



Amministrare BlueXP

Setup and administration

NetApp
April 26, 2024

This PDF was generated from <https://docs.netapp.com/it-it/bluexp-setup-admin/concept-federation.html> on April 26, 2024. Always check docs.netapp.com for the latest.

Sommario

- Amministrare BlueXP 1
 - Utilizzo della federazione delle identità con BlueXP 1
 - BlueXP 7
 - Connettori 21
 - Credenziali e iscrizioni 40

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:

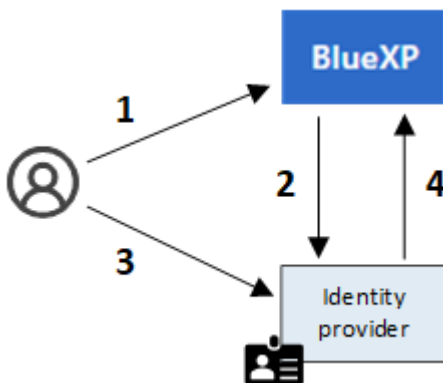
- Scaricare e completare il "[Modulo di richiesta della Federazione NetApp](#)"
- Inviare il modulo all'indirizzo e-mail specificato nel modulo

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)	<p>Configura il tuo provider di identità SAML per abilitare la federazione delle identità con BlueXP.</p> <p>Visualizza le istruzioni per il tuo provider di identità SAML:</p> <ul style="list-style-type: none"> • "ADFS" • "OKTA" • "OneLogin" • "PingFederate" • "Salesforce" • "Siteminder" • "SSOCircle" <p>Se il provider di identità non compare nell'elenco precedente, "seguire queste istruzioni generiche"</p> <div>  <p>Non completare i passaggi che descrivono come creare una connessione in auth0. La connessione verrà creata nel passaggio successivo.</p> </div>
2	Amministratore di BlueXP	<p>Accedere alla "Pagina NetApp Federation Setup" E creare la connessione con BlueXP.</p> <p>Per completare questo passaggio, è necessario ottenere quanto segue dall'amministratore ad in merito al provider di identità:</p> <ul style="list-style-type: none"> • URL di accesso • Un certificato di firma X509 (formato PEM o CER) • URL di disconnessione (opzionale) <p>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.</p> <div>  <p>Prendere nota della data di scadenza del certificato. È necessario tornare alla pagina Federation Setup e aggiornare il certificato <i>prima</i> 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.</p> </div>
3	AD admin	<p>Completare la configurazione sul provider di identità utilizzando i parametri mostrati nella pagina Federation Setup (impostazione federazione) al termine del passaggio 2.</p>

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

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	<p>Configurare Microsoft Entra ID per abilitare la federazione delle identità con BlueXP.</p> <p>"Visualizzare le istruzioni per la registrazione dell'applicazione con Microsoft Entra ID"</p> <div>  <p>Non completare i passaggi che descrivono come creare una connessione in auth0. La connessione verrà creata nel passaggio successivo.</p> </div>
2	Amministratore di BlueXP	<p>Accedere alla "Pagina NetApp Federation Setup" E creare la connessione con BlueXP.</p> <p>Per completare questo passaggio, è necessario ottenere quanto segue dall'amministratore di ad:</p> <ul style="list-style-type: none"> • ID client • Valore segreto del client • Dominio Microsoft Entra ID <p>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.</p> <div>  <p>Prendere nota della data di scadenza della chiave segreta. È necessario tornare alla pagina Federation Setup e aggiornare il certificato <i>prima</i> 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.</p> </div>
3	AD admin	<p>Completare la configurazione in Microsoft Entra ID utilizzando i parametri mostrati nella pagina impostazione Federazione dopo aver completato il passaggio 2.</p>

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

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	<p>Configurare il server ADFS per abilitare la federazione delle identità con BlueXP.</p> <p>"Visualizza le istruzioni per la configurazione del server ADFS con auth0"</p>
2	Amministratore di BlueXP	<p>Accedere alla "Pagina NetApp Federation Setup" E creare la connessione con BlueXP.</p> <p>Per completare questo passaggio, è necessario ottenere quanto segue dall'amministratore ad: L'URL del server ADFS o il file di metadati della federazione.</p> <p>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.</p> <div>  <p>Prendere nota della data di scadenza del certificato. È necessario tornare alla pagina Federation Setup e aggiornare il certificato <i>prima</i> 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.</p> </div>
3	AD admin	<p>Completare la configurazione sul server ADFS utilizzando i parametri mostrati nella pagina Federation Setup (impostazione federazione) al termine del passaggio 2.</p>
4	Amministratore di BlueXP	<p>Verificare e attivare la connessione da "Pagina NetApp Federation Setup"</p> <p>Si noti che la pagina viene aggiornata tra il test della connessione e l'abilitazione della connessione.</p>

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	<p>Configurare il server PingFederate per abilitare la federazione delle identità con BlueXP.</p> <p>"Visualizza le istruzioni per la creazione di una connessione"</p> <div>  <p>Non completare i passaggi che descrivono come creare una connessione in auth0. La connessione verrà creata nel passaggio successivo.</p> </div>
2	Amministratore di BlueXP	<p>Accedere alla "Pagina NetApp Federation Setup" E creare la connessione con BlueXP.</p> <p>Per completare questo passaggio, è necessario ottenere quanto segue dall'amministratore di ad:</p> <ul style="list-style-type: none"> • URL del server PingFederate • Un certificato di firma X509 (formato PEM o CER) <p>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.</p> <div>  <p>Prendere nota della data di scadenza del certificato. È necessario tornare alla pagina Federation Setup e aggiornare il certificato <i>prima</i> 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.</p> </div>
3	AD admin	<p>Completare la configurazione sul server PingFederate utilizzando i parametri mostrati nella pagina Federation Setup (impostazione federazione) al termine del passaggio 2.</p>
4	Amministratore di BlueXP	<p>Verificare e attivare la connessione da "Pagina NetApp Federation Setup"</p> <p>Si noti che la pagina viene aggiornata tra il test della connessione e l'abilitazione della connessione.</p>

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

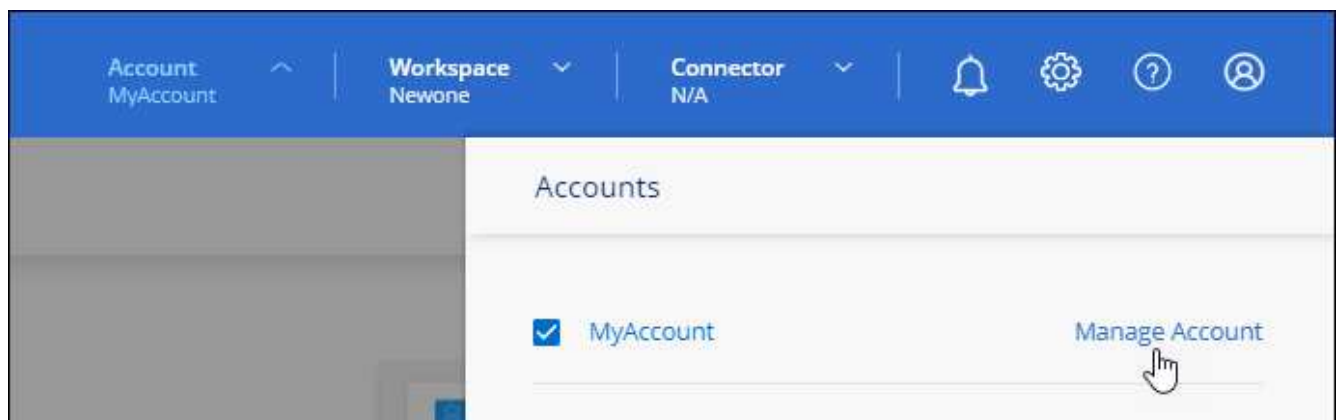
Associare gli utenti al proprio account BlueXP in modo che possano creare e gestire ambienti di lavoro in BlueXP.

Fasi

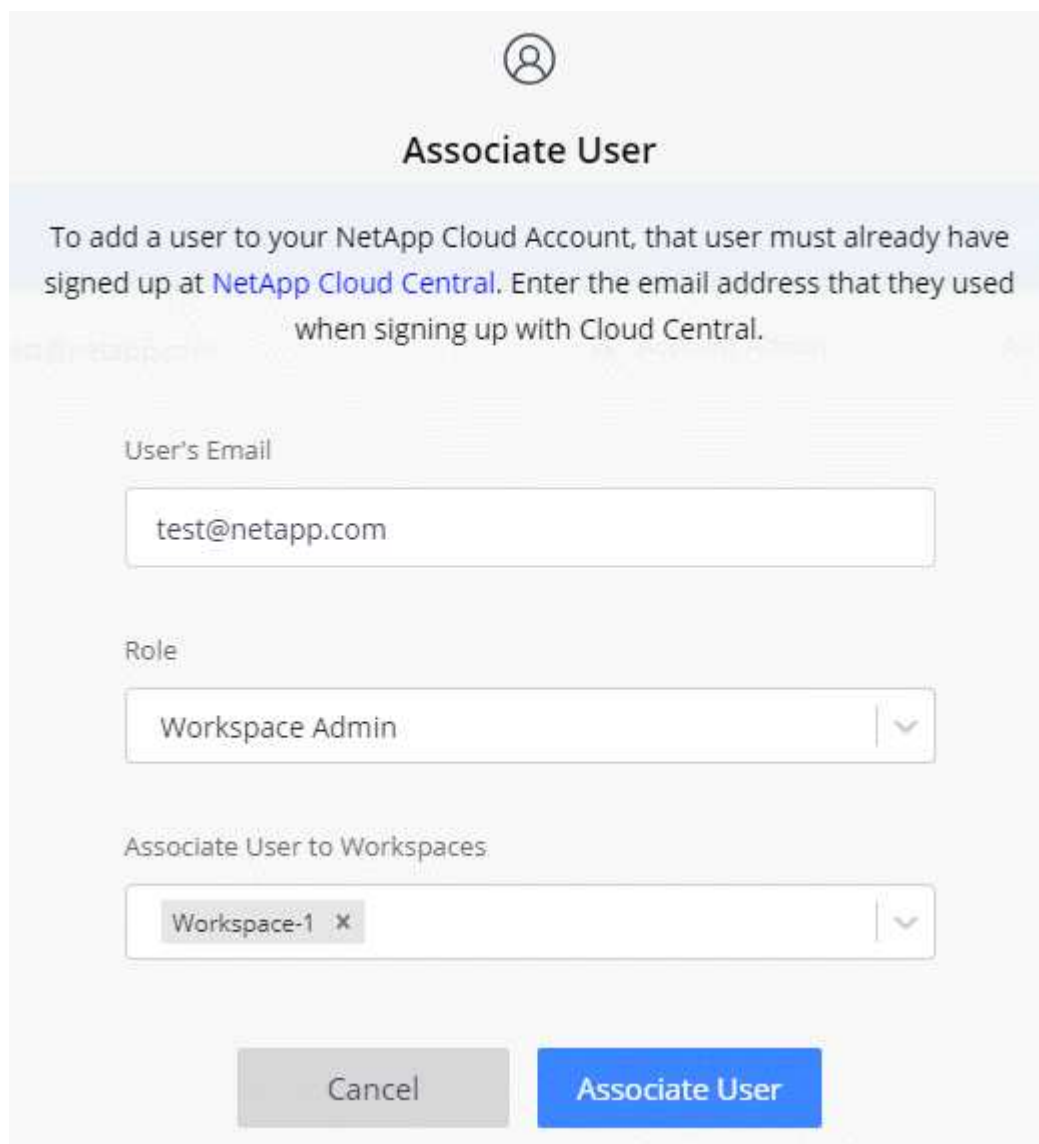
1. Se l'utente non l'ha già fatto, chiedere all'utente di accedere a ["Sito Web di NetApp BlueXP"](#) e iscriverti.
2. Nella parte superiore di BlueXP, selezionare l'elenco a discesa **account**.




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.





Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1 x

Cancel Associate User

7. Selezionare **Associa**.

Risultato

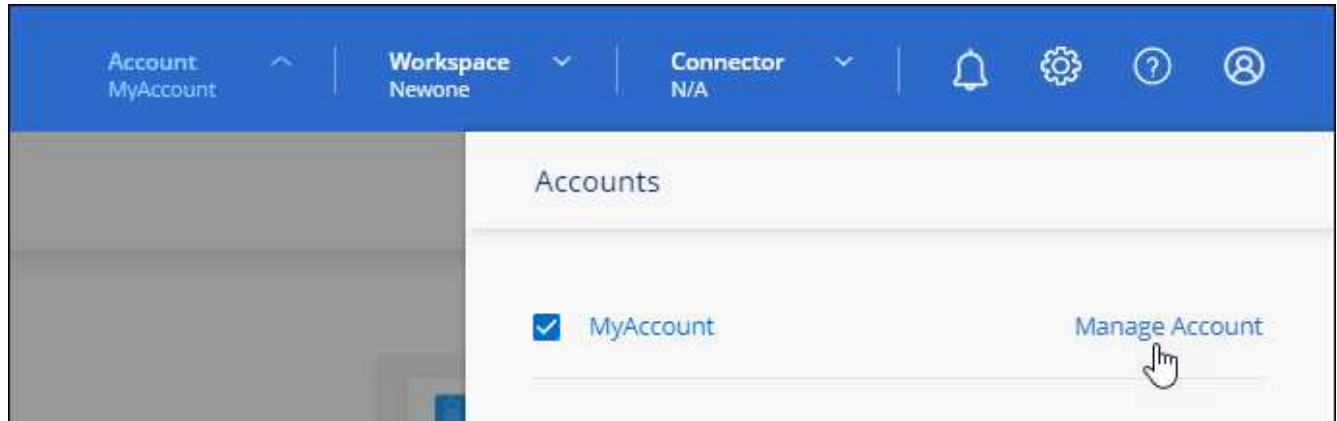
L'utente deve ricevere un'e-mail da NetApp BlueXP intitolata "account Association". L'e-mail include le informazioni necessarie per accedere a BlueXP.

Rimuovere gli utenti

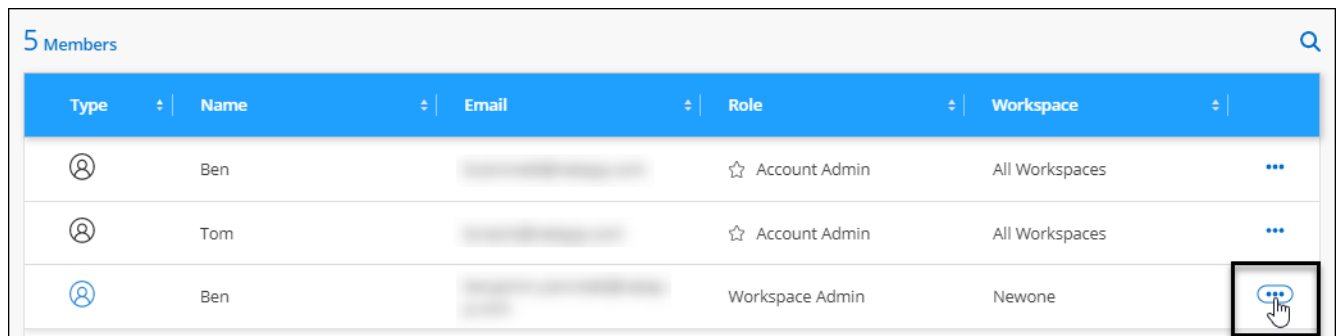
La disassociazione di un utente lo rende in modo che non possa più accedere alle risorse in un account BlueXP.

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.



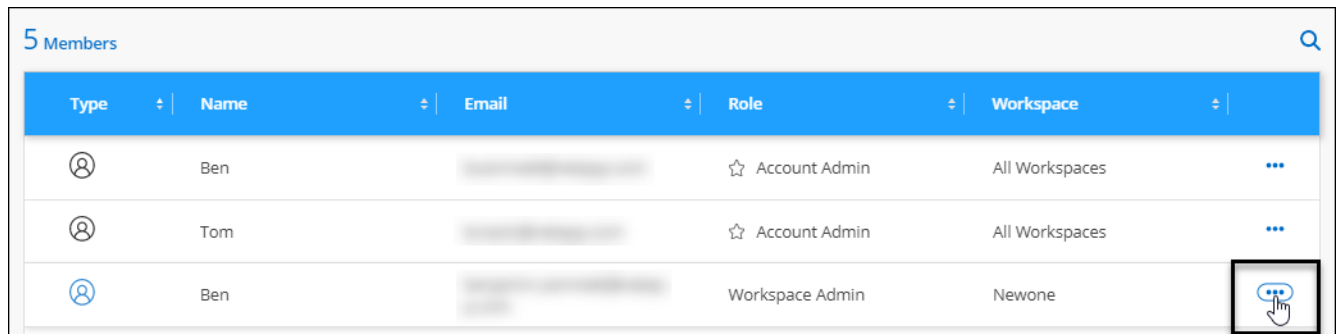
Inoltre, è necessario associare il connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano accedervi da BlueXP. ["Scopri come gestire le aree di lavoro di un connettore"](#).

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 assegnandogli 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.

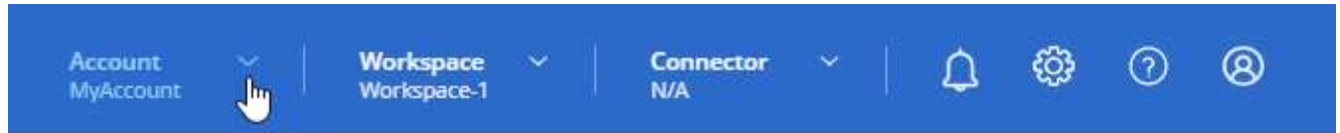
Tenere presente che non è necessario un token di aggiornamento per le operazioni API quando si utilizza un account di servizio. ["Informazioni sui token di aggiornamento"](#)

Creare un account di servizio

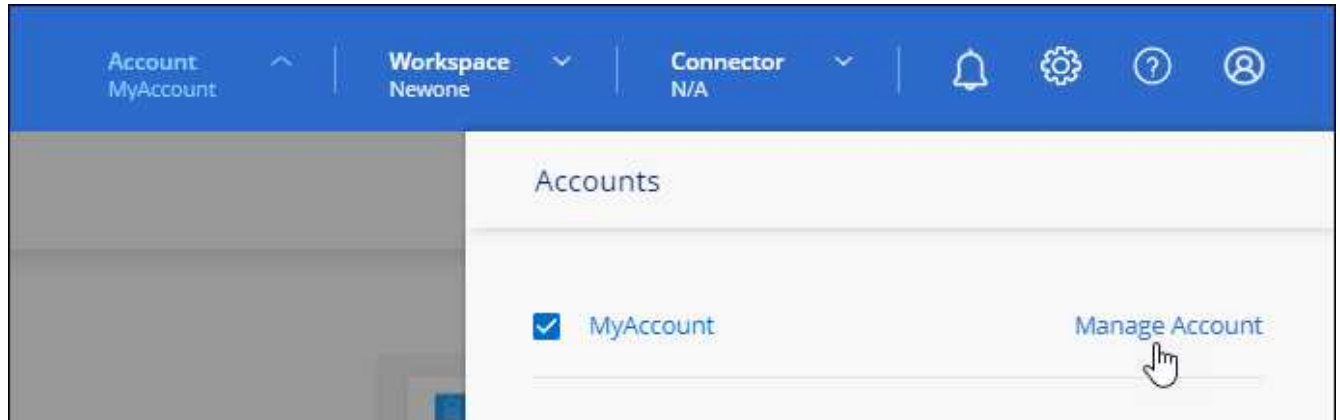
Creare tutti gli account di servizio necessari per gestire le risorse negli ambienti di lavoro.

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.

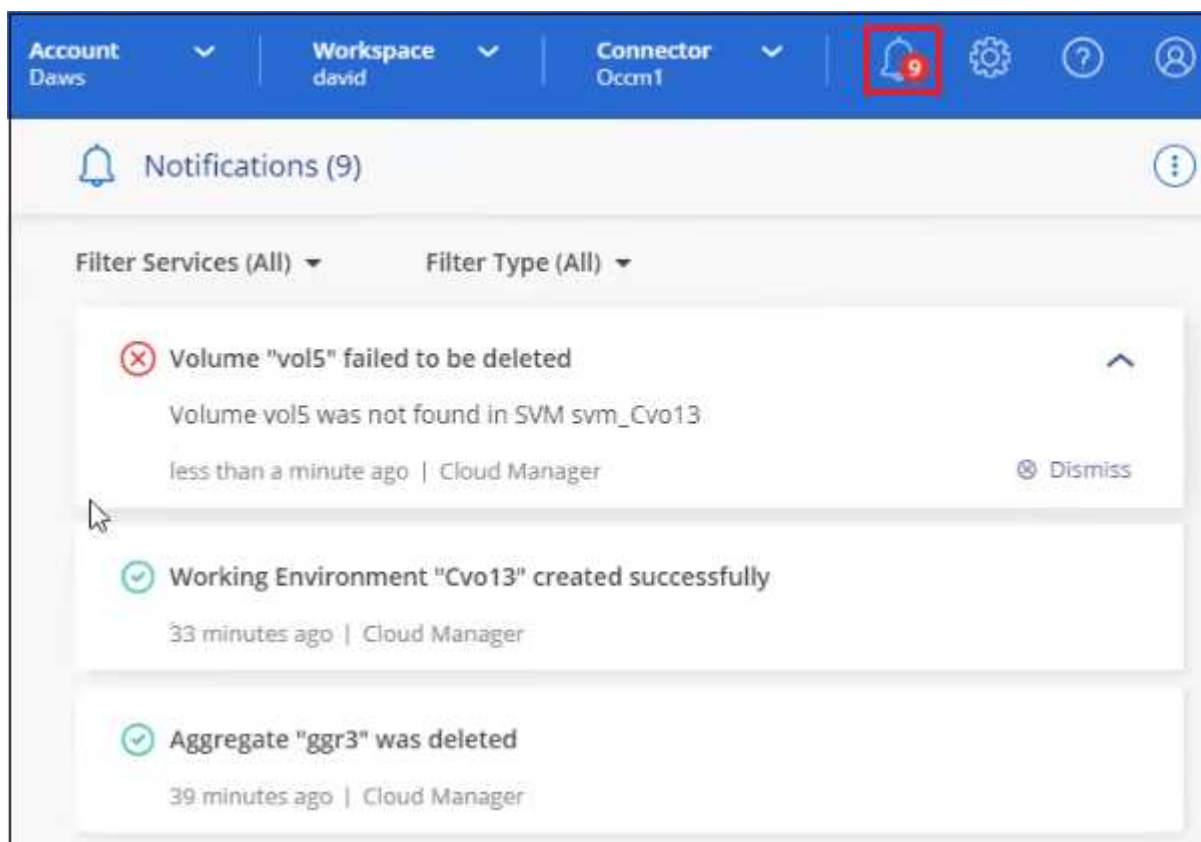
Centro notifiche	Tempistiche
Mostra lo stato di alto livello per eventi e azioni	Fornisce informazioni dettagliate su ciascun evento o azione per ulteriori indagini
Mostra lo stato della sessione di accesso corrente (le informazioni non vengono visualizzate nel Centro notifiche dopo la disconnessione)	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".

Filter Services (All) ▲

☒ Digital Wallet (3)
☒ Active IQ (2)
☐ AppTemplate (1)

Clear
Apply

Filter Type (All) ▲

☐ Information (0)
☐ Success (1)
☒ Warning (2)
☒ Error (1)
☒ Critical (0)
☐ Recommendation (0)

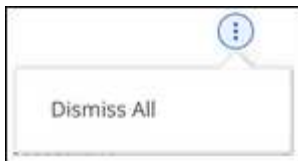
Clear
Apply

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.

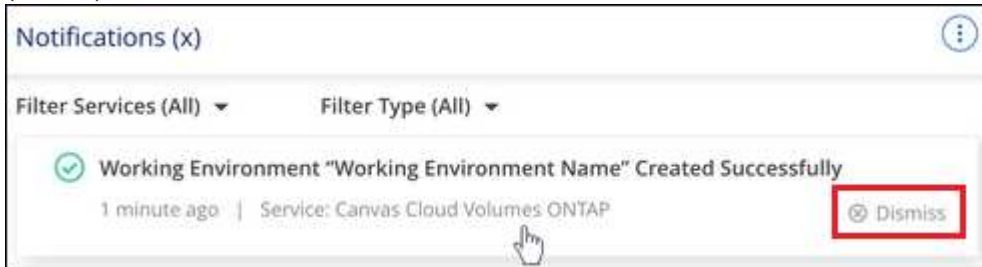
Consente di chiudere le notifiche

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.

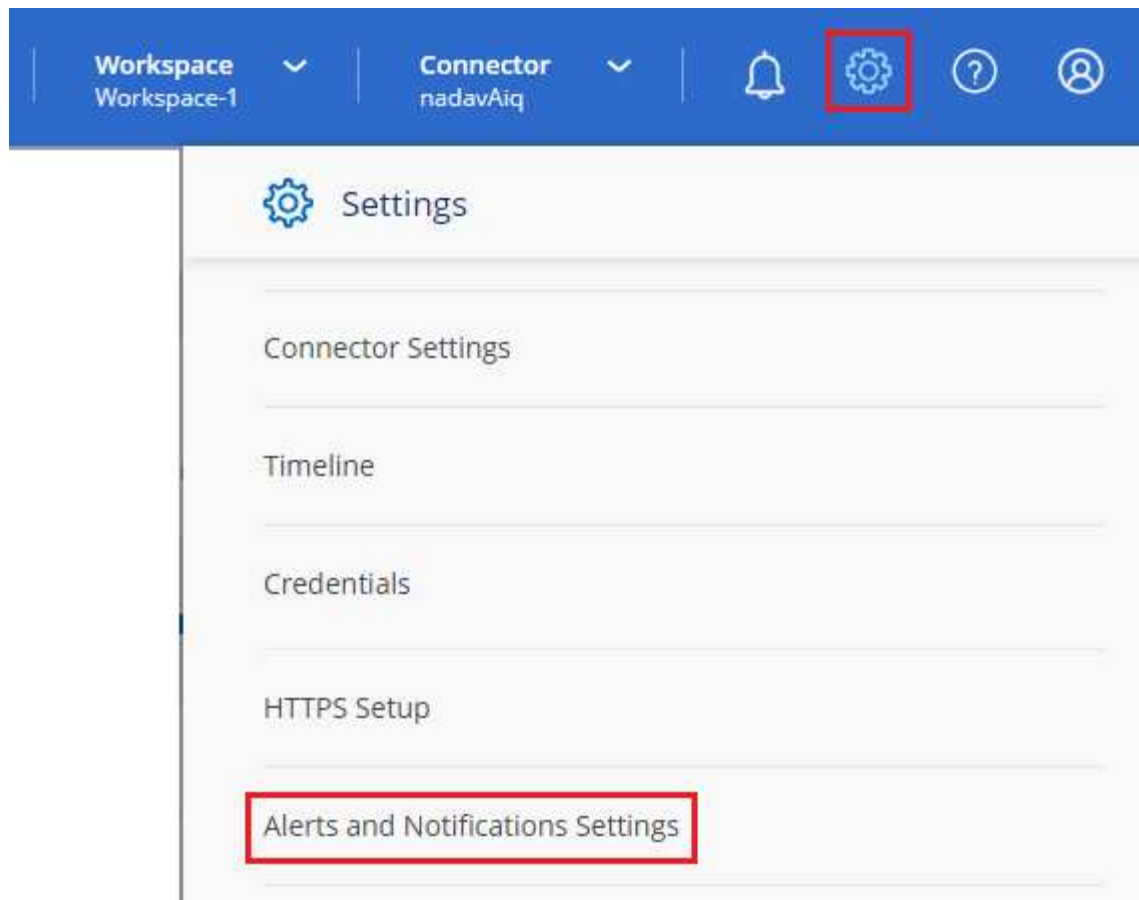
I filtri impostati nel Centro notifiche non determinano i tipi di notifiche che verranno inviate tramite e-mail. Per impostazione predefinita, gli account Admins di BlueXP riceveranno e-mail per tutte le notifiche "critiche" e "consigliate". Queste notifiche si applicano a tutti i servizi: Non è possibile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

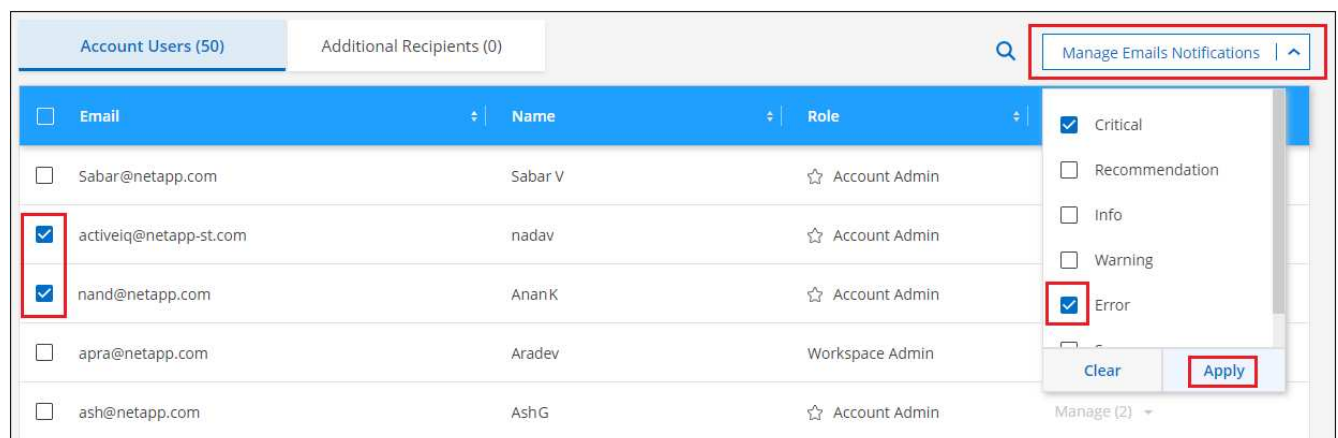
Fasi

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**.



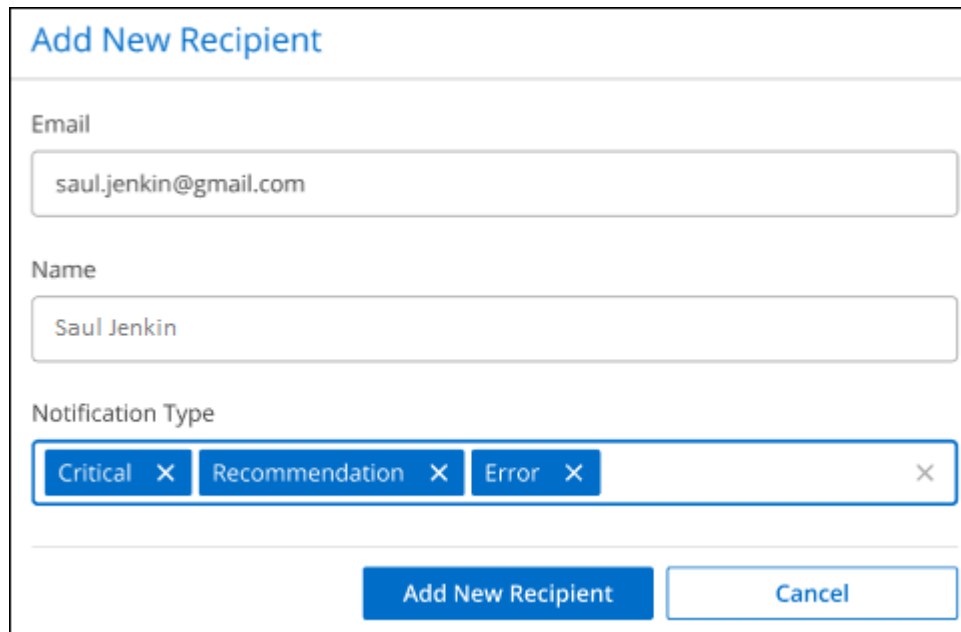
Aggiungere altri destinatari di posta elettronica

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**.



Add New Recipient

Email
saul.jenkin@gmail.com

Name
Saul Jenkin

Notification Type
Critical × Recommendation × Error ×

Add New Recipient Cancel

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

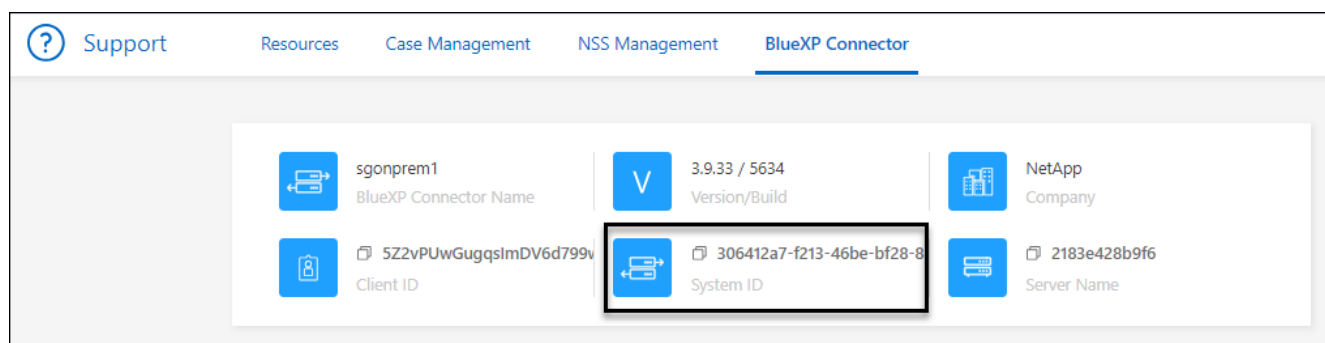
Per iniziare, il rappresentante NetApp potrebbe richiedere l'ID di sistema del connettore. L'ID viene generalmente utilizzato a scopo di licensing e troubleshooting.

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

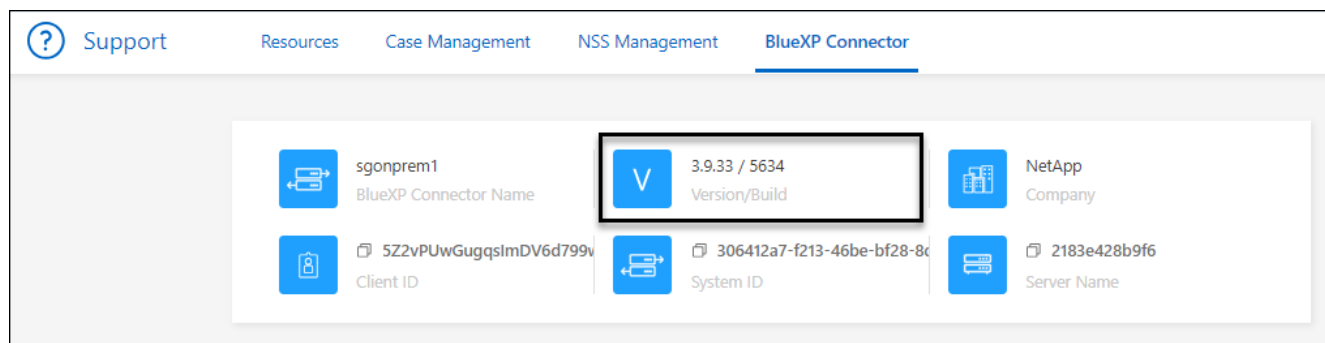
È possibile visualizzare la versione del connettore per verificare che il connettore sia stato aggiornato automaticamente alla versione più recente o perché è necessario condividerlo con il rappresentante NetApp.

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.



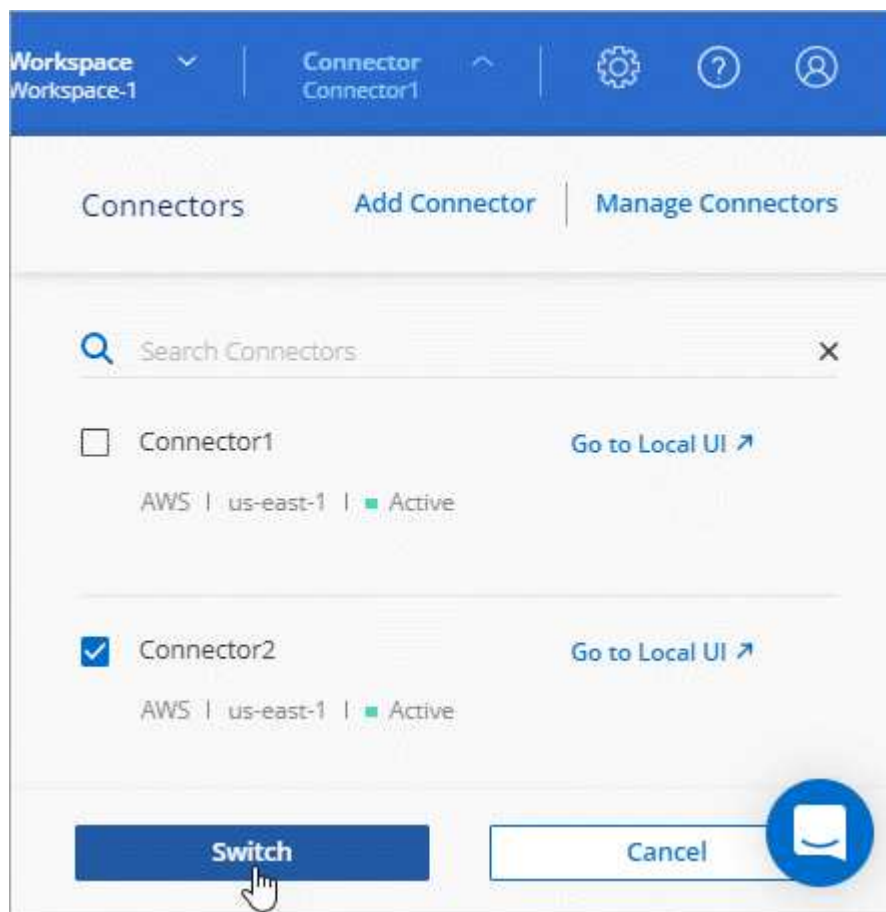
Passare da un connettore all'altro

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

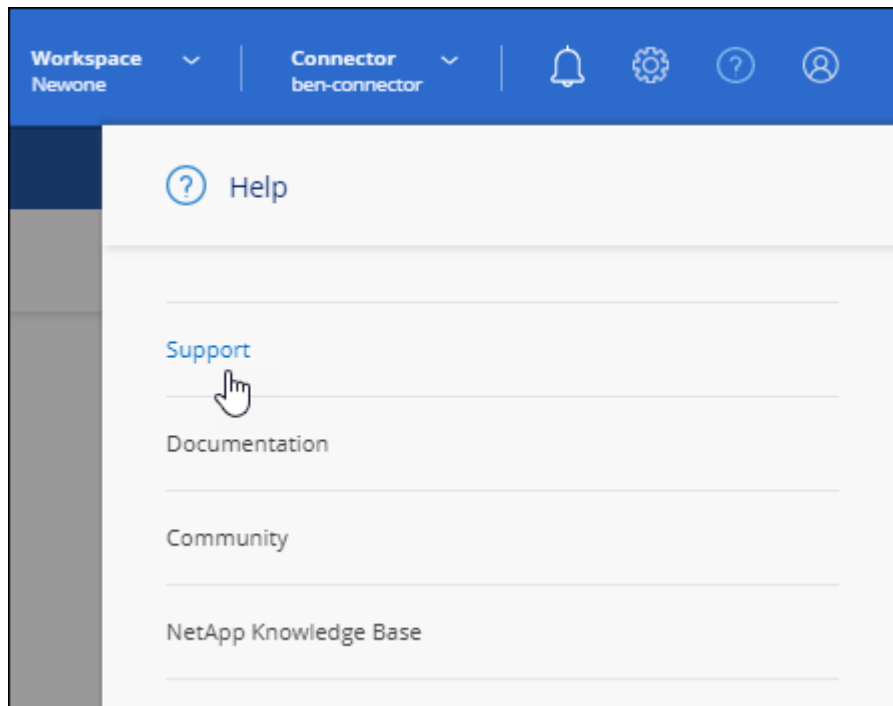
BlueXP aggiorna e mostra gli ambienti di lavoro associati al connettore selezionato.

Scaricare o inviare un messaggio AutoSupport

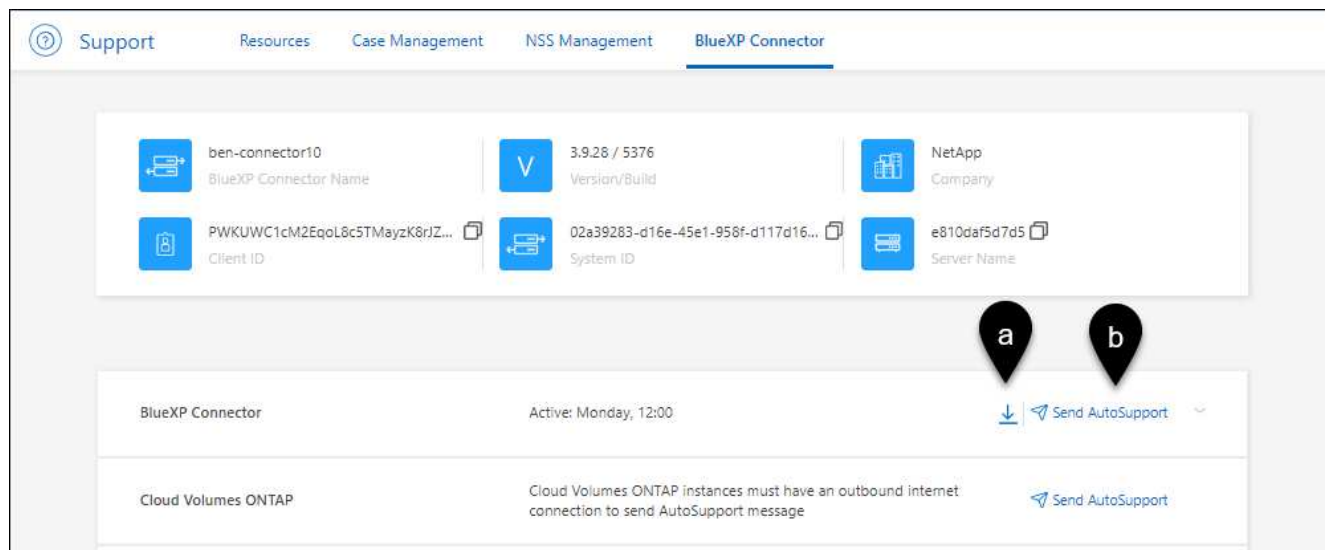
In caso di problemi, il personale NetApp potrebbe richiedere di inviare un messaggio AutoSupport al supporto NetApp per la risoluzione dei problemi.

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](#)

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'interfaccia 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**.

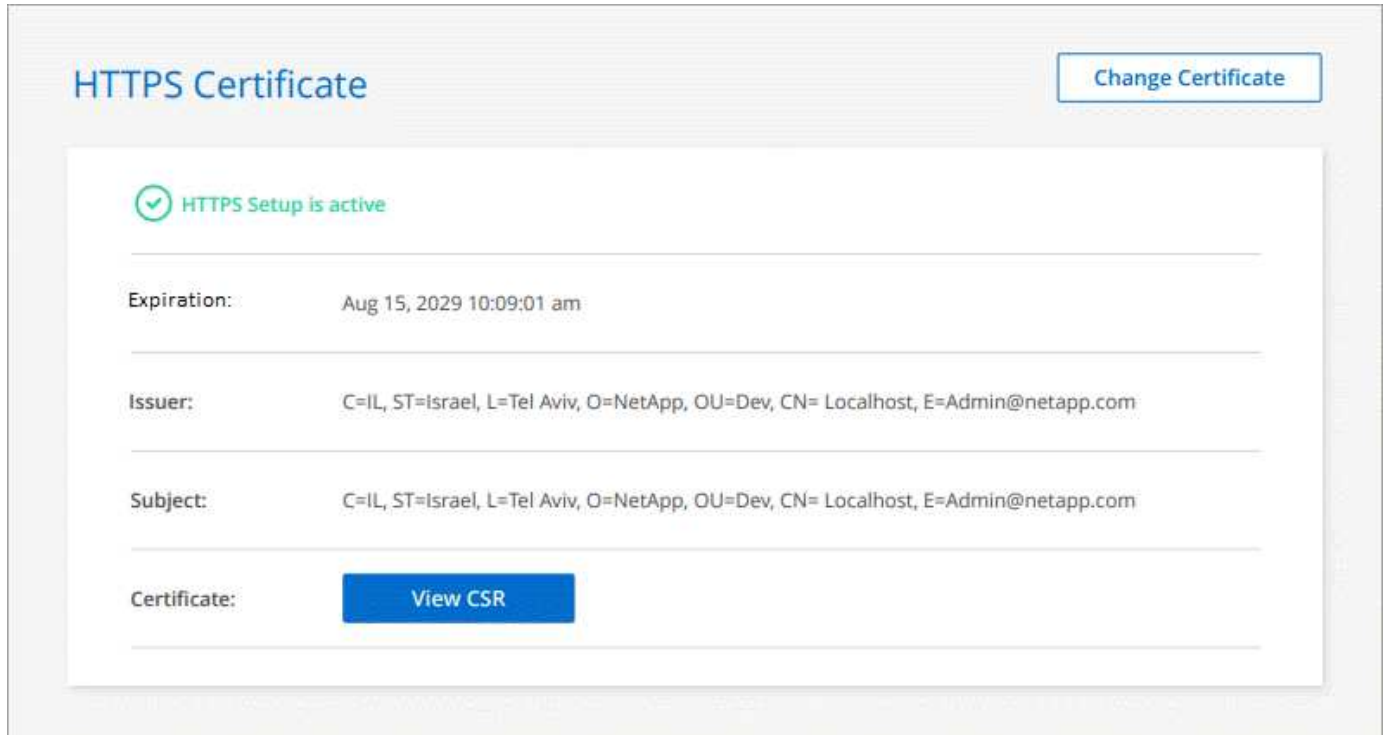


2. Nella pagina HTTPS Setup (Configurazione HTTPS), installare un certificato generando una richiesta di firma del certificato (CSR) o installando il proprio certificato firmato dalla CA:

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

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.

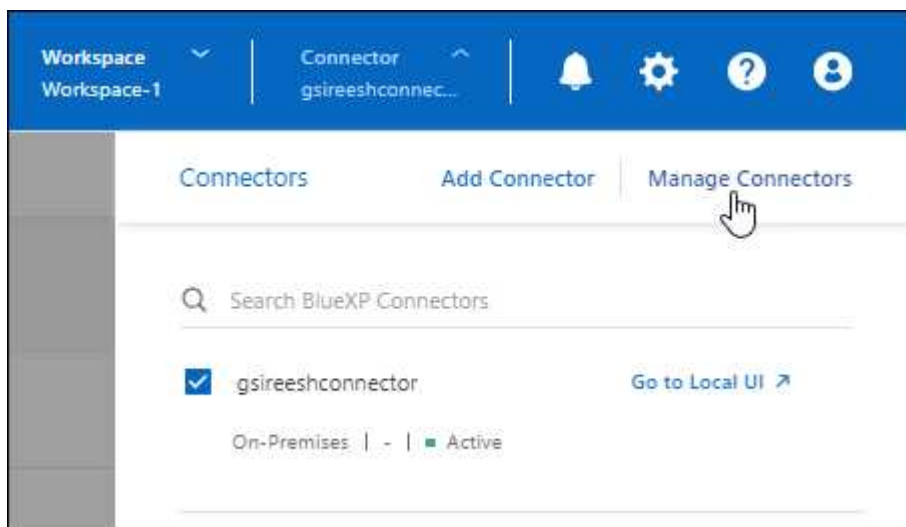
Fasi

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

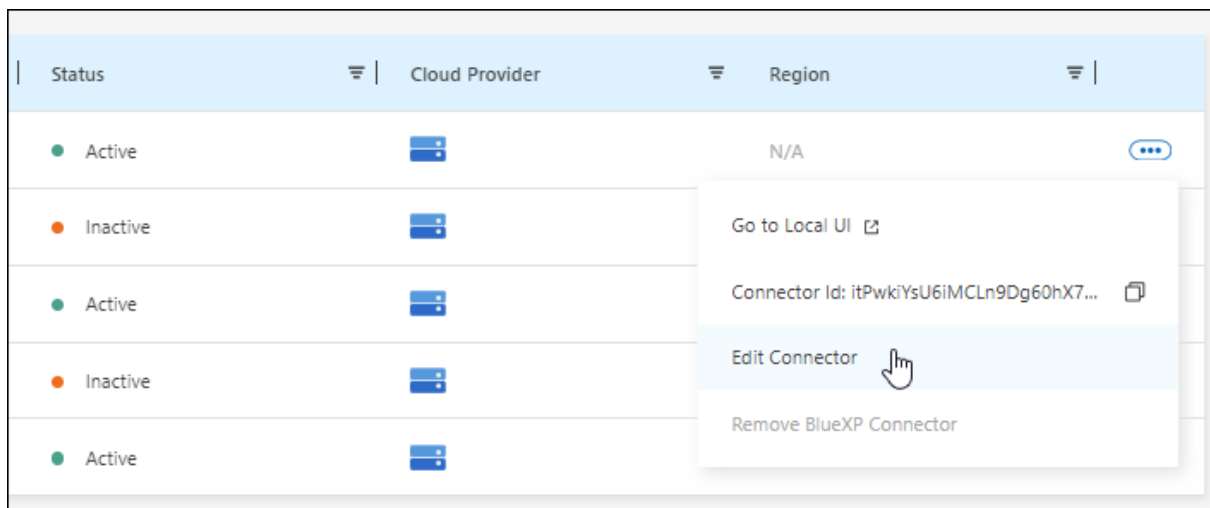
La navigazione dipende dall'utilizzo di BlueXP in modalità standard (accesso all'interfaccia BlueXP dal sito Web SaaS) o in modalità limitata o privata (accesso all'interfaccia BlueXP localmente dall'host del connettore).

Modalità standard

- Selezionare l'elenco a discesa **Connector** dall'interfaccia BlueXP.
- Selezionare **Gestisci connettori**.

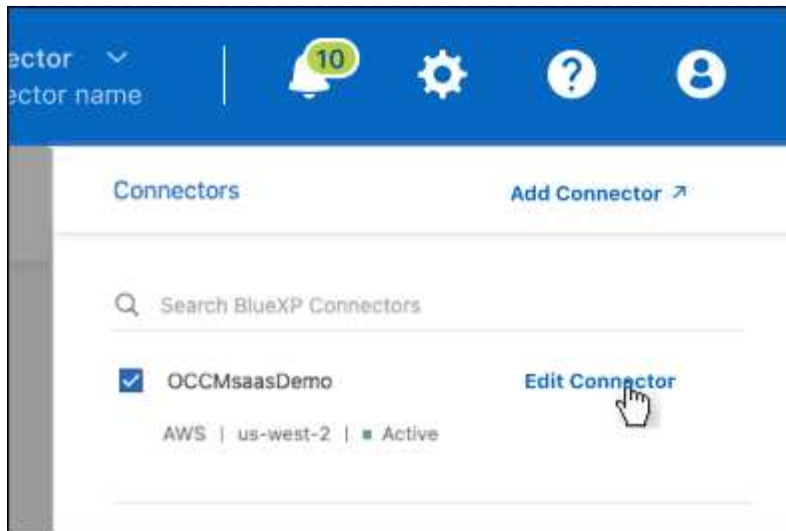


- Selezionare il menu azione per un connettore e selezionare **Modifica connettore**.



Modalità limitata o privata

- Selezionare l'elenco a discesa **Connector** dall'interfaccia BlueXP.
- Selezionare **Modifica connettore**.



2. Selezionare **Configurazione proxy HTTP**.

3. Configurare il proxy:

- Selezionare **Enable Proxy** (attiva proxy).
- Specificare il server utilizzando la sintassi `http://address:port` oppure `https://address:port`
- 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"](#)

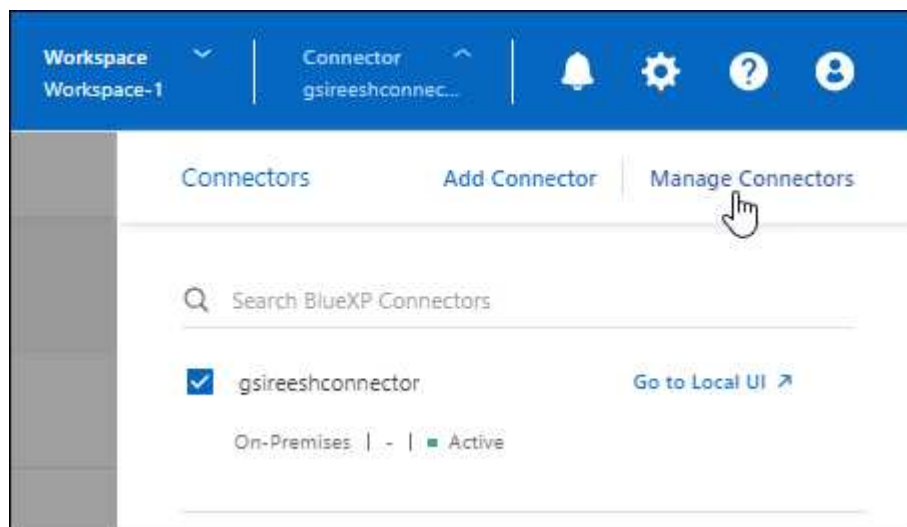
Fasi

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

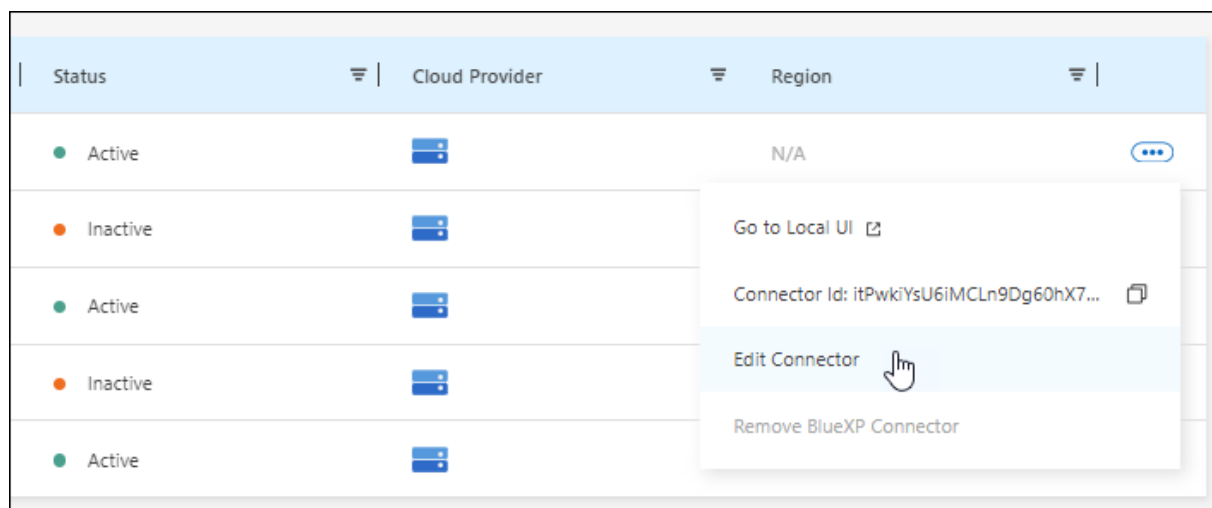
La navigazione dipende dall'utilizzo di BlueXP in modalità standard (accesso all'interfaccia BlueXP dal sito Web SaaS) o in modalità limitata o privata (accesso all'interfaccia BlueXP localmente dall'host del connettore).

Modalità standard

- Selezionare l'elenco a discesa **Connector** dall'interfaccia BlueXP.
- Selezionare **Gestisci connettori**.

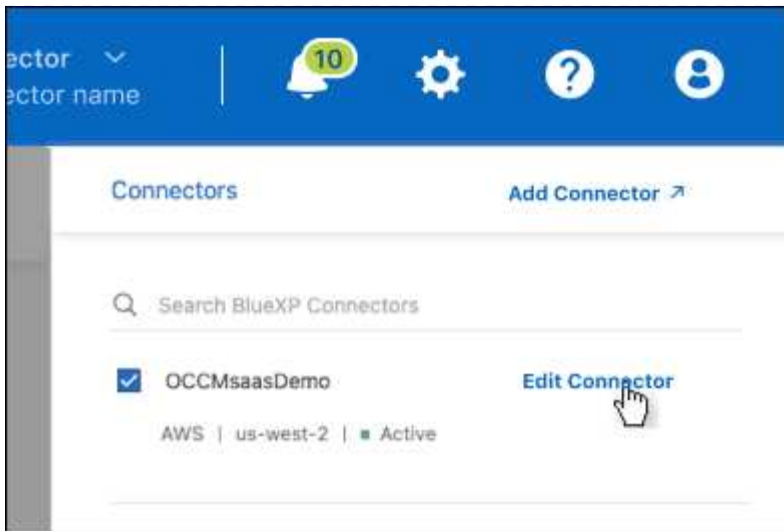


- Selezionare il menu azione per un connettore e selezionare **Modifica connettore**.



Modalità limitata o privata

- Selezionare l'elenco a discesa **Connector** dall'interfaccia BlueXP.
- 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

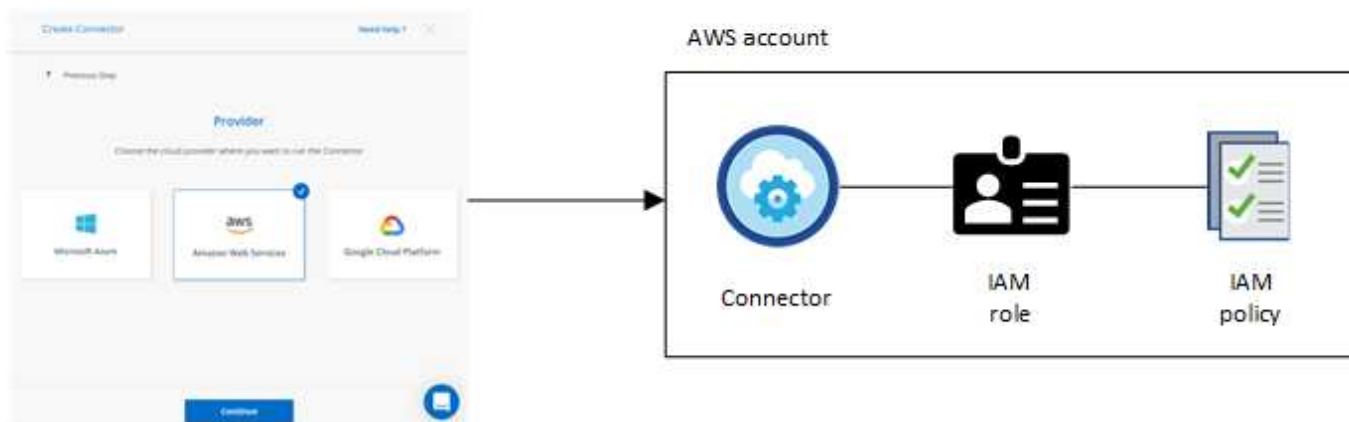
Scopri le credenziali e le autorizzazioni AWS

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:

Details & Credentials			
Instance Profile	Account ID	QA Subscription	Edit Credentials
Credentials		Marketplace Subscription	

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

Credenziali AWS aggiuntive

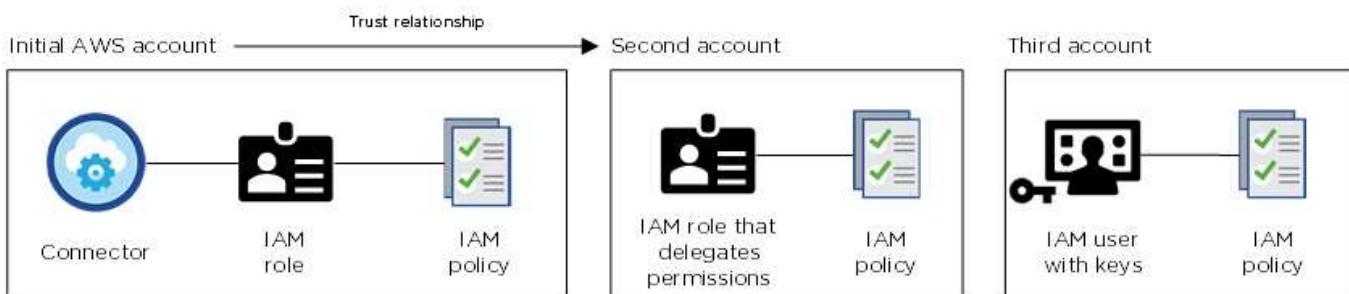
Esistono due modi per aggiungere ulteriori credenziali AWS:

- 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.

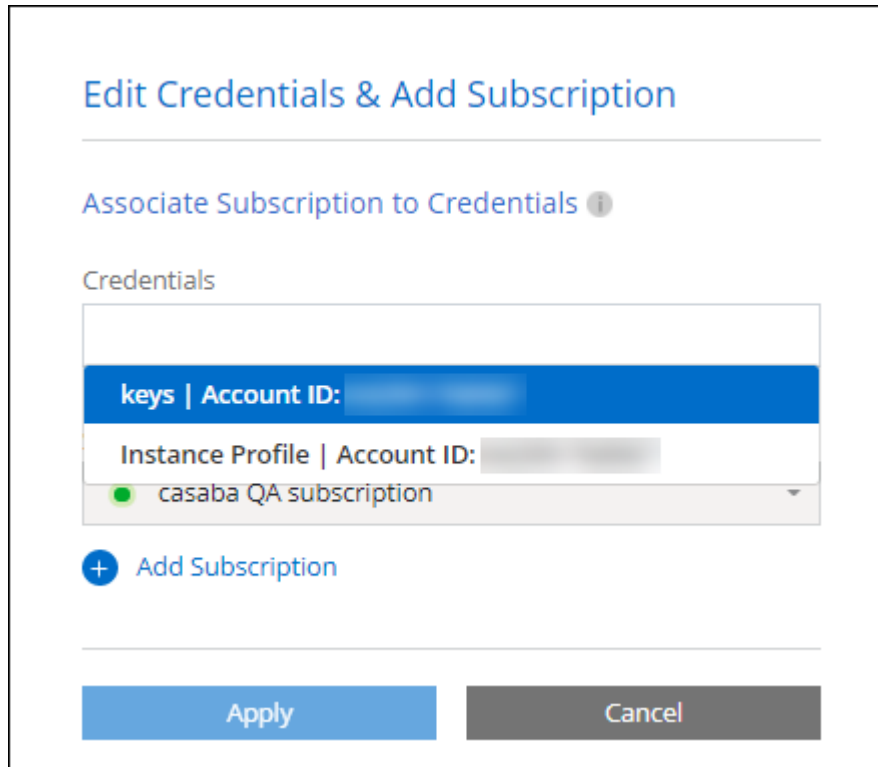
Aggiungere le credenziali AWS a un connettore esistente

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:



Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

keys | Account ID: [redacted]

Instance Profile | Account ID: [redacted]

casaba QA subscription

+ Add Subscription

Apply Cancel

["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:

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

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

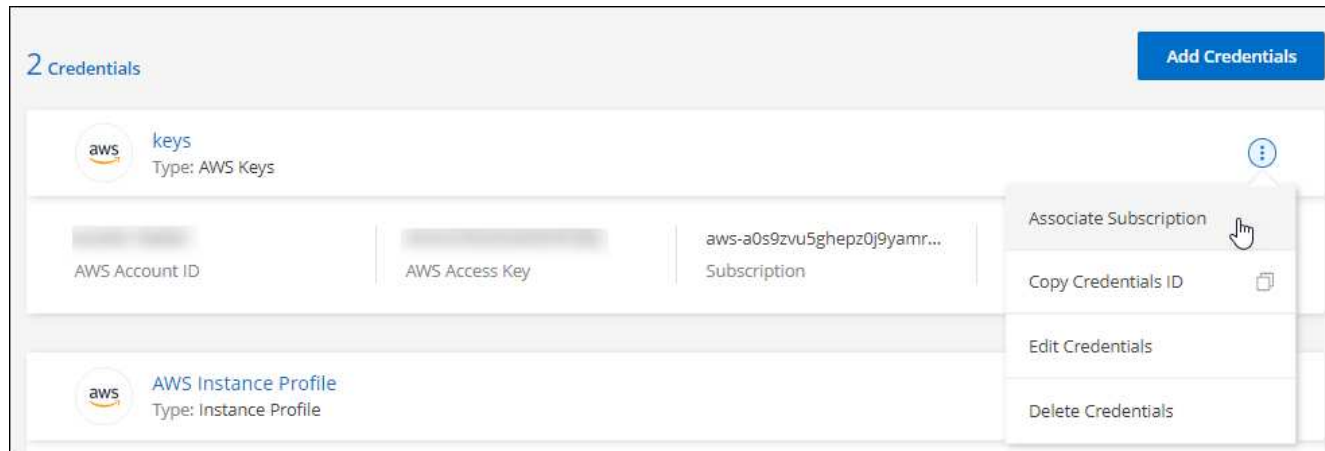
È necessario creare un connettore prima di poter modificare le impostazioni di BlueXP. ["Scopri come creare un connettore"](#).

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.

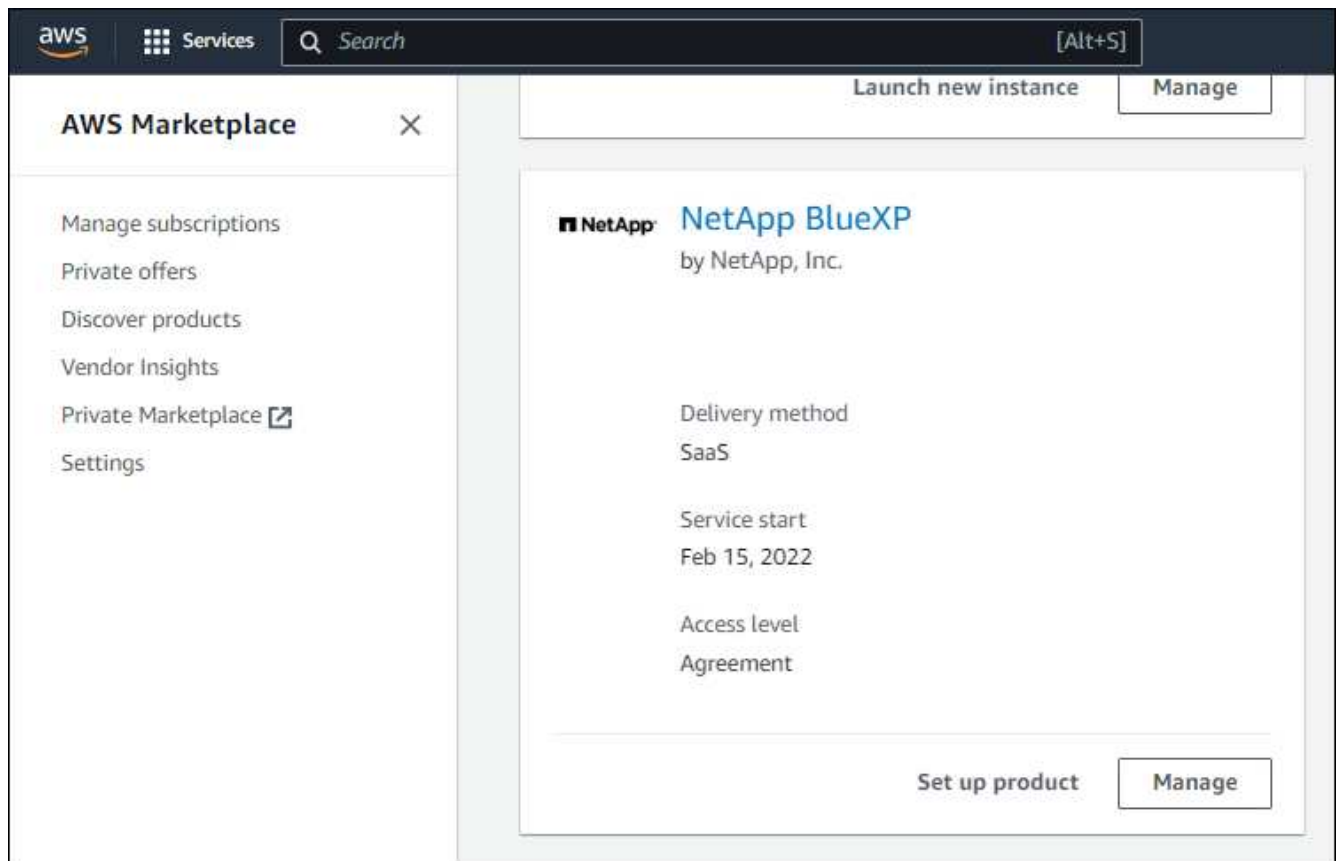
Segui i passaggi riportati di seguito se ti sei abbonato a BlueXP da AWS Marketplace, ma non hai fatto la procedura per associare l'abbonamento all'account.

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.

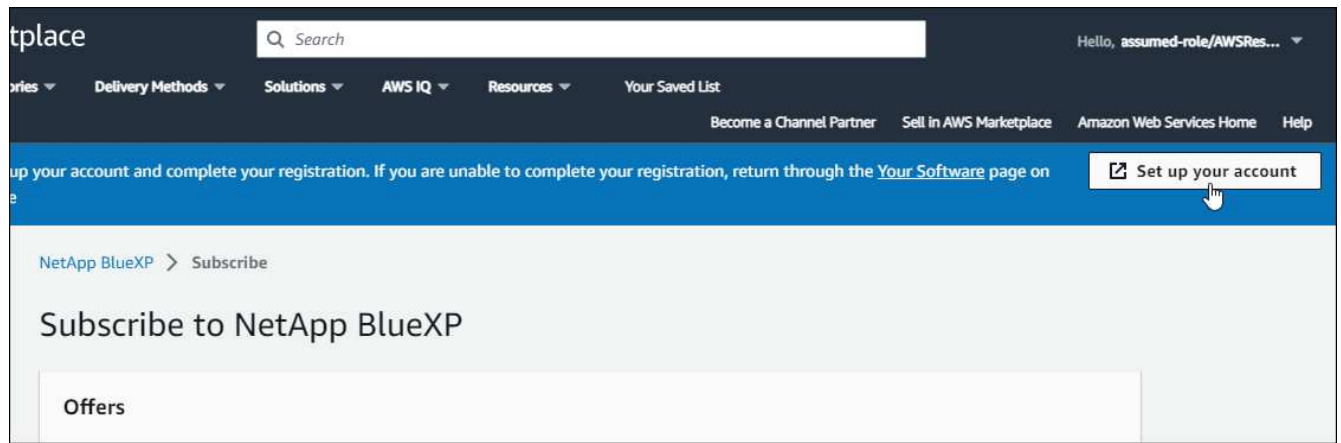
2. Accedi alla console AWS e accedi a **sottoscrizioni al marketplace AWS**.
3. Trova l'iscrizione a NetApp BlueXP.



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.

Subscription Assignment

✓

Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name

PayAsYouGo

Select the NetApp accounts that you'd like to associate this subscription with.

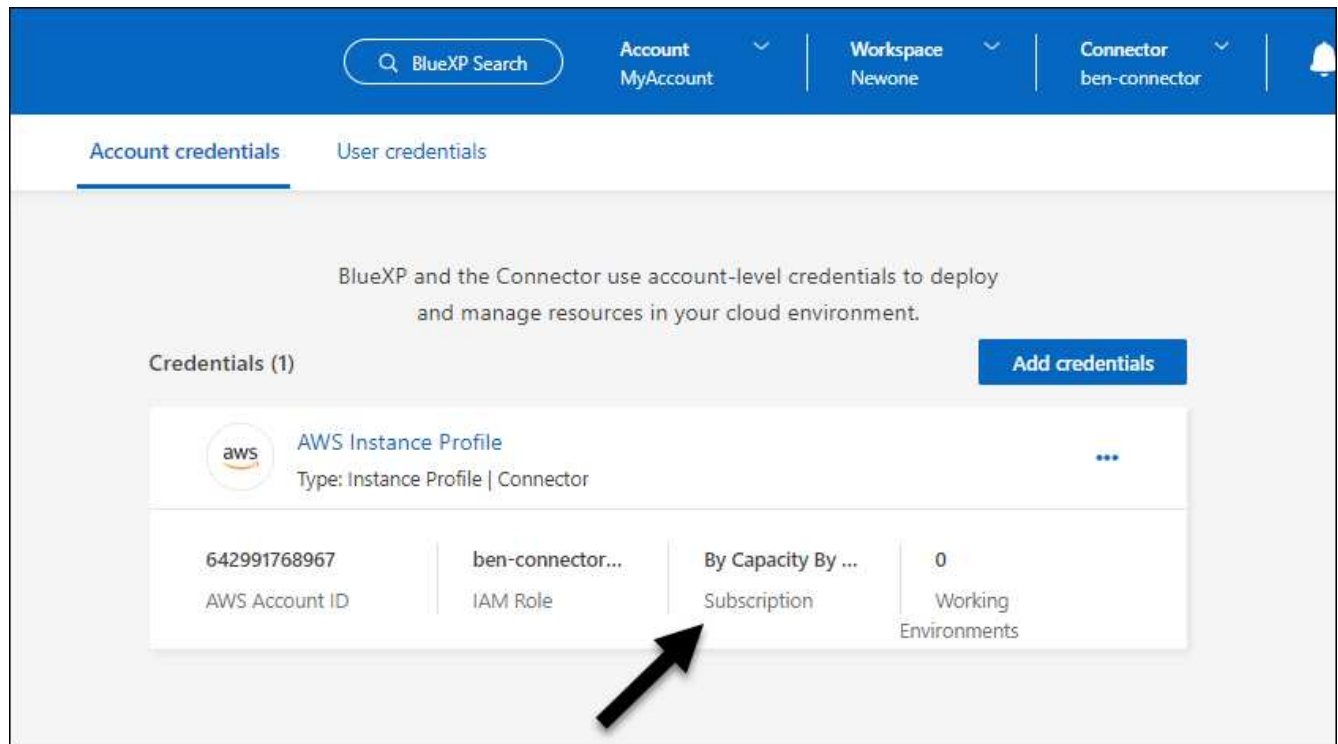
You can automatically replace the existing subscription for one account with this new subscription.

NetApp account	Replace existing subscription
<input checked="" type="checkbox"/> cloudTiering_undefined	<input type="checkbox"/>
<input checked="" type="checkbox"/> CS-HhewH	<input type="checkbox"/>
<input checked="" type="checkbox"/> benAccount	<input checked="" type="checkbox"/>

Save

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

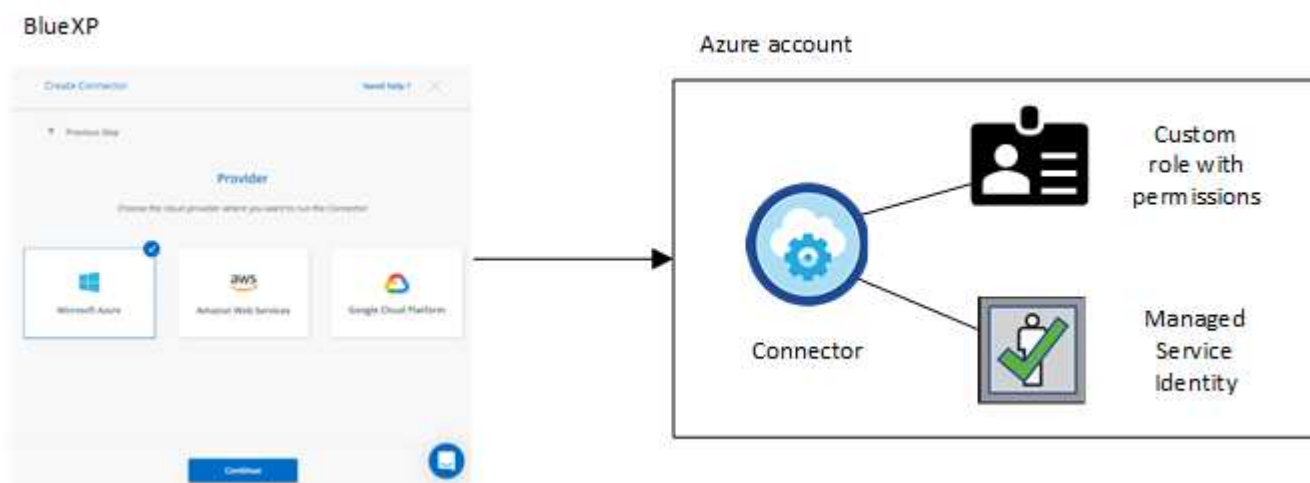
Scopri le credenziali e le autorizzazioni di Azure

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:

Details & Credentials			
Managed Service Ide...	OCCM QA1	ⓘ No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

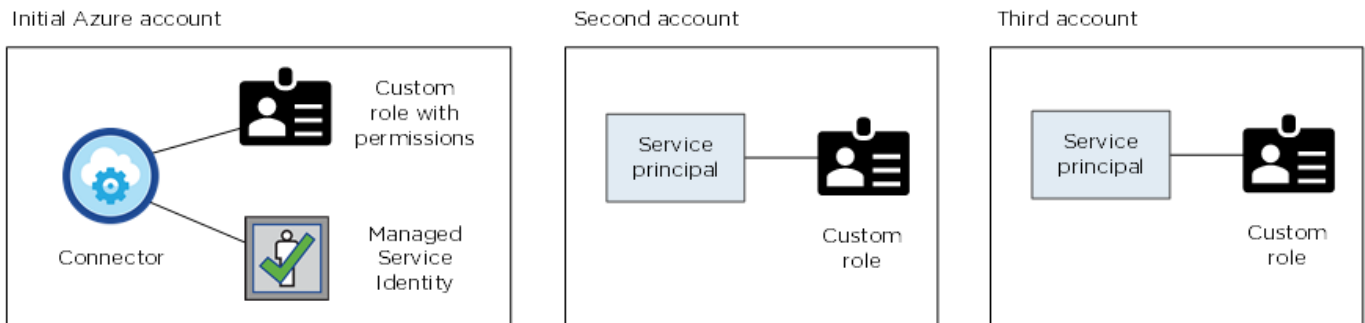
È possibile implementare tutti i sistemi Cloud Volumes ONTAP utilizzando le credenziali iniziali di Azure oppure aggiungere ulteriori credenziali.

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"](#).

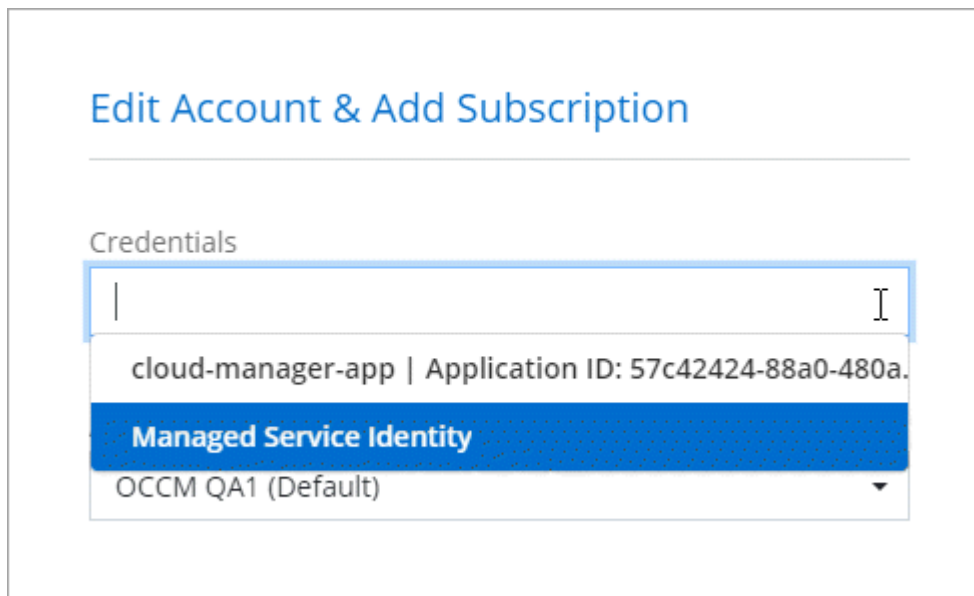
Credenziali Azure aggiuntive

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.

Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

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

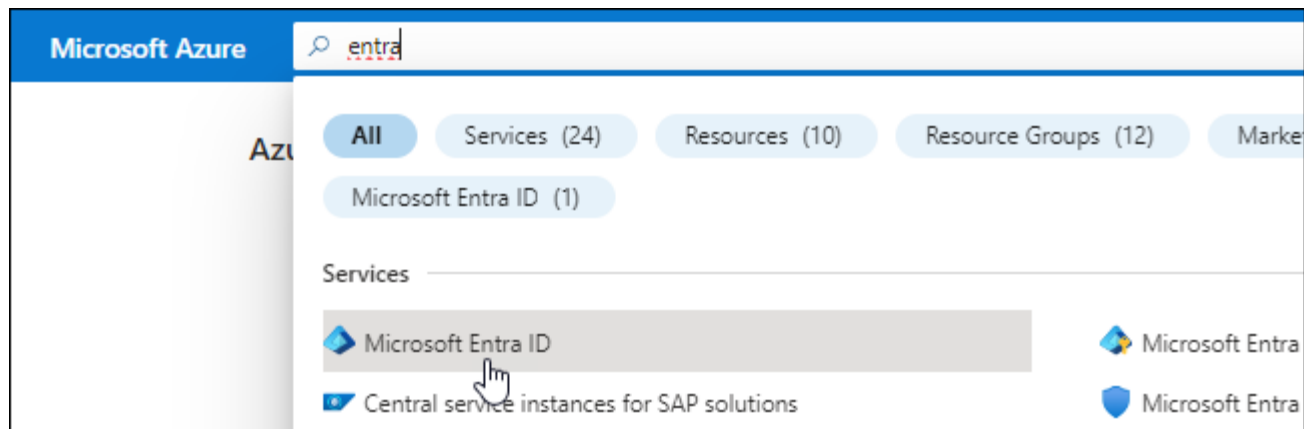
Creare un'applicazione e un'entità di servizio Microsoft Entra che BlueXP possa utilizzare per il role-based access control.

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.

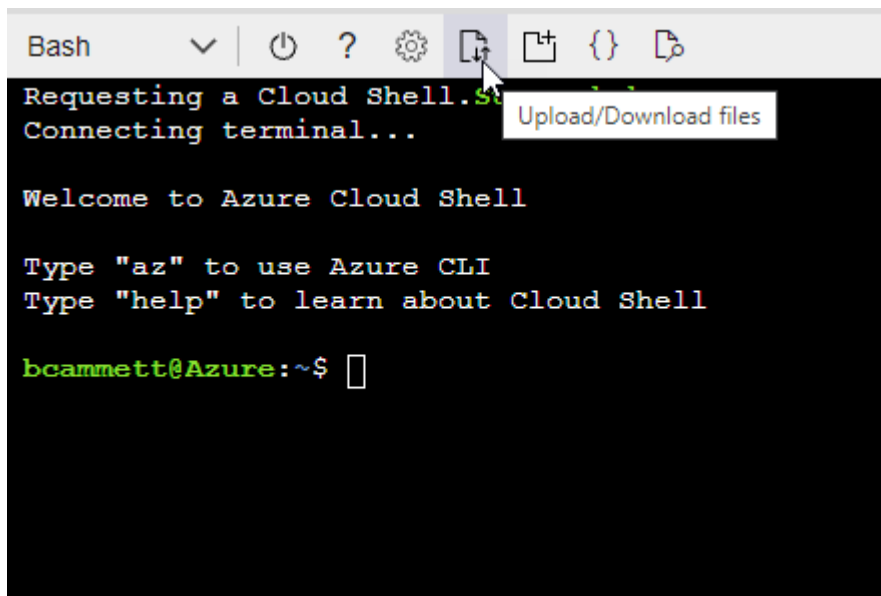
Esempio

```
"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**.

Add role assignment ...

Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

- Cercare il nome dell'applicazione.

Ecco un esempio:

Select members ✕

Select ⓘ

test-service-principal

test-service-principal

- 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**.

Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Commonly used Microsoft APIs



Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 <p>Azure Batch Schedule large-scale parallel and HPC applications in the cloud</p>	 <p>Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets</p>	 <p>Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p>
 <p>Azure Data Lake Access to storage and compute for big data analytic scenarios</p>	 <p>Azure DevOps Integrate with Azure DevOps and Azure DevOps server</p>	 <p>Azure Import/Export Programmatic control of import/export jobs</p>
 <p>Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p>	 <p>Azure Rights Management Services Allow validated users to read and write protected content</p>	 <p>Azure Service Management Programmatic access to much of the functionality available through the Azure portal</p>
 <p>Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p>	 <p>Customer Insights Create profile and interaction models for your products</p>	 <p>Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination</p>

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

Request API permissions

< All APIs



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret			
DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA	

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**.

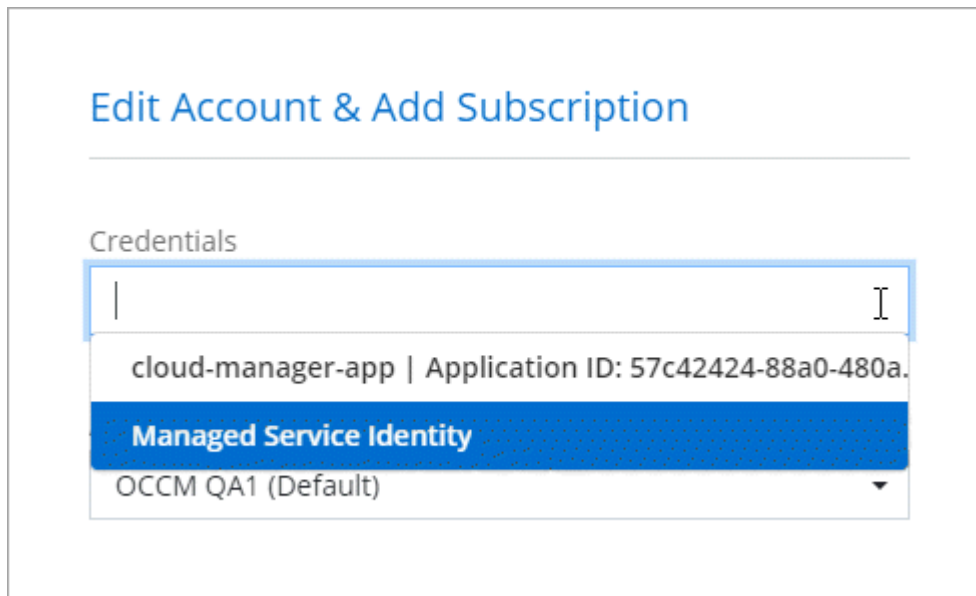


2. Selezionare **Aggiungi credenziali** e seguire la procedura guidata.
 - a. **Credentials Location**: Selezionare **Microsoft Azure > Connector**.

- 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"](#)



Edit Account & Add Subscription

Credentials

|

cloud-manager-app | Application ID: 57c42424-88a0-480a...

Managed Service Identity

OCCM QA1 (Default)

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.

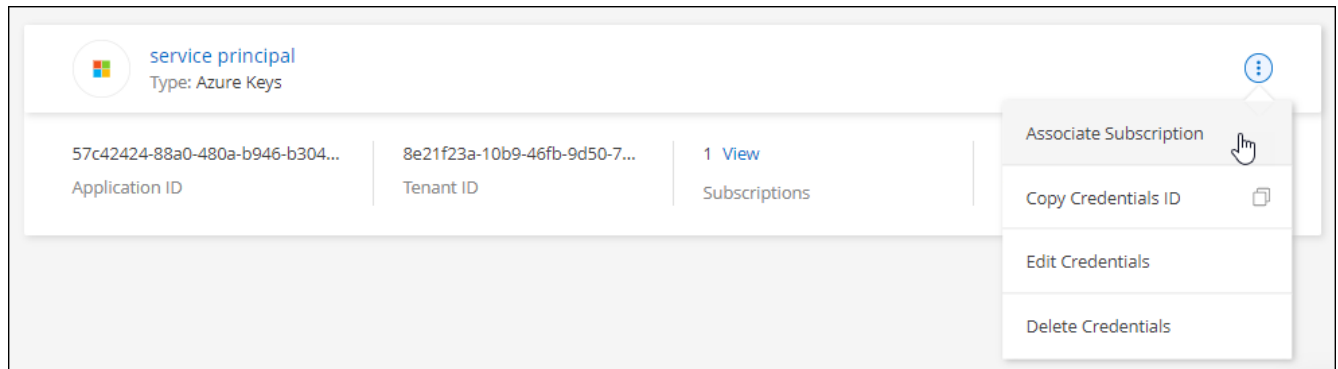
Prima di iniziare

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:

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

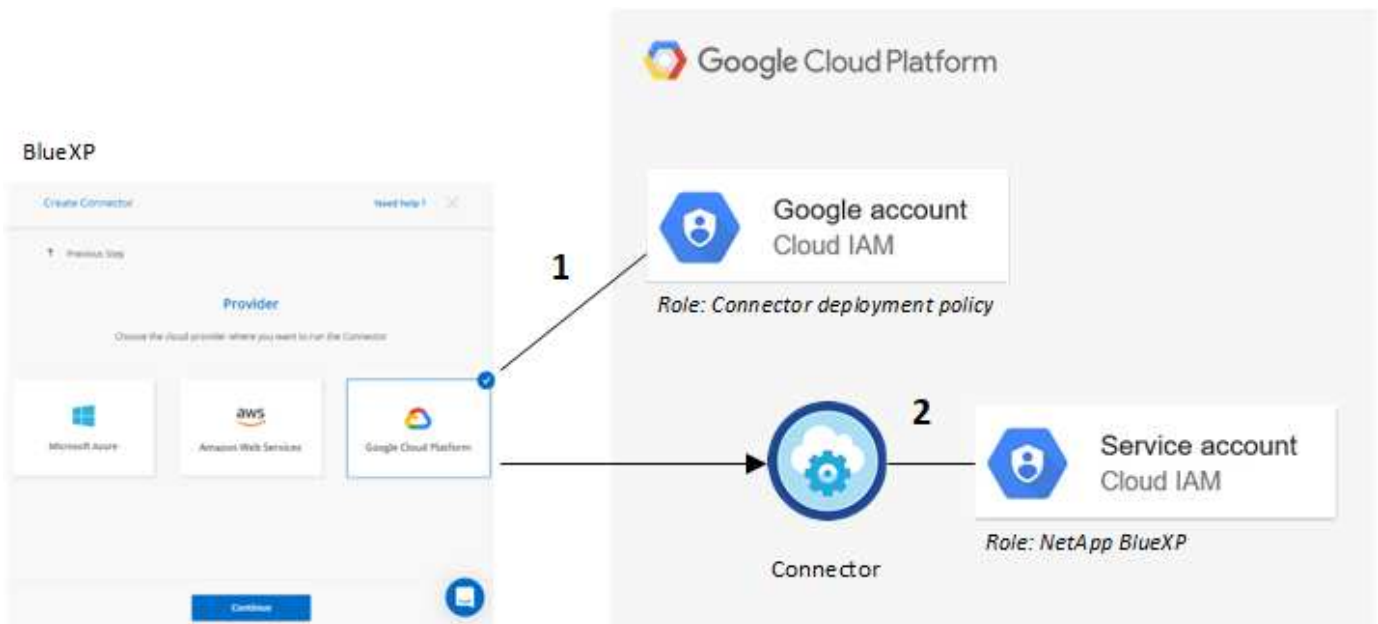
Prima di poter utilizzare BlueXP per gestire le risorse nel progetto Google Cloud, è necessario implementare un connettore. Il connettore non può essere in esecuzione in sede o in un altro cloud provider.

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.

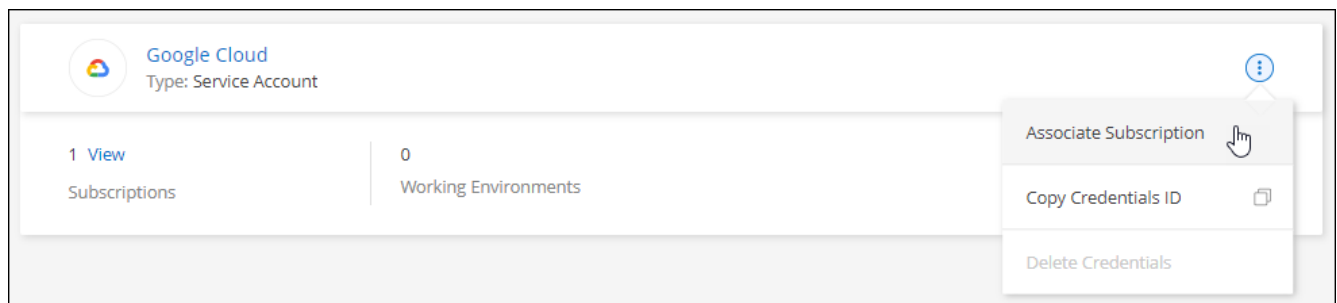
Associare un abbonamento Marketplace alle credenziali Google Cloud

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.

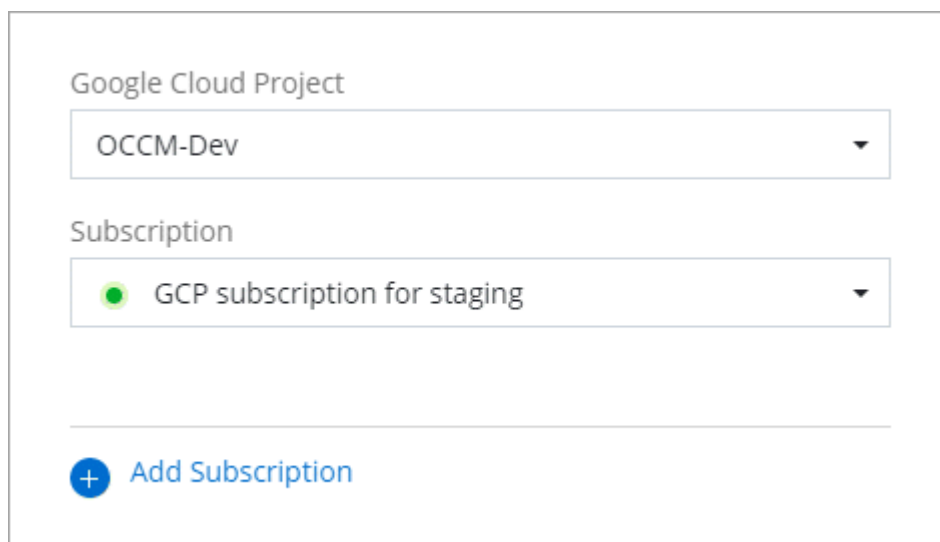
Sostituendo l'attuale sottoscrizione al marketplace con una nuova sottoscrizione, l'abbonamento al marketplace viene modificato per qualsiasi ambiente di lavoro Cloud Volumes ONTAP esistente e per tutti i nuovi ambienti di lavoro.

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**.

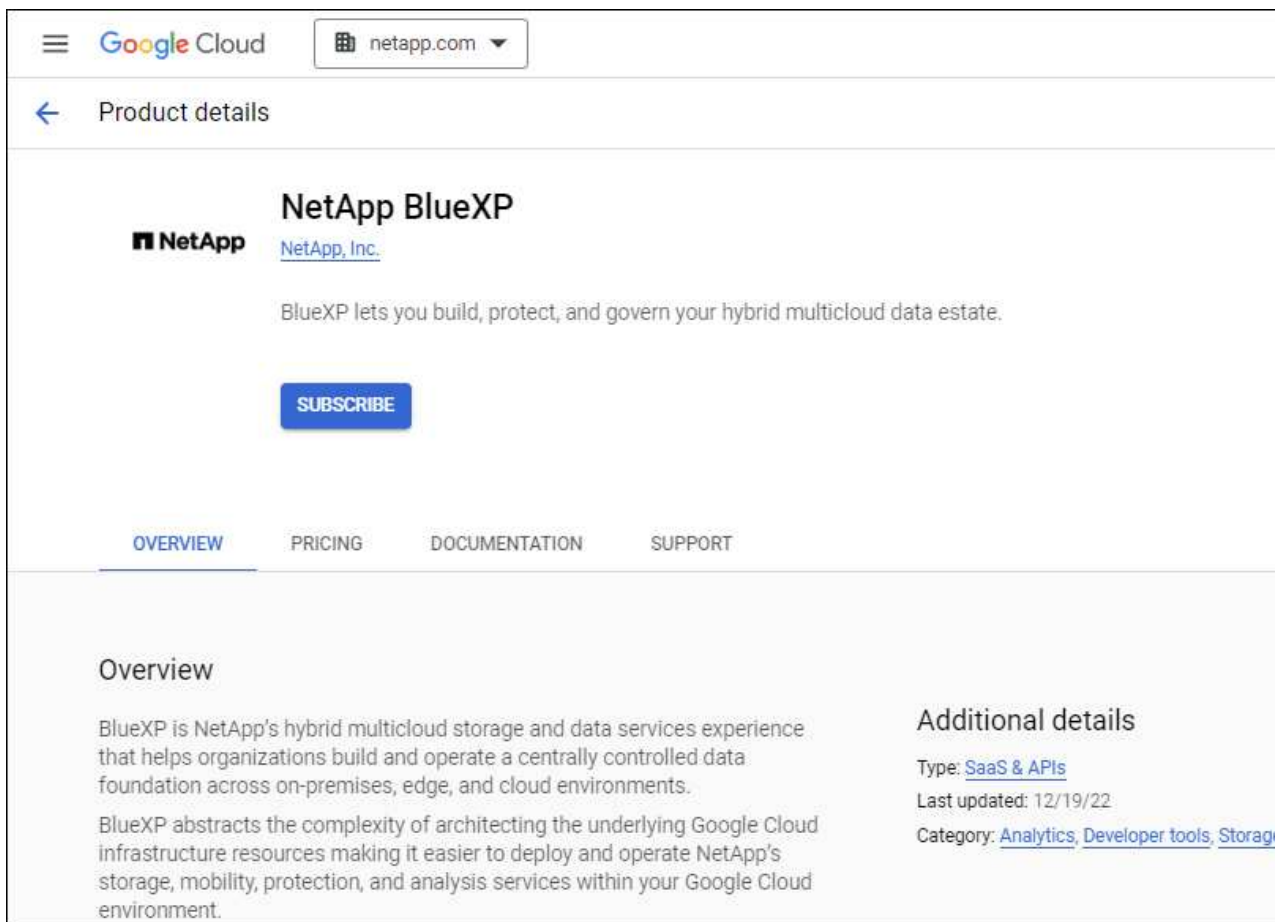


4. Se non disponi già di un abbonamento, seleziona **Aggiungi abbonamento > continua** e segui la procedura in Google Cloud Marketplace.



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.

Google Cloud Project

OCCM-Dev

Subscription

 GCP subscription for staging



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**.

Pricing






The product was purchased on 12/9/20.

[MANAGE ORDERS](#)

- 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.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	2eebbc... 	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	

- 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.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	d56c66... 	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	

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"](#)

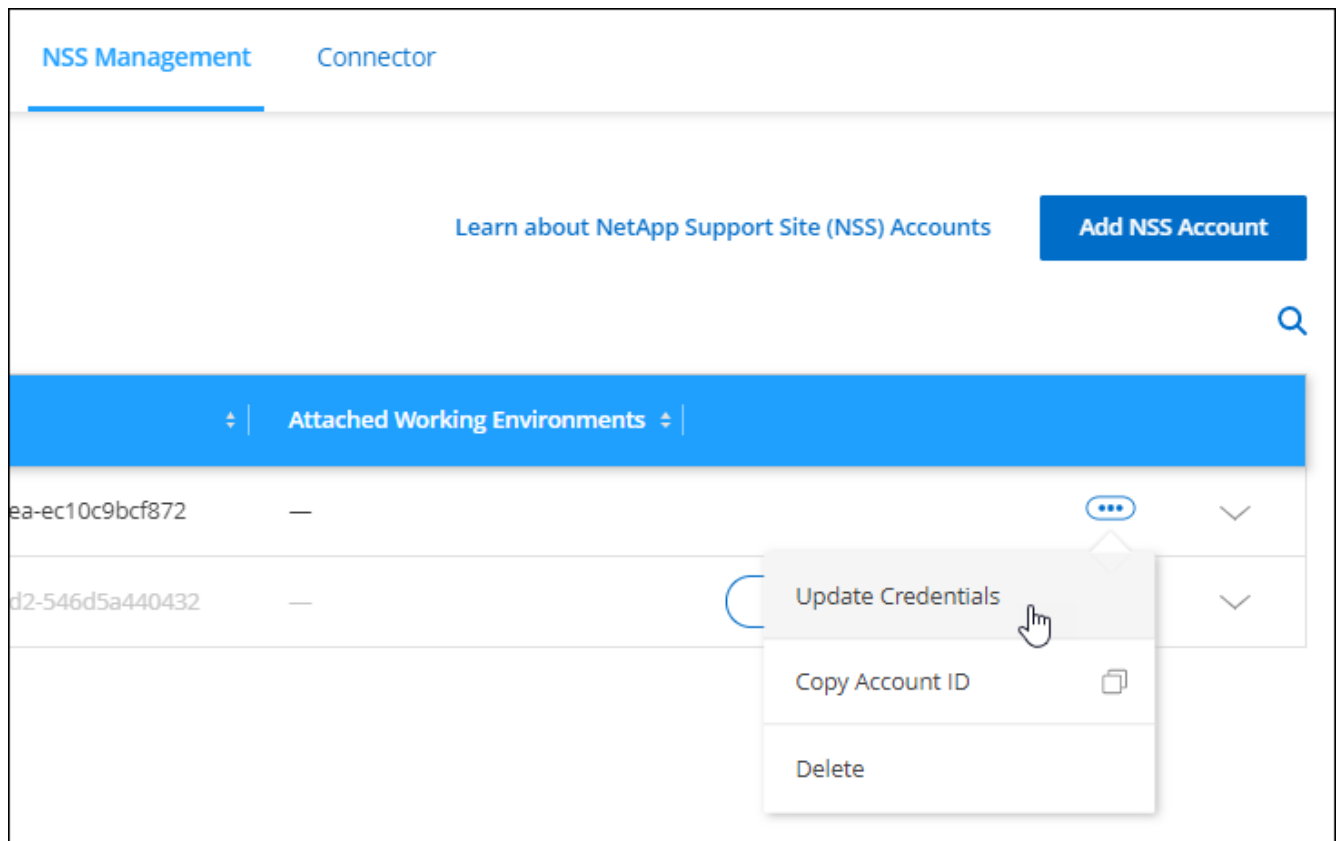
Aggiornare le credenziali NSS

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.

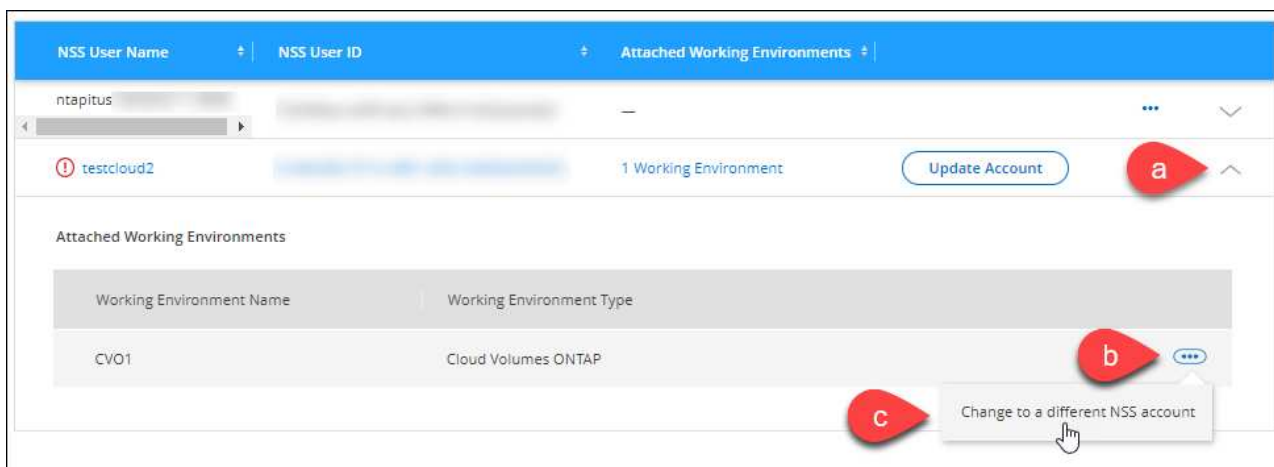
Collegare un ambiente di lavoro a un altro account NSS

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

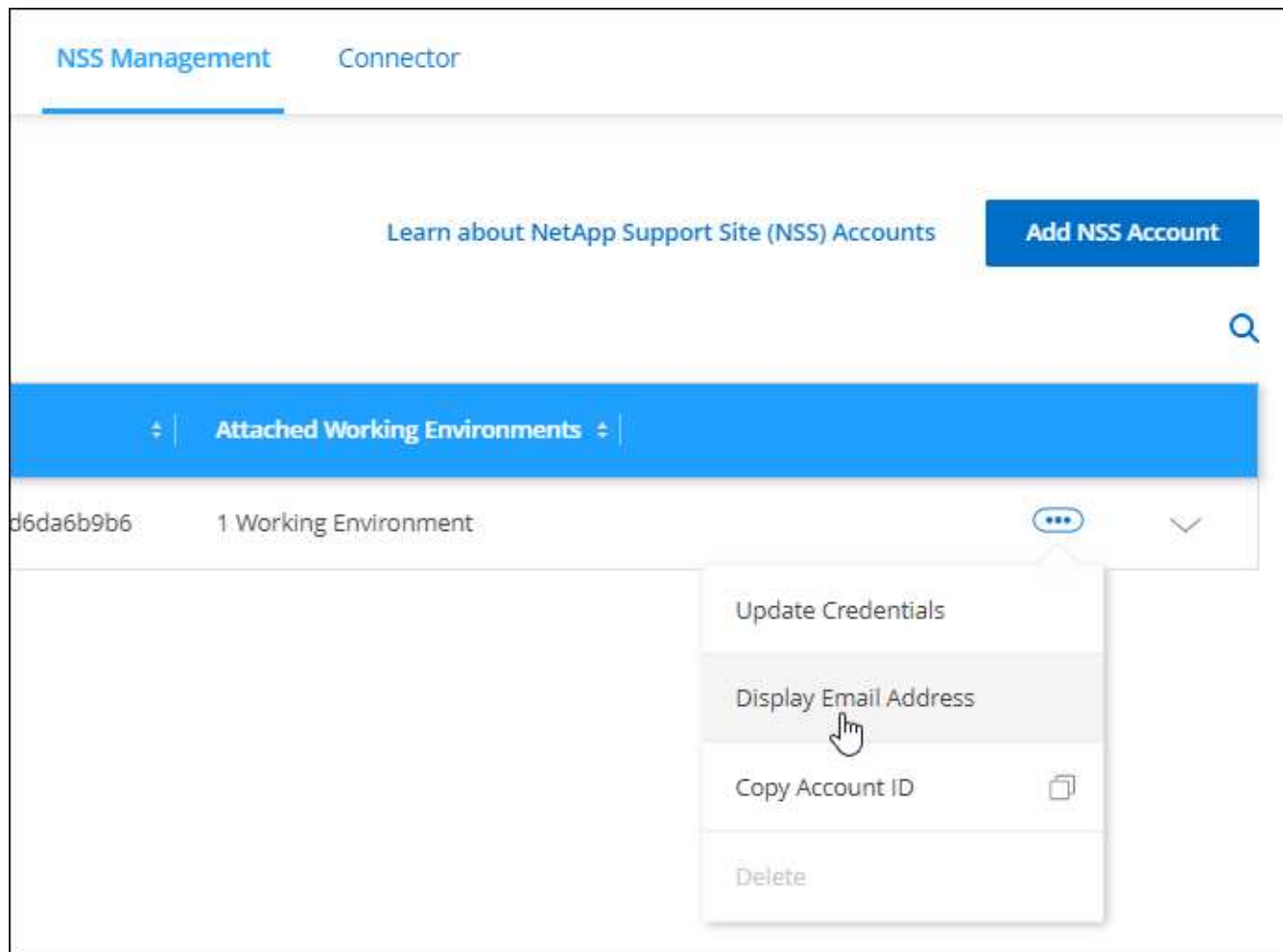
Ora che gli account del sito di supporto NetApp utilizzano l'Entra ID Microsoft per i servizi di autenticazione, il nome utente NSS visualizzato in BlueXP è in genere un identificatore generato da Microsoft Entra. Di conseguenza, potresti non conoscere immediatamente l'indirizzo e-mail associato a tale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

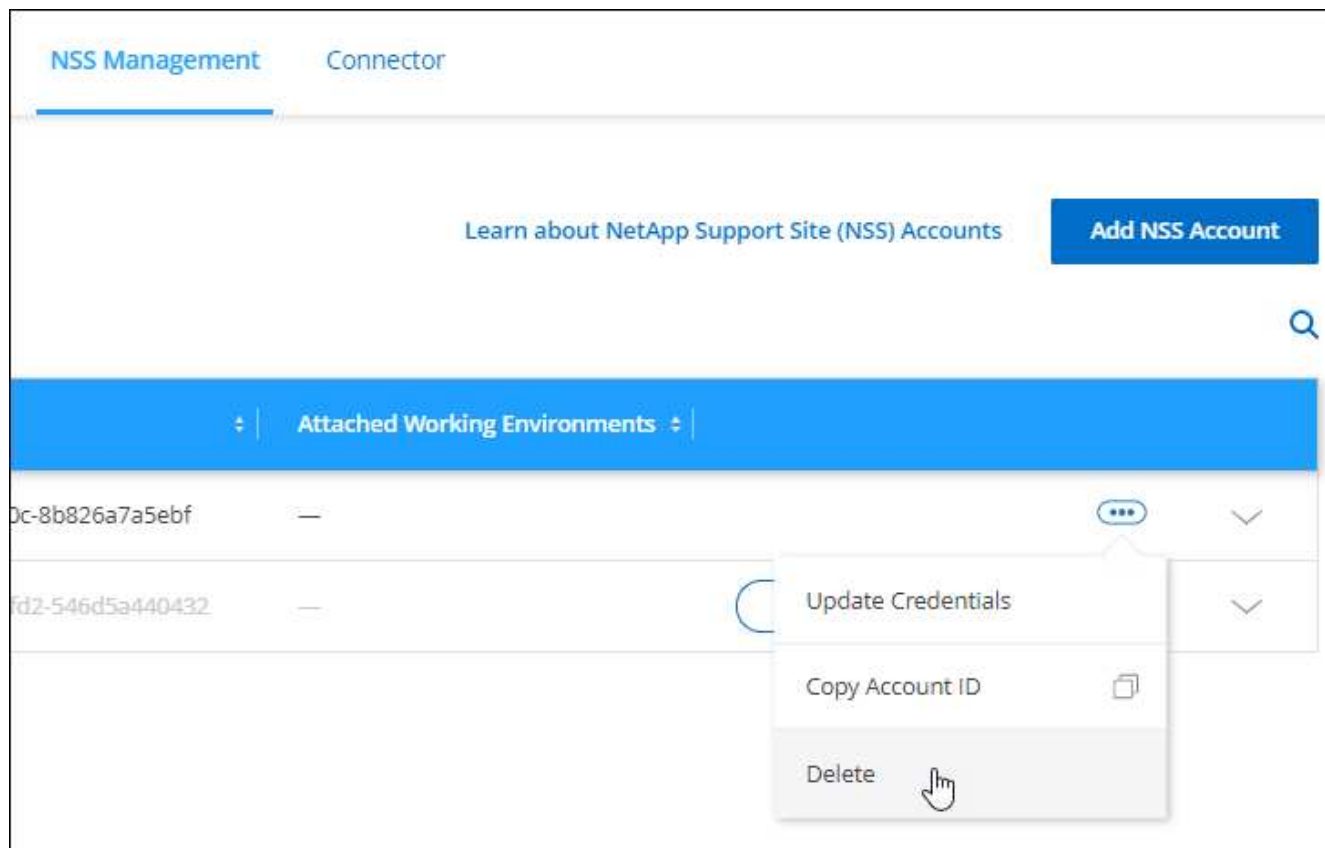
Rimuovere un account NSS

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.

[Account credentials](#)[User credentials](#)

BlueXP uses these credentials to authenticate you with your digital advisor account, for support case management, and for on-premises ONTAP clusters accessed without a Connector.

Credentials (2)

Add NSS credentials




tami@netapp.com

Type: NSS

1234567890123456789012345678901234567890

User ID


 OK

Status

...

Update credentials

Delete credentials



tami

Type: ONTAP

10.20.3.0

Cluster IP

id-324553636

Working environment ID

Risultato

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

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.