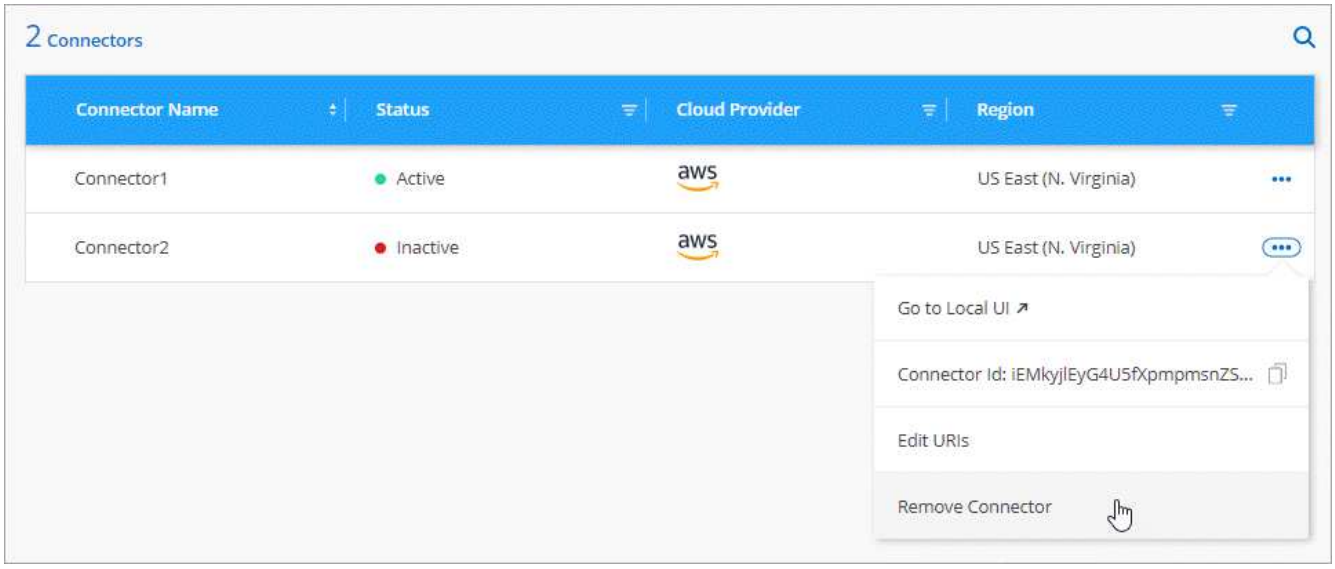
Se un connettore non è attivo, è possibile rimuoverlo dall'elenco dei connettori in BlueXP. Questa operazione può essere eseguita se la macchina virtuale Connector è stata eliminata o se il software Connector è stato disinstallato.

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**.

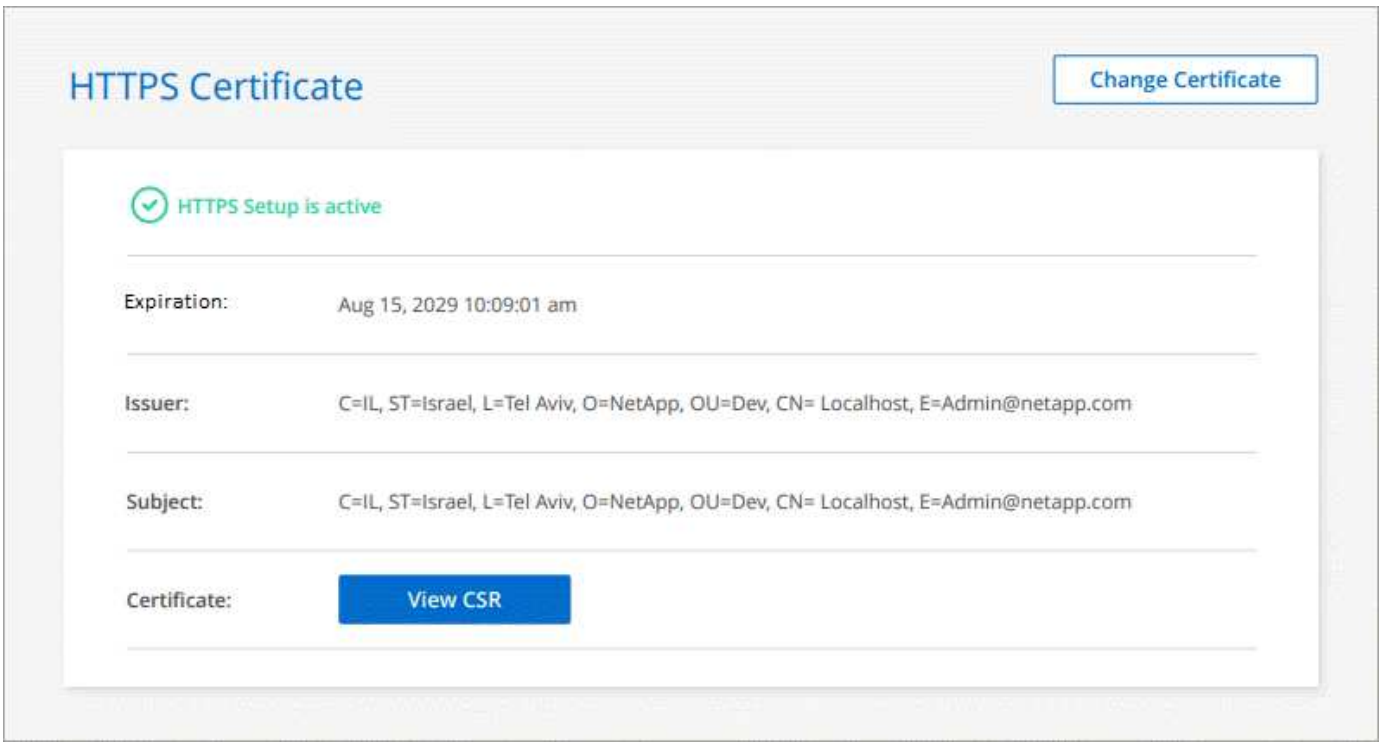
2. Nella pagina HTTPS Setup (Configurazione HTTPS), installare un certificato generando una richiesta di

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**.

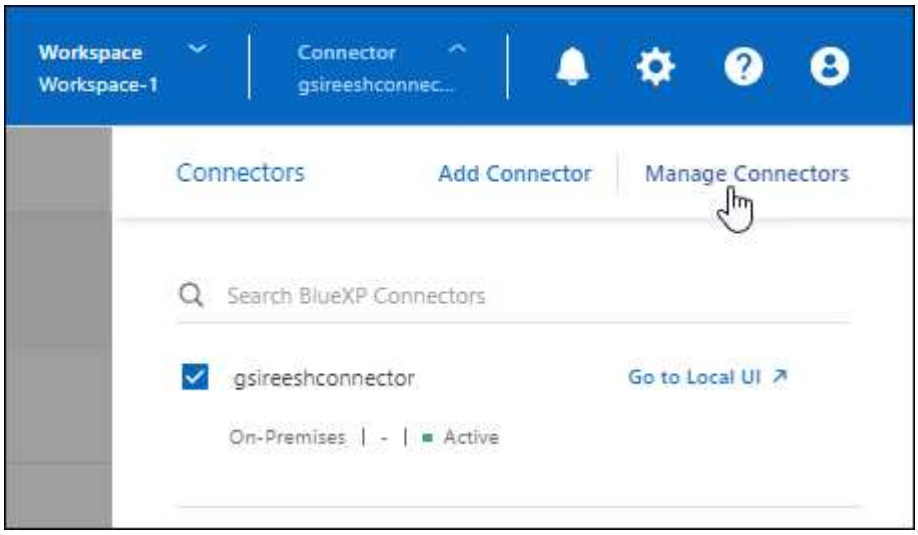
   La navigazione dipende dall'utilizzo di BlueXP in modalità standard (accesso all'interfaccia BlueXP dal sito

Web SaaS) o in modalità limitata o privata (accesso all’interfaccia BlueXP localmente dall’host del connettore).

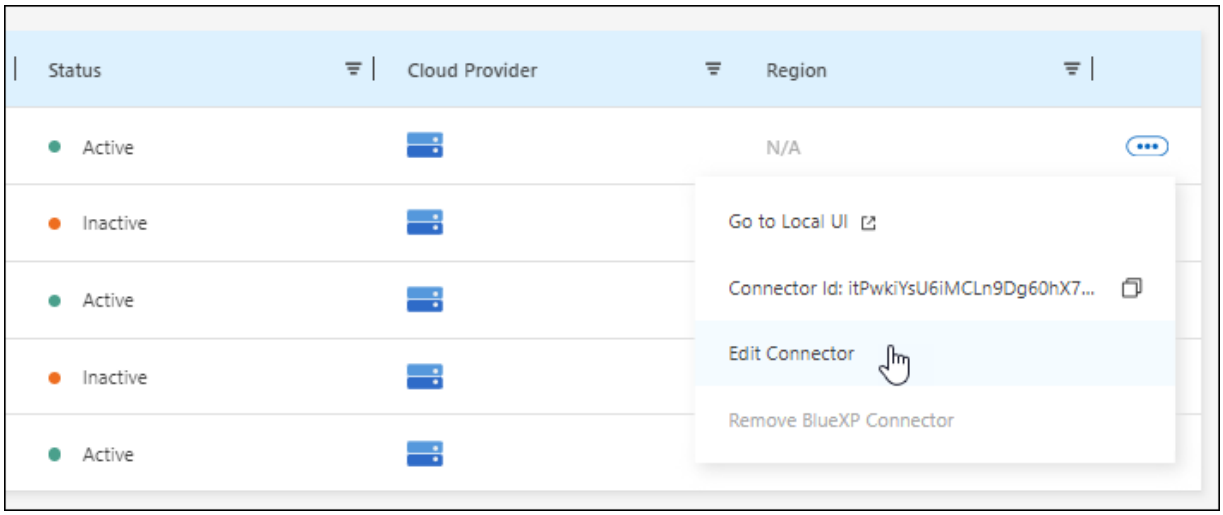
Modalità standard

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

b. Selezionare **Gestisci connettori**.



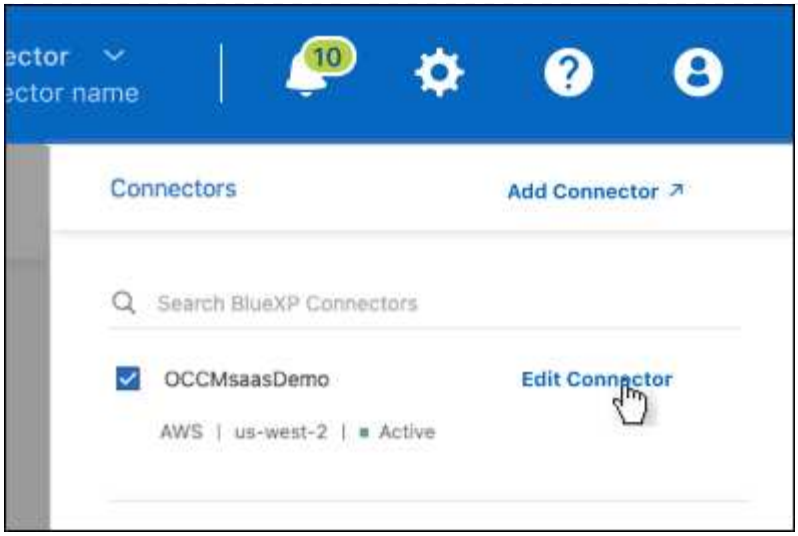
c. Selezionare il menu azione per un connettore e selezionare **Modifica connettore**.



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

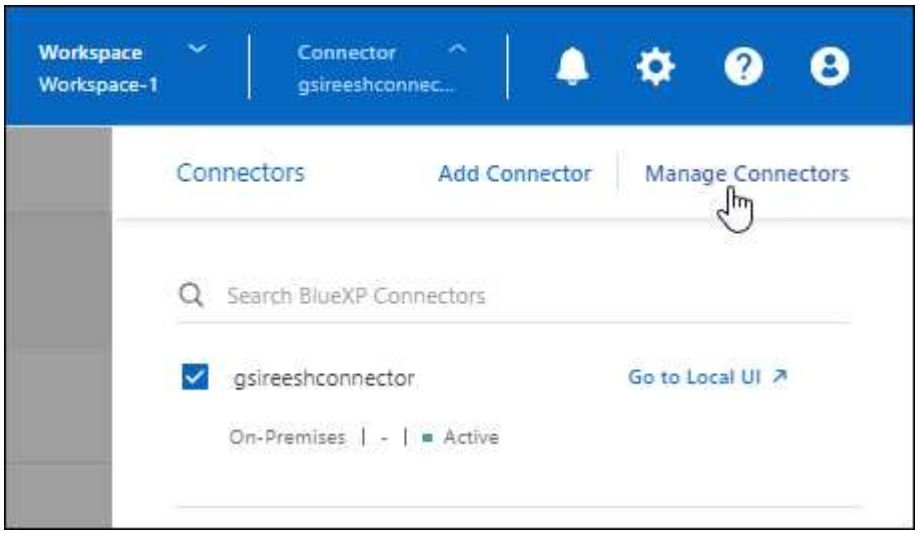
1. Accedere alla pagina **Modifica connettore BlueXP**:

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).

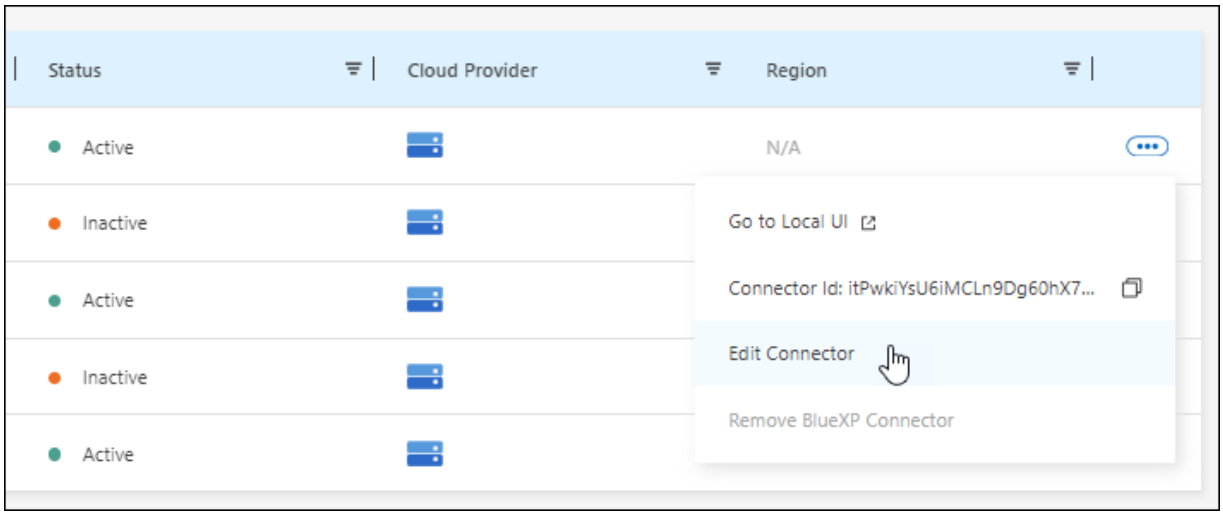
Modalità standard

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

b. Selezionare **Gestisci connettori**.



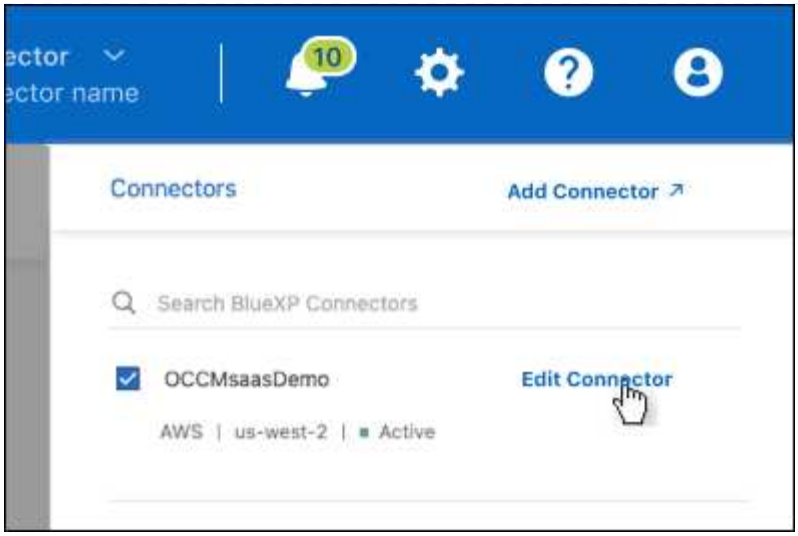
c. Selezionare il menu azione per un connettore e selezionare **Modifica connettore**.



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