Verwalten von BlueXP

BlueXP setup and administration

NetApp
August 21, 2025

Inhalt

Verwalten von BlueXP

Identitäts- und Zugriffsmanagement

Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP

Mit dem Identitäts- und Zugriffsmanagement (BlueXP Identity and Access Management, IAM) können Sie den Zugriff auf Ihre NetApp-Ressourcen organisieren und kontrollieren. Sie können Ihre Ressourcen nach der Hierarchie Ihrer Organisation organisieren. Sie können beispielsweise Ressourcen nach geographischem Standort, Standort oder Geschäftseinheit organisieren. Anschließend können Sie den Mitgliedern in bestimmten Teilen der Hierarchie IAM-Rollen zuweisen, wodurch der Zugriff auf Ressourcen in anderen Teilen der Hierarchie verhindert wird.

- "Weitere Informationen zu BlueXP Implementierungsmodi"

Wie BlueXP IAM funktioniert

Mit BlueXP IAM können Sie Ressourcenzugriff gewähren, indem Sie Benutzern Zugriffsrollen für bestimmte Bereiche der Hierarchie zuweisen. Beispielsweise kann einem Mitglied die Rolle „Ordner- oder Projektadministrator“ für ein Projekt mit fünf Ressourcen zugewiesen werden.

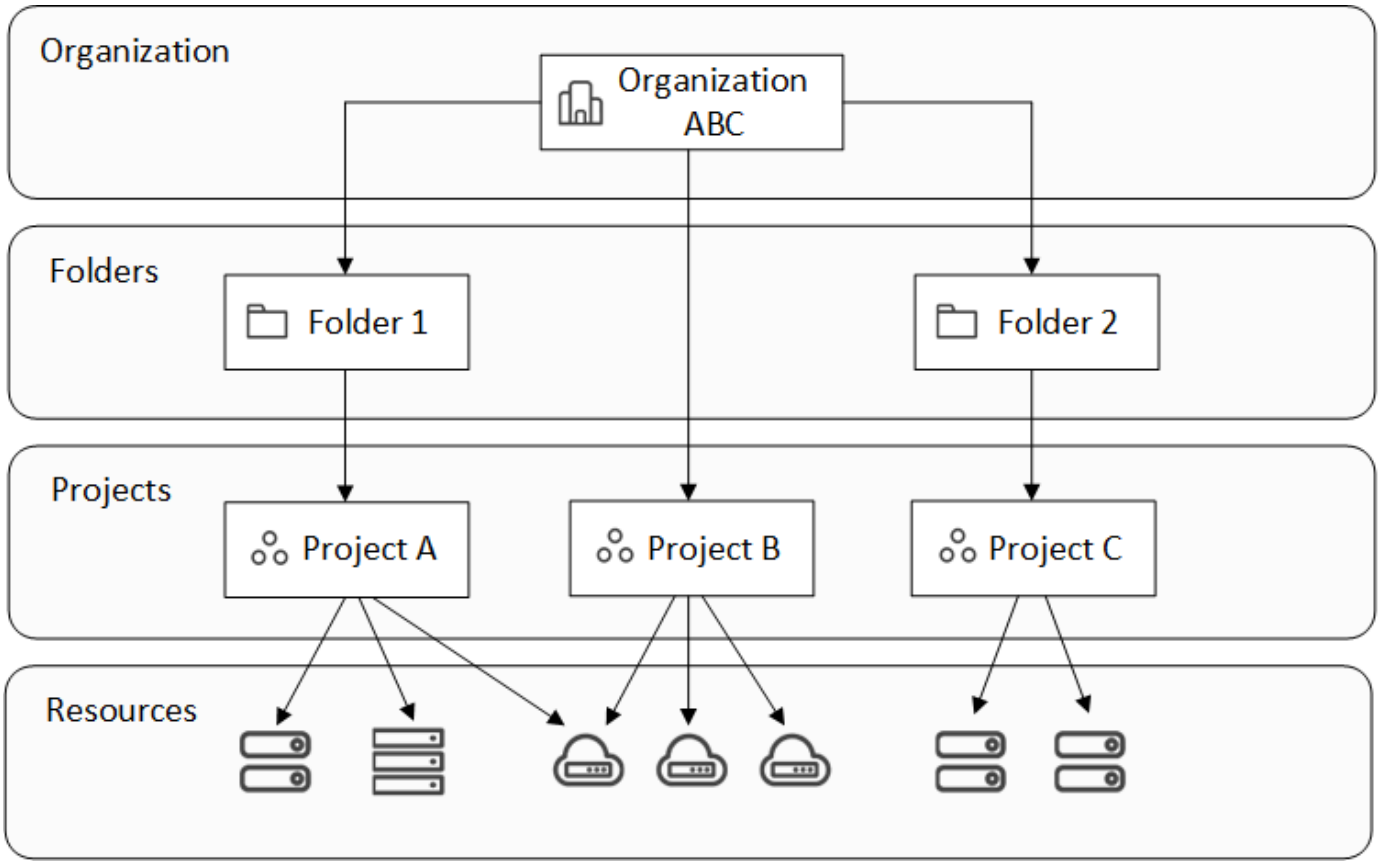
Bei der Verwendung von BlueXP IAM verwalten Sie die folgenden Komponenten:

- Der Organisation
- Ordner
- Projekte
- Ressourcen
- Mitglieder
- Rollen und Berechtigungen
- Anschlüsse

BlueXP -Ressourcen sind hierarchisch organisiert:

- Die Organisation ist die oberste der Hierarchie.
- Ordner sind untergeordnete Elemente der Organisation oder eines anderen Ordners.
- Projekte sind untergeordnete Elemente der Organisation oder eines Ordners.
- Ressourcen sind einem oder mehreren Ordnern oder Projekten zugeordnet.

Das folgende Bild veranschaulicht diese Hierarchie auf einer grundlegenden Ebene.



Organisation

Eine *Organisation* ist die oberste Ebene des IAM-Systems von BlueXP und repräsentiert in der Regel Ihr Unternehmen. Ihr Unternehmen besteht aus Ordnern, Projekten, Mitgliedern, Rollen und Ressourcen. Konnektoren sind bestimmten Projekten in der Organisation zugeordnet.

Ordner

Ein *Ordner* ermöglicht Ihnen, verwandte Projekte zu gruppieren und von anderen Projekten in Ihrer Organisation zu trennen. Ein Ordner kann beispielsweise einen geografischen Standort (EU oder US-Osten), einen Standort (London oder Toronto) oder eine Geschäftseinheit (Engineering oder Marketing) repräsentieren.

Ordner können Projekte, andere Ordner oder beides enthalten. Das Erstellen von Ordnern ist optional.

Projekte

Ein *Projekt* stellt einen Arbeitsbereich in BlueXP dar, auf den Organisationsmitglieder über den BlueXP -Bildschirm zugreifen können, um Ressourcen zu verwalten. Ein Projekt kann beispielsweise ein Cloud Volumes ONTAP System, ein On-Premises-ONTAP-Cluster oder ein FSX für ONTAP Filesystem umfassen.

Eine Organisation kann ein oder mehrere Projekte haben. Ein Projekt kann sich direkt unter der Organisation oder in einem Ordner befinden.

Ressourcen

Eine *Ressource* ist eine Arbeitsumgebung, die Sie in BlueXP erstellt oder entdeckt haben.

Wenn Sie eine Ressource erstellen oder ermitteln, ist die Ressource mit dem aktuell ausgewählten Projekt verknüpft. Dies ist möglicherweise das einzige Projekt, dem Sie diese Ressource zuordnen möchten. Sie

können die Ressource jedoch anderen Projekten in Ihrer Organisation zuordnen.

Sie können beispielsweise ein Cloud Volumes ONTAP-System einem weiteren Projekt oder allen Projekten in Ihrer Organisation zuordnen. Wie Sie eine Ressource zuordnen, hängt von den Anforderungen Ihres Unternehmens ab.

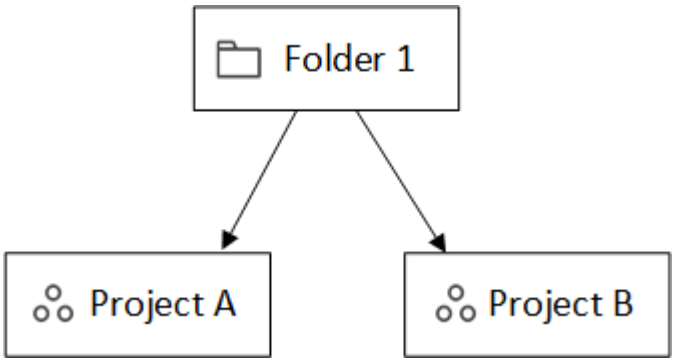
Sie können einen Connector auch einem anderen Ordner oder Projekt in Ihrer Organisation zuordnen. Erfahren Sie mehr über die Verwendung von Steckverbindern mit BlueXP IAM.

Wann eine Ressource einem Ordner zugeordnet werden soll

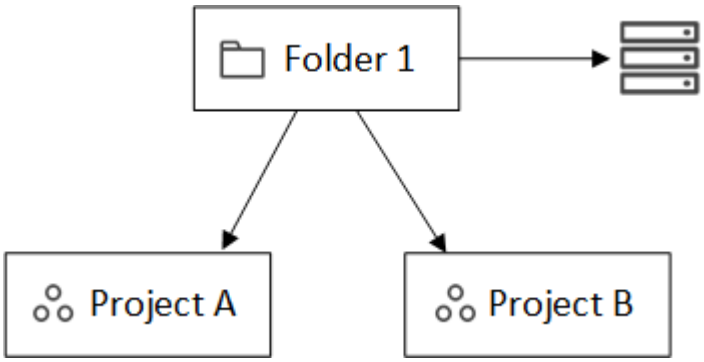
Sie haben auch die Möglichkeit, eine Ressource einem Ordner zuzuordnen. Dies ist jedoch optional und erfüllt die Anforderungen eines bestimmten Anwendungsfalls.

Ein *Organisationsadministrator* kann eine Ressource mit einem Ordner verknüpfen, um einem *Ordner- oder Projektadministrator* zu ermöglichen, diese Ressource mit den entsprechenden Projekten im Ordner zu verknüpfen.

Angenommen, Sie haben einen Ordner, der zwei Projekte enthält:

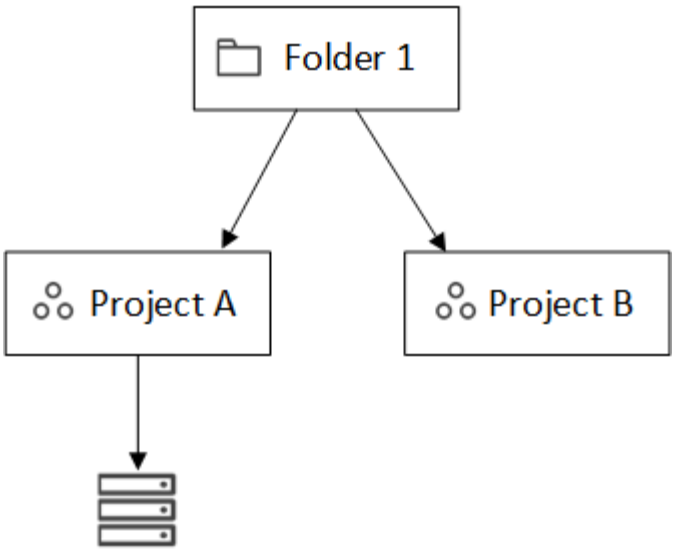


Der *Organisation admin* kann dem Ordner eine Ressource zuordnen:



Durch die Verknüpfung einer Ressource mit einem Ordner wird diese nicht für alle Projekte zugänglich; nur der Ordner- oder Projektadministrator kann sie sehen. Der Ordner- oder Projektadministrator entscheidet, welche Projekte darauf zugreifen können, und ordnet die Ressource den entsprechenden Projekten zu.

In diesem Beispiel verknüpft der Administrator die Ressource mit Projekt A:



Mitglieder, die über Berechtigungen für Projekt A verfügen, können jetzt auf die Ressource zugreifen.

Mitglieder

Mitglieder Ihrer Organisation sind Benutzerkonten oder Servicekonten. Ein Servicekonto wird normalerweise von einer Anwendung verwendet, um bestimmte Aufgaben ohne menschliches Eingreifen zu erledigen.

Jede Organisation umfasst mindestens einen Benutzer mit der Rolle „Organisationsadministrator“ (BlueXP weist diese Rolle automatisch dem Benutzer zu, der die Organisation erstellt). Sie können der Organisation weitere Mitglieder hinzufügen und verschiedene Berechtigungen auf verschiedenen Ebenen der Ressourcenhierarchie zuweisen.

Rollen und Berechtigungen

In BlueXP IAM erteilen Sie den Mitgliedern der Organisation keine Berechtigungen direkt. Stattdessen gewähren Sie jedem Mitglied eine Rolle. Eine Rolle enthält einen Satz von Berechtigungen, mit denen ein Mitglied bestimmte Aktionen auf einer bestimmten Ebene der Ressourcenhierarchie ausführen kann.

Durch die Erteilung von Berechtigungen auf einer bestimmten Hierarchieebene wird der Zugriff auf die Ressourcen eingeschränkt, die ein Mitglied benötigt, und auf die Dienste, die es mit diesen Ressourcen nutzen kann.

Hier können Sie Rollen in der Hierarchie zuweisen

Wenn Sie ein Mitglied einer Rolle zuordnen, müssen Sie die gesamte Organisation, einen bestimmten Ordner oder ein bestimmtes Projekt auswählen. Die ausgewählte Rolle gibt einem Mitglied Berechtigungen für die Ressourcen im ausgewählten Teil der Hierarchie.

Rollenvererbung

Wenn Sie eine Rolle zuweisen, wird die Rolle in der Organisationshierarchie übernommen:

Organisation
: Wenn Sie einem Mitglied eine Zugriffsrolle auf Organisationsebene erteilen, erhält es Berechtigungen für alle Ordner, Projekte und Ressourcen.

Ordner

Wenn Sie eine Zugriffsrolle auf Ordnerebene erben, erben alle Ordner, Projekte und Ressourcen im Ordner diese Rolle.

Wenn Sie beispielsweise eine Rolle auf Ordnerebene zuweisen und dieser Ordner drei Projekte hat, hat das Mitglied Berechtigungen für diese drei Projekte und alle zugehörigen Ressourcen.

Projekte

Wenn Sie eine Zugriffsrolle auf Projektebene erteilen, erben alle mit diesem Projekt verknüpften Ressourcen diese Rolle.

Mehreren Rollen

Sie können jedem Organisationsmitglied eine Rolle auf verschiedenen Ebenen der Organisationshierarchie zuweisen. Es kann die gleiche Rolle oder eine andere Rolle sein. Sie können beispielsweise eine Mitgliedrolle A für Projekt 1 und Projekt 2 zuweisen. Oder Sie können eine Mitgliedrolle A für Projekt 1 und Rolle B für Projekt 2 zuweisen.

Zugriffsrollen

BlueXP unterstützt mehrere vordefinierte Rollen, die Sie den Mitgliedern Ihres Unternehmens zuweisen können.

"Erfahren Sie mehr über Zugriffsrollen".

Anschlüsse

Wenn ein *Organisationsadministrator* einen Konnektor erstellt, ordnet BlueXP diesen Connector automatisch der Organisation und dem aktuell ausgewählten Projekt zu. Der *Organisation admin* hat automatisch von überall im Unternehmen Zugriff auf diesen Connector. Wenn Sie jedoch andere Mitglieder in Ihrer Organisation mit unterschiedlichen Rollen haben, können diese Mitglieder nur aus dem Projekt, in dem sie erstellt wurde, auf diesen Connector zugreifen, es sei denn, Sie verknüpfen diesen Connector mit anderen Projekten.

In diesen Fällen stellen Sie einen Connector für ein anderes Projekt zur Verfügung:

- Sie möchten Mitgliedern in Ihrer Organisation erlauben, einen vorhandenen Connector zu verwenden, um zusätzliche Arbeitsumgebungen in einem anderen Projekt zu erstellen oder zu erkennen
- Sie haben eine vorhandene Ressource einem anderen Projekt zugeordnet und diese Ressource wird von einem Connector verwaltet

  Wenn eine Ressource, die Sie mit einem zusätzlichen Projekt verknüpfen, mithilfe eines BlueXP-Connectors erkannt wird, müssen Sie den Connector auch mit dem Projekt verknüpfen, mit dem die Ressource jetzt verknüpft ist. Andernfalls sind der Connector und die zugehörige Ressource für Mitglieder, die nicht über die Rolle „Organisationsadministrator“ verfügen, über die BlueXP-Leinwand nicht zugänglich.

Sie können eine Zuordnung auf der Seite **Connectors** in BlueXP IAM erstellen:

- Zuordnen eines Konnektors zu einem Projekt

  Wenn Sie einem Projekt einen Konnektor zuordnen, ist dieser Connector beim Anzeigen des Projekts über den BlueXP -Bildschirm zugänglich.

- Zuordnen eines Konnektors zu einem Ordner

Durch das Zuordnen eines Connectors zu einem Ordner wird dieser Connector nicht automatisch von allen Projekten im Ordner zugänglich gemacht. Organisationsmitglieder können erst dann auf einen Connector aus einem Projekt zugreifen, wenn Sie den Connector mit diesem spezifischen Projekt verknüpfen.

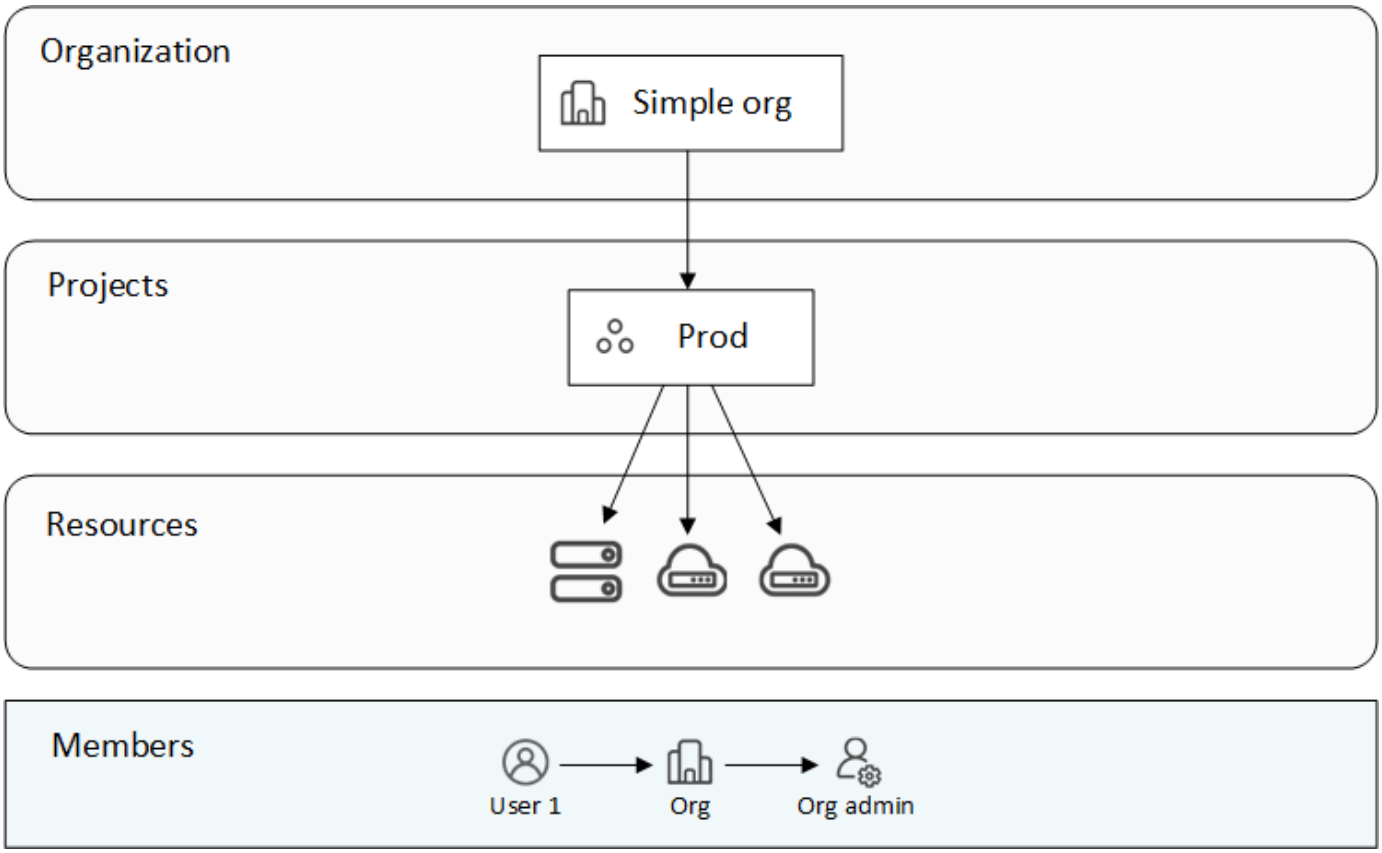
Ein „*Organisation admin*“ kann einen Connector mit einem Ordner verknüpfen, so dass der „_Ordner“ oder „Projekt admin“ die Entscheidung treffen kann, diesen Connector mit den entsprechenden Projekten im Ordner zu verknüpfen.

Beispiele für IAM

Diese Beispiele zeigen, wie Sie Ihre Organisation aufbauen könnten.

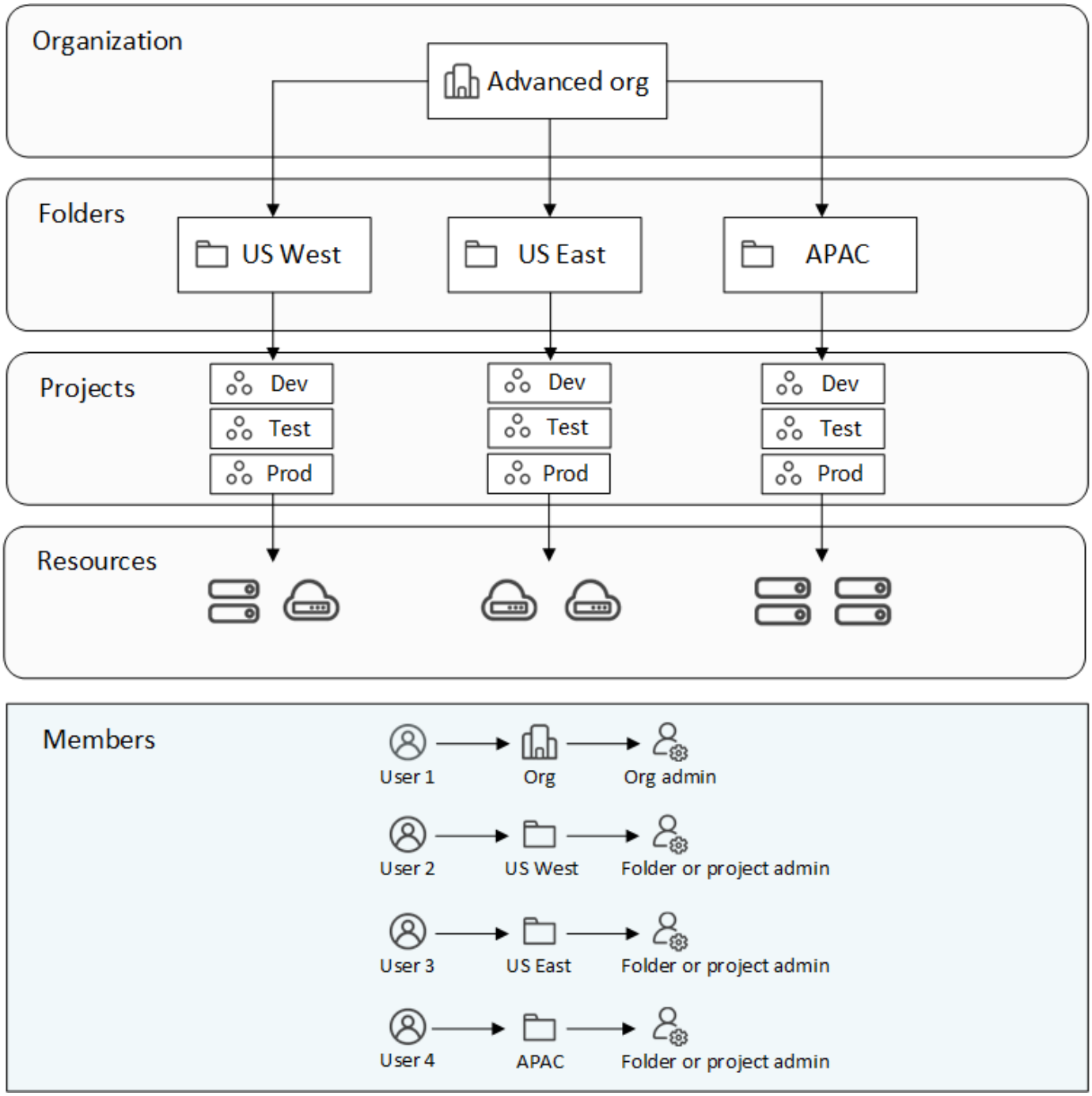
Einfache Organisation

Das folgende Diagramm zeigt ein einfaches Beispiel für eine Organisation, die das Standardprojekt und keine Ordner verwendet. Ein einziges Mitglied verwaltet die gesamte Organisation.



Fortschrittliche Organisation

Das folgende Diagramm zeigt eine Organisation, die die Projekte anhand von Ordnern für jeden geografischen Standort im Unternehmen organisiert. Jedes Projekt verfügt über einen eigenen Satz an Ressourcen. Zu den Mitgliedern gehören ein Organisationsadministrator und ein Administrator für jeden Ordner in der Organisation.



Was Sie mit BlueXP IAM erreichen können

In den folgenden Beispielen wird beschrieben, wie Sie IAM zur Verwaltung Ihrer BlueXP -Organisation einsetzen können:

- Erteilen Sie bestimmten Mitgliedern bestimmte Rollen, damit sie nur die erforderlichen Aufgaben ausführen können.
- Ändern Sie die Mitglieds-Berechtigungen, weil sie Abteilungen verschoben haben oder weil sie zusätzliche Verantwortlichkeiten haben.
- Entfernen Sie einen Benutzer, der das Unternehmen verlassen hat.
- Fügen Sie Ihrer Hierarchie Ordner oder Projekte hinzu, da eine neue Geschäftseinheit NetApp-Speicher hinzugefügt hat.

- Verknüpfen Sie eine Ressource mit einem anderen Projekt, da diese Ressource über Kapazitäten verfügt, die ein anderes Team nutzen kann.
- Zeigen Sie die Ressourcen an, auf die ein Mitglied zugreifen kann.
- Zeigen Sie die Mitglieder und Ressourcen an, die einem bestimmten Projekt zugeordnet sind.

Weitere Schritte

- "Erste Schritte mit BlueXP IAM"
- "Organisieren Sie Ihre Ressourcen in BlueXP mit Ordnern und Projekten"
- "Verwalten von BlueXP -Mitgliedern und deren Berechtigungen"
- "Management der Ressourcenhierarchie in Ihrer BlueXP -Organisation"
- "Connectors mit Ordnern und Projekten verknüpfen"
- "Wechsel zwischen BlueXP -Projekten und Organisationen"
- "Benennen Sie Ihre BlueXP -Organisation um"
- "Überwachung oder Prüfung der IAM-Aktivität"
- "Zugriffsrollen für BlueXP"
- "Erfahren Sie mehr über die API für BlueXP IAM"

Erste Schritte mit BlueXP -Identitäts- und Zugriffsmanagement

Wenn Sie sich bei BlueXP anmelden, werden Sie aufgefordert, ein neues Unternehmen zu erstellen. Die Organisation umfasst ein Mitglied (einen Organisationsadministrator) und ein Standardprojekt. Um das Identitäts- und Zugriffsmanagement (BlueXP Identity and Access Management, IAM) für Ihre geschäftlichen Anforderungen einzurichten, müssen Sie die Hierarchie Ihres Unternehmens anpassen, zusätzliche Mitglieder hinzufügen, Ressourcen hinzufügen oder ermitteln und diese Ressourcen in Ihrer Hierarchie zuordnen.

Sie müssen über **Organisationsadministrator**-Berechtigungen verfügen, um die gesamte Organisation über BlueXP IAM verwalten zu können. Wenn Sie **Ordner- oder Projektadministrator**-Berechtigungen haben, können Sie nur die Ordner und Projekte verwalten, für die Sie Berechtigungen haben.

Führen Sie diese Schritte aus, um eine neue BlueXP -Organisation einzurichten. Die Reihenfolge, in der Sie diese Schritte durchführen, kann je nach den Anforderungen Ihres Unternehmens unterschiedlich sein.

Bearbeiten Sie das Standardprojekt, oder fügen Sie es der Hierarchie Ihrer Organisation hinzu

Verwenden Sie das Standardprojekt oder erstellen Sie zusätzliche Projekte und Ordner, die Ihrer Unternehmenshierarchie entsprechen.

"Erfahren Sie, wie Sie Ihre Ressourcen mit Ordnern und Projekten organisieren".

Ordnen Sie Mitglieder Ihrer Organisation zu

Wenn mehrere Personen in Ihrem Unternehmen Zugriff auf BlueXP benötigen, verknüpfen Sie deren Benutzerkonten mit Ihrer Organisation und weisen Sie die erforderlichen Berechtigungen zu. Sie haben auch

die Möglichkeit, Servicekonten zu Ihrer Organisation hinzuzufügen.

"Erfahren Sie, wie Sie Mitglieder und ihre Berechtigungen verwalten".

Ressourcen hinzufügen oder erkennen

Fügen Sie Ressourcen in BlueXP als Arbeitsumgebungen hinzu oder entdecken Sie sie. Organisationsmitglieder verwalten eine Arbeitsumgebung, die ein Speichersystem darstellt, innerhalb eines Projekts.

Erfahren Sie, wie Sie Ressourcen erstellen oder entdecken:

- "Amazon FSX für NetApp ONTAP"
- "Azure NetApp Dateien"
- "Cloud Volumes ONTAP"
- "E-Series Systeme"
- "On-Premises ONTAP Cluster"
- "StorageGRID"

Ressourcen mit zusätzlichen Projekten verknüpfen

Wenn Sie eine Ressource in BlueXP erstellen oder ermitteln, wird diese Ressource automatisch mit dem Projekt verknüpft, das beim Erstellen oder Erkennen der Arbeitsumgebung ausgewählt wurde. Wenn Sie diese Ressource einem anderen Projekt in Ihrer Organisation zur Verfügung stellen möchten, müssen Sie eine Verknüpfung zwischen ihnen erstellen. Wenn ein Connector die Ressource verwaltet, verknüpfen Sie den Connector mit dem entsprechenden Projekt.

- "Erfahren Sie, wie Sie die Ressourcenhierarchie Ihres Unternehmens verwalten".
- "Erfahren Sie, wie Sie einen Connector einem Ordner oder Projekt zuordnen".

Verwandte Informationen

- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "
- "Erfahren Sie mehr über die API für BlueXP IAM"

Organisieren Sie Ihre Ressourcen in BlueXP IAM mit Ordnern und Projekten

Mit dem Identitäts- und Zugriffsmanagement (BlueXP Identity and Access Management, IAM) können Sie Ihre NetApp-Ressourcen mithilfe von Projekten und Ordnern organisieren. Ein *Project* stellt einen Arbeitsbereich in BlueXP dar, auf den Organisationsmitglieder zur Verwaltung von *Resources* zugreifen (z. B. ein Cloud Volumes ONTAP-System). Ein *Ordner* gruppiert verwandte Projekte zusammen. Nachdem Sie Ihre Ressourcen in Ordnern und Projekten organisiert haben, können Sie granularen Zugriff auf Ressourcen gewähren, indem Sie Organisationsmitgliedern Berechtigungen für bestimmte Ordner und Projekte gewähren.

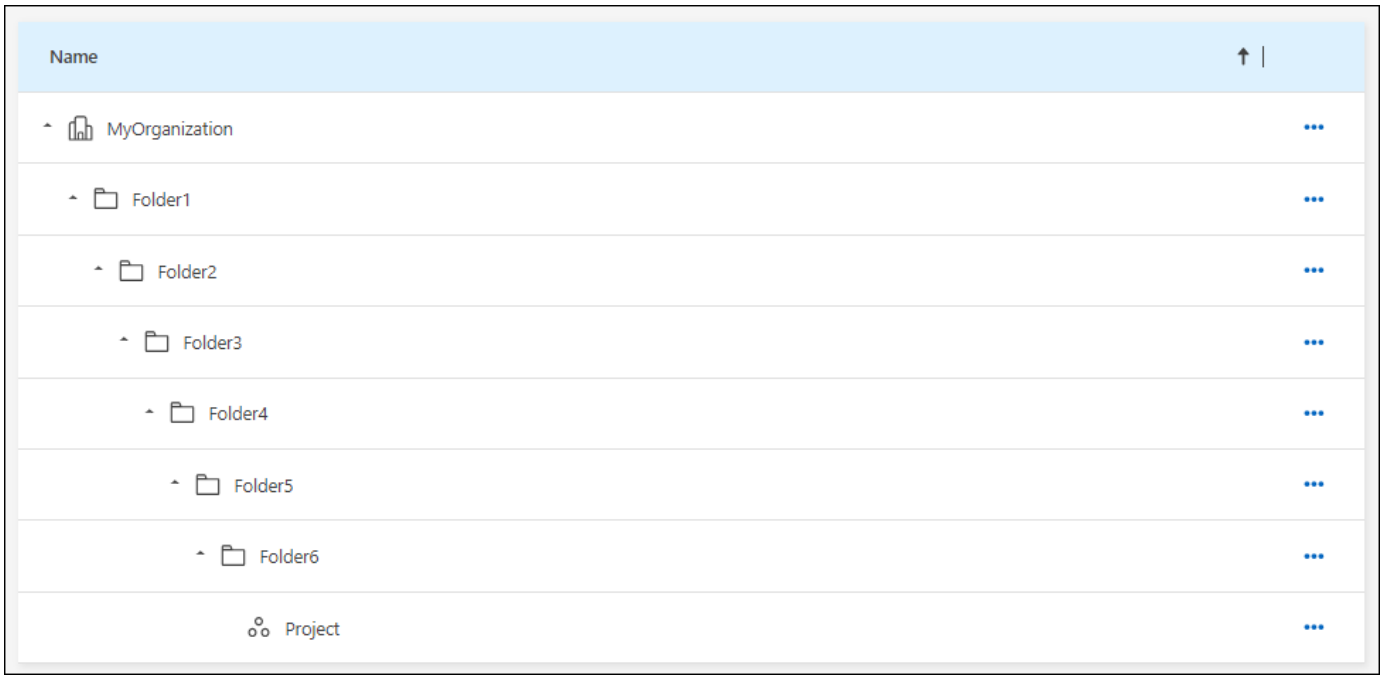
Fügen Sie einen Ordner oder ein Projekt hinzu

Wenn Sie Ihre BlueXP -Organisation erstellen, umfasst diese ein einzelnes Projekt. Sie können weitere Projekte erstellen, um die Ressourcen Ihres Unternehmens zu verwalten. Sie können optional Ordner erstellen, um verwandte Projekte zu gruppieren.

Über diese Aufgabe

Die Ressourcenhierarchie Ihrer Organisation kann bis zu sieben Ebenen umfassen, mit verschachtelten Ordnern bis hinunter auf sechs Ebenen und Projekten auf der siebten Ebene.

Das folgende Bild zeigt die maximale Tiefe der Ressourcenhierarchie Ihres Unternehmens:



Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie auf der Seite **Organisation** die Option **Ordner oder Projekt hinzufügen** aus.
3. Wählen Sie **Ordner** oder **Projekt**.
4. Geben Sie Details zum Ordner oder Projekt an:

    - **Name und Ort**: Geben Sie einen Namen ein und wählen Sie einen Speicherort in der Hierarchie für den Ordner oder das Projekt. Ein Ordner oder Projekt kann sich direkt unter der Organisation oder in einem Ordner befinden.
    - **Ressourcen**: Wählen Sie die Ressourcen aus, die Sie diesem Ordner oder Projekt zuordnen möchten.

      Sie können Ressourcen auswählen, die mit dem übergeordneten Ordner oder Projekt verknüpft sind: alle Ressourcen für ein übergeordnetes Organisationselement oder ordnerspezifische Ressourcen für ein übergeordnetes Ordnerelement.

      "Erfahren Sie, wann Sie eine Ressource einem Ordner zuordnen können".

    - **Access**: Zeigen Sie die Mitglieder an, die auf Basis der bereits in Ihrer Ressourcenhierarchie definierten Berechtigungen Zugriff auf den Ordner oder das Projekt haben.

Wählen Sie bei Bedarf **Mitglied hinzufügen**, um zusätzliche Organisationsmitglieder anzugeben, die Zugriff auf den Ordner oder das Projekt haben sollen, und wählen Sie dann eine Rolle aus. Eine Rolle definiert die Berechtigungen, die Mitglieder für den Ordner oder das Projekt haben.

"Erfahren Sie mehr über vordefinierte IAM-Rollen".

5. Wählen Sie **Hinzufügen**.

Die ID für ein Projekt abrufen

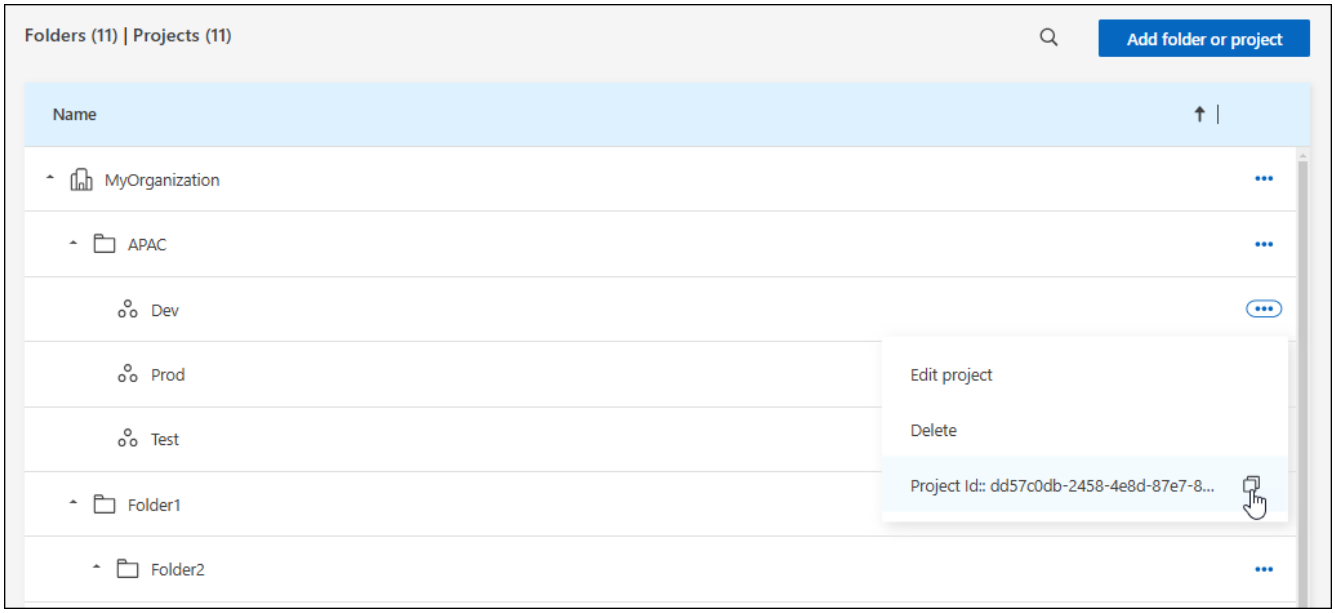
Wenn Sie die BlueXP -API verwenden, benötigen Sie möglicherweise die ID für ein Projekt. Beispiel: Beim Erstellen einer Cloud Volumes ONTAP-Arbeitsumgebung.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt in der Tabelle und wählen Sie aus •••

   Das System zeigt die Projekt-ID an.

2. Um die ID zu kopieren, wählen Sie die Schaltfläche Kopieren.



Umbenennen eines Ordners oder Projekts

Bei Bedarf können Sie den Namen Ihrer Ordner und Projekte ändern.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Geben Sie auf der Seite **Bearbeiten** einen neuen Namen ein und wählen Sie **Anwenden**.

Löschen Sie einen Ordner oder ein Projekt

Sie können die Ordner und Projekte löschen, die Sie nicht mehr benötigen.

Bevor Sie beginnen

- Dem Ordner oder Projekt dürfen keine Ressourcen zugeordnet sein. Erfahren Sie, wie Sie Ressourcen auflösen können.
- Ein Ordner darf keine Unterordner oder Projekte enthalten. Sie müssen diese Ordner und Projekte zuerst löschen.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Löschen** aus.
2. Bestätigen Sie, dass Sie den Ordner oder das Projekt löschen möchten.

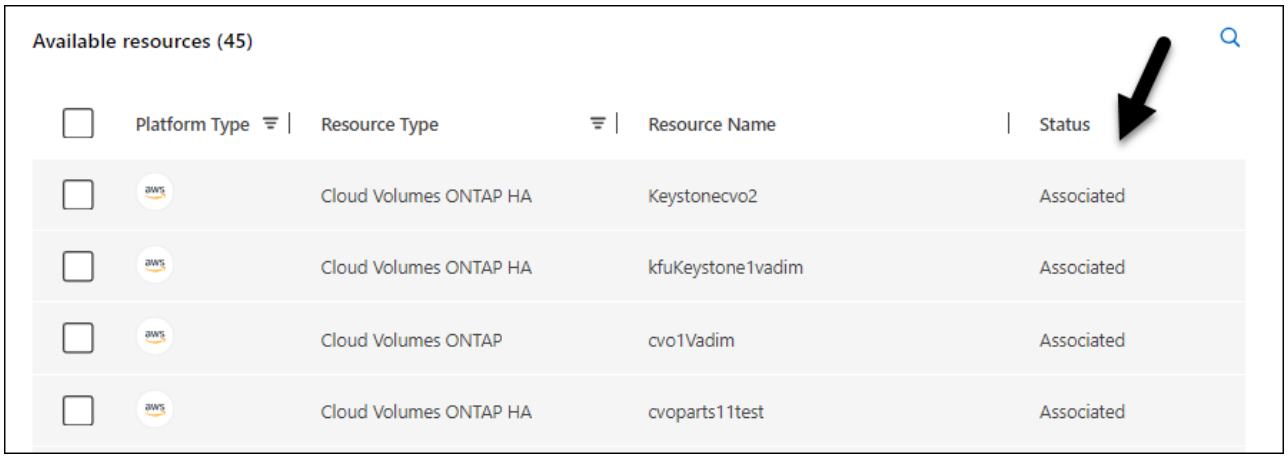
Zeigen Sie die Ressourcen an, die einem Ordner oder Projekt zugeordnet sind

Um zu überprüfen, ob Ihre Ressourcen angemessen organisiert sind und für die richtigen Mitglieder in Ihrer Organisation zugänglich sind, können Sie anzeigen, welche Ressourcen und Mitglieder einem Ordner oder Projekt zugeordnet sind.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.

2. Auf der Seite **Bearbeiten** können Sie Details zum ausgewählten Ordner oder Projekt anzeigen, indem Sie die Abschnitte **Ressourcen** oder **Zugriff** erweitern.
   - Wählen Sie **Ressourcen**, um die zugehörigen Ressourcen anzuzeigen. In der Tabelle werden in der Spalte **Status** die Ressourcen angezeigt, die dem Ordner oder Projekt zugeordnet sind.



Ändern Sie die Ressourcen, die einem Ordner oder Projekt zugeordnet sind

Mitglieder mit Berechtigungen für einen Ordner oder ein Projekt können auf die zugehörigen Ressourcen

zugreifen.

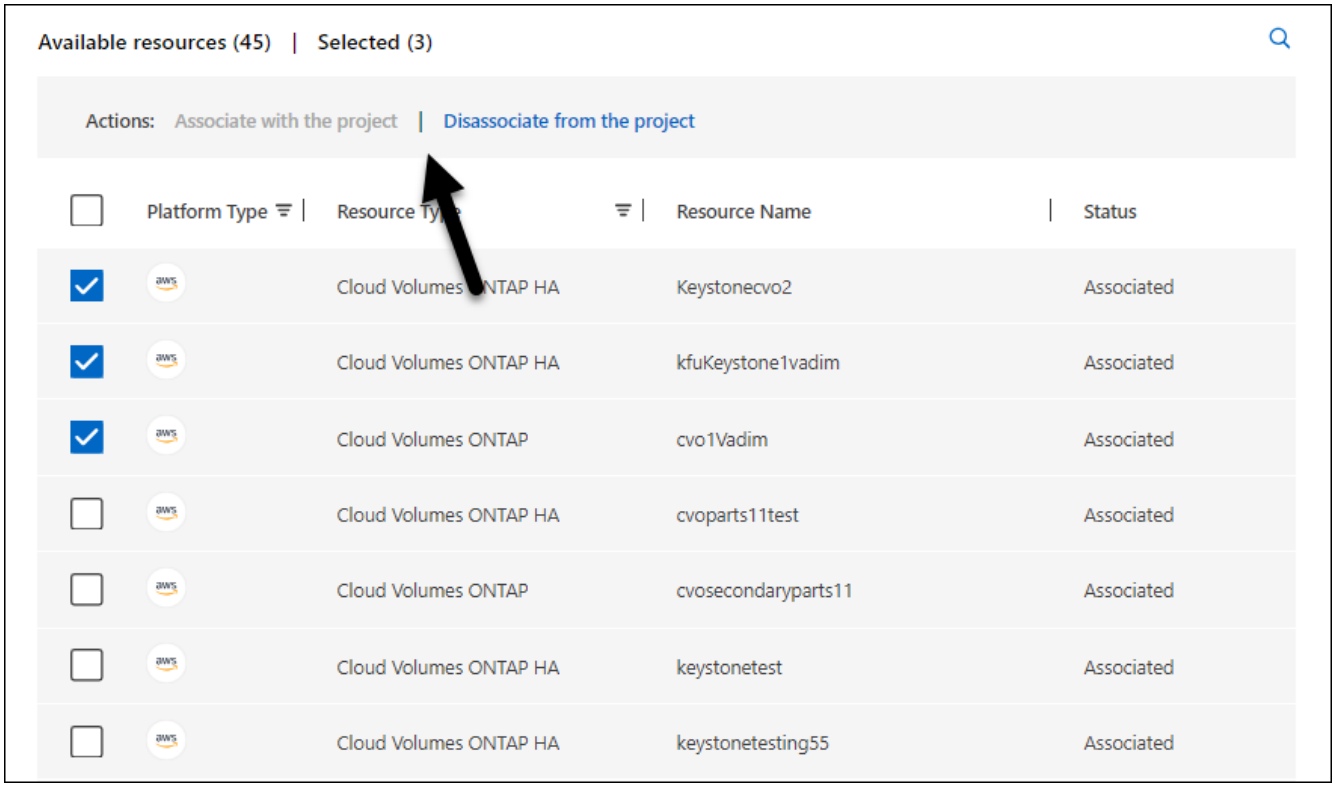
Bevor Sie beginnen

"Erfahren Sie, wann Sie eine Ressource einem Ordner zuordnen können".

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Wählen Sie auf der Seite **Bearbeiten Ressourcen** aus.

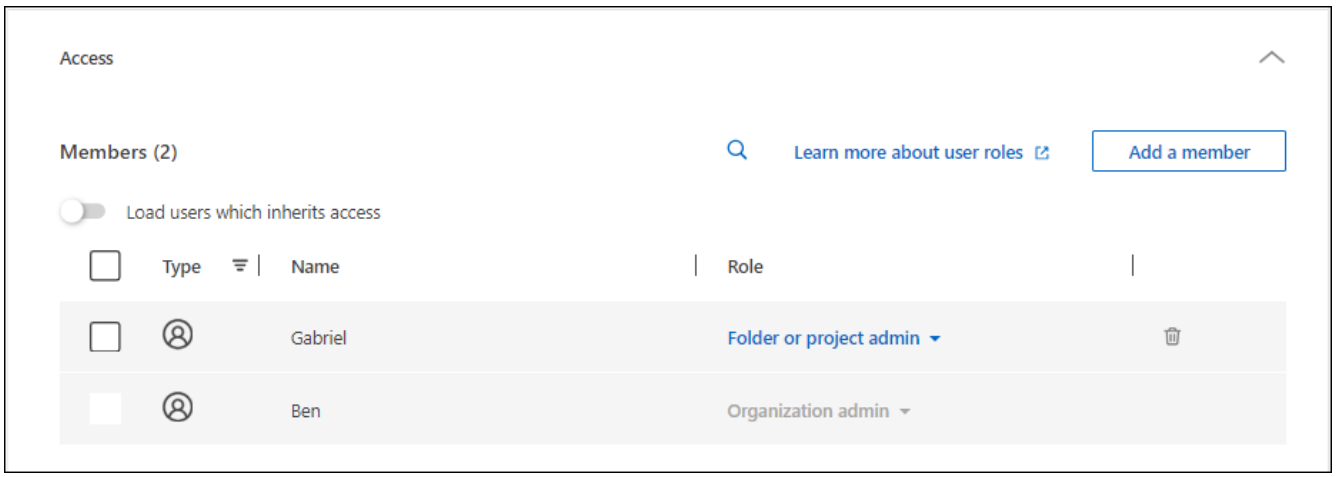
   In der Tabelle werden in der Spalte **Status** die Ressourcen angezeigt, die dem Ordner oder Projekt zugeordnet sind.
3. Wählen Sie die Ressourcen aus, die Sie verknüpfen oder aufheben möchten.
4. Wählen Sie je nach den ausgewählten Ressourcen entweder **mit dem Projekt verknüpfen** oder **mit dem Projekt absetzen** aus.



5. Wählen Sie **Anwenden**

Anzeigen von Mitgliedern, die einem Ordner oder Projekt zugeordnet sind

- Wählen Sie **Access**, um die Mitglieder anzuzeigen, die Zugriff auf den Ordner oder das Projekt haben.



Ändern Sie den Mitgliederzugriff auf einen Ordner oder ein Projekt

Ändern Sie den Mitgliederzugriff, um sicherzustellen, dass die richtigen Mitglieder auf die zugehörigen Ressourcen zugreifen können.

Der auf einer höheren Hierarchieebene gewährte Mitgliederzugriff kann auf niedrigeren Ebenen nicht geändert werden. Sie müssen zu diesem Teil der Hierarchie wechseln und dort die Berechtigungen des Mitglieds aktualisieren. Alternativ können Sie "Verwalten Sie Berechtigungen über die Seite Mitglieder".

"Erfahren Sie mehr über Rollenvererbung".

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
2. Wählen Sie auf der Seite **Bearbeiten Zugriff** aus, um die Liste der Mitglieder anzuzeigen, die Zugriff auf den ausgewählten Ordner oder das ausgewählte Projekt haben.
3. Mitgliederzugriff ändern:
   - **Mitglied hinzufügen**: Wählen Sie das Mitglied aus, das Sie dem Ordner oder Projekt hinzufügen möchten, und weisen Sie ihm eine Rolle zu.
   - **Rolle eines Mitglieds ändern**: Wählen Sie für alle Mitglieder mit einer anderen Rolle als Organisationsadministrator ihre vorhandene Rolle aus und wählen Sie dann eine neue Rolle aus.
   - **Mitgliederzugriff entfernen**: Für Mitglieder, die eine Rolle in dem Ordner oder Projekt definiert haben, für das Sie sich die Datei ansehen, können Sie deren Zugriff entfernen.
4. Wählen Sie **Anwenden**.

Verwandte Informationen

- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "
- "Erste Schritte mit BlueXP IAM"
- "Erfahren Sie mehr über die API für BlueXP IAM"

BlueXP-Mitglieder und Dienstkonten hinzufügen

Mit BlueXP Identity and Access Management (IAM) können Sie Ihrer Organisation Mitglieder hinzufügen und ihnen eine oder mehrere Rollen innerhalb Ihrer

Ressourcenhierarchie zuweisen. Eine *Rolle* enthält einen Satz von Berechtigungen, mit denen ein Mitglied bestimmte Aktionen auf einer bestimmten Ebene der Ressourcenhierarchie ausführen kann. Sie können neue Benutzerkonten und Dienstkonten zuordnen, Mitgliederrollen verwalten und vieles mehr.

Stellen Sie sicher, dass zwei Mitglieder über die Rolle des Organisationsadministrators verfügen, um den Zugriff auf Ihre BlueXP-Organisation nicht zu verlieren.

Um Benutzer und deren Berechtigungen zu verwalten, müssen Sie eine der folgenden Rollen zuweisen:

- Organisationsadministrator

  Benutzer mit dieser Rolle können alle Mitglieder verwalten

- Ordner- oder Projektadministrator

  Benutzer mit dieser Rolle können nur Mitglieder eines bestimmten Ordners oder Projekts verwalten.

  ```
  _Folder or project admin_ can view all members on the *Members* page but
  manage permissions only for folders and projects they have access to.
  xref:{relative_path}reference-iam-predefined-roles.html[Learn more about
  the actions that a _Folder or project admin_ can complete].
  ```

Fügen Sie Mitglieder zu Ihrer Organisation hinzu

Sie können Ihrer Organisation zwei Arten von Mitgliedern hinzufügen: ein Benutzerkonto und ein Dienstkonto. Ein Dienstkonto wird von Anwendungen verwendet, um Aufgaben über die BlueXP API ohne menschliches Eingreifen auszuführen. Ein Benutzerkonto wird normalerweise von einer Person verwendet, um sich bei BlueXP anzumelden und Ressourcen zu verwalten.

Benutzer müssen sich für BlueXP anmelden, bevor sie einer Organisation hinzugefügt oder ihnen eine Rolle zugewiesen werden. Sie können jedoch Dienstkonten direkt von BlueXP aus erstellen.

Um Benutzer und deren Berechtigungen zu verwalten, müssen Sie über die Rolle **Organisationsadministrator** oder die Rolle **Ordner oder Projektadministrator** verfügen. Denken Sie daran, dass Benutzer mit der Rolle **Ordner oder Projektadministrator** nur Mitglieder für den Ordner oder Projekte verwalten können, für die sie Administratorrechte besitzen.

Benutzerkonto

Schritte

1. Leiten Sie den Benutzer zum Besuch weiter "NetApp BlueXP Website" um sich anzumelden.

   Sobald sich Benutzer angemeldet haben, füllen sie die Seite **Anmelden** aus, überprüfen ihre E-Mails und melden sich an. Wenn BlueXP Benutzer auffordert, eine Organisation zu erstellen, schließen sie diese und benachrichtigen Sie über die Kontoerstellung. Anschließend können Sie den Benutzer zu Ihrer bestehenden BlueXP -Organisation hinzufügen.

   "Erfahren Sie, wie Sie sich bei BlueXP anmelden können".

2. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus  .
3. Wählen Sie **Mitglieder**.
4. Wählen Sie **Mitglied hinzufügen**.
5. Führen Sie zum Hinzufügen des Mitglieds die folgenden Schritte im Dialogfeld aus:
   - **Entity Type**: Behalten Sie **User** ausgewählt.
   - **Benutzer-E-Mail**: Geben Sie die E-Mail-Adresse des Benutzers ein, die mit dem von ihnen erstellten BlueXP -Login verknüpft ist.
   - **Wählen Sie eine Organisation, einen Ordner oder ein Projekt**: Wählen Sie die Ebene Ihrer Ressourcenhierarchie aus, für die das Mitglied Berechtigungen haben soll.

     Beachten Sie Folgendes:

     - Sie können nur aus den Ordnern und Projekten auswählen, für die Sie Administratorrechte haben.
     - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Zugriff auf alle Inhalte.
   - **Wählen Sie eine Kategorie** und wählen Sie dann eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen bereitstellt, die mit der Organisation, dem Ordner oder dem Projekt verknüpft sind, das Sie ausgewählt haben.
     - Wenn Sie einen Ordner oder ein Projekt ausgewählt haben, können Sie aus jeder anderen Rolle als **Organisationsadministrator** wählen.

       "Erfahren Sie mehr über Zugriffsrollen".
   - **Rolle hinzufügen**: Wenn Sie Zugriff auf zusätzliche Ordner oder Projekte innerhalb Ihrer Organisation gewähren möchten oder dem Benutzer weitere Berechtigungen im ausgewählten Bereich gewähren möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen anderen Ordner oder ein anderes Projekt oder eine andere Rollenkategorie an und wählen Sie dann eine Rolle.
6. Wählen Sie **Hinzufügen**.

   NetApp BlueXP sendet dem Benutzer eine E-Mail mit Informationen zum Zugriff auf BlueXP.

Dienstkonto

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus  .

2. Wählen Sie **Mitglieder**.
3. Wählen Sie **Mitglied hinzufügen**.
4. Führen Sie zum Hinzufügen des Mitglieds die folgenden Schritte im Dialogfeld aus:
   - **Entitätstyp**: Wählen Sie **Service-Konto**.
   - **Name des Service-Kontos**: Geben Sie einen Namen für das Service-Konto ein.
   - **Wählen Sie eine Organisation, einen Ordner oder ein Projekt**: Wählen Sie die Ebene Ihrer Ressourcenhierarchie aus, für die das Mitglied Berechtigungen haben soll.

     Beachten Sie Folgendes:

     - Sie können nur aus den Ordnern und Projekten auswählen, für die Sie Administratorrechte haben.
     - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Zugriff auf alle Inhalte.
   - **Wählen Sie eine Kategorie** und dann eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.
     - Wenn Sie einen Ordner oder ein Projekt ausgewählt haben, können Sie aus jeder anderen Rolle als **Organisationsadministrator** wählen.

       "Erfahren Sie mehr über vordefinierte IAM-Rollen".
   - **Rolle hinzufügen**: Wenn Sie Zugriff auf zusätzliche Ordner oder Projekte innerhalb Ihrer Organisation gewähren möchten oder dem Benutzer weitere Berechtigungen im ausgewählten Bereich gewähren möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen anderen Ordner oder ein anderes Projekt oder eine andere Rollenkategorie an und wählen Sie dann eine Rolle.
5. Laden Sie die Client-ID und den Client-Schlüssel herunter, oder kopieren Sie ihn.

   BlueXP zeigt das Client-Geheimnis nur einmal an. Kopieren oder laden Sie es herunter und speichern Sie es sicher. Beachten Sie, dass Sie die Client-ID und das Client-Geheimnis später bei Bedarf neu erstellen können.
6. Wählen Sie **Schließen**.

Anzeigen von Organisationsmitgliedern

Sie können eine Liste aller Mitglieder in Ihrer BlueXP -Organisation anzeigen. Um zu verstehen, welche Ressourcen und Berechtigungen einem Mitglied zur Verfügung stehen, können Sie die dem Mitglied zugewiesenen Rollen auf verschiedenen Ebenen der Ressourcenhierarchie Ihres Unternehmens anzeigen. "Erfahren Sie, wie Sie mit Rollen den Zugriff auf BlueXP -Ressourcen steuern."

Sie können sowohl Benutzerkonten als auch Dienstkonten auf der Seite **Mitglieder** anzeigen.

Sie können auch alle Mitglieder anzeigen, die einem bestimmten Ordner oder Projekt zugeordnet sind. "Weitere Informationen .".

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.

2. Wählen Sie **Mitglieder**.

   In der Tabelle **Mitglieder** sind die Mitglieder Ihrer Organisation aufgelistet.

3. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen** aus.

Entfernen Sie ein Mitglied aus Ihrer Organisation

Möglicherweise müssen Sie ein Mitglied aus Ihrer Organisation entfernen, beispielsweise wenn es Ihr Unternehmen verlässt.

Durch das Entfernen eines Mitglieds werden dessen Berechtigungen entfernt, seine BlueXP und NetApp -Support-Site-Konten bleiben jedoch erhalten.

Schritte

1. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• Wählen Sie dann **Benutzer löschen**.
2. Bestätigen Sie, dass Sie das Mitglied aus Ihrer Organisation entfernen möchten.

Erstellen Sie die Anmeldeinformationen für ein Dienstkonto neu

Erstellen Sie neue Anmeldeinformationen, wenn diese verloren gehen oder eine Aktualisierung der Sicherheitsanmeldeinformationen erforderlich ist.

Über diese Aufgabe

Wenn Sie die Anmeldeinformationen neu erstellen, löschen Sie die vorhandenen Anmeldeinformationen für das Dienstkonto und erstellen neue. Sie können die vorherigen Anmeldeinformationen nicht verwenden.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie **Mitglieder**.
3. Navigieren Sie in der Tabelle **Members** zu einem Servicekonto, wählen Sie ••• und wählen Sie dann **Recreate Secrets** aus.
4. Wählen Sie **Recreate**.
5. Laden Sie die Client-ID und den Client-Schlüssel herunter, oder kopieren Sie ihn.

   BlueXP zeigt das Client-Geheimnis nur einmal an. Kopieren oder laden Sie es herunter und speichern Sie es sicher.

Verwalten der Multi-Faktor-Authentifizierung (MFA) eines Benutzers

Wenn ein Benutzer den Zugriff auf sein MFA-Gerät verliert, können Sie seine MFA-Konfiguration entweder entfernen oder deaktivieren.

Wenn Sie die MFA-Konfiguration entfernen, muss der Benutzer MFA bei der Anmeldung bei BlueXP erneut einrichten. Wenn der Benutzer nur vorübergehend den Zugriff auf sein MFA-Gerät verloren hat, kann er den Wiederherstellungscode verwenden, den er bei der Einrichtung von MFA gespeichert hat, um sich bei BlueXP anzumelden.

Wenn sie ihren Wiederherstellungscode nicht haben, deaktivieren Sie MFA vorübergehend, um die Anmeldung

zu ermöglichen. Wenn Sie MFA für einen Benutzer deaktivieren, wird es nur für acht Stunden deaktiviert und dann automatisch wieder aktiviert. Dem Benutzer ist während dieser Zeit eine Anmeldung ohne MFA gestattet. Nach den acht Stunden muss der Benutzer MFA verwenden, um sich bei BlueXP anzumelden.

Sie müssen über eine E-Mail-Adresse in derselben Domäne wie der betroffene Benutzer verfügen, um die Multi-Faktor-Authentifizierung dieses Benutzers zu verwalten.

Schritte

1. Wählen Sie oben rechts in der Konsole > **Identitäts- und Zugriffsverwaltung**.
2. Wählen Sie **Mitglieder**.

   Die Mitglieder Ihrer Organisation erscheinen in der Tabelle **Mitglieder**.

3. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Multi-Faktor-Authentifizierung verwalten**.
4. Wählen Sie, ob die MFA-Konfiguration des Benutzers entfernt oder deaktiviert werden soll.

Verwandte Informationen

- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "
- "Erste Schritte mit BlueXP IAM"
- "Vordefinierte BlueXP IAM-Rollen"
- "Erfahren Sie mehr über die API für BlueXP IAM"

Verwenden Sie Rollen, um den Benutzerzugriff auf Ressourcen zu verwalten

Innerhalb von BlueXP können Sie Benutzern Rollen zuweisen, je nachdem, was sie tun müssen und wo.

Benutzer mit der Rolle **Organisationsadministrator** oder **Ordner- oder Projektadministrator** sind dafür verantwortlich, anderen Benutzern Rollen zuzuweisen. Sie können Zugriffsrollen auf Projekt- oder Ordnerbasis zuweisen. Sie können einem Benutzer beispielsweise die Administratorrolle für Ransomware-Schutz für ein Projekt und die SnapCenter-Administratorrolle für ein anderes Projekt zuweisen. Wenn ein Benutzer alternativ die Klassifizierungsadministratorrolle für alle Projekte in einem bestimmten Ordner benötigt, können Sie ihm diese Rolle auf Ordnerebene zuweisen.

Verwenden Sie Zugriffsrollen, um den Zugriff auf Speicherressourcen basierend auf den spezifischen Aufgaben zuzuweisen, die Benutzer ausführen müssen. Wenn ein Benutzer beispielsweise mit Ransomware-Schutzdiensten interagieren muss, benötigt er eine Zugriffsrolle, die entweder Anzeige- oder Administratorberechtigungen für den Ransomware-Schutzdienst für das Projekt umfasst, für das die Zugriffsrolle gewährt wurde.

Weisen Sie Benutzern Rollen basierend auf Ihrer IAM-Strategie zu, um die Sicherheit zu erhöhen. IAM-Rollen stellen sicher, dass Benutzer nur den Zugriff haben, den sie benötigen.

Denken Sie daran, dass Sie keinen direkten Zugriff auf Ressourcen gewähren können. Weisen Sie den Projekten zunächst Ressourcen zu. Sie sollten Ihre Ressourcenhierarchie einrichten, bevor Sie Benutzerzugriff zuweisen. "Erfahren Sie, wie Sie Ihre Ressourcen in BlueXP IAM mit Ordnern und Projekten organisieren."

Rollen anzeigen, die einem Mitglied zugewiesen sind

Wenn Sie Ihrer Organisation ein Mitglied hinzufügen, werden Sie aufgefordert, ihm eine Rolle zuzuweisen. Sie können Mitglieder überprüfen, welche Rollen sie derzeit zugewiesen haben.

Wenn Sie die Rolle *Ordner oder Projektadministrator* haben, werden auf der Seite alle Mitglieder der Organisation angezeigt. Sie können jedoch nur Mitgliederberechtigungen für die Ordner und Projekte anzeigen und verwalten, für die Sie Berechtigungen haben. "Erfahren Sie mehr über die Aktionen, die ein *Ordner- oder Projektadministrator* durchführen kann".

1. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen** aus.
2. Erweitern Sie in der Tabelle die entsprechende Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds anzeigen möchten, und wählen Sie in der Spalte **Rolle Ansicht** aus.

Einem Mitglied eine Zugriffsrolle hinzufügen

Normalerweise weisen Sie eine Rolle zu, wenn Sie ein Mitglied zu Ihrer Organisation hinzufügen, Sie können sie jedoch jederzeit aktualisieren, indem Sie Rollen entfernen oder hinzufügen.

Sie können einem Benutzer eine Zugriffsrolle für Ihr Unternehmen, Ihren Ordner oder Ihr Projekt zuweisen.

Mitglieder können innerhalb eines Projekts und in verschiedenen Projekten mehrere Rollen haben. Beispielsweise können kleinere Organisationen alle verfügbaren Zugriffsrollen demselben Benutzer zuweisen, während größere Organisationen Benutzer mit spezialisierteren Aufgaben betrauen. Alternativ können Sie einem Benutzer auch die Administratorrolle für den Ransomware-Schutz einer Organisation zuweisen. So könnte der Benutzer beispielsweise bei allen Projekten im Unternehmen Ransomware-Schutzaufgaben durchführen.

Ihre Zugriffsrollenstrategie sollte mit der Art und Weise übereinstimmen, wie Sie Ihre NetApp-Ressourcen organisiert haben.

> Einem Mitglied, dem die Rolle „Organisationsadministrator“ zugewiesen ist, können keine zusätzlichen Rollen zugewiesen werden. Sie verfügen bereits über Berechtigungen im gesamten Unternehmen. Einem Mitglied mit der Rolle „Ordner“ oder „Projekt“ können keine anderen Rollen innerhalb des Ordners oder Projekts zugewiesen werden, in denen diese Rolle bereits vorhanden ist. Beide Rollen bieten Zugriff auf alle Dienste im ihnen zugewiesenen Umfang.

Schritte

1. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Rolle hinzufügen** aus.
2. Führen Sie zum Hinzufügen einer Rolle die folgenden Schritte im Dialogfeld aus:
   - **Wählen Sie eine Organisation, einen Ordner oder ein Projekt**: Wählen Sie die Ebene Ihrer Ressourcenhierarchie aus, für die das Mitglied Berechtigungen haben soll.

     Wenn Sie die Organisation oder einen Ordner auswählen, hat das Mitglied Berechtigungen für alles, was sich in der Organisation oder im Ordner befindet.

   - **Kategorie auswählen**: Wählen Sie eine Rollenkategorie. "Erfahren Sie mehr über Zugriffsrollen".
   - Wählen Sie eine **Rolle**: Wählen Sie eine Rolle aus, die dem Mitglied Berechtigungen für die Ressourcen bereitstellt, die mit der Organisation, dem Ordner oder dem Projekt verknüpft sind, das Sie

ausgewählt haben.

"Erfahren Sie mehr über Zugriffsrollen". * **Rolle hinzufügen**: Wenn Sie Zugriff auf zusätzliche Ordner oder Projekte innerhalb Ihrer Organisation gewähren möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen anderen Ordner oder ein anderes Projekt oder eine Rollenkategorie an und wählen Sie dann eine Rollenkategorie und eine entsprechende Rolle aus.

1. Wählen Sie **Neue Rollen hinzufügen**.

Ändern Sie die zugewiesene Rolle eines Mitglieds

Sie können die zugewiesenen Rollen für ein Mitglied ändern, wenn Sie den Zugriff für einen Benutzer anpassen müssen.

> Benutzern muss mindestens eine Rolle zugewiesen sein. Sie können einem Benutzer nicht alle Rollen entfernen. Wenn Sie alle Rollen entfernen möchten, müssen Sie den Benutzer aus Ihrer Organisation löschen.

Schritte

1. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen** aus.
2. Erweitern Sie in der Tabelle die entsprechende Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds ändern möchten, und wählen Sie in der Spalte **Rolle Ansicht** aus, um die diesem Mitglied zugewiesenen Rollen anzuzeigen.
3. Sie können eine vorhandene Rolle für ein Mitglied ändern oder eine Rolle entfernen.
   a. Um die Rolle eines Mitglieds zu ändern, wählen Sie neben der gewünschten Rolle **Ändern** aus. Sie können diese Rolle nur in eine Rolle innerhalb derselben Rollenkategorie ändern. Sie können beispielsweise von einer Datenservice-Rolle zu einer anderen wechseln. Bestätigen Sie die Änderung.
   b. Um die Zuweisung der Rolle eines Mitglieds aufzuheben, wählen Sie neben der Rolle aus, um die Zuweisung des Mitglieds zur entsprechenden Rolle aufzuheben. Sie werden aufgefordert, die Entfernung zu bestätigen.

Management der Ressourcenhierarchie in Ihrer BlueXP -Organisation

Wenn Sie ein Mitglied Ihrer Organisation zuordnen, erteilen Sie Berechtigungen auf Organisations-, Ordner- oder Projektebene. Um sicherzustellen, dass diese Mitglieder über Berechtigungen für den Zugriff auf die richtigen Ressourcen verfügen, müssen Sie die Ressourcenhierarchie Ihres Unternehmens verwalten, indem Sie Ressourcen bestimmten Projekten und Ordnern zuordnen. Eine *Resource* ist eine Speicherressource, die BlueXP bereits managt oder bereits kennt.

Zeigen Sie die Ressourcen in Ihrem Unternehmen an

Sie können sowohl entdeckte als auch unentdeckte Ressourcen anzeigen, die mit Ihrer Organisation verknüpft sind. Unentdeckte Ressourcen sind Speicherressourcen, die vom Digital Advisor identifiziert, aber nicht als Arbeitsumgebungen hinzugefügt wurden.

> Auf der IAM-Ressourcenseite sind Amazon FSx for NetApp ONTAP -Ressourcen nicht enthalten, da Sie sie keiner IAM-Rolle zuordnen können. Zeigen Sie diese Ressourcen auf ihrer jeweiligen Leinwand oder aus Workloads an.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie **Ressourcen**, um die Seite Ressourcen anzuzeigen.
3. Wählen Sie **Erweiterte Suche Und Filterung**.
4. Verwenden Sie eine der verfügbaren Optionen, um die gesuchte Ressource zu finden:
   - **Suche nach Ressourcenname**: Geben Sie eine Textzeichenfolge ein und wählen Sie **Hinzufügen**.
   - **Plattform**: Wählen Sie eine oder mehrere Plattformen wie Amazon Web Services.
   - **Ressourcen**: Wählen Sie eine oder mehrere Ressourcen, wie z. B. Cloud Volumes ONTAP.
   - **Organisation, Ordner oder Projekt**: Wählen Sie die gesamte Organisation, einen bestimmten Ordner oder ein bestimmtes Projekt aus.
5. Wählen Sie **Suche**.

Verknüpfen Sie eine Ressource mit Ordnern und Projekten

Ordnen Sie eine Ressource einem Ordner oder Projekt zu, um sie verfügbar zu machen.

Bevor Sie beginnen

Sie sollten verstehen, wie die Ressourcenzuordnung funktioniert. "Erfahren Sie mehr über Ressourcen, einschließlich wann Sie eine Ressource einem Ordner zuordnen".

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Zuordnung zu Ordnern oder Projekten** aus.
2. Wählen Sie einen Ordner oder ein Projekt aus und wählen Sie dann **Accept** aus.
3. Um einen zusätzlichen Ordner oder ein weiteres Projekt zuzuordnen, wählen Sie **Ordner oder Projekt hinzufügen** und wählen Sie dann den Ordner oder das Projekt aus.

   Beachten Sie, dass Sie nur aus den Ordnern und Projekten auswählen können, für die Sie Administratorberechtigungen haben.

4. Wählen Sie **Ressourcen zuordnen**.
   - Wenn Sie die Ressource mit Projekten verknüpft haben, können Mitglieder, die Berechtigungen für diese Projekte haben, jetzt in BlueXP auf die Ressource zugreifen.
   - Wenn Sie die Ressource einem Ordner zugeordnet haben, kann ein *Ordner oder Projektadministrator* nun von BlueXP IAM aus auf die Ressource zugreifen. "Erfahren Sie mehr über das Zuordnen einer Ressource zu einem Ordner".

Nachdem Sie fertig sind

Wenn Sie mithilfe eines BlueXP Connectors eine Ressource entdecken, verknüpfen Sie den Connector mit dem Projekt, um ihm Zugriff zu gewähren. Andernfalls sind der Connector und die zugehörige Ressource für Mitglieder ohne die Rolle „Organisationsadministrator“ über die BlueXP Leinwand nicht zugänglich.

"Erfahren Sie, wie Sie einen Connector einem Ordner oder Projekt zuordnen".

Zeigen Sie die mit einer Ressource verbundenen Ordner und Projekte an

Um zu ermitteln, wo eine Ressource in der Hierarchie Ihrer Organisation verfügbar ist, können Sie die Ordner und Projekte anzeigen, die mit dieser Ressource verknüpft sind.

Wenn Sie herausfinden möchten, welche Organisationsmitglieder Zugriff auf die Ressource haben, können Sie "Zeigen Sie die Mitglieder an, die Zugriff auf die Ordner und Projekte haben, die der Ressource zugeordnet sind".

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen** aus.

Das folgende Beispiel zeigt eine Ressource, die einem Projekt zugeordnet ist.

Wenn Sie herausfinden möchten, welche Organisationsmitglieder Zugriff auf die Ressource haben, können Sie "Zeigen Sie die Mitglieder an, die Zugriff auf die Ordner und Projekte haben, die der Ressource zugeordnet sind".

Eine Ressource aus einem Ordner oder Projekt entfernen

Um eine Ressource aus einem Ordner oder Projekt zu entfernen, müssen Sie die Verknüpfung zwischen dem Ordner oder Projekt und der Ressource entfernen. Durch das Entfernen der Zuordnung wird verhindert, dass Mitglieder die Ressource im Ordner oder Projekt verwalten.

Wenn Sie eine erkannte Ressource aus der gesamten Organisation entfernen möchten, müssen Sie die Arbeitsumgebung aus dem BlueXP -Bildschirm entfernen.

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen** aus.
2. Wählen Sie für den Ordner oder das Projekt aus, für den Sie die Ressource entfernen möchten 🗑
3. Bestätigen Sie, dass Sie die Verknüpfung entfernen möchten, indem Sie **Löschen** auswählen.

Verwandte Informationen

- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "
- "Erste Schritte mit BlueXP IAM"
- "Erfahren Sie mehr über die API für BlueXP IAM"

Verknüpfen Sie einen BlueXP -Konnektor mit anderen Ordnern und Projekten

```
 When an _Organization admin_ creates a Connector, it is automatcially
associated with currently selected project within the organization.
Although someone with the _Organization admin_  can access to that
Connector from anywhere in the organization. Other members in your
organization can only access that Connector from the project in which it
was created, unless you associate that Connector with other projects.
.Bevor Sie beginnen
Sie sollten verstehen, wie die Verbindungszuordnung funktioniert.
xref:{relative_path}concept-identity-and-access-management.html#associate-
connectors["Erfahren Sie mehr über die Verwendung von Steckverbindern mit
BlueXP  IAM"].
```

Über diese Aufgabe

- Wenn ein *Ordner- oder Projektadministrator* die Seite **Connectors** anzeigt, werden auf der Seite alle Connectors in der Organisation angezeigt. Ein Mitglied mit dieser Rolle kann jedoch nur Connectors anzeigen und mit den Ordnern und Projekten verknüpfen, für die sie Berechtigungen haben. "Erfahren Sie mehr über die Aktionen, die ein *Ordner- oder Projektadministrator* durchführen kann".

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie **Connectors**.
3. Suchen Sie in der Tabelle den Konnektor, den Sie verknüpfen möchten.

   Verwenden Sie die Suche über der Tabelle, um einen bestimmten Connector zu finden, oder filtern Sie die Tabelle nach Ressourcenhierarchie.

4. Um die mit dem Connector verknüpften Ordner und Projekte anzuzeigen, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

   BlueXP zeigt Details zu den Ordnern und Projekten an, denen der Connector zugeordnet ist.

5. Wählen Sie **Zuordnung zu Ordner oder Projekt**.
6. Wählen Sie einen Ordner oder ein Projekt aus und wählen Sie dann **Accept** aus.
7. Um den Connector einem zusätzlichen Ordner oder Projekt zuzuordnen, wählen Sie **Ordner oder Projekt hinzufügen** und wählen dann den Ordner oder das Projekt aus.
8. Wählen Sie **Associate Connector**.

Nachdem Sie fertig sind

Wenn Sie die vom Connector verwalteten Ressourcen mit denselben Ordnern und Projekten verknüpfen möchten, können Sie dies auf der Seite „Ressourcen“ tun.

"Erfahren Sie, wie Sie eine Ressource mit Ordnern und Projekten verknüpfen".

Verwandte Informationen

- "Erfahren Sie mehr über BlueXP -Steckverbinder"
- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "

- "Erste Schritte mit BlueXP IAM"
- "Erfahren Sie mehr über die API für BlueXP IAM"

Wechseln Sie zwischen BlueXP -Organisationen, -Projekten und -Konnektoren

Sie gehören möglicherweise mehreren BlueXP -Organisationen an oder haben die Berechtigung, auf mehrere Projekte oder Connectors innerhalb einer BlueXP -Organisation zuzugreifen. Bei Bedarf können Sie einfach zwischen Organisationen, Projekten und Connectors wechseln, um auf die Ressourcen zuzugreifen, die mit dieser Organisation, diesem Projekt oder Connector verknüpft sind.

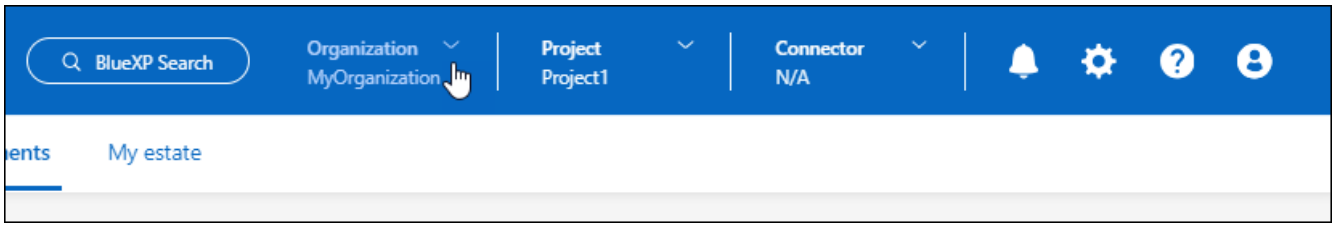
Sie können mehreren Organisationen angehören, wenn Sie eingeladen wurden, einer anderen Organisation beizutreten, oder wenn Sie selbst eine zusätzliche Organisation erstellt haben. Sie können mithilfe der API eine zusätzliche Organisation erstellen. "Erfahren Sie, wie Sie eine neue Organisation erstellen"

Wechseln Sie zwischen Organisationen

Wenn Sie Mitglied mehrerer Organisationen sind, können Sie jederzeit zwischen diesen wechseln.

Schritte

1. Wählen Sie oben in BlueXP **Organisation** aus.



2. Wählen Sie eine andere Organisation aus und wählen Sie dann **Switch**.

Ergebnis

BlueXP wechselt zur ausgewählten Organisation und zeigt die mit dieser Organisation verknüpften Ressourcen an.

Wechseln Sie zwischen Projekten

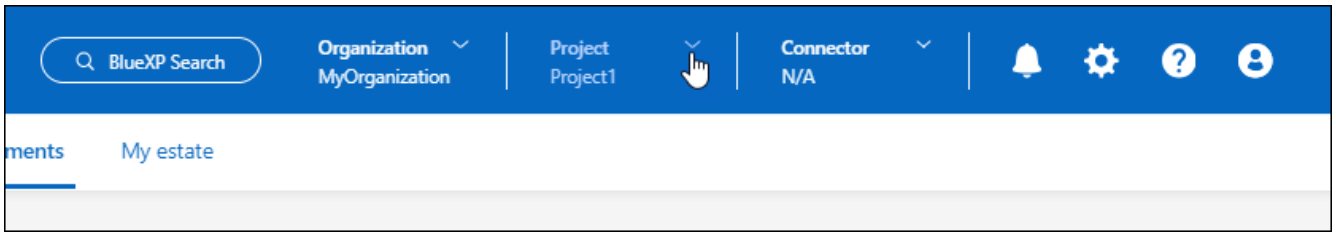
Wenn Ihr Unternehmen mehrere Projekte umfasst und Sie Zugriff auf diese Projekte haben, können Sie jederzeit zwischen ihnen wechseln.

Bevor Sie beginnen

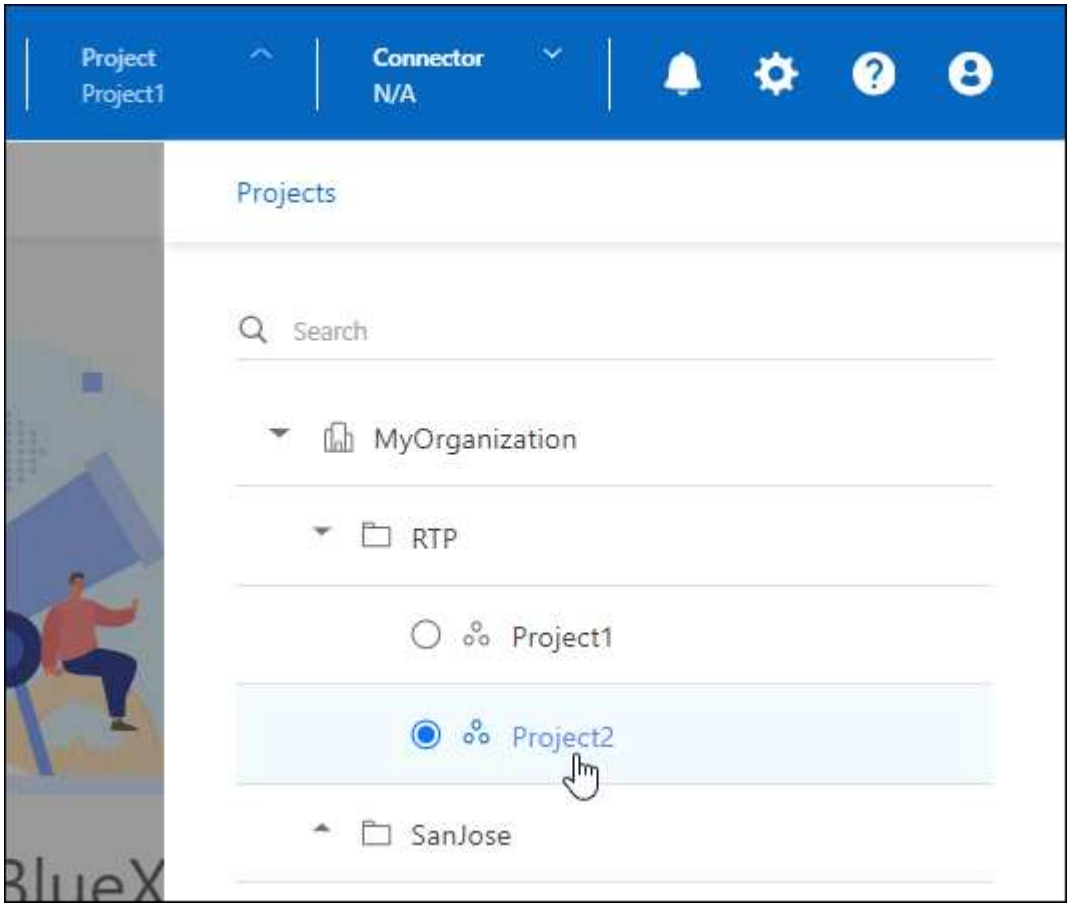
Sie müssen sich auf einer beliebigen Seite der BlueXP -Konsole befinden, außer auf den IAM-Seiten (BlueXP Identity and Access Management). Sie können nicht zu einem anderen Projekt wechseln, wenn Sie eine der IAM-Seiten anzeigen.

Schritte

1. Wählen Sie oben in BlueXP **Projekt** aus.



2. Durchsuchen Sie die Ordner und Projekte in Ihrer Organisation, wählen Sie das gewünschte Projekt aus und wählen Sie dann **Switch** aus.



Ergebnis

BlueXP wechselt zum ausgewählten Projekt und zeigt die mit diesem Projekt verknüpften Ressourcen an.

Zwischen den Anschlüssen wechseln

Wenn Sie über mehrere Anschlüsse verfügen, können Sie zwischen diesen wechseln, um die Arbeitsumgebungen anzuzeigen, die einem bestimmten Connector zugeordnet sind.

Schritte

1. Wählen Sie oben in BlueXP **Connector** aus.
2. Wählen Sie einen anderen Anschluss und dann **Switch**.

Ergebnis

BlueXP aktualisiert und zeigt die Arbeitsumgebungen an, die dem ausgewählten Konnektor zugeordnet sind.

Verwandte Informationen

"Connectors mit Ordnern und Projekten verknüpfen".

Verwandte Informationen

- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "
- "Erste Schritte mit BlueXP IAM"
- "Erfahren Sie mehr über die API für BlueXP IAM"

Organisations- und Projekt-IDs

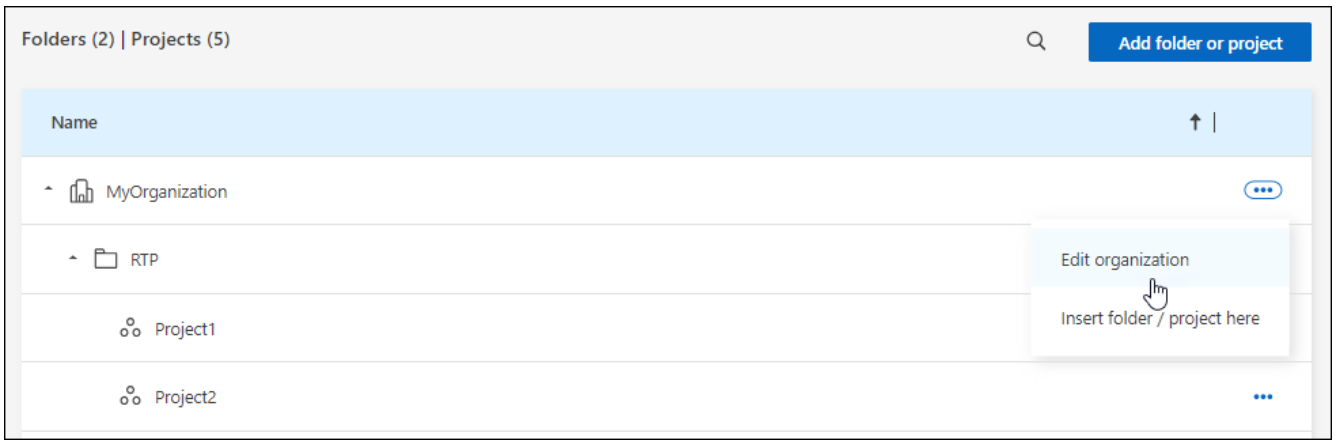
Ihre BlueXP -Organisation hat einen Namen und eine ID. Sie können einen Namen für Ihr Unternehmen auswählen, um ihn in Ihrer BlueXP -Bereitstellung zu identifizieren. Möglicherweise müssen Sie auch die Organisations-ID für bestimmte Integrationen abrufen.

Benennen Sie Ihre Organisation um

Sie können Ihre Organisation in BlueXP umbenennen. Dies ist hilfreich, wenn Sie mehr als nur das Unternehmen in Ihrer BlueXP Implementierung unterstützen.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Navigieren Sie auf der Seite **Organisation** zur ersten Zeile in der Tabelle, wählen Sie ••• und wählen Sie dann **Organisation bearbeiten** aus.



3. Geben Sie einen neuen Organisationsnamen ein und wählen Sie **Anwenden**.

Rufen Sie die Organisations-ID ab

Die Organisations-ID wird für bestimmte Integrationen mit BlueXP verwendet.

Sie können die Organisations-ID auf der Seite „Organisationen“ anzeigen und für Ihre Anforderungen in die Zwischenablage kopieren.

Schritte

1.

Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.

2. Wählen Sie die Registerkarte **Organisation**, um die Seite **Organisation** anzuzeigen.
3. Suchen Sie auf der Seite **Organisation** in der Übersichtsleiste nach Ihrer Organisations-ID und kopieren Sie diese in die Zwischenablage. Sie können diese für eine spätere Verwendung speichern oder direkt an die gewünschten Stellen kopieren.

Die ID für ein Projekt abrufen

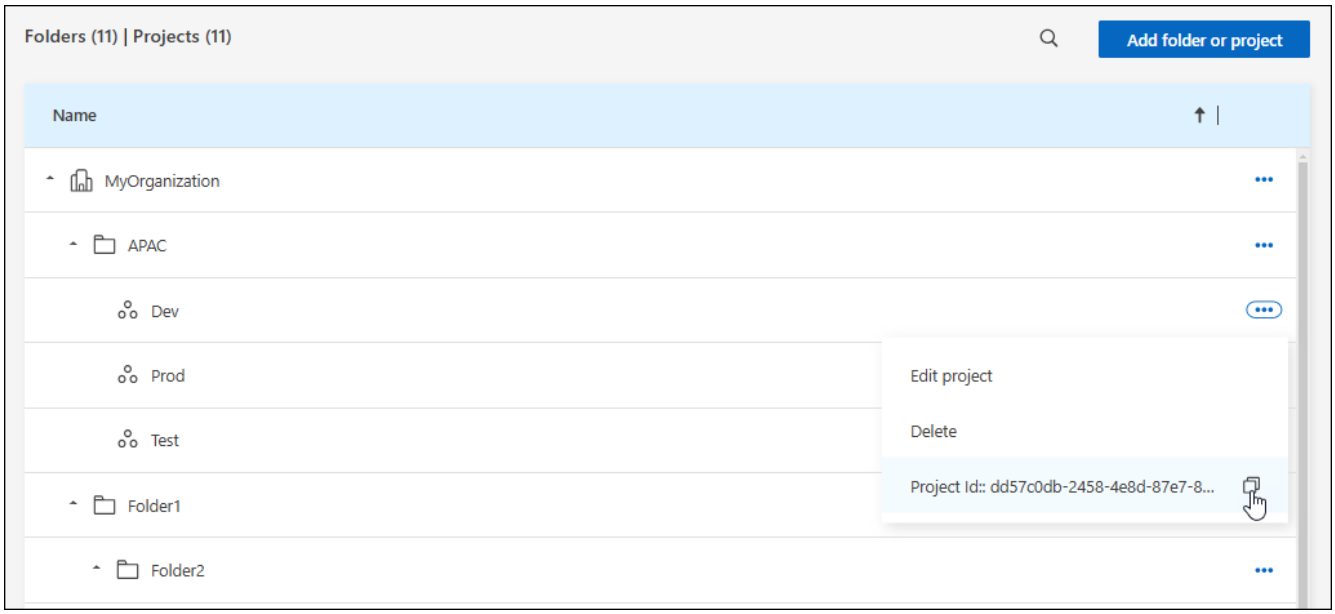
Wenn Sie die BlueXP -API verwenden, benötigen Sie möglicherweise die ID für ein Projekt. Beispiel: Beim Erstellen einer Cloud Volumes ONTAP-Arbeitsumgebung.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt in der Tabelle und wählen Sie aus •••

   Die Projekt-ID wird angezeigt.

2. Um die ID zu kopieren, wählen Sie die Schaltfläche Kopieren.



Verwandte Informationen

- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "
- "Erste Schritte mit BlueXP IAM"
- "Erfahren Sie mehr über die API für BlueXP IAM"

Überwachen oder prüfen Sie die IAM-Aktivität über den BlueXP -Zeitplan

Wenn Sie eine Aktion überwachen oder überwachen müssen, die über das BlueXP -Identitäts- und Zugriffsmanagement (IAM) abgeschlossen wurde, können Sie Details in der BlueXP -Zeitleiste anzeigen. Sie können beispielsweise überprüfen, wer ein Mitglied zu einer Organisation hinzugefügt hat oder ob ein Projekt erfolgreich gelöscht wurde.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Zeitleiste** aus  .
2. Wählen Sie aus den Filtern **Service** und dann **Tenancy** aus.
3. Verwenden Sie einen der anderen Filter, um zu ändern, welche Aktionen in der Tabelle angezeigt werden.

   Zum Beispiel können Sie den Filter **User** verwenden, um Aktionen anzuzeigen, die mit einem bestimmten Benutzerkonto zusammenhängen.

Ergebnis

Die Zeitleiste wird aktualisiert, um Ihnen abgeschlossene Verwaltungsaktionen im Zusammenhang mit BlueXP IAM anzuzeigen.

Zugriffsrollen für BlueXP

Informieren Sie sich über Zugriffsrollen von BlueXP

Das Identitäts- und Zugriffsmanagement (IAM) von BlueXP umfasst vordefinierte Rollen, die Sie den Mitgliedern Ihrer Organisation auf verschiedenen Ebenen Ihrer Ressourcenhierarchie zuweisen können. Bevor Sie diese Rollen zuweisen, sollten Sie die Berechtigungen verstehen, die jede Rolle beinhaltet. Die Rollen lassen sich in folgende Kategorien einteilen: Plattform, Applikation und Datenservice.

Plattformrollen

Plattformrollen gewähren alle BlueXP Administrationsberechtigungen, einschließlich der Rollenzuweisung und Benutzeranlegung. Plattformrollen ermöglichen den Zugriff auf alle BlueXP Datendienste und -Anwendungen. BlueXP IAM umfasst zwei Plattformrollen: Organisationsadministrator und Ordner- oder Projektadministrator. Der Hauptunterschied zwischen den beiden BlueXP IAM-Plattformrollen ist der Umfang.

Plattformrolle	Zuständigkeiten
"Organisationsadministrator"	Ermöglicht einem Benutzer uneingeschränkten Zugriff auf alle Projekte und Ordner innerhalb einer Organisation, das Hinzufügen von Mitgliedern zu jedem Projekt oder Ordner sowie das Ausführen beliebiger BlueXP -Aufgaben und die Verwendung beliebiger Datendienste, denen keine explizite Rolle zugeordnet ist. Benutzer mit dieser Rolle organisieren und verwalten Ihre BlueXP -Organisation. Sie erstellen Ordner und Projekte, weisen Rollen zu, fügen Benutzer hinzu und können alle Arbeitsumgebungen verwalten, sofern sie über die entsprechenden Anmeldeinformationen verfügen. Dies ist die einzige Zugriffsrolle, die Connectors erstellen kann.
"Ordner- oder Projektadministrator"	Ermöglicht einem Benutzer uneingeschränkten Zugriff auf bestimmte Projekte und Ordner, denen er zugewiesen ist. Sie können Mitglieder zu Ordnern oder Projekten hinzufügen, die sie verwalten, sowie beliebige BlueXP -Aufgaben ausführen und beliebige Datendienste oder Anwendungen auf Ressourcen innerhalb des Ordners oder Projekts verwenden, denen sie zugewiesen sind. Ordner- oder Projektadministratoren können keine Konnektoren erstellen.

Plattformrolle	Zuständigkeiten
"Föderationsadministrator"	Ermöglicht einem Benutzer das Erstellen und Verwalten von Föderationen mit BlueXP, wodurch Single-Sign-On (SSO) ermöglicht wird.
"Föderationsbetrachter"	Ermöglicht einem Benutzer, vorhandene Föderationen mit BlueXP anzuzeigen. Föderationen können nicht erstellt oder verwaltet werden

Anwendungsrollen

Im Folgenden finden Sie eine Liste der Rollen in der Anwendungskategorie. Jede Rolle gewährt bestimmte Berechtigungen innerhalb ihres festgelegten Umfangs. Benutzer, die nicht über die erforderliche Anwendungsrolle oder eine Plattformrolle verfügen, können nicht auf die Anwendung zugreifen.

Anwendungsrolle	Zuständigkeiten
"Google Cloud NetApp Volumes Administrator"	Benutzer mit der Rolle „Google Cloud NetApp Volumes“ können Google Cloud NetApp Volumes erkennen und verwalten.
"Keystone Admin"	Benutzer mit der Keystone Administratorrolle können Serviceanfragen erstellen. Ermöglicht Benutzern das Monitoring und Anzeigen von Nutzungsinformationen, Ressourcen und Administratorinformationen innerhalb des Keystone Mandanten, auf den sie zugreifen.
"Keystone Viewer"	Benutzer mit der Keystone-Viewer-Rolle KÖNNEN KEINE Serviceanfragen erstellen. Ermöglicht Benutzern das Monitoring und Anzeigen von Nutzungsinformationen, Ressourcen und Administratorinformationen innerhalb des Keystone Mandanten, auf den sie zugreifen.
ONTAP Mediator-Setup-Rolle	Servicekonten mit der Setup-Rolle ONTAP Mediator können Serviceanfragen erstellen. Diese Rolle ist in einem Servicekonto erforderlich, um eine Instanz des "ONTAP Cloud Mediator" .
"Betriebsunterstützungsanalyst"	Bietet Zugriff auf Warn- und Überwachungstools sowie die Möglichkeit, Supportfälle einzugeben und zu verwalten.
"Storage-Admin"	Verwaltung von Storage-Zustands- und Governance-Funktionen, Erkennung von Storage-Ressourcen sowie Ändern und Löschen vorhandener Arbeitsumgebungen
"Storage-Prüfer"	Zeigen Sie den Speicherzustand und die Governance-Funktionen an und zeigen Sie zuvor erkannte Speicherressourcen an. Vorhandene Speicherarbeitsumgebungen können nicht erkannt, geändert oder gelöscht werden.
"Spezialist für den Systemzustand"	Verwaltung von Storage- und Funktionszustands- und Governance-Funktionen; alle Berechtigungen des Storage-Administrators außer bestehende Arbeitsumgebungen können nicht geändert oder gelöscht werden.

Datenservice-Rollen

Nachfolgend finden Sie eine Liste der Rollen in der Datenservicekategorie. Jede Rolle gewährt bestimmte Berechtigungen innerhalb ihres festgelegten Umfangs. Benutzer, die nicht über die erforderliche Rolle für den Datenservice oder eine Plattformfunktion verfügen, können nicht auf den Datenservice zugreifen.

Datenservice-Rolle	Zuständigkeiten
"Superadministrator für Sicherung und Wiederherstellung"	Führen Sie beliebige Aktionen im Sicherungs- und Wiederherstellungsdienst aus.
"Backup- und Wiederherstellungsadministrator"	Führen Sie Sicherungen auf lokalen Snapshots durch, replizieren Sie auf sekundären Speicher und sichern Sie auf Objektspeicher.
"Administrator für die Wiederherstellung von Backup und Wiederherstellung"	Stellen Sie Workloads im Sicherungs- und Wiederherstellungsdienst wieder her.
"Backup- und Wiederherstellungsklon-Administrator"	Klonen Sie Anwendungen und Daten im Sicherungs- und Wiederherstellungsdienst.
"Backup- und Wiederherstellungs-Viewer"	Informationen zur Sicherung und Wiederherstellung anzeigen.
"Notfallwiederherstellungsadministrator"	Führen Sie beliebige Aktionen im Disaster Recovery-Dienst durch.
"Administrator für Notfallwiederherstellungs-Failover"	Führen Sie Failover und Migrationen durch.
"Administrator der Notfallwiederherstellungsanwendung"	Erstellen Sie Replikationspläne, ändern Sie Replikationspläne und starten Sie Test-Failover.
"Disaster Recovery-Viewer"	Nur Informationen anzeigen.
Klassifizierungsanzeige	Bietet die Möglichkeit, die Ergebnisse des BlueXP classification anzuzeigen. Benutzer mit dieser Rolle können Compliance-Informationen anzeigen und Berichte für Ressourcen erstellen, auf die sie zugreifen dürfen. Diese Benutzer können das Scannen von Volumes, Buckets oder Datenbankschemas nicht aktivieren oder deaktivieren. Klassifizierung hat keine Viewer-Rolle.
"Administrator für Ransomware-Schutz"	Verwalten Sie Aktionen auf den Registerkarten Schützen, Warnungen, Wiederherstellen, Einstellungen und Berichte des Ransomware-Schutz-Service.
"Viewer für Ransomware-Schutz"	Anzeigen von Workload-Daten, Anzeigen von Warnungsdaten, Herunterladen von Wiederherstellungsdaten und Herunterladen von Berichten im Ransomware-Schutzdienst.
SnapCenter-Admin	Bietet die Möglichkeit, Snapshots aus lokalen ONTAP Clustern mithilfe von BlueXP Backup und Recovery für Applikationen zu sichern. Ein Mitglied mit dieser Rolle kann die folgenden Aktionen in BlueXP ausführen: * Alle Aktionen unter „Sicherung und Wiederherstellung > Anwendungen“ ausführen * Alle Arbeitsumgebungen in den Projekten und Ordnern verwalten, für die es Berechtigungen hat * Alle BlueXP-Dienste verwenden SnapCenter hat keine Viewer-Rolle.

Weiterführende Links

- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "
- "Erste Schritte mit BlueXP IAM"
- "Verwalten von BlueXP -Mitgliedern und deren Berechtigungen"
- "Erfahren Sie mehr über die API für BlueXP IAM"

Zugriffsrollen für die BlueXP -Plattform

Weisen Sie Benutzern Plattformrollen zu, um ihnen Berechtigungen zum Ausführen von Verwaltungsaufgaben in BlueXP zu erteilen, Rollen zuzuweisen, Benutzer hinzuzufügen, Konnektoren zu erstellen und Föderationen zu verwalten.

Beispiel für Organisationsrollen in BlueXP für eine große multinationale Organisation

Die XYZ Corporation organisiert den Datenspeicherzugriff nach Regionen – Nordamerika, Europa und Asien-Pazifik – und bietet regionale Kontrolle mit zentraler Aufsicht.

Der **Organisationsadministrator** in BlueXP der XYZ Corporation erstellt eine anfängliche Organisation und separate Ordner für jede Region. Der **Ordner- oder Projektadministrator** für jede Region organisiert Projekte (mit zugehörigen Ressourcen) innerhalb des Ordners der Region.

Regionale Administratoren mit der Rolle **Ordner- oder Projektadministrator** verwalten ihre Ordner aktiv, indem sie Ressourcen und Benutzer hinzufügen. Diese regionalen Administratoren können auch von ihnen verwaltete Ordner und Projekte hinzufügen, entfernen oder umbenennen. Der **Organisationsadministrator** erbt Berechtigungen für alle neuen Ressourcen und behält so die Übersicht über die Speichernutzung in der gesamten Organisation.

Innerhalb derselben Organisation wird einem Benutzer die Rolle **Föderationsadministrator** zugewiesen, um die Föderation der Organisation mit ihrem Unternehmens-IdP zu verwalten. Dieser Benutzer kann föderierte Organisationen hinzufügen oder entfernen, kann jedoch keine Benutzer oder Ressourcen innerhalb der Organisation verwalten. Der **Organisationsadministrator** weist einem Benutzer die Rolle **Föderationsbetrachter** zu, um den Föderationsstatus zu überprüfen und föderierte Organisationen anzuzeigen.

Die folgenden Tabellen zeigen die Aktionen, die jede BlueXP Plattformrolle ausführen kann.

Rollen in der Organisationsverwaltung

Aufgabe	Organisationsadministrator	Ordner- oder Projektadministrator
Anschlüsse Erstellen	Ja.	Nein
Erstellen, Ändern oder Löschen von Arbeitsumgebungen (Hinzufügen oder Erkennen neuer Ressourcen über den BlueXP -Bildschirm)	Ja.	Ja.
Erstellen Sie Ordner und Projekte, einschließlich Löschen	Ja.	Nein
Umbenennen vorhandener Ordner und Projekte	Ja.	Ja.
Rollen zuweisen und Benutzer hinzufügen	Ja.	Ja.
Ressourcen mit Ordnern und Projekten verknüpfen	Ja.	Ja.

Aufgabe	Organisationsadministrator	Ordner- oder Projektadministrator
Connectors mit Ordnern und Projekten verknüpfen	Ja.	Nein
Entfernen Sie Connectors aus Ordnern und Projekten	Ja.	Nein
Connectors verwalten (Zertifikate, Einstellungen usw. bearbeiten)	Ja.	Nein
Verwalten Sie Anmeldeinformationen über Einstellungen > Anmeldeinformationen	Ja.	Ja.
Erstellen, Verwalten und Anzeigen von Föderationen	Ja.	Nein
Registrieren Sie sich für Support und reichen Sie Fälle über BlueXP ein	Ja.	Ja.
Datendienste nutzen	Ja.	Ja.
Sehen Sie sich die BlueXP Zeitleiste und -Benachrichtigungen an	Ja.	Ja.

Föderationsrollen

Aufgabe	Föderationsadministrator	Föderationsbetrachter
Erstellen einer Föderation	Ja.	Nein
Verifizieren einer Domäne	Ja.	Nein
Hinzufügen einer Domäne zu einem Verbund	Ja.	Nein
Deaktivieren und Löschen von Föderationen	Ja.	Nein
Testverbände	Ja.	Nein
Verbände und ihre Details anzeigen	Ja.	Ja.

Anwendungsrollen

Keystone Zugriffsrollen für BlueXP

Keystone Rollen bieten Zugriff auf die Keystone Dashboards und ermöglichen Benutzern das Anzeigen und Managen ihres Keystone Abonnements. Es gibt zwei Keystone Rollen: Keystone Administrator und Keystone Viewer. Der Hauptunterschied zwischen den beiden Rollen ist die Aktionen, die sie in Keystone ergreifen können. Die Keystone-Administratorrolle ist die einzige Rolle, die erlaubt ist, Serviceanfragen zu erstellen oder Abonnements zu ändern.

Beispiel für Keystone-Rollen in BlueXP

Bei der XYZ Corporation sind vier Speicheringenieure aus verschiedenen Abteilungen damit beschäftigt, die Keystone-Abonnementinformationen anzuzeigen. Obwohl alle diese Benutzer das Keystone Abonnement überwachen müssen, darf nur der Teamleiter Serviceanfragen stellen. Drei der Teammitglieder erhalten die Rolle **Keystone Viewer**, während der Teamleiter die Rolle **Keystone Admin** erhält, so dass ein Kontrollpunkt für Serviceanfragen für das Unternehmen besteht.

Die folgende Tabelle zeigt die Aktionen, die die einzelnen Keystone Rollen durchführen können.

Funktion und Aktion	Keystone Admin	Keystone Viewer
Zeigen Sie die folgenden Registerkarten an: Abonnement, Assets, Monitor und Administration	Ja.	Ja.
Keystone Abonnementseite:		
Abonnements anzeigen	Ja.	Ja.
Abonnements ändern oder erneuern	Ja.	Nein
Seite „Keystone Assets“:		
Assets anzeigen	Ja.	Ja.
Verwalten von Assets	Ja.	Nein
Keystone-Alerts-Seite:		
Anzeigen von Meldungen	Ja.	Nein
Verwalten von Meldungen	Ja.	Nein
Erstellen Sie Warnmeldungen für sich selbst.	Ja.	Ja.
Digital Wallet:		
Digital Wallet anzeigen können	Ja.	Ja.
Keystone-Berichtsseite:		
Berichte herunterladen	Ja.	Ja.
Verwalten von Berichten	Ja.	Ja.
Erstellen Sie Berichte für sich selbst.	Ja.	Ja.
Serviceanfragen:		
Erstellen Sie Serviceanfragen	Ja.	Nein
Service-Requests anzeigen, die von einem beliebigen Benutzer innerhalb der Organisation erstellt wurden	Ja.	Ja.

Zugriffsrolle „Operational Support Analyst“ für BlueXP

Sie können Benutzern die folgende Rolle zuweisen, um ihnen Zugriff auf Warnungen und Überwachung zu gewähren. Benutzer mit dieser Rolle können auch Supportfälle eröffnen.

Analyst für operative Unterstützung

Aufgabe	Kann durchführen
Verwalten Sie Ihre eigenen Benutzeranmeldeinformationen unter „Einstellungen > Anmeldeinformationen“.	Ja.
Erkannte Ressourcen anzeigen	Ja.
Registrieren Sie sich für Support und reichen Sie Fälle über BlueXP ein	Ja.
Sehen Sie sich die BlueXP Zeitleiste und -Benachrichtigungen an	Ja.
Anzeigen, Herunterladen und Konfigurieren von Warnungen	Ja.

Storage-Zugriffsrollen für BlueXP

Sie können Benutzern folgende Rollen zuweisen, um ihnen Zugriff auf die Storage-Managementfunktionen in BlueXP zu ermöglichen, die mit unterstützten Speicherressourcen verknüpft sind. Sie können Benutzern eine Administratorrolle zum Verwalten des Speichers oder eine Viewer-Rolle zum Überwachen zuweisen.

Diese Rollen sind über die BlueXP-Partnerschafts-API nicht verfügbar.

Administratoren können Benutzern Speicherrollen für die folgenden Speicherressourcen und -funktionen zuweisen:

Storage-Ressourcen:

- On-Premises ONTAP Cluster
- StorageGRID
- E-Series

BlueXP Services und Funktionen:

- Digitaler Berater
- Software-Updates
- Wirtschaftliche Effizienz
- Nachhaltigkeit

Beispiel für Storage-Rollen in BlueXP

Bei der XYZ Corporation, einem multinationalen Unternehmen, gibt es ein großes Team aus Storage Engineers und Storage-Administratoren. Sie ermöglichen diesem Team die Verwaltung von Speicherressourcen für ihre Regionen und beschränken gleichzeitig den Zugriff auf zentrale BlueXP-Aufgaben wie Benutzerverwaltung, Connector-Erstellung und Kostentools wie die digitale Geldbörse.

In einem Team von 12 Benutzern wird die Rolle **Storage Viewer** zugewiesen, mit der sie die Speicherressourcen für die BlueXP -Projekte überwachen können, denen sie zugewiesen sind. Die restlichen neun erhalten die Rolle **Speicheradministrator**, die die Möglichkeit beinhaltet, Softwareupdates zu verwalten, über BlueXP auf ONTAP-System-Manager zuzugreifen sowie Speicherressourcen zu erkennen (funktionierende Umgebungen hinzufügen). Eine Person im Team erhält die Rolle **Systemgesundheitsspezialist**, damit sie den Zustand der Speicherressourcen in ihrer Region verwalten können, aber keine Arbeitsumgebungen ändern oder löschen können. Diese Person kann auch Software-Updates für die Speicherressourcen für Projekte durchführen, denen sie zugewiesen sind.

Die Organisation hat zwei zusätzliche Benutzer mit der Rolle **Organisationsadministrator**, die alle Aspekte von BlueXP verwalten können, einschließlich Benutzerverwaltung, Connector-Erstellung und Kostenmanagement-Tools wie Digital Wallet, sowie mehrere Benutzer mit der Rolle **Ordner oder Projektadministrator**, die BlueXP -Verwaltungsaufgaben für die Ordner und Projekte, denen sie zugewiesen sind, durchführen können.

Die folgende Tabelle zeigt die Aktionen, die jede BlueXP-Speicherrolle ausführt.

Funktion und Aktion	**Storage-Admin**	**Spezialist für den Systemzustand**	**Storage-Prüfer**
* Leinwand*:			
Neue Ressourcen entdecken (neue Arbeitsumgebung schaffen)	Ja.	Ja.	Nein
Erkannte Ressourcen anzeigen	Ja.	Ja.	Nein
Arbeitsumgebungen löschen	Ja.	Nein	Nein
Ändern von Arbeitsumgebungen	Ja.	Nein	Nein
Connector Erstellen	Nein	Nein	Nein
Digitale Beraterin			
Alle Seiten und Funktionen anzeigen	Ja.	Ja.	Ja.
Digital Wallet			
Alle Seiten und Funktionen anzeigen	Nein	Nein	Nein
Software-Updates			
Landing Page und Empfehlungen anzeigen	Ja.	Ja.	Ja.
Besprechen Sie mögliche Versionsempfehlungen und die wichtigsten Vorteile	Ja.	Ja.	Ja.
Anzeigen von Aktualisierungsdetails für ein Cluster	Ja.	Ja.	Ja.

Funktion und Aktion	Storage-Admin	Spezialist für den Systemzustand	Storage-Prüfer
Führen Sie Prüfungen vor dem Update durch, und laden Sie den Upgrade-Plan herunter	Ja.	Ja.	Ja.
Installieren Sie Softwareupdates	Ja.	Ja.	Nein
Wirtschaftliche Effizienz			
Überprüfen Sie den Kapazitätsplanungsstatus	Ja.	Ja.	Ja.
Nächste Aktion auswählen (Best Practice, Stufe)	Ja.	Nein	Nein
Tiering selten genutzter Daten in den Cloud-Storage und Freigabe des Storage –	Ja.	Ja.	Nein
Erinnerungen einrichten	Ja.	Ja.	Ja.
Nachhaltigkeit			
Dashboard und Empfehlungen anzeigen	Ja.	Ja.	Ja.
Berichtdaten herunterladen	Ja.	Ja.	Ja.
Bearbeiten Sie den Prozentsatz der CO2-Minderung	Ja.	Ja.	Nein
Empfehlungen festlegen	Ja.	Ja.	Nein
Empfehlungen zurückstellen	Ja.	Ja.	Nein
Zugang zum System Manager			
Kann Anmeldeinformationen eingeben	Ja.	Ja.	Nein
Anmeldeinformationen			
Benutzeranmeldeinformationen	Ja.	Ja.	Nein

Datenservices

BlueXP backup and recovery und Wiederherstellungsrollen

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf den Backup- und Recovery-Dienst in BlueXP zu gewähren. Backup- und Recovery-Rollen bieten Ihnen die Flexibilität, Benutzern spezifische Rollen für die Aufgaben zuzuweisen, die sie in Ihrem Unternehmen erledigen müssen. Die Rollenzuweisung hängt von Ihren Geschäfts- und Speicherverwaltungspraktiken ab.

Für die Sicherung und Wiederherstellung werden die folgenden Rollen verwendet:

- **Superadministrator für Sicherung und Wiederherstellung**: Führen Sie beliebige Aktionen aus.
- **Backup- und Wiederherstellungsadministrator**: Führen Sie Sicherungen auf lokalen Snapshots durch, replizieren Sie auf sekundären Speicher und sichern Sie auf Objektspeicher.
- **Administrator für Backup- und Wiederherstellungswiederherstellung**: Workloads wiederherstellen.
- **Backup- und Wiederherstellungsklon-Administrator**: Klonen Sie Anwendungen und Daten.
- **Backup- und Wiederherstellungs-Viewer**: Zeigen Sie Backup- und Wiederherstellungsinformationen an.

In der folgenden Tabelle sind die Aktionen aufgeführt, die jede Rolle ausführen kann.

Funktion und Aktion	Superadministrator für Sicherung und Wiederherstellung	Backup-Admin	Administrator wiederherstellen	Klonadministrator	Prüfer
Hosts hinzufügen, bearbeiten oder löschen	Ja.	Nein	Nein	Nein	Nein
Plugins installieren	Ja.	Nein	Nein	Nein	Nein
Anmeldeinformationen hinzufügen (Host, Instanz, vCenter)	Ja.	Nein	Nein	Nein	Nein
Dashboard und alle Registerkarten anzeigen	Ja.	Ja.	Ja.	Ja.	Ja.
Kostenlos testen	Ja.	Nein	Nein	Nein	Nein
Beginnen Sie mit der Erkennung von Workloads	Nein	Ja.	Ja.	Ja.	Nein
Lizenzinformationen anzeigen	Ja.	Ja.	Ja.	Ja.	Ja.
Lizenz aktivieren	Ja.	Nein	Nein	Nein	Nein
Hosts anzeigen	Ja.	Ja.	Ja.	Ja.	Ja.
Zeitpläne:					
Zeitpläne aktivieren	Ja.	Ja.	Ja.	Ja.	Nein
Zeitpläne aussetzen	Ja.	Ja.	Ja.	Ja.	Nein
Richtlinien und Schutz:					
Schutzpläne anzeigen	Ja.	Ja.	Ja.	Ja.	Ja.

Funktion und Aktion	Superadministrator für Sicherung und Wiederherstellung	Backup-Admin	Administrator wiederherstellen	Klonadministrator	Prüfer
Erstellen, Ändern oder Löschen von Schutzplänen	Ja.	Ja.	Nein	Nein	Nein
Wiederherstellen von Workloads	Ja.	Nein	Ja.	Nein	Nein
Erstellen, Teilen oder Löschen von Klonen	Ja.	Nein	Nein	Ja.	Nein
Richtlinie erstellen, ändern oder löschen	Ja.	Ja.	Nein	Nein	Nein
Berichte:					
Berichte anzeigen	Ja.	Ja.	Ja.	Ja.	Ja.
Erstellen von Berichten	Ja.	Ja.	Ja.	Ja.	Nein
Berichte löschen	Ja.	Nein	Nein	Nein	Nein
Von SnapCenter importieren und Host verwalten:					
Importierte SnapCenter -Daten anzeigen	Ja.	Ja.	Ja.	Ja.	Ja.
Daten aus SnapCenter importieren	Ja.	Ja.	Nein	Nein	Nein
Host verwalten (migrieren)	Ja.	Ja.	Nein	Nein	Nein
Einstellungen konfigurieren:					
Protokollverzeichnis konfigurieren	Ja.	Ja.	Ja.	Nein	Nein
Instanzanmeldeinformationen zuordnen oder entfernen	Ja.	Ja.	Ja.	Nein	Nein
Eimer:					
Speicherbereiche anzeigen	Ja.	Ja.	Ja.	Ja.	Ja.
Erstellen, Bearbeiten oder Löschen von Speicher-Buckets	Ja.	Ja.	Nein	Nein	Nein

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf die Katastrophenwiederherstellung innerhalb von BlueXP zu gewähren. Mithilfe von Disaster-Recovery-Rollen können Sie Benutzern flexibel Rollen zuweisen, die speziell auf die Aufgaben zugeschnitten sind, die sie in Ihrem Unternehmen erledigen müssen. Wie Sie Rollen zuweisen, hängt von Ihren eigenen Geschäfts- und Speicherverwaltungspraktiken ab.

Bei der Notfallwiederherstellung werden die folgenden Rollen verwendet:

- **Notfallwiederherstellungsadministrator**: Führen Sie beliebige Aktionen aus.
- **Disaster Recovery-Failover-Administrator**: Führen Sie Failover und Migrationen durch.
- **Administrator der Notfallwiederherstellungsanwendung**: Replikationspläne erstellen. Replikationspläne ändern. Test-Failover starten.
- **Disaster Recovery Viewer**: Nur Informationen anzeigen.

In der folgenden Tabelle sind die Aktionen aufgeführt, die jede Rolle ausführen kann.

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Dashboard und alle Registerkarten anzeigen	Ja.	Ja.	Ja.	Ja.
Kostenlos testen	Ja.	Nein	Nein	Nein
Beginnen Sie mit der Erkennung von Workloads	Ja.	Nein	Nein	Nein
Lizenzinformationen anzeigen	Ja.	Ja.	Ja.	Ja.
Lizenz aktivieren	Ja.	Nein	Ja.	Nein
Auf der Registerkarte „Sites“:				
Websites anzeigen	Ja.	Ja.	Ja.	Ja.
Websites hinzufügen, ändern oder löschen	Ja.	Nein	Nein	Nein
Auf der Registerkarte Replikationspläne:				
Anzeigen von Replikationsplänen	Ja.	Ja.	Ja.	Ja.
Anzeigen von Replikationsplandetails	Ja.	Ja.	Ja.	Ja.
Erstellen oder Ändern von Replikationsplänen	Ja.	Ja.	Ja.	Nein

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Erstellen von Berichten	Ja.	Nein	Nein	Nein
Snapshots anzeigen	Ja.	Ja.	Ja.	Ja.
Durchführen von Failover-Tests	Ja.	Ja.	Ja.	Nein
Durchführen von Failovern	Ja.	Ja.	Nein	Nein
Durchführen von Failbacks	Ja.	Ja.	Nein	Nein
Migrationen durchführen	Ja.	Ja.	Nein	Nein
Auf der Registerkarte „Ressourcengruppen“:				
Anzeigen von Ressourcengruppen	Ja.	Ja.	Ja.	Ja.
Erstellen, Ändern oder Löschen von Ressourcengruppen	Ja.	Nein	Ja.	Nein
Auf der Registerkarte „Jobüberwachung“:				
Jobs anzeigen	Ja.	Nein	Ja.	Ja.
Aufträge abbrechen	Ja.	Ja.	Ja.	Nein

Zugriffsrollen für Ransomware-Schutz für BlueXP

Ransomware-Rollen ermöglichen Benutzern den Zugriff auf den Ransomware-Schutzdienst. Die beiden Rollen sind Ransomware Protection Admin und Ransomware Protection Viewer. Der Hauptunterschied zwischen den beiden Rollen sind die Aktionen, die sie zum Schutz vor Ransomware ergreifen können.

Die folgende Tabelle zeigt die Aktionen, die jede BlueXP-Ransomware-Schutzrolle ausführen kann.

Funktion und Aktion	Administrator für Ransomware-Schutz	Viewer für Ransomware-Schutz
Dashboard und alle Registerkarten anzeigen	Ja.	Ja.
Kostenlos testen	Ja.	Nein
Workloads erkennen	Ja.	Nein

Funktion und Aktion	Administrator für Ransomware-Schutz	Viewer für Ransomware-Schutz
Auf der Registerkarte Schutz:		
Richtlinien hinzufügen, ändern oder löschen	Ja.	Nein
Schutz von Workloads	Ja.	Nein
Sensible Daten erkennen	Ja.	Nein
Bearbeiten Sie den Workload-Schutz	Ja.	Nein
Workload-Details anzeigen	Ja.	Ja.
Download von Daten	Ja.	Ja.
Auf der Registerkarte Warnungen:		
Anzeigen von Alarmdetails	Ja.	Ja.
Bearbeiten Sie den Ereignisstatus	Ja.	Nein
Anzeigen von Vorfalldetails	Ja.	Ja.
Vollständige Liste der betroffenen Dateien abrufen	Ja.	Nein
Warnmeldungen herunterladen	Ja.	Ja.
Auf der Registerkarte Wiederherstellen:		
Betroffene Dateien herunterladen	Ja.	Nein
Restore-Workload	Ja.	Nein
Wiederherstellungsdaten herunterladen	Ja.	Ja.
Berichte herunterladen	Ja.	Ja.
Auf der Registerkarte Einstellungen:		
Backup-Ziele hinzufügen oder ändern	Ja.	Nein
SIEM-Ziele hinzufügen oder ändern	Ja.	Nein
Auf der Registerkarte Berichte:		
Berichte herunterladen	Ja.	Ja.

Identitätsföderation

Aktivieren Sie Single Sign-On mithilfe von Identity Federation mit BlueXP

Single-Sign-On (Federation) vereinfacht den Anmeldevorgang und erhöht die Sicherheit, indem Benutzer sich mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden können. Sie können Single Sign-On (SSO) bei Ihrem Identitätsanbieter (IdP) oder über die NetApp Support-Website aktivieren.

Erforderliche Rolle

Organisationsadministrator, Föderationsadministrator, Föderationsbetrachter. "Erfahren Sie mehr über Zugriffsrollen."

Identitätsföderation mit der NetApp Support Site

Wenn Sie eine Verbindung mit der NetApp Support Site herstellen, können sich Benutzer mit denselben Anmeldeinformationen für den Zugriff auf BlueXP anmelden, die Sie für die NetApp Support Site, Active IQ Digital Advisor und andere mit Ihrem NetApp Support Site-Konto verknüpfte Apps verwenden. Nachdem Sie die Föderation eingerichtet haben, können alle neuen Benutzer, die ein NetApp Support Site-Konto erstellen, auch auf BlueXP zugreifen.

> Wenn Sie eine Verbindung mit der NetApp Support-Site herstellen, ist dies nicht gleichzeitig mit Ihrem Corporate Identity Management-Anbieter möglich. Wählen Sie den Anbieter aus, der für Ihr Unternehmen am besten geeignet ist.

Schritte

1. Laden Sie das "Antragsformular für die NetApp Föderation" .
2. Senden Sie das Formular an die im Formular angegebene E-Mail-Adresse.

   Das NetApp Supportteam prüft und bearbeitet Ihre Anfrage.

Richten Sie eine Verbundverbindung mit Ihrem Identitätsanbieter ein

Sie können eine Verbundverbindung mit Ihrem Identitätsanbieter einrichten, um Single Sign-On (SSO) für BlueXP zu aktivieren. Dazu konfigurieren Sie Ihren Identitätsanbieter so, dass er NetApp als Dienstanbieter vertraut, und erstellen anschließend die Verbindung in BlueXP.

> Wenn Sie die Föderation zuvor mit NetApp Cloud Central (einer externen Anwendung für BlueXP) konfiguriert haben, müssen Sie Ihre Föderation mithilfe der BlueXP -Föderationsseite importieren, um sie innerhalb von BlueXP verwalten zu können."Erfahren Sie, wie Sie Ihre Föderation importieren."

Unterstützte Identitätsanbieter

NetApp unterstützt die folgenden Protokolle und Identitätsanbieter für die Föderation:

Protokolle

- Security Assertion Markup Language (SAML)-Identitätsanbieter
- Active Directory-Verbunddienste (AD FS)

Identitätsanbieter

- Microsoft Entra-ID
- PingFederate

Föderation mit BlueXP Workflow

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in BlueXP eine Verbindung herstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Föderation mit Ihrer E-Mail-Domäne oder einer anderen Domäne, die Ihnen gehört, herstellen. Um eine Föderation mit einer anderen Domäne als Ihrer E-Mail-Domäne herzustellen, bestätigen Sie zunächst, dass Sie der Eigentümer der Domäne sind.

Bestätigen Sie Ihre Domäne (falls Sie nicht Ihre E-Mail-Domäne verwenden)

Um eine Föderation mit einer anderen Domäne als Ihrer E-Mail-Domäne herzustellen, bestätigen Sie, dass Sie deren Eigentümer sind. Sie können Ihre E-Mail-Domäne ohne zusätzliche Schritte föderieren.

Konfigurieren Sie Ihren IdP so, dass er NetApp als Serviceprovider vertraut

Konfigurieren Sie Ihren Identitätsanbieter so, dass er NetApp vertraut, indem Sie eine neue Anwendung erstellen und die erforderlichen Informationen angeben, z. B. die ACS-URL, die Entitäts-ID oder andere Anmeldeinformationen. Die Informationen zum Dienstanbieter variieren je nach Identitätsanbieter. Weitere Informationen finden Sie in der Dokumentation Ihres spezifischen Identitätsanbieters. Sie müssen mit Ihrem IdP-Administrator zusammenarbeiten, um diesen Schritt abzuschließen.

Erstellen Sie die Verbundverbindung in BlueXP

Um die Verbindung herzustellen, müssen Sie die erforderlichen Informationen von Ihrem Identitätsanbieter bereitstellen, z. B. die SAML-Metadaten-URL oder -Datei. Diese Informationen werden verwendet, um die Vertrauensbeziehung zwischen BlueXP und Ihrem Identitätsanbieter herzustellen. Die von Ihnen bereitgestellten Informationen hängen von dem von Ihnen verwendeten IdP ab. Wenn Sie beispielsweise die Microsoft Entra ID verwenden, müssen Sie die Client-ID, das Geheimnis und die Domäne angeben.

Testen Sie Ihre Föderation in BlueXP

Testen Sie Ihre Verbundverbindung, bevor Sie sie aktivieren. Die Federation-Seite in BlueXP bietet eine Testoption, mit der Sie überprüfen können, ob sich Ihr Testbenutzer erfolgreich authentifizieren kann. Wenn der Test erfolgreich ist, können Sie die Verbindung aktivieren.

Aktivieren Sie Ihre Verbindung in BlueXP

Nachdem Sie die Verbindung aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden.

Sehen Sie sich zunächst das Thema für Ihr jeweiliges Protokoll oder Ihren IdP an:

- "Einrichten einer Verbundverbindung mit AD FS"

- "Einrichten einer Verbundverbindung mit der Microsoft Entra ID"
- "Einrichten einer Verbundverbindung mit PingFederate"
- "Einrichten einer Verbundverbindung mit einem SAML-Identitätsanbieter"

Domänenüberprüfung

Überprüfen Sie die E-Mail-Domäne für Ihre Verbundverbindung

Wenn Sie eine Föderation mit einer anderen Domäne als Ihrer E-Mail-Domäne durchführen möchten, müssen Sie zunächst bestätigen, dass Sie der Domäneninhaber sind. Sie können für die Föderation nur verifizierte Domänen verwenden.

Erforderliche Rollen

Organisationsadministrator oder Föderationsadministrator. "Erfahren Sie mehr über Zugriffsrollen."

Zur Verifizierung Ihrer Domäne fügen Sie den DNS-Einstellungen Ihrer Domäne einen TXT-Eintrag hinzu. Dieser Eintrag dient als Nachweis dafür, dass Sie die Domäne besitzen, und ermöglicht BlueXP , der Domäne für die Föderation zu vertrauen. Möglicherweise müssen Sie sich mit Ihrem IT- oder Netzwerkadministrator abstimmen, um diesen Schritt abzuschließen.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Wählen Sie **Domänenbesitz bestätigen**.
5. Geben Sie die Domäne ein, die Sie verifizieren möchten, und wählen Sie **Weiter**.
6. Kopieren Sie den bereitgestellten TXT-Eintrag.
7. Rufen Sie die DNS-Einstellungen Ihrer Domain auf und konfigurieren Sie den TXT-Wert, der als TXT-Eintrag für Ihre Domain bereitgestellt wurde. Wenden Sie sich bei Bedarf an Ihren IT- oder Netzwerkadministrator.
8. Nachdem der TXT-Eintrag hinzugefügt wurde, kehren Sie zu BlueXP zurück und wählen Sie **Überprüfen**.

Konfigurieren von Föderationen

Verbinden Sie BlueXP mit Active Directory Federation Services (AD FS)

Verbinden Sie Ihre Active Directory Federation Services (AD FS) mit BlueXP , um Single Sign-On (SSO) für BlueXP zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist ein Organisations- oder Föderationsadministrator erforderlich. Der Föderationsbetrachter kann die Föderationsseite anzeigen. "Erfahren Sie mehr über Zugriffsrollen."

Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, entweder das eine oder das andere zu wählen, aber nicht beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Konfigurieren Sie zunächst den Identitätsanbieter so, dass er BlueXP als Dienstanbieter vertraut. Erstellen Sie anschließend eine Verbindung in BlueXP mithilfe der Konfiguration Ihres Identitätsanbieters.

Sie können eine Föderation mit Ihrem AD FS-Server einrichten, um Single Sign-On (SSO) für BlueXP zu aktivieren. Dazu konfigurieren Sie Ihr AD FS so, dass BlueXP als Dienstanbieter vertraut, und erstellen anschließend die Verbindung in BlueXP.

Bevor Sie beginnen

- Sie benötigen ein IdP-Konto mit Administratorrechten. Sprechen Sie die Schritte mit Ihrem IdP-Administrator ab.
- Identifizieren Sie die Domäne, die Sie für die Föderation verwenden möchten. Sie können Ihre E-Mail-Domäne oder eine andere Domäne verwenden, die Sie besitzen. Wenn Sie eine andere Domäne als Ihre E-Mail-Domäne verwenden möchten, müssen Sie diese zunächst in BlueXP verifizieren. Folgen Sie dazu den Schritten im "Verifizieren Sie Ihre Domain in BlueXP" Thema.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Protokoll** und dann **Active Directory Federation Services (AD FS)**.
7. Wählen Sie **Weiter**.
8. Erstellen Sie eine Vertrauensstellung der vertrauenden Seite auf Ihrem AD FS-Server. Sie können PowerShell verwenden oder die Konfiguration manuell auf Ihrem AD FS-Server vornehmen. Weitere Informationen zum Erstellen einer Vertrauensstellung der vertrauenden Seite finden Sie in der AD FS-Dokumentation.
   a. Erstellen Sie die Vertrauensstellung mithilfe von PowerShell und dem folgenden Skript:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

   b. Alternativ können Sie die Vertrauensstellung manuell in der AD FS-Verwaltungskonsole erstellen.

Verwenden Sie beim Erstellen der Vertrauensstellung die folgenden BlueXP -Werte:

- Verwenden Sie beim Erstellen der Relying Trust Identifier den Wert **YOUR_TENANT**: `netapp-cloud-account`
- Wenn Sie **Unterstützung für WS-Federation aktivieren** auswählen, verwenden Sie den Wert **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`

c. Kopieren Sie nach dem Erstellen der Vertrauensstellung die Metadaten-URL von Ihrem AD FS-Server oder laden Sie die Verbundmetadatendatei herunter. Sie benötigen diese URL oder Datei, um die Verbindung in BlueXP herzustellen.

NetApp empfiehlt die Verwendung der Metadaten-URL, damit BlueXP automatisch die neueste AD FS-Konfiguration abruft. Wenn Sie die Federation-Metadatendatei herunterladen, müssen Sie sie bei Änderungen an Ihrer AD FS-Konfiguration manuell in BlueXP aktualisieren.

9. Kehren Sie zu BlueXP zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
10. Stellen Sie die Verbindung mit AD FS her.
    a. Geben Sie die **AD FS-URL** ein, die Sie im vorherigen Schritt von Ihrem AD FS-Server kopiert haben, oder laden Sie die Verbundmetadatendatei hoch, die Sie von Ihrem AD FS-Server heruntergeladen haben.
11. Wählen Sie **Verbindung erstellen**. Das Erstellen der Verbindung kann einige Sekunden dauern.
12. Wählen Sie **Weiter**.
13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zur Anmeldeseite Ihres IdP-Servers weitergeleitet. Melden Sie sich mit Ihren IdP-Anmeldedaten an, um den Test abzuschließen, und kehren Sie zu BlueXP zurück, um die Verbindung zu aktivieren.
14. Wählen Sie **Weiter**.
15. Überprüfen Sie auf der Seite **Föderation aktivieren** die Föderationsdetails und wählen Sie dann **Föderation aktivieren** aus.
16. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nachdem Sie die Föderation aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden.

Verbinden Sie BlueXP mit der Microsoft Entra ID

Verbinden Sie sich mit Ihrem Microsoft Entra ID IdP-Anbieter, um Single Sign-On (SSO) für BlueXP zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist ein Organisations- oder Föderationsadministrator erforderlich. Der Föderationsbetrachter kann die Föderationsseite anzeigen. "Erfahren Sie mehr über Zugriffsrollen."

Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, entweder das eine oder das andere zu wählen, aber nicht beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in BlueXP eine Verbindung herstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Verbundverbindung mit der Microsoft Entra ID einrichten, um Single Sign-On (SSO) für BlueXP zu aktivieren. Dazu konfigurieren Sie Ihre Microsoft Entra ID so, dass BlueXP als Dienstanbieter vertraut wird. Anschließend erstellen Sie die Verbindung in BlueXP.

Bevor Sie beginnen

- Sie benötigen ein IdP-Konto mit Administratorrechten. Sprechen Sie die Schritte mit Ihrem IdP-Administrator ab.
- Identifizieren Sie die Domäne, die Sie für die Föderation verwenden möchten. Sie können Ihre E-Mail-Domäne oder eine andere Domäne verwenden, die Sie besitzen. Wenn Sie eine andere Domäne als Ihre E-Mail-Domäne verwenden möchten, müssen Sie diese zunächst in BlueXP verifizieren. Folgen Sie dazu den Schritten im "Verifizieren Sie Ihre Domain in BlueXP" Thema.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie **Neue Föderation konfigurieren**.

Domänendetails

1. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
2. Wählen Sie **Weiter**.

Verbindungsmethode

1. Wählen Sie als Verbindungsmethode **Anbieter** und dann **Microsoft Entra ID**.
2. Wählen Sie **Weiter**.

Konfigurationshinweise

1. Konfigurieren Sie Ihre Microsoft Entra ID so, dass NetApp als Dienstanbieter vertraut. Dieser Schritt muss auf Ihrem Microsoft Entra ID-Server ausgeführt werden.
   a. Verwenden Sie die folgenden Werte, wenn Sie Ihre Microsoft Entra ID-App registrieren, um BlueXP zu vertrauen:
      - Verwenden Sie für die **Umleitungs-URL** `https://services.cloud.netapp.com`
      - Verwenden Sie für die **Antwort-URL** `https://netapp-cloud-account.auth0.com/login/callback`
   b. Erstellen Sie einen geheimen Clientschlüssel für Ihre Microsoft Entra ID-App. Sie müssen die Client-ID, den geheimen Clientschlüssel und den Entra ID-Domänennamen angeben, um die Föderation abzuschließen.
2. Kehren Sie zu BlueXP zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.

Verbindung erstellen

1. Erstellen Sie die Verbindung mit der Microsoft Entra ID
   a. Geben Sie die Client-ID und das Client-Geheimnis ein, die Sie im vorherigen Schritt erstellt haben.
   b. Geben Sie den Domänennamen der Microsoft Entra ID ein.
2. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung innerhalb weniger Sekunden her.

Testen und Aktivieren der Verbindung

1. Wählen Sie **Weiter**.
2. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zur Anmeldeseite Ihres IdP-Servers weitergeleitet. Melden Sie sich mit Ihren IdP-Anmeldedaten an, um den Test abzuschließen, und kehren Sie zu BlueXP zurück, um die Verbindung zu aktivieren.
3. Wählen Sie **Weiter**.
4. Überprüfen Sie auf der Seite **Föderation aktivieren** die Föderationsdetails und wählen Sie dann **Föderation aktivieren** aus.
5. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nachdem Sie die Föderation aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden.

Föderieren Sie BlueXP mit PingFederate

Verbinden Sie sich mit Ihrem PingFederate-IdP-Anbieter, um Single Sign-On (SSO) für BlueXP zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist ein Organisations- oder Föderationsadministrator erforderlich. Der Föderationsbetrachter kann die Föderationsseite anzeigen. "Erfahren Sie mehr über Zugriffsrollen."

Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. NetApp empfiehlt, entweder das eine oder das andere zu wählen, aber nicht beides.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in BlueXP eine Verbindung herstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Verbundverbindung mit PingFederate einrichten, um Single Sign-On (SSO) für BlueXP zu aktivieren. Dazu konfigurieren Sie Ihren PingFederate-Server so, dass er BlueXP als Dienstanbieter vertraut, und erstellen anschließend die Verbindung in BlueXP.

Bevor Sie beginnen

- Sie benötigen ein IdP-Konto mit Administratorrechten. Sprechen Sie die Schritte mit Ihrem IdP-Administrator ab.
- Identifizieren Sie die Domäne, die Sie für die Föderation verwenden möchten. Sie können Ihre E-Mail-Domäne oder eine andere Domäne verwenden, die Sie besitzen. Wenn Sie eine andere Domäne als Ihre E-Mail-Domäne verwenden möchten, müssen Sie diese zunächst in BlueXP verifizieren. Folgen Sie dazu den Schritten im "Verifizieren Sie Ihre Domain in BlueXP" Thema.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Provider** und dann **PingFederate**.
7. Wählen Sie **Weiter**.
8. Konfigurieren Sie Ihren PingFederate-Server so, dass NetApp als Dienstanbieter vertraut. Dieser Schritt muss auf Ihrem PingFederate-Server ausgeführt werden.
   a. Verwenden Sie die folgenden Werte, wenn Sie PingFederate so konfigurieren, dass es BlueXP vertraut:
      - Für die **Antwort-URL** oder **Assertion Consumer Service (ACS)-URL** verwenden Sie `https://netapp-cloud-account.auth0.com/login/callback`
      - Verwenden Sie für die **Abmelde-URL** `https://netapp-cloud-account.auth0.com/logout`
      - Für **Zielgruppen-/Entitäts-ID** verwenden Sie `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` wobei <fed-domain-name-pingfederate> der Domänenname für den Verbund ist. Wenn Ihre Domäne beispielsweise `example.com` , wäre die Zielgruppen-/Entitäts-ID `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Kopieren Sie die PingFederate-Server-URL. Sie benötigen diese URL beim Herstellen der Verbindung in BlueXP.
   c. Laden Sie das X.509-Zertifikat von Ihrem PingFederate-Server herunter. Es muss im Base64-codierten PEM-Format (.pem, .crt, .cer) vorliegen.
9. Kehren Sie zu BlueXP zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
10. Erstellen Sie die Verbindung mit PingFederate
    a. Geben Sie die PingFederate-Server-URL ein, die Sie im vorherigen Schritt kopiert haben.
    b. Laden Sie das X.509-Signaturzertifikat hoch. Das Zertifikat muss im PEM-, CER- oder CRT-Format vorliegen.
11. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung innerhalb weniger Sekunden her.
12. Wählen Sie **Weiter**.
13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zur Anmeldeseite Ihres IdP-Servers weitergeleitet. Melden Sie sich mit Ihren IdP-Anmeldedaten an, um den Test abzuschließen, und kehren Sie zu BlueXP zurück, um die Verbindung zu aktivieren.
14. Wählen Sie **Weiter**.
15. Überprüfen Sie auf der Seite **Föderation aktivieren** die Föderationsdetails und wählen Sie dann **Föderation aktivieren** aus.
16. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nachdem Sie die Föderation aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden.

Föderieren Sie mit einem SAML-Identitätsanbieter

Verbinden Sie sich mit Ihrem SAML 2.0-IdP-Anbieter, um Single Sign-On (SSO) für BlueXP zu aktivieren. Dadurch können sich Benutzer mit ihren Unternehmensanmeldeinformationen anmelden.

Erforderliche Rolle

Organisationsadministrator. "Erfahren Sie mehr über Zugriffsrollen."

> Sie können eine Föderation mit Ihrem Unternehmens-IdP oder mit der NetApp -Support-Site herstellen. Eine Föderation mit beiden ist nicht möglich.

NetApp unterstützt nur vom Dienstanbieter initiiertes (SP-initiiertes) SSO. Sie müssen zunächst den Identitätsanbieter so konfigurieren, dass er NetApp als Dienstanbieter vertraut. Anschließend können Sie in BlueXP eine Verbindung herstellen, die die Konfiguration des Identitätsanbieters verwendet.

Sie können eine Verbundverbindung mit Ihrem SAML 2.0-Anbieter einrichten, um Single Sign-On (SSO) für BlueXP zu aktivieren. Dazu konfigurieren Sie Ihren Anbieter so, dass er NetApp als Service-Provider anerkennt, und erstellen anschließend die Verbindung in BlueXP.

Bevor Sie beginnen

- Sie benötigen ein IdP-Konto mit Administratorrechten. Sprechen Sie die Schritte mit Ihrem IdP-Administrator ab.
- Identifizieren Sie die Domäne, die Sie für die Föderation verwenden möchten. Sie können Ihre E-Mail-Domäne oder eine andere Domäne verwenden, die Sie besitzen. Wenn Sie eine andere Domäne als Ihre E-Mail-Domäne verwenden möchten, müssen Sie diese zunächst in BlueXP verifizieren. Folgen Sie dazu den Schritten im "Verifizieren Sie Ihre Domain in BlueXP" Thema.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie **Neue Föderation konfigurieren**.
4. Geben Sie Ihre Domänendetails ein:
   a. Wählen Sie, ob Sie eine verifizierte Domäne oder Ihre E-Mail-Domäne verwenden möchten. Die E-Mail-Domäne ist die Domäne, die mit dem Konto verknüpft ist, mit dem Sie angemeldet sind.
   b. Geben Sie den Namen der Föderation ein, die Sie konfigurieren.
   c. Wenn Sie eine verifizierte Domäne auswählen, wählen Sie die Domäne aus der Liste aus.
5. Wählen Sie **Weiter**.
6. Wählen Sie als Verbindungsmethode **Protokoll** und dann **SAML-Identitätsanbieter**.
7. Wählen Sie **Weiter**.
8. Konfigurieren Sie Ihren SAML-Identitätsanbieter so, dass NetApp als Dienstanbieter vertraut. Sie müssen diesen Schritt auf dem Server Ihres SAML-Anbieters ausführen.
   a. Stellen Sie sicher, dass Ihr IdP das Attribut hat `email` auf die E-Mail-Adresse des Benutzers gesetzt.

Dies ist erforderlich, damit BlueXP Benutzer korrekt identifizieren kann:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
        <saml:AttributeValue xsi:type="xs:string">
email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

b. Verwenden Sie die folgenden Werte, wenn Sie Ihre SAML-Anwendung bei BlueXP registrieren:
   - Für die **Antwort-URL** oder **Assertion Consumer Service (ACS)-URL** verwenden Sie `https://netapp-cloud-account.auth0.com/login/callback`
   - Verwenden Sie für die **Abmelde-URL** `https://netapp-cloud-account.auth0.com/logout`
   - Für **Zielgruppen-/Entitäts-ID** verwenden Sie `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` wobei <fed-domain-name-saml> der Domänenname ist, den Sie für die Föderation verwenden möchten. Wenn Ihre Domäne beispielsweise `example.com` , wäre die Zielgruppen-/Entitäts-ID `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .

c. Kopieren Sie nach dem Erstellen der Vertrauensstellung die folgenden Werte vom Server Ihres SAML-Anbieters:
   - Anmelde-URL
   - Abmelde-URL (optional)

d. Laden Sie das X.509-Zertifikat vom Server Ihres SAML-Anbieters herunter. Es muss im PEM-, CER- oder CRT-Format vorliegen.

9. Kehren Sie zu BlueXP zurück und wählen Sie **Weiter**, um die Verbindung herzustellen.
10. Stellen Sie die Verbindung mit SAML her.
    a. Geben Sie die **Anmelde-URL** Ihres SAML-Servers ein.
    b. Laden Sie das X.509-Zertifikat hoch, das Sie vom Server Ihres SAML-Anbieters heruntergeladen haben.
    c. Geben Sie optional die **Abmelde-URL** Ihres SAML-Servers ein.
11. Wählen Sie **Verbindung erstellen**. Das System stellt die Verbindung innerhalb weniger Sekunden her.
12. Wählen Sie **Weiter**.
13. Wählen Sie **Verbindung testen**, um Ihre Verbindung zu testen. Sie werden zur Anmeldeseite Ihres IdP-Servers weitergeleitet. Melden Sie sich mit Ihren IdP-Anmeldedaten an, um den Test abzuschließen, und kehren Sie zu BlueXP zurück, um die Verbindung zu aktivieren.
14. Wählen Sie **Weiter**.
15. Überprüfen Sie auf der Seite **Föderation aktivieren** die Föderationsdetails und wählen Sie dann **Föderation aktivieren** aus.

16. Wählen Sie **Fertig**, um den Vorgang abzuschließen.

Nachdem Sie die Föderation aktiviert haben, können sich Benutzer mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden.

Föderationen in BLueXP verwalten

Sie können Ihre Föderation in BlueXP verwalten. Sie können sie deaktivieren, abgelaufene Anmeldeinformationen aktualisieren und sie deaktivieren, wenn Sie sie nicht mehr benötigen.

Wenn Sie die Föderation zuvor mit NetApp Cloud Central (einer externen Anwendung für BlueXP) konfiguriert haben, müssen Sie Ihre Föderation mithilfe der BlueXP -Föderationsseite importieren, um sie innerhalb von BlueXP verwalten zu können."Erfahren Sie, wie Sie Ihre Föderation importieren"

Sie können einer vorhandenen Föderation auch eine verifizierte Domäne hinzufügen, wodurch Sie mehrere Domänen für Ihre föderierte Verbindung verwenden können.

Ereignisse der Föderationsverwaltung wie das Aktivieren, Deaktivieren und Aktualisieren von Föderationen werden in der Zeitleiste angezeigt. "Erfahren Sie mehr über Überwachungsvorgänge in BlueXP."

Erforderliche Rollen

Zum Erstellen und Verwalten von Föderationen ist ein Organisations- oder Föderationsadministrator erforderlich. Der Föderationsbetrachter kann die Föderationsseite anzeigen. "Erfahren Sie mehr über Zugriffsrollen."

Aktivieren einer Föderation

Wenn Sie eine Föderation erstellt haben, diese aber noch nicht aktiviert ist, können Sie sie über die Registerkarte „Föderation“ in BlueXP aktivieren. Durch die Aktivierung einer Föderation können sich die zugehörigen Benutzer mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden. Sie müssen die Föderation bereits erstellt und erfolgreich getestet haben, bevor Sie sie aktivieren.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie das Aktionsmenü ••• neben der Föderation, die Sie aktivieren möchten, und wählen Sie **Aktivieren** aus.

Hinzufügen einer verifizierten Domäne zu einer vorhandenen Föderation

Sie können einer vorhandenen Föderation in BlueXP eine verifizierte Domäne hinzufügen, um mehrere Domänen mit demselben Identitätsanbieter (IdP) zu verwenden.

Sie müssen die Domäne bereits in BlueXP verifiziert haben, bevor Sie sie zu einer Föderation hinzufügen können. Wenn Sie die Domäne noch nicht verifiziert haben, können Sie dies tun, indem Sie die Schritte in "Verifizieren Sie Ihre Domain in BlueXP" .

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Domänen aktualisieren** aus. Im Dialogfeld **Domänen aktualisieren** werden die Domänen aufgelistet, die diesem Verbund bereits zugeordnet sind.
4. Wählen Sie eine verifizierte Domäne aus der Liste der verfügbaren Domänen aus.
5. Wählen Sie **Aktualisieren**. Es kann bis zu 30 Sekunden dauern, bis Benutzer der neuen Domäne föderierten Zugriff auf BlueXP haben.

Aktualisieren einer ablaufenden Verbundverbindung

Sie können die Details einer Föderation in BlueXP aktualisieren. Beispielsweise müssen Sie die Föderation aktualisieren, wenn Anmeldeinformationen wie ein Zertifikat oder ein Client-Geheimnis ablaufen. Aktualisieren Sie bei Bedarf das Benachrichtigungsdatum, um Sie daran zu erinnern, die Verbindung vor Ablauf zu aktualisieren.

Aktualisieren Sie BlueXP zuerst, bevor Sie Ihren IdP aktualisieren, um Anmeldeprobleme zu vermeiden. Bleiben Sie während des Vorgangs bei BlueXP angemeldet.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie das Aktionsmenü (drei vertikale Punkte) neben der Föderation, die Sie aktualisieren möchten, und wählen Sie **Föderation aktualisieren**.
4. Aktualisieren Sie die Details der Föderation nach Bedarf.
5. Wählen Sie **Aktualisieren**.

Testen einer vorhandenen Föderation

Wenn Sie Probleme mit einer bestehenden Föderation haben, können Sie die Verbindung testen, um zu prüfen, ob sie ordnungsgemäß funktioniert. Dies kann Ihnen helfen, etwaige Probleme mit der Föderation zu identifizieren und zu beheben.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie das Aktionsmenü neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Verbindung testen** aus.
4. Wählen Sie **Test**. Sie werden aufgefordert, sich mit Ihren Unternehmensanmeldeinformationen anzumelden. Bei erfolgreicher Verbindung werden Sie zur BlueXP Konsole weitergeleitet. Schlägt die Verbindung fehl, wird eine Fehlermeldung angezeigt, die auf das Problem mit der Föderation hinweist.
5. Wählen Sie **Fertig**, um zur Registerkarte **Föderation** zurückzukehren.

Deaktivieren einer Föderation

Wenn Sie die Föderation nicht mehr benötigen, können Sie sie deaktivieren. Dadurch wird verhindert, dass sich die der Föderation zugeordneten Benutzer mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden. Sie können die Föderation später bei Bedarf wieder aktivieren.

Sie sollten eine Föderation deaktivieren, bevor Sie sie löschen. Dies ist beispielsweise der Fall, wenn Sie den IdP zugunsten eines anderen IdP außer Betrieb nehmen oder die Föderation nicht mehr nutzen möchten. So können Sie sie später bei Bedarf wieder aktivieren.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie das Aktionsmenü ⋮ neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Deaktivieren** aus.

Löschen einer Föderation

Wenn Sie eine Föderation nicht mehr benötigen, können Sie sie löschen. Dadurch wird die Föderation aus BlueXP entfernt und alle zugehörigen Benutzer können sich nicht mehr mit ihren Unternehmensanmeldeinformationen bei BlueXP anmelden. Dies ist beispielsweise der Fall, wenn der IdP außer Betrieb genommen wird oder die Föderation nicht mehr benötigt wird. Eine gelöschte Föderation kann nicht wiederhergestellt werden. Sie müssen eine neue Föderation erstellen.

Sie müssen eine Föderation deaktivieren, bevor Sie sie löschen können. Sie können eine gelöschte Föderation nicht wiederherstellen.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie das Aktionsmenü ⋮ neben dem Verbund, dem Sie eine verifizierte Domäne hinzufügen möchten, und wählen Sie **Löschen** aus.

Importieren Sie Ihre Föderation in BlueXP

Wenn Sie die Föderation zuvor über NetApp Cloud Central (eine externe Anwendung für BlueXP) eingerichtet haben, werden Sie auf der Föderationsseite aufgefordert, Ihre vorhandene föderierte Verbindung zu BlueXP zu importieren, um sie in der neuen Schnittstelle zu verwalten. Auf diese Weise können Sie die neuesten Verbesserungen nutzen, ohne Ihre Verbundverbindungen neu erstellen zu müssen.

Bestehende Kunden, die bereits Verbundverbindungen zu BlueXP eingerichtet haben, können ihre bestehenden Verbundverbindungen in die neue Oberfläche importieren. So können Sie Ihre Verbundverbindungen auf der neuen Seite „Verbände“ verwalten, ohne sie neu erstellen zu müssen.

Nachdem Sie Ihre vorhandene Föderation importiert haben, können Sie die Föderation von der Seite „Föderationen“ aus verwalten. "Erfahren Sie mehr über die Verwaltung von Föderationen."

Erforderliche Rolle

Organisationsadministrator oder Föderationsadministrator. "Erfahren Sie mehr über Zugriffsrollen."

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Identitäts- und Zugriffsmanagement** aus.
2. Wählen Sie die Registerkarte **Föderation**.
3. Wählen Sie **Föderation importieren**.

Anschlüsse

Wartung der Connector VM und des Betriebssystems

Die Wartung des Betriebssystems auf dem Connector-Host liegt in Ihrer (Kunden-)Verantwortung. Sie (der Kunde) sollten beispielsweise Sicherheitsupdates auf das Betriebssystem auf dem Connector-Host anwenden und dabei die Standardverfahren Ihres Unternehmens zur Betriebssystemverteilung befolgen.

Wenn Sie bereits über einen Connector verfügen, sollten Sie sich dessen bewusst sein "Änderungen an unterstützten Linux-Betriebssystemen".

Betriebssystem-Patches und der Connector

Wenden Sie Betriebssystem-Sicherheitspatches an, ohne die Connector-Hostdienste zu stoppen.

VM oder Instanztyp

Wenn Sie einen Connector aus BlueXP erstellen, wird eine VM-Instanz mit einer Standardkonfiguration bei Ihrem Cloud-Anbieter bereitgestellt. Wechseln Sie nach der Erstellung des Connectors nicht zu einer kleineren VM-Instanz mit weniger CPU oder RAM.

In der folgenden Tabelle sind die CPU- und RAM-Anforderungen aufgeführt:

CPU
: 8 Kerne oder 8 vCPUs

RAM
: 32GB

"Informieren Sie sich über die Standardkonfiguration des Connectors".

Überwachen des Connectors

BlueXP benachrichtigt Sie, wenn die Connector-VM Probleme mit Speicherplatz, RAM und CPU aufweist. Überwachen Sie diese Benachrichtigungen im Benachrichtigungscenter von BlueXP oder konfigurieren Sie E-Mail-Benachrichtigungen. Gelegentliche Erhöhungen von Speicherplatz, Arbeitsspeicher oder CPU-Auslastung sind normal. Tritt dies jedoch häufig auf, sollten Sie Maßnahmen zur Behebung ergreifen.

BlueXP benachrichtigt Sie, wenn eine Connector-Ressource (CPU, RAM oder Festplattenspeicher) 30 Minuten lang 90 % ihrer Gesamtkapazität überschreitet. Sinkt die Ressourcennutzung anschließend unter diesen Schwellenwert, wird die Benachrichtigung im Benachrichtigungscenter als behoben (grün) angezeigt.

Wenden Sie sich an den NetApp Support, wenn Sie Fragen zum Ändern Ihrer Connector-VM haben.

"Weitere Informationen ."

Benachrichtigung	Handlungsbedarf
Der Speicherplatz ist zu groß	"Lesen Sie den NetApp Knowledge Base-Artikel".
Die CPU-Auslastung ist zu hoch	Erhöhen Sie die CPU-Größe der Connector-VM in Ihrem Hyperscaler oder lokal, je nachdem, wo Sie sie installiert haben. Alternativ können Sie zusätzliche Connectors erstellen und die Workload auf mehrere Connectors verteilen. Die RAM-Auslastung kann je nach Umgebung, ONTAP Workloads, Anzahl der Cloud Volumes ONTAP Systeme und den von Ihnen genutzten Datendiensten variieren.
Die RAM-Auslastung ist zu hoch	Erhöhen Sie den RAM der Connector-VM in Ihrem Hyperscaler oder vor Ort, je nachdem, wo Sie sie installiert haben. Alternativ können Sie zusätzliche Connectors erstellen und die Workload auf mehrere Connectors verteilen. Die RAM-Auslastung kann je nach Umgebung, ONTAP Workloads, Anzahl der Cloud Volumes ONTAP Systeme und den von Ihnen genutzten Datendiensten variieren.

Anhalten und Starten der Konnektor-VM

Stoppen und starten Sie die Connector-VM bei Bedarf über die Konsole Ihres Cloud-Anbieters oder mithilfe standardmäßiger Verfahren vor Ort.

"Beachten Sie, dass der Connector jederzeit betriebsbereit sein muss".

Stellen Sie eine Verbindung zur Linux VM her

Wenn Sie eine Verbindung mit der Linux-VM herstellen müssen, auf der der Connector ausgeführt wird, verwenden Sie die Konnektivitätsoptionen Ihres Cloud-Anbieters.

AWS

Geben Sie beim Erstellen der Connector-Instanz in AWS einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel an. Sie können dieses Schlüsselpaar für SSH zur Instanz verwenden. Verwenden Sie den Benutzernamen „ubuntu“ für die EC2-Linux-Instanz. Verwenden Sie für Connectors, die vor Mai 2023 erstellt wurden, den Benutzernamen „ec2-user“.

"AWS Docs: Stellen Sie eine Verbindung zu Ihrer Linux-Instanz her"

Azure

Wenn Sie die Connector-VM in Azure erstellen, geben Sie einen Benutzernamen an und wählen die Authentifizierung mit einem Kennwort oder einem öffentlichen SSH-Schlüssel. Verwenden Sie die Authentifizierungsmethode, die Sie für die Verbindung zur VM ausgewählt haben.

"Azure Docs: SSH in Ihre VM"

Google Cloud

Sie können keine Authentifizierungsmethode angeben, wenn Sie einen Connector in Google Cloud erstellen. Sie können eine Verbindung zur Linux VM-Instanz jedoch über die Google Cloud Console oder Google Cloud CLI (gcloudd) herstellen.

"Google Cloud Docs: Verbindung zu Linux-VMs herstellen"

Ändern Sie die IP-Adresse für einen Konnektor

Sie können die internen und öffentlichen IP-Adressen der Connector-Instanz, die Ihnen von Ihrem Cloud-Anbieter zugewiesen wurden, bei Bedarf ändern.

Schritte

1. Befolgen Sie die Anweisungen Ihres Cloud-Providers, um die lokale IP-Adresse oder die öffentliche IP-Adresse (oder beide) für die Connector-Instanz zu ändern.
2. Starten Sie die Connector-Instanz neu, um eine neue öffentliche IP-Adresse bei BlueXP zu registrieren.
3. Wenn Sie die private IP-Adresse geändert haben, aktualisieren Sie den Backup-Speicherort für Cloud Volumes ONTAP-Konfigurationsdateien, so dass die Backups an die neue private IP-Adresse des Connectors gesendet werden.

   Aktualisieren Sie den Sicherungsspeicherort für jedes Cloud Volumes ONTAP -System.

   a. Legen Sie über die Cloud Volumes ONTAP-CLI die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

   b. Führen Sie den folgenden Befehl aus, um das aktuelle Backup-Ziel anzuzeigen:

   ```
   system configuration backup settings show
   ```

   c. Führen Sie den folgenden Befehl aus, um die IP-Adresse für das Backup-Ziel zu aktualisieren:

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

Bearbeiten Sie die URIs eines Connectors

Sie können den Uniform Resource Identifier (URI) für einen Connector hinzufügen und entfernen.

Schritte

1. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.
2. Wählen Sie **Connectors Verwalten**.
3. Erweitern Sie die Leiste **Connector-URIs**, um Connector-URIs anzuzeigen.
4. Fügen Sie URIs hinzu und entfernen Sie sie, und wählen Sie dann **Apply**.

Installieren Sie ein CA-signiertes Zertifikat für den webbasierten Konsolenzugriff

Wenn Sie BlueXP im eingeschränkten oder privaten Modus verwenden, kann auf die Benutzeroberfläche über die virtuelle Connector-Maschine zugegriffen werden, die in Ihrer Cloud-Region oder vor Ort bereitgestellt wird. Standardmäßig verwendet BlueXP ein selbstsigniertes SSL-Zertifikat, um einen sicheren HTTPS-Zugriff auf die webbasierte Konsole zu ermöglichen, die auf dem Connector ausgeführt wird. Falls Ihr Unternehmen dies erfordert, können Sie ein von einer Zertifizierungsstelle signiertes Zertifikat installieren, das einen besseren Schutz bietet als ein selbstsigniertes Zertifikat. Nach der Installation des Zertifikats verwendet BlueXP das CA-signierte Zertifikat, wenn Benutzer auf die webbasierte Konsole zugreifen.

Bevor Sie beginnen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "Erfahren Sie, wie Sie einen Konnektor erstellen".

Installieren Sie ein HTTPS-Zertifikat

Installieren Sie ein von einer Zertifizierungsstelle signiertes Zertifikat für den sicheren Zugriff auf die webbasierte Konsole, die auf dem Connector ausgeführt wird.

Über diese Aufgabe

Sie können das Zertifikat mithilfe einer der folgenden Optionen installieren:

- Erstellen Sie eine Zertifikatsignierungsanforderung (CSR) von BlueXP , senden Sie die Zertifikatsanforderung an eine Zertifizierungsstelle, und installieren Sie dann das CA-signierte Zertifikat auf dem Konnektor.

  Das Schlüsselpaar, das BlueXP zur Generierung der CSR verwendet, wird intern auf dem Konnektor gespeichert. BlueXP ruft automatisch das gleiche Schlüsselpaar (privater Schlüssel) ab, wenn Sie das Zertifikat auf dem Connector installieren.

- Installieren Sie ein Zertifikat mit CA-Signatur, das Sie bereits besitzen.

  Mit dieser Option wird die CSR nicht über BlueXP generiert. Sie generieren die CSR separat und speichern den privaten Schlüssel extern. Sie geben BlueXP den privaten Schlüssel an, wenn Sie das Zertifikat installieren.

Schritte

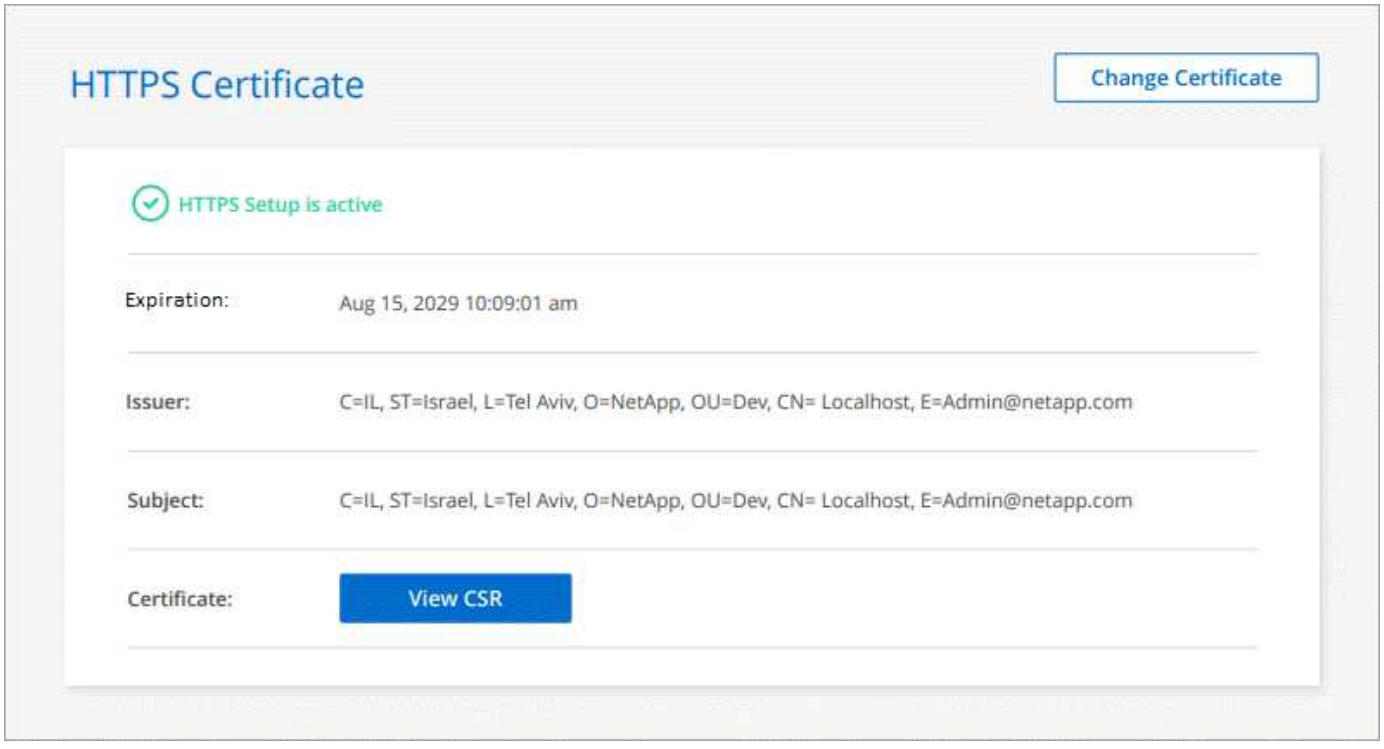
1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **HTTPS Setup** aus.

2. Installieren Sie auf der Seite HTTPS Setup ein Zertifikat, indem Sie eine Zertifikatsignierungsanforderung (CSR) erstellen oder Ihr eigenes, von der Zertifizierungsstelle signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	a. Geben Sie den Host-Namen oder DNS des Connector-Hosts ein (dessen allgemeiner Name), und wählen Sie dann **CSR generieren** aus. BlueXP zeigt eine Anfrage zum Signieren des Zertifikats an. b. Verwenden Sie die CSR, um eine SSL-Zertifikatsanforderung an eine Zertifizierungsstelle zu senden. Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden. c. Laden Sie die Zertifikatdatei hoch und wählen Sie dann **Installieren**.
Installieren Sie Ihr eigenes CA-signiertes Zertifikat	a. Wählen Sie **CA-signiertes Zertifikat installieren**. b. Laden Sie sowohl die Zertifikatdatei als auch den privaten Schlüssel und wählen Sie dann **Installieren**. Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.

Ergebnis

BlueXP verwendet jetzt das von der Zertifizierungsstelle signierte Zertifikat, um einen sicheren HTTPS-Zugriff zu ermöglichen. Die folgende Abbildung zeigt einen Connector, der für sicheren Zugriff konfiguriert ist:



Erneuern Sie das BlueXP HTTPS-Zertifikat

Sie sollten das BlueXP HTTPS-Zertifikat erneuern, bevor es abläuft, um einen sicheren Zugriff auf die BlueXP-

Konsole zu gewährleisten. Wenn Sie das Zertifikat nicht erneuern, bevor es abläuft, wird eine Warnung angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **HTTPS Setup** aus.

   Es werden Details zum BlueXP-Zertifikat angezeigt, einschließlich des Ablaufdatums.

2. Wählen Sie **Zertifikat ändern** und folgen Sie den Schritten, um eine CSR zu generieren oder Ihr eigenes CA-signiertes Zertifikat zu installieren.

Ergebnis

BlueXP verwendet das neue CA-signierte Zertifikat, um sicheren HTTPS-Zugriff bereitzustellen.

Konfigurieren Sie einen Konnektor für die Verwendung eines Proxy-Servers

Wenn Sie in Ihren Unternehmensrichtlinien einen Proxyserver für die gesamte Kommunikation mit dem Internet verwenden müssen, müssen Sie Ihre Connectors so konfigurieren, dass sie diesen Proxy-Server verwenden. Wenn Sie während der Installation keinen Connector so konfiguriert haben, dass er einen Proxyserver verwendet, können Sie den Connector so konfigurieren, dass er diesen Proxyserver verwendet.

Der Proxyserver des Connectors ermöglicht ausgehenden Internetzugriff ohne öffentliche IP oder NAT-Gateway. Der Proxyserver bietet ausgehende Konnektivität nur für den Connector, nicht für Cloud Volumes ONTAP-Systeme.

Wenn Cloud Volumes ONTAP -Systeme keinen ausgehenden Internetzugang haben, konfiguriert BlueXP sie für die Verwendung des Proxyservers des Connectors. Sie müssen sicherstellen, dass die Sicherheitsgruppe des Connectors eingehende Verbindungen über Port 3128 zulässt. Öffnen Sie diesen Port, nachdem Sie den Connector bereitgestellt haben.

Wenn der Connector selbst keine ausgehende Internetverbindung hat, können Cloud Volumes ONTAP -Systeme den konfigurierten Proxyserver nicht verwenden.

Unterstützte Konfigurationen

- Transparente Proxyserver werden für Connectors unterstützt, die Cloud Volumes ONTAP -Systeme bedienen. Wenn Sie BlueXP -Dienste mit Cloud Volumes ONTAP verwenden, erstellen Sie einen dedizierten Connector für Cloud Volumes ONTAP , in dem Sie einen transparenten Proxyserver verwenden können.
- Explizite Proxyserver werden von allen Connectors unterstützt, einschließlich derjenigen, die Cloud Volumes ONTAP Systeme verwalten, und derjenigen, die BlueXP -Dienste verwalten.
- HTTP und HTTPS.
- Der Proxyserver kann sich in der Cloud oder in Ihrem Netzwerk befinden.

Sobald Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Connector und fügen Sie einen neuen Connector mit dem neuen Proxy-Typ hinzu.

Aktivieren eines expliziten Proxys auf einem Connector

Wenn Sie einen Connector so konfigurieren, dass er einen Proxy-Server verwendet, verwenden dieser Connector und die von ihm verwalteten Cloud Volumes ONTAP-Systeme (einschließlich aller HA-Mediatoren) den Proxy-Server.

Dieser Vorgang startet den Connector neu. Stellen Sie sicher, dass der Connector im Leerlauf ist, bevor Sie fortfahren.

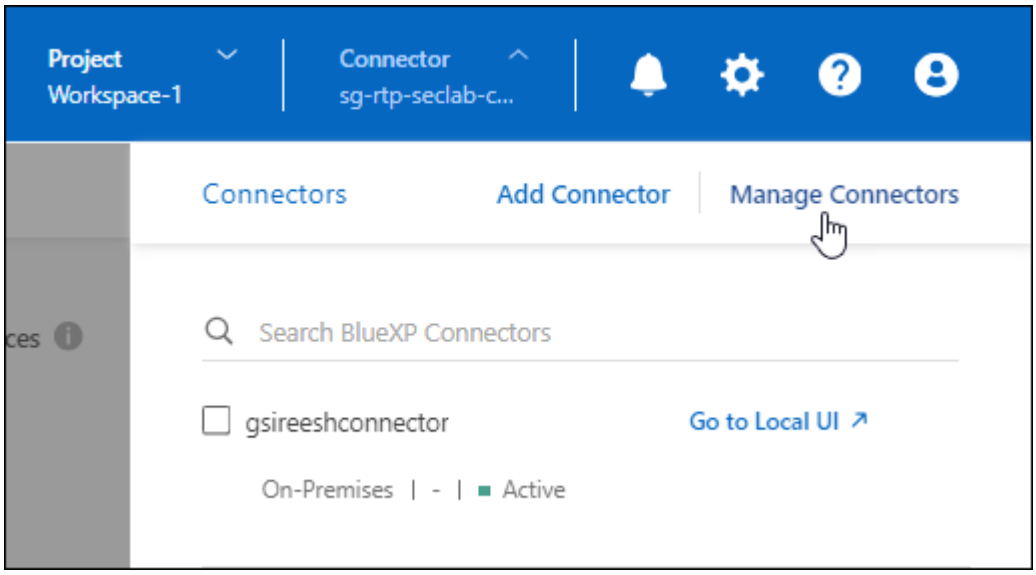
Schritte

1. Navigieren Sie zur Seite **BlueXP Connector bearbeiten**.

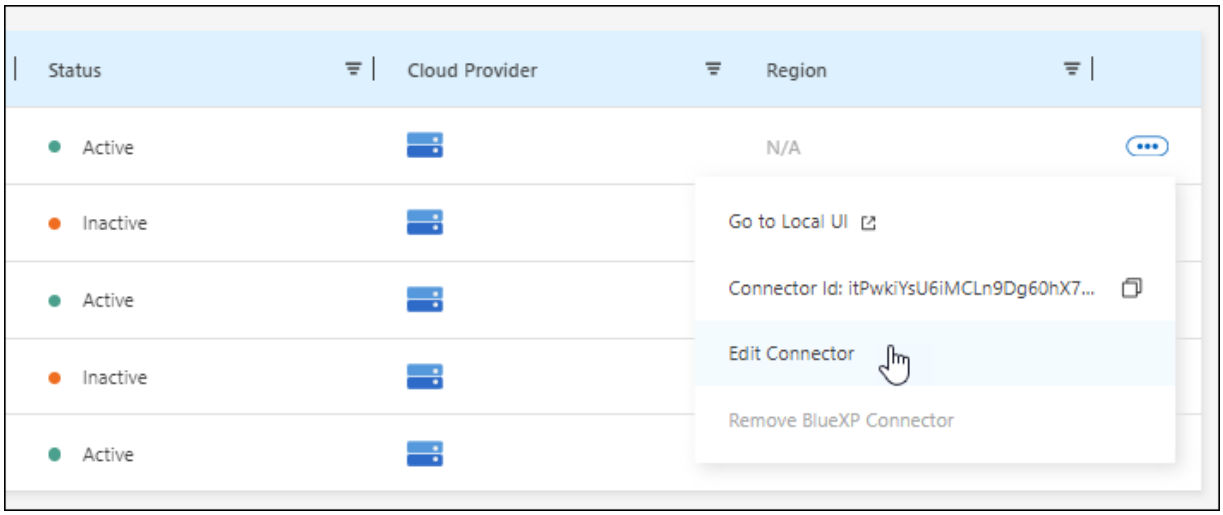
Standardmodus

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connectors Verwalten**.



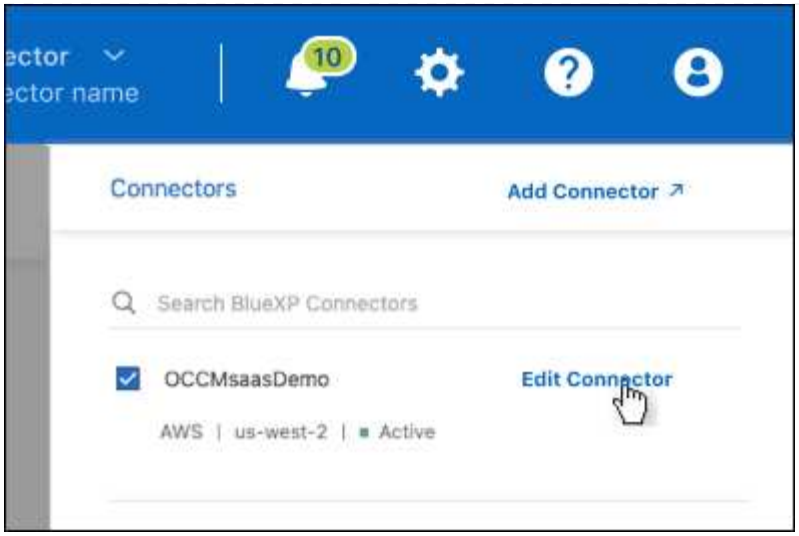
c. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **Connector bearbeiten**.



Eingeschränkter oder privater Modus

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connector Bearbeiten**.



2. Wählen Sie **HTTP Proxy Configuration** aus.
3. Wählen Sie im Feld „Konfigurationstyp“ **Expliziter Proxy** aus.
4. Wählen Sie **Proxy Aktivieren**.
5. Geben Sie den Server mithilfe der Syntax an http://address:port Oder https://address:port
6. Geben Sie einen Benutzernamen und ein Kennwort an, wenn eine grundlegende Authentifizierung für den Server erforderlich ist.

   Beachten Sie Folgendes:

   - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
   - Für einen Domänenbenutzer müssen Sie den ASCII-Code für den \ wie folgt eingeben: Domain-Name%92user-Name

     Beispiel: netapp%92Proxy

   - BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.
7. Wählen Sie **Speichern**.

Aktivieren eines transparenten Proxys auf einem Connector

Nur Cloud Volumes ONTAP unterstützt die Verwendung eines transparenten Proxys auf dem Connector. Wenn Sie zusätzlich zu Cloud Volumes ONTAP BlueXP -Dienste nutzen, sollten Sie einen separaten Connector für Datendienste oder für Cloud Volumes ONTAP erstellen.

Stellen Sie vor der Aktivierung eines transparenten Proxys sicher, dass die folgenden Anforderungen erfüllt sind:

- Der Connector wird im selben Netzwerk wie der transparente Proxyserver installiert.
- Die TLS-Prüfung ist auf dem Proxyserver aktiviert.
- Sie verfügen über ein Zertifikat im PEM-Format, das mit dem auf dem transparenten Proxyserver verwendeten Zertifikat übereinstimmt.

- Sie verwenden den Connector für keine anderen NetApp -Datendienste als Cloud Volumes ONTAP.

Um einen vorhandenen Connector für die Verwendung eines transparenten Proxyservers zu konfigurieren, verwenden Sie das Connector-Wartungstool, das über die Befehlszeile auf dem Connector-Host verfügbar ist.

Wenn Sie einen Proxyserver konfigurieren, wird der Connector neu gestartet. Stellen Sie sicher, dass der Connector im Leerlauf ist, bevor Sie fortfahren.

Schritte

Stellen Sie sicher, dass Sie über eine Zertifikatsdatei im PEM-Format für den Proxyserver verfügen. Sollten Sie kein Zertifikat besitzen, wenden Sie sich bitte an Ihren Netzwerkadministrator.

1. Öffnen Sie eine Befehlszeilenschnittstelle auf dem Connector-Host.
2. Navigieren Sie zum Verzeichnis des Connector-Wartungstools: `/opt/application/netapp/service-manager-2/connector-maint-console`
3. Führen Sie den folgenden Befehl aus, um den transparenten Proxy zu aktivieren. `/home/ubuntu/<certificate-file>.pem` ist das Verzeichnis und der Name der Zertifikatsdatei, die Sie für den Proxyserver haben:

   ```
   ./connector-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

   Stellen Sie sicher, dass die Zertifikatsdatei im PEM-Format vorliegt und sich im selben Verzeichnis wie der Befehl befindet, oder geben Sie den vollständigen Pfad zur Zertifikatsdatei an.

   ```
   ./connector-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

Ändern Sie den transparenten Proxy für den Connector

Sie können den vorhandenen transparenten Proxy-Server eines Connectors aktualisieren, indem Sie den `proxy update` Befehl oder entfernen Sie den transparenten Proxy-Server mithilfe des `proxy remove` Befehl. Weitere Informationen finden Sie in der Dokumentation zu "Connector-Wartungskonsole" .

> Sobald Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Connector und fügen Sie einen neuen Connector mit dem neuen Proxy-Typ hinzu.

Aktualisieren Sie den Connector-Proxy, wenn er den Zugriff auf das Internet verliert

Wenn sich die Proxy-Konfiguration Ihres Netzwerks ändert, kann Ihr Connector den Internetzugang verlieren. Dies kann beispielsweise der Fall sein, wenn jemand das Kennwort für den Proxyserver ändert oder das Zertifikat aktualisiert. In diesem Fall müssen Sie direkt vom Connector-Host auf die Benutzeroberfläche zugreifen und die Einstellungen aktualisieren. Stellen Sie sicher, dass Sie Netzwerkzugriff auf den Connector-Host haben und sich bei der BlueXP -Benutzeroberfläche anmelden können.

Aktivieren Sie direkten API-Verkehr

Wenn Sie einen Connector für die Verwendung eines Proxy-Servers konfiguriert haben, können Sie direkten API-Datenverkehr auf dem Connector aktivieren, um API-Aufrufe direkt an Cloud-Provider-Dienste zu senden, ohne über den Proxy zu gehen. In AWS, Azure oder Google Cloud ausgeführte Konnektoren unterstützen diese Option.

Wenn Sie Azure Private Links mit Cloud Volumes ONTAP deaktivieren und Service-Endpunkte verwenden, aktivieren Sie den direkten API-Verkehr. Andernfalls wird der Datenverkehr nicht korrekt geleitet.

"Weitere Informationen zur Verwendung eines Azure Private Links oder von Service-Endpunkten mit Cloud Volumes ONTAP"

Schritte

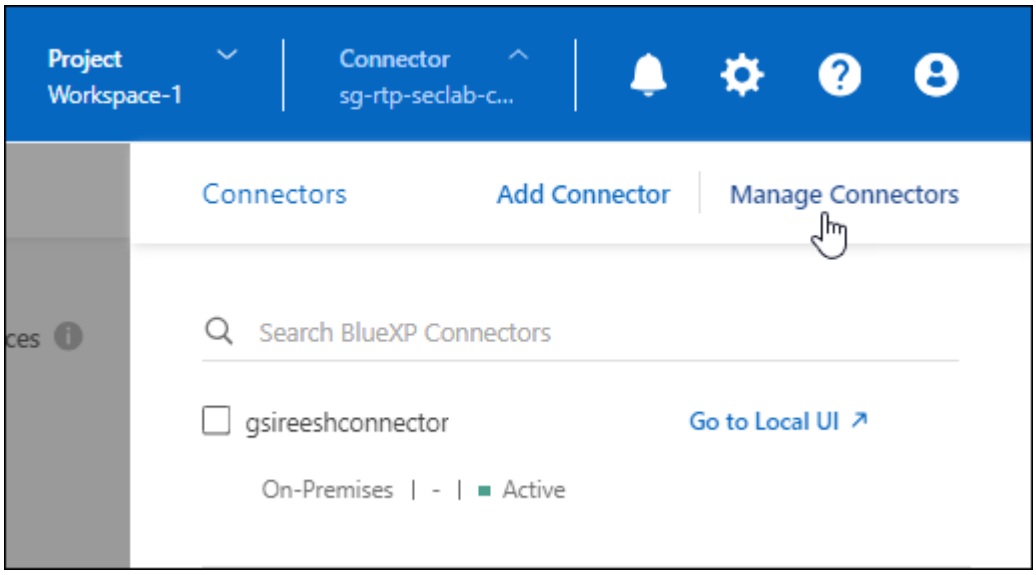
1. Navigieren Sie zur Seite **BlueXP Connector bearbeiten**:

   Die Navigation hängt von Ihrem BlueXP-Modus ab. Im Standardmodus greifen Sie über die SaaS-Website auf die Benutzeroberfläche zu. Im eingeschränkten oder privaten Modus greifen Sie lokal über den Connector-Host darauf zu.

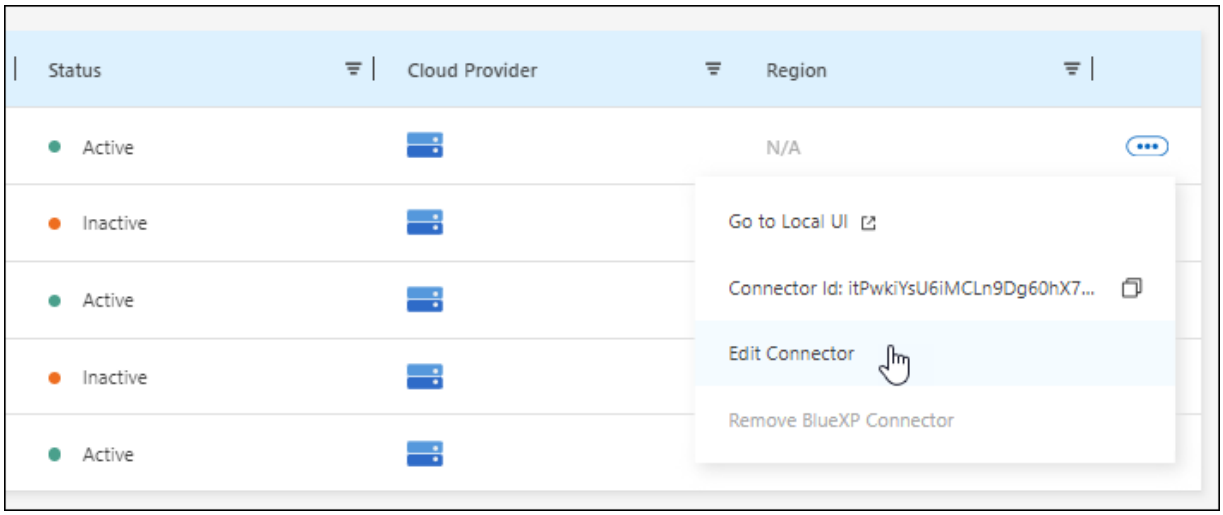
Standardmodus

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connectors Verwalten**.



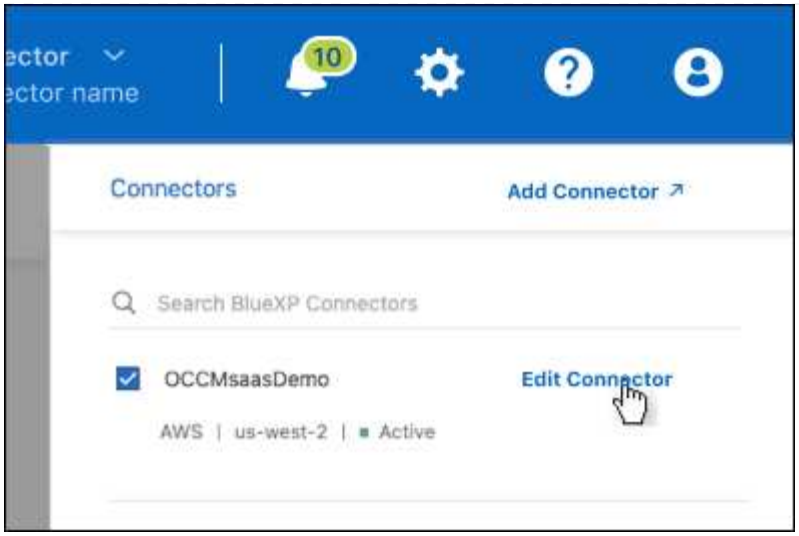
c. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **Connector bearbeiten**.



Eingeschränkter oder privater Modus

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connector Bearbeiten**.



2. Wählen Sie **Support Direct API Traffic**.
3. Aktivieren Sie das Kontrollkästchen, um die Option zu aktivieren, und wählen Sie dann **Speichern**.

Erfordern die Verwendung von IMDSv2 auf Amazon EC2 Instanzen

BlueXP unterstützt den Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) mit dem Connector und Cloud Volumes ONTAP (einschließlich des Mediators für HA-Implementierungen). In den meisten Fällen wird IMDSv2 automatisch auf neuen EC2-Instanzen konfiguriert. IMDSv1 wurde vor März 2024 aktiviert. Falls dies durch Ihre Sicherheitsrichtlinien erforderlich ist, müssen Sie IMDSv2 möglicherweise manuell auf Ihren EC2-Instanzen konfigurieren.

Bevor Sie beginnen

- Die Connector-Version muss 3.9.38 oder höher sein.
- Cloud Volumes ONTAP muss eine der folgenden Versionen ausführen:
  - 9.12.1 P2 (oder jedes weitere Patch)
  - 9.13.0 P4 (oder jedes weitere Patch)
  - 9.13.1 oder eine beliebige Version nach dieser Version
- Diese Änderung erfordert einen Neustart der Cloud Volumes ONTAP-Instanzen.
- Für diese Schritte ist die Verwendung der AWS CLI erforderlich, da Sie das Limit für den Response-Hop auf 3 ändern müssen.

Über diese Aufgabe

IMDSv2 bietet einen verbesserten Schutz vor Schwachstellen. "Weitere Informationen zu IMDSv2 finden Sie im AWS Security Blog"

Der Instance Metadata Service (IMDS) wird in EC2-Instanzen wie folgt aktiviert:

- Für neue Connector-Implementierungen von BlueXP oder durch die Nutzung von "Terraform-Skripte", IMDSv2 ist standardmäßig auf der EC2-Instanz aktiviert.
- Wenn Sie eine neue EC2-Instanz in AWS starten und dann die Connector-Software manuell installieren, ist

IMDSv2 standardmäßig ebenfalls aktiviert.

- Wenn Sie den Connector vom AWS Marketplace starten, ist IMDSv1 standardmäßig aktiviert. Sie können IMDSv2 auf der EC2-Instanz manuell konfigurieren.
- Für bestehende Connectors wird IMDSv1 weiterhin unterstützt, Sie können IMDSv2 jedoch manuell auf der EC2-Instanz konfigurieren, wenn Sie dies wünschen.
- Für Cloud Volumes ONTAP ist IMDSv1 standardmäßig auf neuen und bestehenden Instanzen aktiviert. Sie können IMDSv2 auf den EC2-Instanzen manuell konfigurieren, wenn Sie möchten.

Schritte

1. Erfordern die Verwendung von IMDSv2 auf der Connector-Instanz:

   a. Stellen Sie eine Verbindung zur Linux-VM für den Connector her.

      Als Sie die Connector-Instanz in AWS erstellt haben, haben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel angegeben. Sie können dieses Schlüsselpaar für SSH zur Instanz verwenden. Der Benutzername für die EC2 Linux-Instanz ist ubuntu (für Connectors, die vor Mai 2023 erstellt wurden, war der Benutzername ec2-user).

      "AWS Docs: Stellen Sie eine Verbindung zu Ihrer Linux-Instanz her"

   b. Installieren Sie die AWS CLI.

      "AWS Docs: Installieren oder aktualisieren Sie auf die neueste Version der AWS CLI"

   c. Verwenden Sie die `aws ec2 modify-instance-metadata-options` Befehl, um die Verwendung von IMDSv2 zu erfordern und das PUT Response Hop Limit auf 3 zu ändern.

      Beispiel

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

      Der `http-tokens` Parameter setzt IMDSv2 auf erforderlich. Wenn `http-tokens` Ist erforderlich, müssen Sie auch festlegen `http-endpoint` Auf aktiviert.

2. Erfordern die Verwendung von IMDSv2 auf Cloud Volumes ONTAP Instanzen:

   a. Wechseln Sie zum "Amazon EC2 Konsole"

   b. Wählen Sie im Navigationsbereich **instances** aus.

   c. Wählen Sie eine Cloud Volumes ONTAP-Instanz aus.

   d. Wählen Sie **Aktionen > Instanzeinstellungen > Optionen für Instanzmetadaten ändern**.

   e. Wählen Sie im Dialogfeld **Modify Instance Metadata options** Folgendes aus:

      - Wählen Sie für **Instance Metadata Service enable** aus.
      - Wählen Sie für **IMDSv2 required** aus.

- Wählen Sie **Speichern**.

f. Wiederholen Sie diese Schritte für andere Cloud Volumes ONTAP Instanzen, einschließlich des HA Mediators.

g. "Stoppen und starten Sie die Cloud Volumes ONTAP-Instanzen"

Ergebnis

Die Connector-Instanz und die Cloud Volumes ONTAP-Instanzen sind jetzt so konfiguriert, dass sie IMDSv2 verwenden.

Management von Connector-Upgrades

Wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden, aktualisiert BlueXP Ihren Connector automatisch auf die neueste Version, sofern der Connector über ausgehenden Internetzugang verfügt, um das Softwareupdate abzurufen. Wenn Sie die Verwaltung bei Aktualisierung des Connectors manuell vornehmen müssen, können Sie automatische Upgrades für den Standardmodus oder den eingeschränkten Modus deaktivieren.

Wenn Sie BlueXP im privaten Modus ausführen, müssen Sie den Connector immer selbst aktualisieren.

Deaktivieren Sie automatische Upgrades

Das Deaktivieren der automatischen Aktualisierung für den Connector besteht aus zwei Schritten. Zunächst müssen Sie sicherstellen, dass Ihr Connector gesund und aktuell ist. Anschließend bearbeiten Sie eine Konfigurationsdatei, um die automatische Aktualisierungsfunktion zu deaktivieren.

Sie können die automatischen Upgrades nur deaktivieren, wenn Sie über Connector-Version 3.9.48 oder höher verfügen.

Überprüfen Sie den Zustand des Connectors

Sie sollten überprüfen, ob Ihr Connector stabil ist und alle Container, die auf Ihrer Konnektor-VM ausgeführt werden, ordnungsgemäß ausgeführt werden. Nachdem Sie die automatischen Upgrades deaktiviert haben, prüft die Connector-VM nicht mehr nach neuen Services oder Upgrade-Paketen.

Verwenden Sie einen der folgenden Befehle, um den Anschluss zu überprüfen. Alle Dienste sollten den Status *Running* haben. Ist dies nicht der Fall, wenden Sie sich vor dem Deaktivieren der automatischen Aktualisierung an den NetApp Support.

Docker

```
docker ps -a
```

Podman

```
podman ps -a
```

Deaktivieren Sie die automatische Aktualisierung für den Connector

Sie deaktivieren die automatischen Upgrades, indem Sie in der Datei *com/opt/Application/NetApp/Service-Manager-2/config.json* das Flag *isUpgradeDisabled* setzen. Standardmäßig ist dieses Flag auf false gesetzt und Ihr Connector wird automatisch aktualisiert. Sie können dieses Flag auf true setzen, um automatische Upgrades zu deaktivieren. Sie sollten mit der JSON-Syntax vertraut sein, bevor Sie diesen Schritt abschließen.

Um die automatische Aktualisierung wieder zu aktivieren, verwenden Sie diese Schritte und setzen Sie das *isUpgradeDisabled*-Flag auf false.

Schritte

1. Stellen Sie sicher, dass Ihr Anschluss auf dem neuesten Stand und in gutem Zustand ist.
2. Erstellen Sie eine Sicherungskopie der Datei */opt/Application/NetApp/Service-Manager-2/config.json*, um sicherzustellen, dass Sie Ihre Änderungen rückgängig machen können.
3. Bearbeiten Sie die Datei */opt/Application/NetApp/Service-Manager-2/config.json* und ändern Sie den Wert des Flags *isUpgradeDisabled* auf true.

   ```
   "isUpgradeDisabled": true,
   ```

4. Speichern Sie Ihre Datei.
5. Starten Sie den Service Manager 2 neu, indem Sie den folgenden Befehl ausführen:

   ```
   systemctl restart netapp-service-manager.service
   ```

6. Führen Sie den folgenden Befehl aus, und überprüfen Sie, ob der Connector-Status als *Active(Running)*: _ Angezeigt wird

   ```
   systemctl status netapp-service-manager.service
   ```

Aktualisieren Sie den Anschluss

Der Connector muss während des Upgrade-Vorgangs neu gestartet werden, damit die webbasierte Konsole während des Upgrades nicht verfügbar ist.

Schritte

1. Laden Sie die Connector-Software von der herunter "NetApp Support Website".

   Stellen Sie sicher, dass Sie das Offline-Installationsprogramm für private Netzwerke ohne Internetzugang herunterladen.

2. Kopieren Sie das Installationsprogramm auf den Linux-Host.
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

Wobei <version> die Version des Connectors ist, den Sie heruntergeladen haben.

4. Führen Sie das Installationsskript aus:

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

Wobei <version> die Version des Connectors ist, den Sie heruntergeladen haben.

5. Nachdem die Aktualisierung abgeschlossen ist, können Sie die Version des Connectors überprüfen, indem Sie **Hilfe > Support > Connector** aufrufen.

Arbeiten Sie mit mehreren Anschlüssen

Wenn Sie mehrere Connectors verwenden, können Sie mit BlueXP direkt von der Konsole aus zwischen diesen Connectors wechseln. Sie können auch eine einzige Arbeitsumgebung mit mehreren Connectors verwalten.

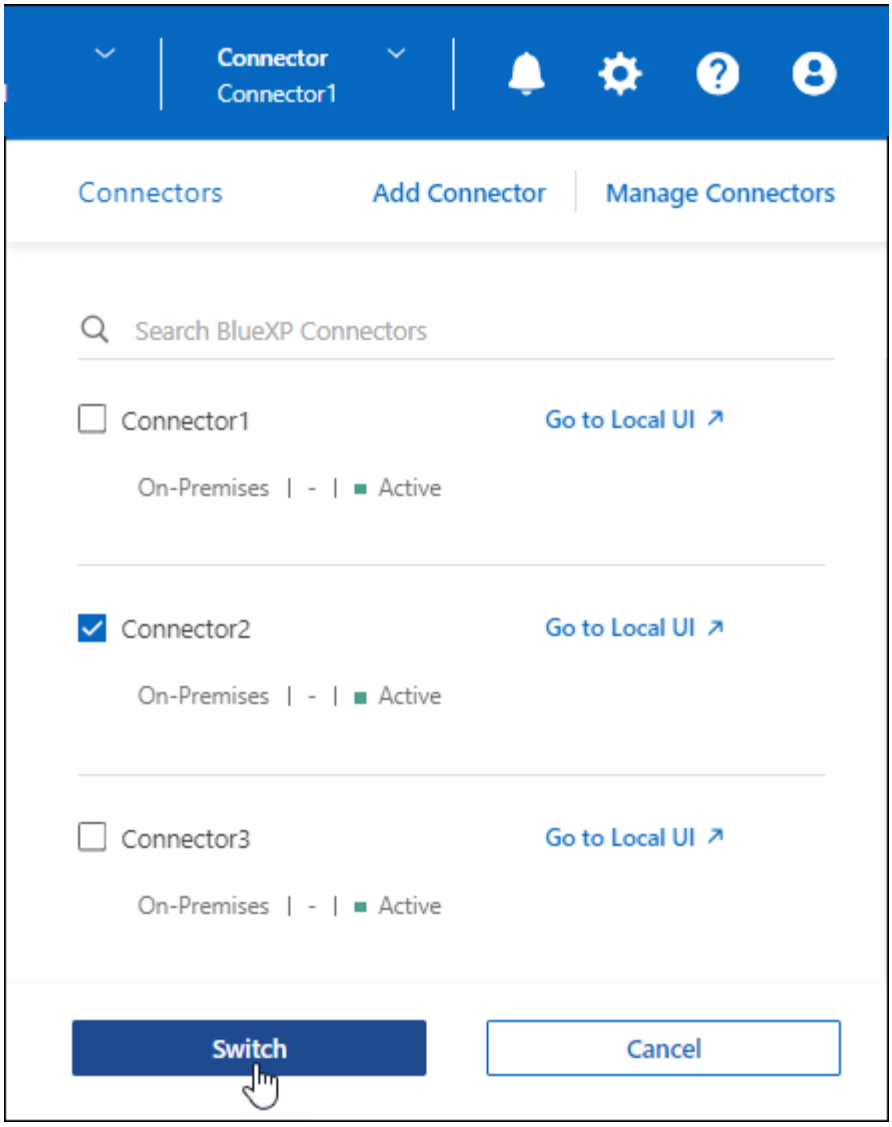
Zwischen den Anschlüssen wechseln

Wenn Sie über mehrere Anschlüsse verfügen, können Sie zwischen diesen wechseln, um die Arbeitsumgebungen zu sehen, die mit einem bestimmten Konnektor verknüpft sind.

Nehmen wir zum Beispiel an, dass Sie in einer Multi-Cloud-Umgebung arbeiten. Möglicherweise verfügen Sie über einen Connector in AWS und einen anderen in Google Cloud. Zum Managen der Cloud Volumes ONTAP Systeme, die in diesen Clouds ausgeführt werden, müsste zwischen diesen Anschlüssen gewechselt werden.

Schritt

1. Wählen Sie die Dropdown-Liste **Connector** aus, wählen Sie einen anderen Konnektor aus und wählen Sie dann **Switch** aus.



Ergebnis

BlueXP aktualisiert und zeigt die Arbeitsumgebungen, die mit dem ausgewählten Connector verknüpft sind.

Richten Sie eine Disaster Recovery-Konfiguration ein

Sie können eine Arbeitsumgebung mit mehreren Connectors gleichzeitig für Disaster Recovery-Zwecke verwalten. Wenn ein Anschluss ausfällt, können Sie zum anderen Connector wechseln, um die Arbeitsumgebung sofort zu verwalten.

Schritte

1. Wechseln Sie zu dem anderen Connector, den Sie mit der Arbeitsumgebung verwalten möchten.
2. Erkennung der vorhandenen Arbeitsumgebung
   - "Fügen Sie vorhandene Cloud Volumes ONTAP-Systeme zu BlueXP hinzu"
   - "ONTAP Cluster erkennen"
3. Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung verwalten, wählen Sie **Einstellungen > Verbindungseinstellungen** und stellen Sie den Modus für die Kapazitätsverwaltung auf **manueller Modus** ein.

Um Konflikte zu vermeiden, sollte nur der Hauptanschluss auf **Automatischer Modus** gesetzt werden.

"Erfahren Sie mehr über den Kapazitätsmanagement-Modus"

Fehlersuche für den Anschluss durchführen

Um Probleme mit dem Konnektor zu beheben, können Sie mit dem NetApp-Support zusammenarbeiten, der Sie möglicherweise nach Ihrer System-ID, der Connector-Version oder den neuesten AutoSupport-Meldungen fragt. Sie können auch die NetApp Wissensdatenbank anzeigen, um Fehler selbst zu beheben.

Verwandte Informationen

"Holen Sie sich Hilfe vom NetApp-Support".

Suchen Sie die System-ID für einen Anschluss

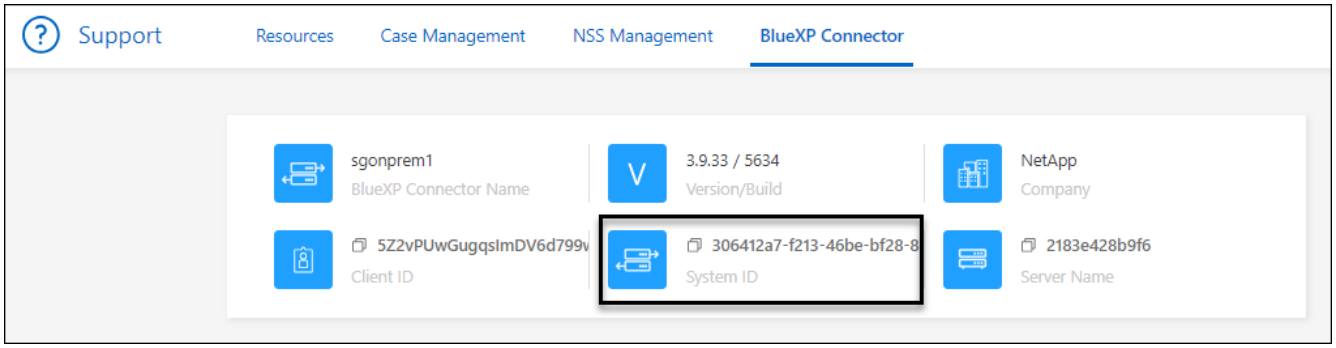
Um Ihnen bei den ersten Schritten zu helfen, fragen Sie möglicherweise Ihr NetApp Ansprechpartner nach der System-ID Ihres Connectors. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol aus.
2. Wählen Sie **Support > BlueXP Connector**.

   Die System-ID wird oben auf der Seite angezeigt.

   Beispiel



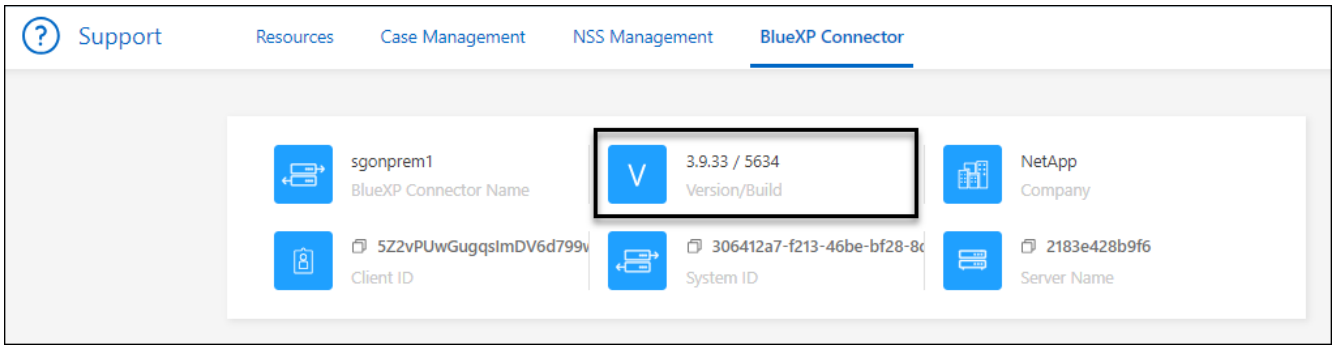
Anzeigen der Version eines Connectors

Sie können die Version Ihres Connectors anzeigen, um zu überprüfen, ob der Connector automatisch auf die neueste Version aktualisiert wurde, oder weil Sie ihn mit Ihrem NetApp-Vertreter teilen müssen.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol aus.
2. Wählen Sie **Support > BlueXP Connector**.

   Die Version wird oben auf der Seite angezeigt.

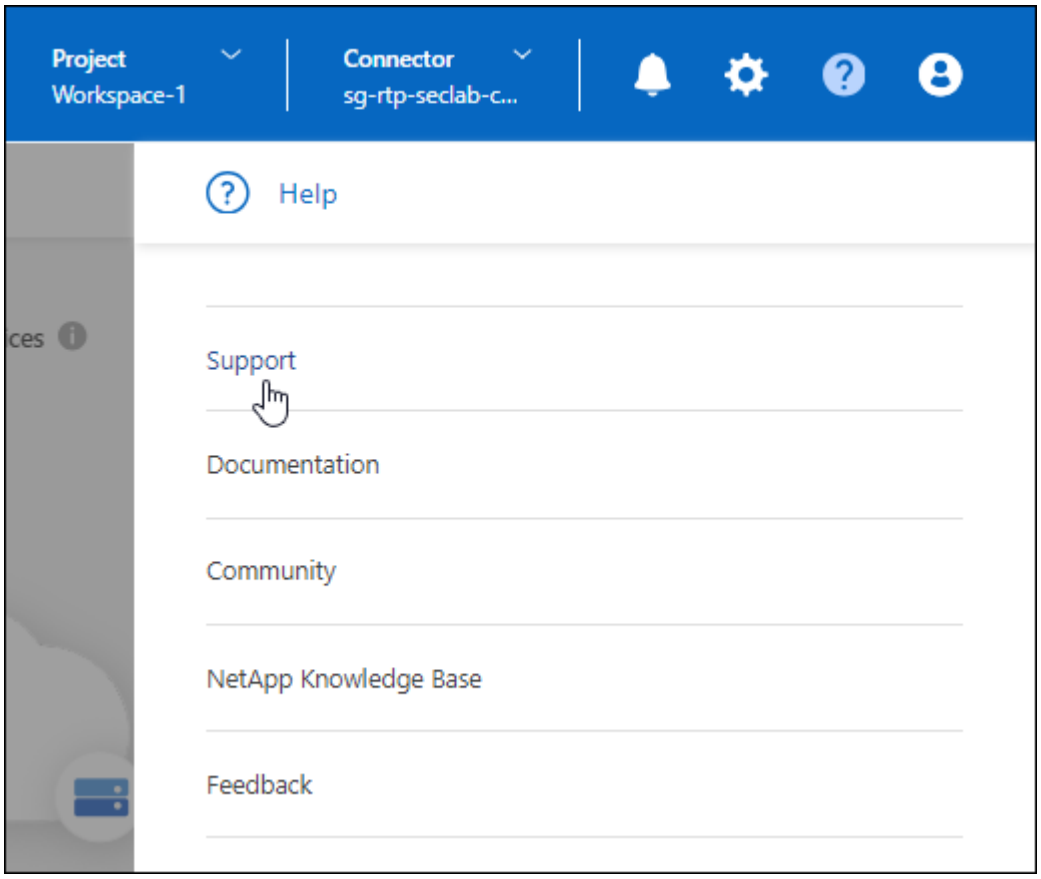


Laden Sie eine AutoSupport Nachricht herunter oder senden Sie sie

Wenn Sie Probleme haben, werden Sie möglicherweise von den Mitarbeitern von NetApp gebeten, zur Fehlerbehebung eine AutoSupport Nachricht an den NetApp Support zu senden.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.

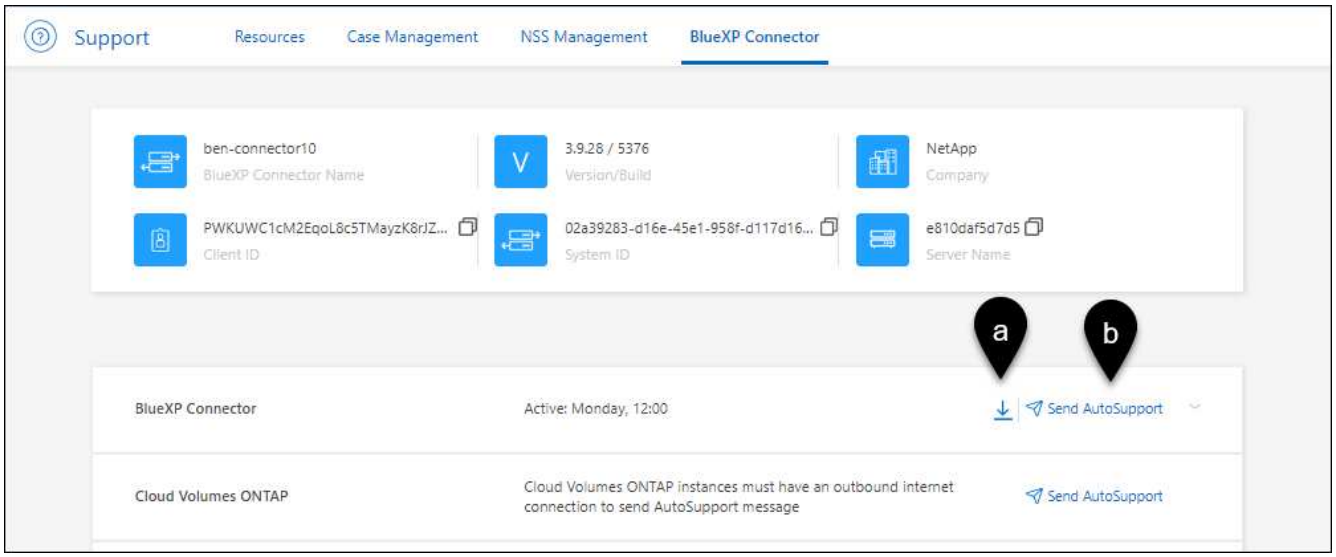


2. Wählen Sie **BlueXP Connector** aus.
3. Je nachdem, wie Sie die Informationen an den NetApp Support senden, wählen Sie eine der folgenden Optionen:

   a. Wählen Sie die Option, um die AutoSupport-Nachricht auf Ihren lokalen Computer herunterzuladen. Sie können es dann auf bevorzugte Art und Weise an den NetApp Support senden.

   b. Wählen Sie **AutoSupport senden**, um die Nachricht direkt an den NetApp Support zu senden.

Aufgrund des Lastenausgleichs kann das Senden von AutoSupport-Nachrichten durch BlueXP bis zu fünf Stunden dauern. Bei dringenden Mitteilungen laden Sie die Datei herunter und senden Sie sie manuell.



Beheben Sie Download-Fehler bei Verwendung eines Google Cloud NAT-Gateways

Der Connector lädt automatisch Software-Updates für Cloud Volumes ONTAP herunter. Der Download kann fehlschlagen, wenn Ihre Konfiguration ein Google Cloud NAT Gateway verwendet. Sie können dieses Problem beheben, indem Sie die Anzahl der Teile begrenzen, in die das Software-Image unterteilt ist. Dieser Schritt muss mithilfe der BlueXP API abgeschlossen werden.

Schritt

1. SENDEN SIE EINE PUT-Anforderung an /occm/config mit dem folgenden JSON als Text:

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

Der Wert für *maxDownloadSessions* kann 1 oder eine beliebige Ganzzahl größer als 1 sein. Wenn der Wert 1 ist, wird das heruntergeladene Bild nicht geteilt.

Beachten Sie, dass 32 ein Beispielwert ist. Der Wert, den Sie verwenden sollten, hängt von Ihrer NAT-Konfiguration und der Anzahl der Sitzungen ab, die Sie gleichzeitig haben können.

"Erfahren Sie mehr über den Aufruf der /occm/config API"

Holen Sie sich Hilfe in der NetApp Knowledge Base

"Zeigen Sie die vom NetApp-Supportteam erstellten Fehlerbehebungsinformationen an".

Deinstallieren Sie den Connector, und entfernen Sie ihn

Deinstallieren Sie die Connector-Software, um Probleme zu beheben oder die Software

dauerhaft vom Host zu entfernen. Welche Schritte Sie durchführen müssen, hängt vom verwendeten Bereitstellungsmodus ab. Sobald ein Connector aus Ihrer Umgebung entfernt wurde, können Sie ihn aus BlueXP entfernen.

"Weitere Informationen zu BlueXP Implementierungsmodi".

Deinstallieren Sie den Connector, wenn Sie den Standard- oder eingeschränkten Modus verwenden

Wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden (mit anderen Worten, der Connector-Host verfügt über eine ausgehende Konnektivität), sollten Sie die folgenden Schritte ausführen, um die Connector-Software zu deinstallieren.

Schritte

1. Stellen Sie eine Verbindung zur Linux-VM für den Connector her.
2. Führen Sie auf dem Linux-Host das Deinstallationsskript aus:

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

   Silent führt das Skript aus, ohne dass Sie zur Bestätigung aufgefordert werden.

Deinstallieren Sie den Connector, wenn Sie den privaten Modus verwenden

Wenn Sie den privaten Modus verwenden (wo der Connector-Host *keine* ausgehende Konnektivität hat), führen Sie die folgenden Schritte aus, um die Connector-Software zu deinstallieren.

Schritt

1. Stellen Sie eine Verbindung zur Linux-VM für den Connector her.
2. Führen Sie auf dem Linux-Host die folgenden Befehle aus:

   ```
   /opt/application/netapp/ds/cleanup.sh
   rm -rf /opt/application/netapp/
   ```

3. Löschen Sie vom Linux-Host alte, nicht verwendete Container-Imagedateien, um im Verzeichnis /var Speicherplatz für die Neuinstallation freizugeben.

   Podman

   ```
   podman system prune --all
   ```

   Docker

   ```
   docker system prune -a
   ```

Entfernen Sie die Anschlüsse von BlueXP

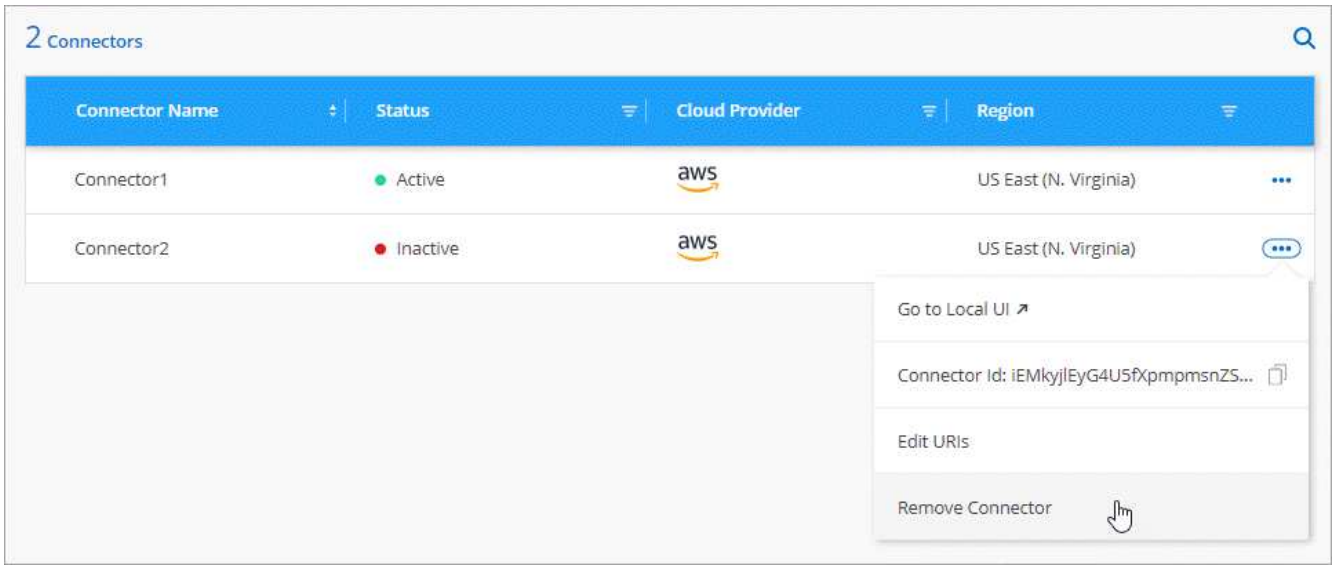
Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Connectors in BlueXP entfernen. Dies ist möglicherweise der Fall, wenn Sie die virtuelle Connector-Maschine löschen oder die Connector-Software deinstallieren.

Beachten Sie Folgendes zum Entfernen eines Konnektors:

- Durch diese Aktion wird die virtuelle Maschine nicht gelöscht.
- Diese Aktion kann nicht rückgängig gemacht werden. Wenn Sie einen Connector einmal entfernt haben, können Sie ihn nicht wieder hinzufügen.

Schritte

1. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.
2. Wählen Sie **Connectors Verwalten**.
3. Wählen Sie das Aktionsmenü für einen inaktiven Konnektor aus und wählen Sie **Connector entfernen**.



4. Geben Sie den Namen des zu bestätigten Connectors ein, und wählen Sie dann **Entfernen**.

Standardkonfiguration für den Konnektor

Möglicherweise möchten Sie mehr über die Konfiguration des Connectors erfahren, bevor Sie ihn bereitstellen, oder wenn Sie Probleme beheben müssen.

Standardkonfiguration mit Internetzugang

Die folgenden Konfigurationsdetails gelten, wenn Sie den Connector von BlueXP, vom Markt Ihres Cloud-Providers oder manuell auf einem lokalen Linux-Host mit Internetzugang installiert haben.

AWS – Details

Wenn Sie den Connector von BlueXP oder vom Marktplatz des Cloud-Providers implementiert haben, beachten Sie Folgendes:

- Der EC2-Instanztyp ist t3.2xlarge.

- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Installation beinhaltet die Docker Engine, das erforderliche Tool zur Container-Orchestrierung.
- Der Benutzername für die EC2 Linux-Instanz ist ubuntu (für Connectors, die vor Mai 2023 erstellt wurden, war der Benutzername ec2-user).
- Die Standardfestplatte des Systems ist eine 100 gib gp2-Festplatte.

Azure – Details

Wenn Sie den Connector von BlueXP oder vom Marktplatz des Cloud-Providers implementiert haben, beachten Sie Folgendes:

- Der VM-Typ ist Standard_D8S_v3.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Installation beinhaltet die Docker Engine, das erforderliche Tool zur Container-Orchestrierung.
- Die Standardfestplatte des Systems beträgt 100 gib Premium-SSD-Festplatte.

Google Cloud-Details

Wenn Sie den Connector von BlueXP implementiert haben, beachten Sie Folgendes:

- Die VM-Instanz ist n2-Standard-8.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Installation beinhaltet die Docker Engine, das erforderliche Tool zur Container-Orchestrierung.
- Die Standardfestplatte des Systems beträgt eine persistente SSD-Festplatte mit 100 gib.

Installationsordner

Der Installationsordner des Connectors befindet sich an folgender Stelle:

/opt/application/netapp/cloudmanager

Log-Dateien

Protokolldateien sind in den folgenden Ordnern enthalten:

- /opt/application/netapp/cloudmanager/log
  Oder
- /Opt/Application/netapp/Service-Manager-2/logs (beginnend mit den neuen 3.9.23 Installationen)

  Die Protokolle in diesen Ordnern enthalten Details zum Connector.

- /Opt/Application/netapp/CloudManager/docker_occm/Data/log

  Die Protokolle in diesem Ordner enthalten Details zu Cloud-Diensten und zum BlueXP-Dienst, der auf dem Connector ausgeführt wird.

Verbindungsdienst

- Der BlueXP-Dienst heißt occm.
- Der occm-Dienst ist vom MySQL-Dienst abhängig.

  Wenn der MySQL-Dienst nicht verfügbar ist, ist auch der occm-Dienst nicht verfügbar.

Ports

Der Connector verwendet die folgenden Ports auf dem Linux-Host:

- 80 für HTTP-Zugriff
- 443 für HTTPS-Zugriff

Standardkonfiguration ohne Internetzugang

Die folgende Konfiguration gilt, wenn Sie den Connector manuell auf einem lokalen Linux-Host installiert haben, der keinen Internetzugang hat. "Erfahren Sie mehr über diese Installationsoption".

- Der Installationsordner des Connectors befindet sich an folgender Stelle:

  /Opt/Application/netapp/ds

- Protokolldateien sind in den folgenden Ordnern enthalten:

  /Var/lib/docker/Volumes/ds_occmdata/data-data/log

  Die Protokolle in diesem Ordner enthalten Details zu den Konnektor- und Docker-Images.

- Alle Services werden in Docker Containern ausgeführt

  Die Dienste sind abhängig vom laufenden Docker Runtime Service

- Der Connector verwendet die folgenden Ports auf dem Linux-Host:
  - 80 für HTTP-Zugriff
  - 443 für HTTPS-Zugriff

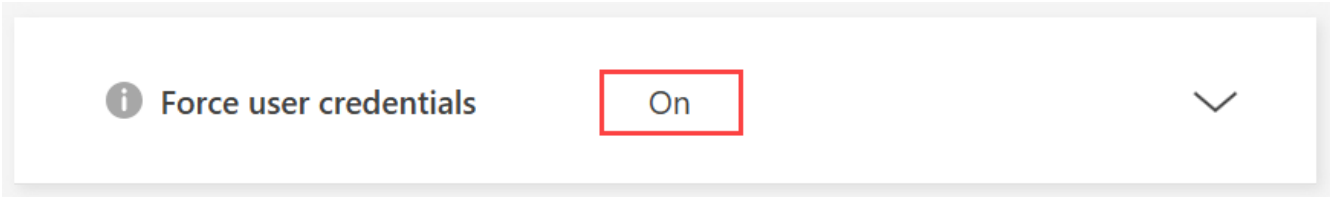
Erzwingen der ONTAP-Berechtigungen für die erweiterte ONTAP-Ansicht (ONTAP System Manager)

Standardmäßig ermöglichen die Connector-Anmeldeinformationen Benutzern den Zugriff auf die erweiterte Ansicht (ONTAP System Manager). Sie können Benutzer stattdessen zur Eingabe ihrer ONTAP-Anmeldeinformationen auffordern. So wird sichergestellt, dass die ONTAP-Berechtigungen eines Benutzers angewendet werden, wenn er mit ONTAP-Clustern sowohl in Cloud Volumes ONTAP- als auch in ONTAP On-Premises-Clustern arbeitet.

Sie müssen über die Rolle des Organisationsadministrators verfügen, um die Connector-Einstellungen bearbeiten zu können.

Schritte

1. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.
2. Wählen Sie **Connectors Verwalten**.
3. Wählen Sie das Aktionsmenü in der Zeile aus, die dem Connector entspricht, den Sie bearbeiten möchten.
4. Erweitern Sie die Option **Anmeldeinformationen erzwingen**.
5. Aktivieren Sie das Kontrollkästchen, um die Option **Anmeldeinformationen erzwingen** zu aktivieren, und wählen Sie dann **Speichern**.
6. Überprüfen Sie, ob die Option **Anmeldeinformationen erzwingen** aktiviert ist.



Anmeldedaten und Abonnements

AWS

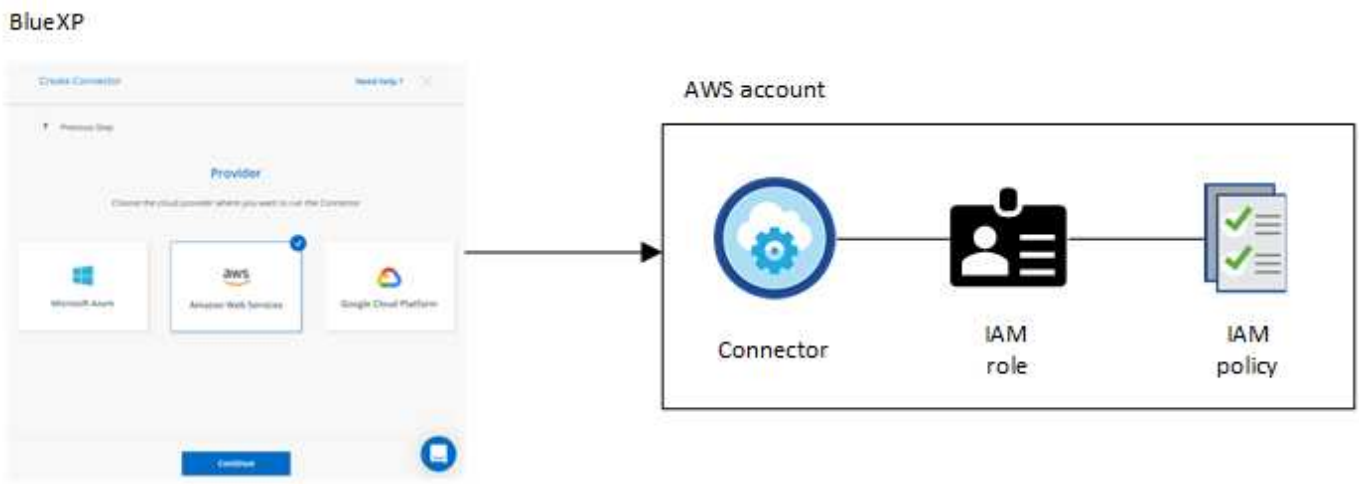
Erfahren Sie mehr über AWS-Anmeldeinformationen und Berechtigungen in BlueXP

Informieren Sie sich, wie BlueXP für Sie AWS Zugangsdaten verwendet, um Aktionen durchzuführen und wie diese Zugangsdaten mit Marketplace-Abonnements verknüpft sind. Diese Details zu verstehen, ist hilfreich, wenn Sie die Anmeldedaten für einen oder mehrere AWS-Konten in BlueXP managen. So könnte es beispielsweise interessant sein, wann Sie BlueXP um zusätzliche AWS Zugangsdaten erweitern können.

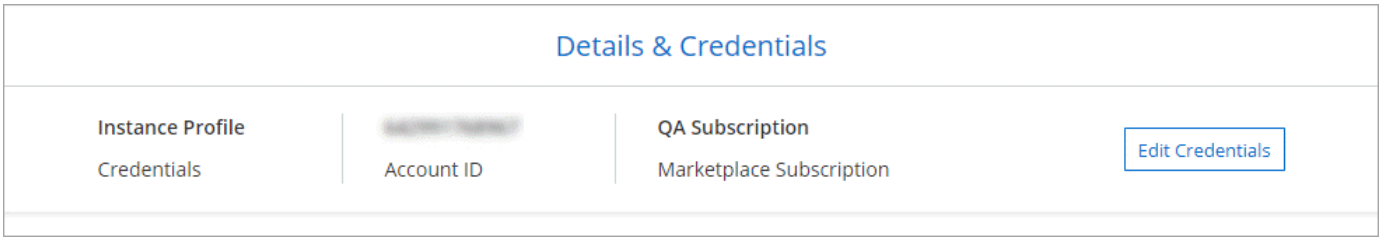
Erste AWS Zugangsdaten

Wenn Sie einen Connector von BlueXP bereitstellen, müssen Sie das ARN einer IAM-Rolle oder Zugriffsschlüssel für einen IAM-Benutzer bereitstellen. Die verwendete Authentifizierungsmethode muss über die erforderlichen Berechtigungen für die Bereitstellung der Connector-Instanz in AWS verfügen. Die erforderlichen Berechtigungen werden im aufgeführt "Connector-Implementierungsrichtlinie für AWS".

Wenn BlueXP die Connector-Instanz in AWS startet, erstellt sie eine IAM-Rolle und ein Instanzprofil für die Instanz. Zudem wird eine Richtlinie angehängt, die dem Connector Berechtigungen für das Management von Ressourcen und Prozessen innerhalb dieses AWS-Kontos bietet. "Überprüfen Sie, wie BlueXP die Berechtigungen verwendet".



Wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen, wählt BlueXP standardmäßig diese AWS Zugangsdaten aus:



Alle Cloud Volumes ONTAP Systeme können über die ersten AWS Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

Zusätzliche AWS Zugangsdaten

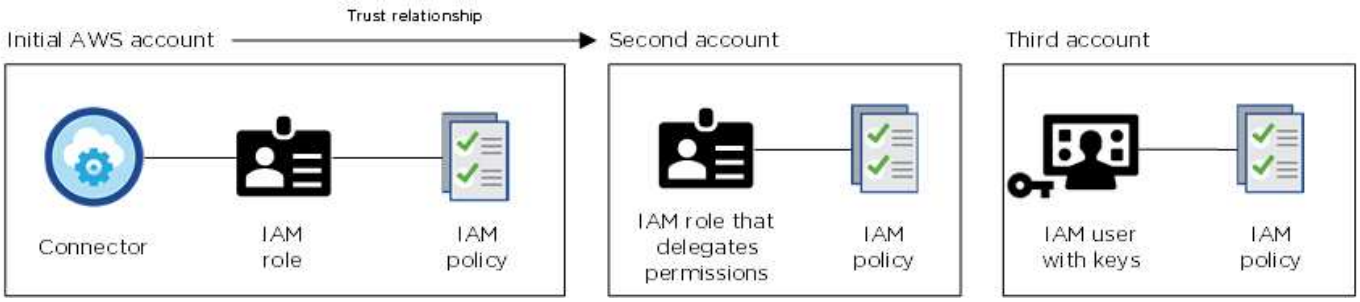
In den folgenden Fällen können Sie BlueXP zusätzliche AWS Zugangsdaten hinzufügen:

- Sie können Ihren bestehenden BlueXP Connector mit einem zusätzlichen AWS-Konto verwenden
- So erstellen Sie einen neuen Connector in einem bestimmten AWS-Konto
- So erstellen und verwalten Sie FSX für ONTAP-Dateisysteme

Weitere Informationen finden Sie in den folgenden Abschnitten.

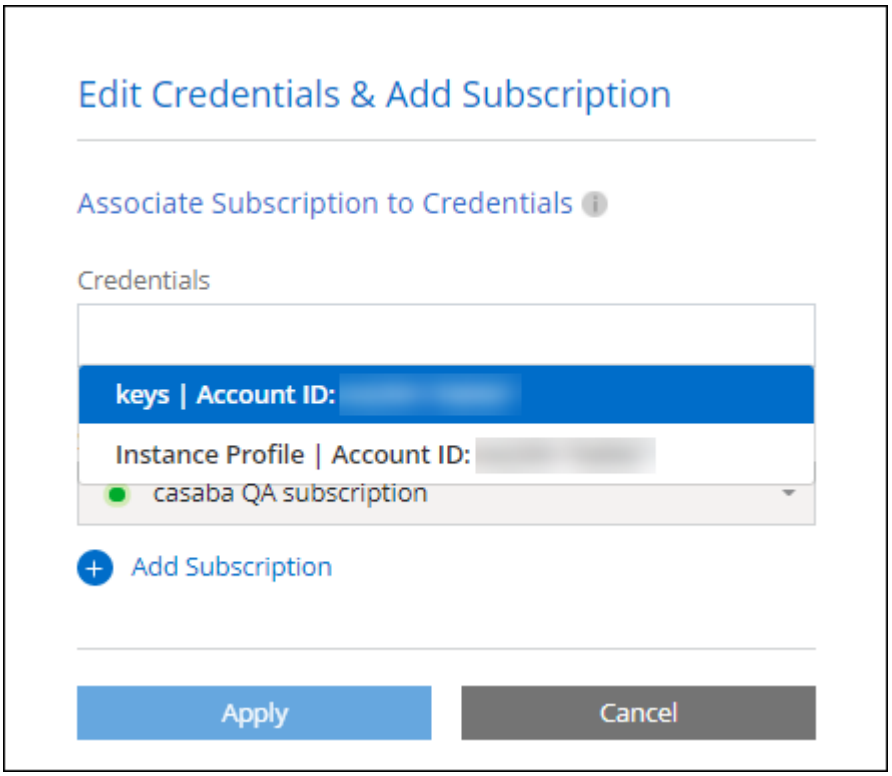
Fügen Sie AWS-Anmeldedaten hinzu, um einen Connector mit einem anderen AWS-Konto zu verwenden

Wenn Sie BlueXP mit zusätzlichen AWS-Konten nutzen möchten, können Sie entweder AWS-Schlüssel für einen IAM-Benutzer oder den ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen. Die folgende Abbildung zeigt zwei zusätzliche Konten: Eines mit Berechtigungen über eine IAM-Rolle in einem vertrauenswürdigen Konto und ein weiteres über die AWS Schlüssel eines IAM-Benutzers:



Sie würden dann die Account-Anmeldedaten zu BlueXP hinzufügen, indem Sie den Amazon Resource Name (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

Sie können beispielsweise beim Erstellen einer neuen Cloud Volumes ONTAP-Arbeitsumgebung zwischen den Anmeldedaten wechseln:



"Informieren Sie sich, wie Sie einem vorhandenen Connector AWS-Anmeldedaten hinzufügen."

Fügen Sie AWS-Anmeldedaten hinzu, um einen Connector zu erstellen

Durch das Hinzufügen neuer AWS Zugangsdaten zu BlueXP werden die zum Erstellen eines Connectors erforderlichen Berechtigungen gewährt.

"Erfahren Sie, wie Sie zur Erstellung eines Connectors AWS Zugangsdaten zu BlueXP hinzufügen"

AWS Zugangsdaten für FSX for ONTAP hinzufügen

Das Hinzufügen neuer AWS Zugangsdaten zu BlueXP bietet die nötigen Berechtigungen zum Erstellen und Managen einer Arbeitsumgebung von FSX für ONTAP.

"Informieren Sie sich, wie Sie BlueXP für Amazon FSX for ONTAP mit AWS Zugangsdaten ergänzen"

Anmeldedaten und Abonnements für den Marktplatz

Die Zugangsdaten, die Sie einem Connector hinzufügen, müssen mit einem AWS Marketplace Abonnement verbunden sein, sodass Sie für Cloud Volumes ONTAP einen Stundensatz (PAYGO) oder über einen Jahresvertrag zahlen und andere BlueXP Services nutzen können.

"Verbinden Sie ein AWS Abonnement".

Beachten Sie Folgendes zu AWS Zugangsdaten und Marketplace-Abonnements:

- Sie können nur ein AWS Marketplace Abonnement mit einem Satz von AWS Zugangsdaten verknüpfen
- Sie können ein bestehendes Marketplace-Abonnement durch ein neues Abonnement ersetzen

Häufig gestellte Fragen

Die folgenden Fragen beziehen sich auf Anmeldeinformationen und Abonnements.

Wie kann ich meine AWS Zugangsdaten sicher drehen?

Wie oben in den Abschnitten beschrieben, können Sie mit BlueXP Ihre AWS Zugangsdaten auf verschiedene Weise bereitstellen: Eine mit der Connector-Instanz verbundene IAM-Rolle, indem Sie eine IAM-Rolle in einem vertrauenswürdigen Konto übernehmen oder AWS Zugriffsschlüssel bereitstellen.

Bei den ersten beiden Optionen verwendet BlueXP den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dies ist die Best Practice, also automatisch und sicher.

Wenn Sie BlueXP mit AWS-Zugriffsschlüsseln zur Verfügung stellen, sollten Sie die Schlüssel durch Aktualisierung in BlueXP in einem regelmäßigen Intervall drehen. Es handelt sich hierbei um einen vollständig manuellen Prozess.

Kann ich das AWS Marketplace Abonnement für Cloud Volumes ONTAP Arbeitsumgebungen ändern?

Ja, können Sie. Wenn Sie das AWS Marketplace Abonnement ändern, das mit einer Reihe von Zugangsdaten verknüpft ist, wird das neue Abonnement für alle vorhandenen und neuen Cloud Volumes ONTAP Arbeitsumgebungen in Rechnung gestellt.

"Verbinden Sie ein AWS Abonnement".

Kann ich mehrere AWS Zugangsdaten mit jeweils unterschiedlichen Marketplace-Abonnements hinzufügen?

Alle AWS Zugangsdaten, die demselben AWS Konto angehören, werden demselben AWS Marketplace Abonnement zugeordnet.

Wenn Sie mehrere AWS-Anmeldeinformationen haben, die zu verschiedenen AWS-Konten gehören, können diese Anmeldeinformationen mit demselben AWS Marketplace Abonnement oder verschiedenen Abonnements verknüpft werden.

Kann ich vorhandene Cloud Volumes ONTAP Arbeitsumgebungen auf ein anderes AWS Konto verschieben?

Nein, es ist nicht möglich, die AWS Ressourcen, die Ihrer Cloud Volumes ONTAP Arbeitsumgebung zugeordnet sind, in ein anderes AWS Konto zu verschieben.

Wie funktionieren Anmeldeinformationen für Marktplatzbereitstellungen und lokale Bereitstellungen?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Connector beschrieben, der aus BlueXP stammt. Sie können einen Connector auch über AWS Marketplace in AWS implementieren und die Connector-Software manuell auf Ihrem eigenen Linux-Host installieren.

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Sie können bei lokalen Implementierungen keine IAM-Rolle für das BlueXP System einrichten, aber mithilfe von AWS Zugriffsschlüsseln bieten Sie Berechtigungen.

Weitere Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- Standardmodus
  - "Richten Sie Berechtigungen für eine AWS Marketplace-Implementierung ein"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"
- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

Management von AWS Zugangsdaten und Marketplace-Abonnements für BlueXP

Fügen Sie AWS-Anmeldeinformationen hinzu und verwalten Sie sie, damit Sie Cloud-Ressourcen in Ihren AWS-Konten von BlueXP aus bereitstellen und verwalten können. Wenn Sie mehrere AWS Marketplace-Abonnements managen, können Sie jede davon auf der Seite Anmeldedaten verschiedenen AWS-Anmeldedaten zuweisen.

Überblick

AWS Zugangsdaten können zu einem vorhandenen Connector oder direkt zu BlueXP hinzugefügt werden:

- Fügen Sie einem vorhandenen Connector zusätzliche AWS Zugangsdaten hinzu

  Fügen Sie einem Connector AWS-Anmeldeinformationen hinzu, um Ressourcen in Ihrer Cloud-Umgebung zu verwalten. Erfahren Sie, wie Sie AWS Zugangsdaten zu einem Connector hinzufügen.

- Fügen Sie zur Erstellung eines Connectors AWS Credentials zu BlueXP hinzu

  Wenn Sie BlueXP neue AWS-Anmeldeinformationen hinzufügen, erhalten Sie mit BlueXP die erforderlichen Berechtigungen zum Erstellen eines Connectors. Erfahren Sie, wie Sie AWS Zugangsdaten zu BlueXP hinzufügen.

- Fügen Sie AWS Credentials zu BlueXP für FSX für ONTAP hinzu

  Fügen Sie BlueXP neue AWS-Anmeldeinformationen hinzu, um FSx für ONTAP zu erstellen und zu verwalten. "Erfahren Sie, wie Sie Berechtigungen für FSX für ONTAP einrichten"

So drehen Sie die Anmeldeinformationen

Mit BlueXP können Sie AWS Zugangsdaten auf verschiedene Arten bereitstellen: Eine mit der Connector-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder AWS-Zugriffsschlüssel.

"Weitere Informationen zu AWS Zugangsdaten und Berechtigungen".

Bei den ersten beiden Optionen verwendet BlueXP den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dieser Prozess ist die Best Practice, da er automatisch und sicher ist.

Rotieren Sie AWS-Zugriffsschlüssel regelmäßig, indem Sie sie in BlueXP aktualisieren. Dieser Vorgang erfolgt manuell.

Fügen Sie zusätzliche Anmeldedaten zu einem Connector hinzu

Fügen Sie einem Connector zusätzliche AWS-Anmeldedaten hinzu, damit dieser über die erforderlichen Berechtigungen zum Management von Ressourcen und Prozessen in der Public-Cloud-Umgebung verfügt. Sie können entweder den ARN einer IAM-Rolle in einem anderen Konto bereitstellen oder AWS-Zugriffsschlüssel bereitstellen.

Wenn Sie gerade erst mit BlueXP starten, "So nutzt BlueXP AWS Zugangsdaten und Berechtigungen".

Berechtigungen erteilen

Geben Sie die erforderlichen Berechtigungen an, bevor Sie einem Connector AWS-Anmeldeinformationen hinzufügen. Die Berechtigungen ermöglichen dem Connector die Verwaltung von Ressourcen und Prozessen innerhalb dieses AWS-Kontos. Sie können die Berechtigungen mit der ARN einer Rolle in einem vertrauenswürdigen Konto oder mit AWS-Schlüsseln erteilen.

> Wenn Sie einen Connector von BlueXP bereitgestellt haben, hat BlueXP automatisch AWS-Anmeldeinformationen für das Konto hinzugefügt, in dem Sie den Connector bereitgestellt haben. Dadurch wird sichergestellt, dass die erforderlichen Berechtigungen zum Verwalten von Ressourcen vorhanden sind. "Weitere Informationen zu AWS Zugangsdaten und Berechtigungen".

Auswahl

- indem Sie eine IAM-Rolle in einem anderen Konto übernehmen
- Erteilen Sie Berechtigungen durch die Bereitstellung von AWS Schlüsseln

Erteilen Sie Berechtigungen, indem Sie eine IAM-Rolle in einem anderen Konto übernehmen

Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Connector-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie BlueXP über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

Wenn der Connector vor Ort installiert ist, können Sie diese Authentifizierungsmethode nicht verwenden. AWS-Schlüssel müssen verwendet werden.

Schritte

1. Rufen Sie die IAM-Konsole im Zielkonto auf, in dem Sie dem Connector Berechtigungen erteilen möchten.
2. Wählen Sie unter Access Management die Option **Rollen > Rolle erstellen** aus, und befolgen Sie die Schritte zum Erstellen der Rolle.

   Gehen Sie wie folgt vor:

   - Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.

- Wählen Sie **ein weiteres AWS-Konto** aus, und geben Sie die ID des Kontos ein, auf dem sich die Connector-Instanz befindet.
- Erstellen Sie die erforderlichen Richtlinien, indem Sie den Inhalt von kopieren und einfügen "Die IAM-Richtlinien für den Connector".

3. Kopieren Sie die Rolle ARN der IAM-Rolle, damit Sie sie später in BlueXP einfügen können.

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können die Anmeldeinformationen jetzt einem Connector hinzufügen.

Erteilen Sie Berechtigungen durch die Bereitstellung von AWS Schlüsseln

Wenn Sie BlueXP für einen IAM-Benutzer AWS-Schlüssel bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die BlueXP IAM-Richtlinie definiert die AWS Aktionen und Ressourcen, die BlueXP verwenden darf.

Sie müssen diese Authentifizierungsmethode verwenden, wenn der Connector vor Ort installiert ist. Sie können keine IAM-Rolle verwenden.

Schritte

1. Erstellen Sie Richtlinien von der IAM-Konsole aus, indem Sie die Inhalte von kopieren und einfügen "Die IAM-Richtlinien für den Connector".

   "AWS Dokumentation: Erstellung von IAM-Richtlinien"

2. Hängen Sie die Richtlinien an eine IAM-Rolle oder einen IAM-Benutzer an.
   - "AWS Documentation: Erstellung von IAM-Rollen"
   - "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können die Anmeldeinformationen jetzt einem Connector hinzufügen.

Fügen Sie die Anmeldeinformationen hinzu

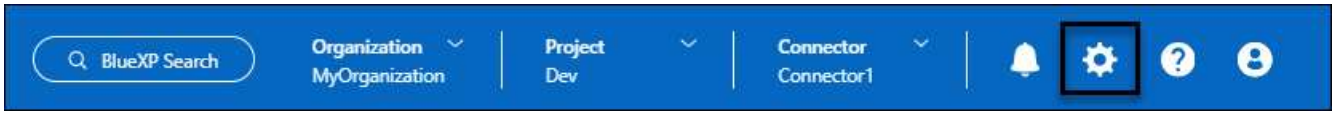
Nachdem Sie ein AWS Konto mit den erforderlichen Berechtigungen bereitgestellt haben, können Sie die Anmeldedaten für dieses Konto einem bestehenden Connector hinzufügen. Damit können Sie Cloud Volumes ONTAP-Systeme in diesem Konto mit demselben Connector starten.

Bevor Sie beginnen

Falls Sie diese Zugangsdaten gerade bei Ihrem Cloud-Provider erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten und fügen Sie dann die Anmeldeinformationen hinzu.

Schritte

1. Wählen Sie über die obere Navigationsleiste den Connector aus, dem Sie Anmeldeinformationen hinzufügen möchten.
2. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.



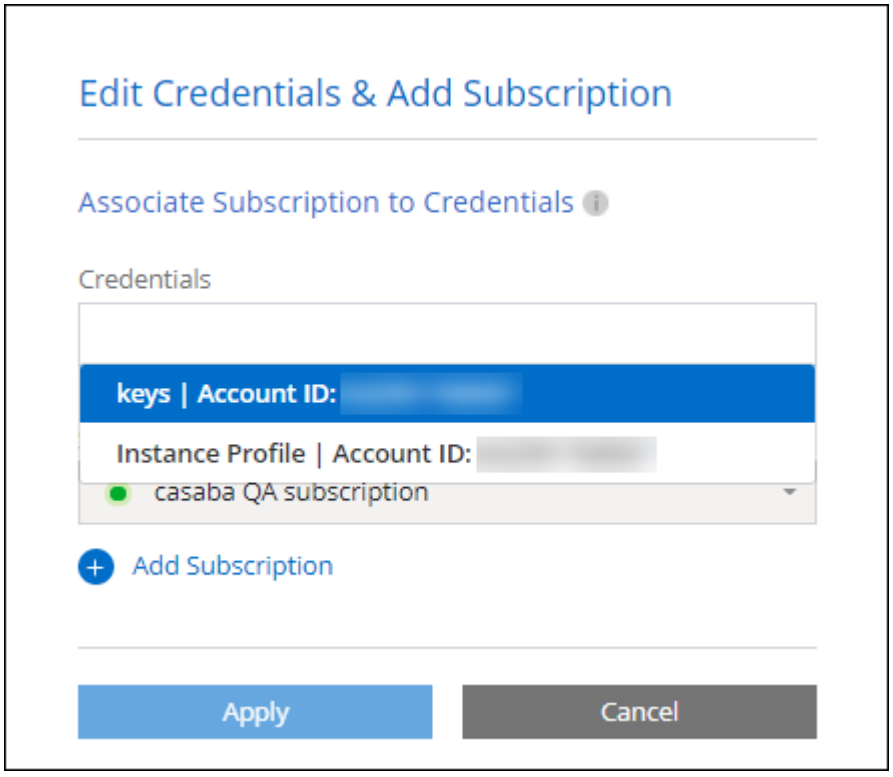
3. Wählen Sie auf der Seite **Unternehmensanmeldeinformationen** oder **Kontoanmeldeinformationen** die Option **Anmeldeinformationen hinzufügen** aus, und befolgen Sie die Schritte im Assistenten.
   a. **Anmeldeort**: Wählen Sie **Amazon Web Services > Connector**.
   b. **Identifizierungsdaten definieren**: Geben Sie den ARN (Amazon Resource Name) einer vertrauenswürdigen IAM-Rolle an, oder geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel ein.
   c. **Marketplace-Abonnement**: Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.

      Um Dienste mit einem Stundensatz (PAYGO) oder mit einem Jahresvertrag zu bezahlen, müssen Sie AWS-Anmeldeinformationen mit Ihrem AWS Marketplace-Abonnement verknüpfen.

   d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

Sie können jetzt bei der Erstellung einer neuen Arbeitsumgebung auf eine andere Gruppe von Anmeldeinformationen von der Seite Details und Anmeldeinformationen wechseln:



Fügen Sie für die Erstellung eines Connectors Anmeldeinformationen zu BlueXP hinzu

Fügen Sie AWS-Anmeldeinformationen hinzu, indem Sie die ARN einer IAM-Rolle angeben, die die zum Erstellen eines Connectors erforderlichen Berechtigungen erteilt. Sie können diese Anmeldeinformationen beim Erstellen eines neuen Connectors auswählen.

Einrichten der IAM-Rolle

Richten Sie eine IAM-Rolle ein, mit der die BlueXP -SaaS-Schicht (Software as a Service) diese Rolle übernehmen kann.

Schritte

1. Wechseln Sie im Zielkonto zur IAM-Konsole.
2. Wählen Sie unter Access Management die Option **Rollen > Rolle erstellen** aus, und befolgen Sie die Schritte zum Erstellen der Rolle.

   Gehen Sie wie folgt vor:

   - Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
   - Wählen Sie **ein weiteres AWS-Konto** und geben Sie die ID des BlueXP SaaS: 952013314444 ein
   - Bearbeiten Sie speziell für Amazon FSx for NetApp ONTAP die Richtlinie **Vertrauensbeziehungen**, um "AWS": "arn:aws:iam::952013314444:root" einzuschließen.

     Die Richtlinie sollte beispielsweise folgendermaßen aussehen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

   +
   Siehe "AWS Identity and Access Management (IAM)-Dokumentation" für weitere Informationen zum kontoübergreifenden Ressourcenzugriff in IAM.

   - Erstellen Sie eine Richtlinie, die die zum Erstellen eines Connectors erforderlichen Berechtigungen enthält.
     - "Zeigen Sie die für FSX für ONTAP erforderlichen Berechtigungen an"
     - "Sehen Sie sich die Richtlinie zur Bereitstellung von Konnektor an"
3. Kopieren Sie die Rolle ARN der IAM-Rolle, sodass Sie sie im nächsten Schritt in BlueXP einfügen können.

Ergebnis

Die IAM-Rolle verfügt nun über die erforderlichen Berechtigungen. Sie können es jetzt zu BlueXP hinzufügen.

Fügen Sie die Anmeldeinformationen hinzu

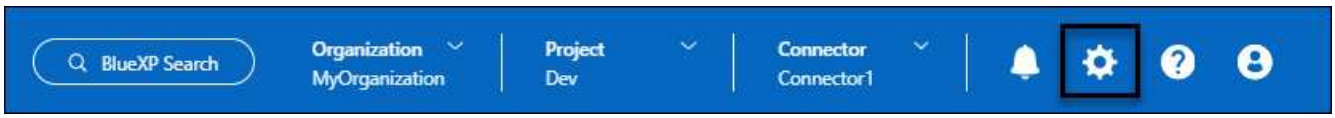
Nachdem Sie die IAM-Rolle mit den erforderlichen Berechtigungen angegeben haben, fügen Sie die Rolle ARN zu BlueXP hinzu.

Bevor Sie beginnen

Wenn Sie gerade die IAM-Rolle erstellt haben, kann es ein paar Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie BlueXP die Anmeldeinformationen hinzufügen.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.



2. Wählen Sie auf der Seite **Unternehmensanmeldeinformationen** oder **Kontoanmeldeinformationen** die Option **Anmeldeinformationen hinzufügen** aus, und befolgen Sie die Schritte im Assistenten.
   a. **Anmeldeort**: Wählen Sie **Amazon Web Services > BlueXP**.
   b. **Anmeldedaten definieren**: Geben Sie den ARN (Amazon Resource Name) der IAM-Rolle an.
   c. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Zugangsdaten zu BlueXP für Amazon FSX for ONTAP hinzufügen

Weitere Informationen finden Sie im "BlueXP Dokumentation für Amazon FSX for ONTAP"

Konfigurieren eines AWS-Abonnements

Nachdem Sie Ihre AWS-Anmeldeinformationen hinzugefügt haben, können Sie mit diesen ein AWS Marketplace-Abonnement konfigurieren. Mit dem Abonnement können Sie Cloud Volumes ONTAP stundenweise (PAYGO) oder mit einem Jahresvertrag bezahlen und weitere Datendienste nutzen.

Es gibt zwei Szenarien, in denen Sie ein AWS Marketplace-Abonnement konfigurieren können, nachdem Sie die Anmeldeinformationen bereits hinzugefügt haben:

- Sie haben beim ersten Hinzufügen der Anmeldeinformationen kein Abonnement konfiguriert.
- Sie möchten das AWS Marketplace-Abonnement ändern, das mit den AWS Zugangsdaten konfiguriert ist.

  Durch den Austausch des aktuellen Marketplace-Abonnements durch ein neues Abonnement wird das Marketplace-Abonnement für alle bestehenden Cloud Volumes ONTAP Arbeitsumgebungen und alle neuen Arbeitsumgebungen geändert.

Bevor Sie beginnen

Sie müssen einen Connector erstellen, bevor Sie ein Abonnement konfigurieren können. "Erfahren Sie, wie Sie einen Konnektor erstellen".

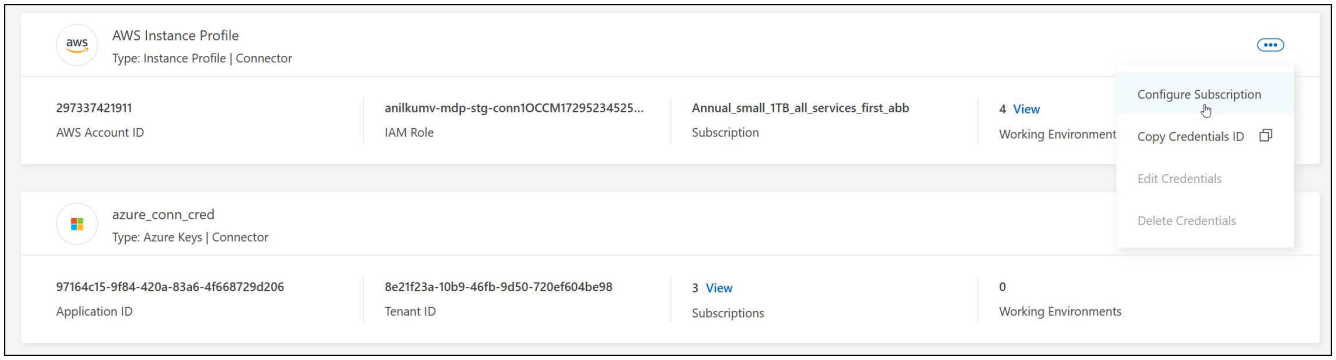
Das folgende Video zeigt die Schritte zum Abonnieren von NetApp Intelligent Services vom AWS Marketplace:

Abonnieren Sie NetApp Intelligent Services vom AWS Marketplace

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen und dann **Abonnement konfigurieren**.

   Sie müssen Anmeldeinformationen auswählen, die einem Connector zugeordnet sind. Sie können kein Marketplace-Abonnement mit Anmeldedaten verknüpfen, die mit BlueXP verknüpft sind.



3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie das Abonnement aus der Down-Liste aus und wählen Sie **Konfigurieren**.
4. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Weiter** und befolgen Sie die Schritte im AWS Marketplace:

   a. Wählen Sie **Kaufoptionen anzeigen**.

   b. Wählen Sie **Abonnieren**.

   c. Wählen Sie **Konto einrichten**.

      Sie werden auf die BlueXP-Website umgeleitet.

   d. Auf der Seite **Subscription Assignment**:

      - Wählen Sie die BlueXP -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
      - Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

        BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

   Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.

   ◦ Wählen Sie **Speichern**.

Verknüpfen Sie ein bestehendes Abonnement mit Ihrer Organisation oder Ihrem Konto

Wenn Sie über den AWS Marketplace abonnieren, besteht der letzte Schritt darin, das Abonnement Ihrer Organisation zuzuordnen. Wenn Sie diesen Schritt nicht abgeschlossen haben, können Sie das Abonnement nicht mit Ihrer Organisation oder Ihrem Konto verwenden.

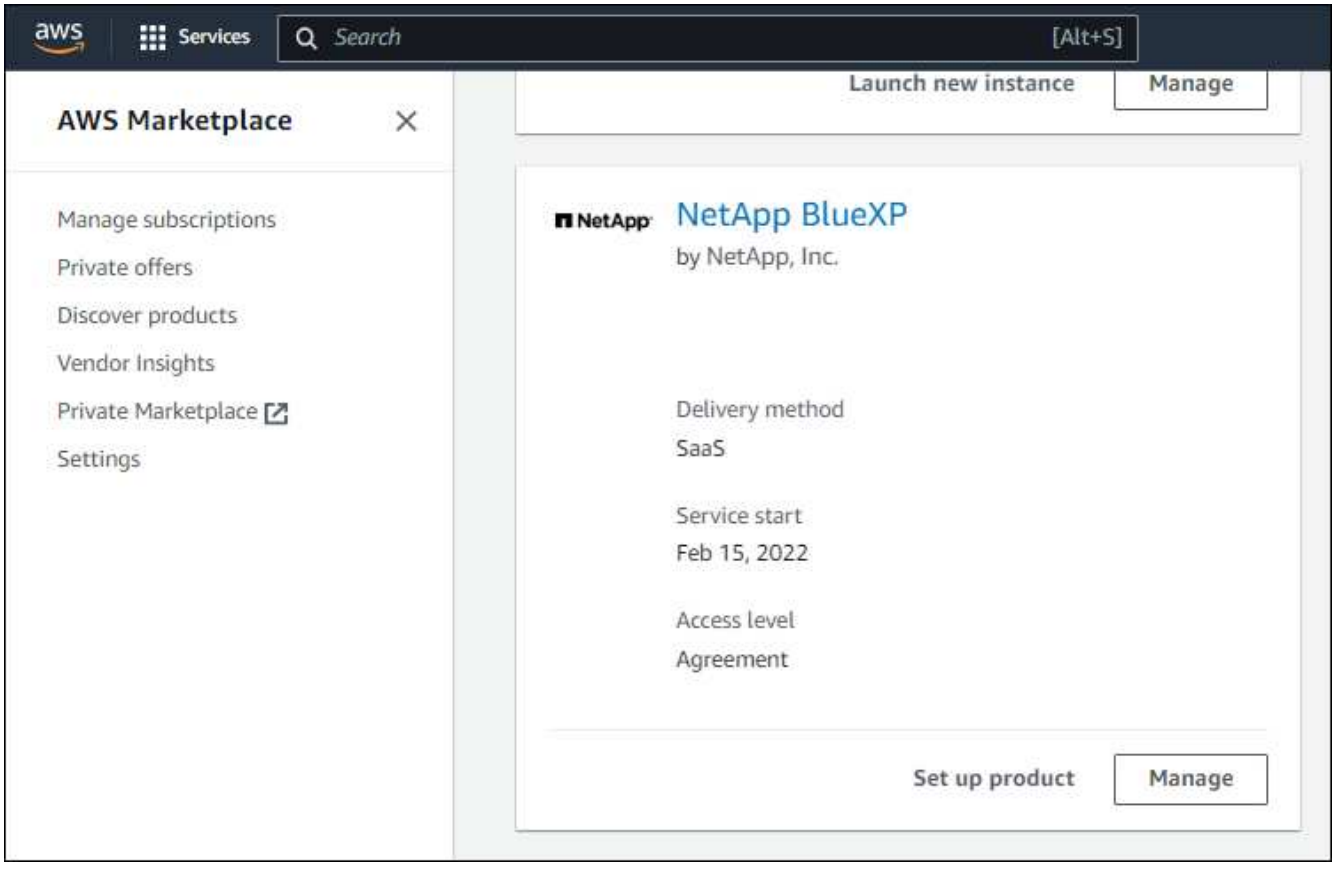
- "Weitere Informationen zu BlueXP Implementierungsmodi"
- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "

Führen Sie die folgenden Schritte aus, wenn Sie intelligente NetApp-Datendienste vom AWS Marketplace abonniert haben, aber den Schritt zum Verknüpfen des Abonnements mit Ihrem Konto vergessen haben.

Schritte

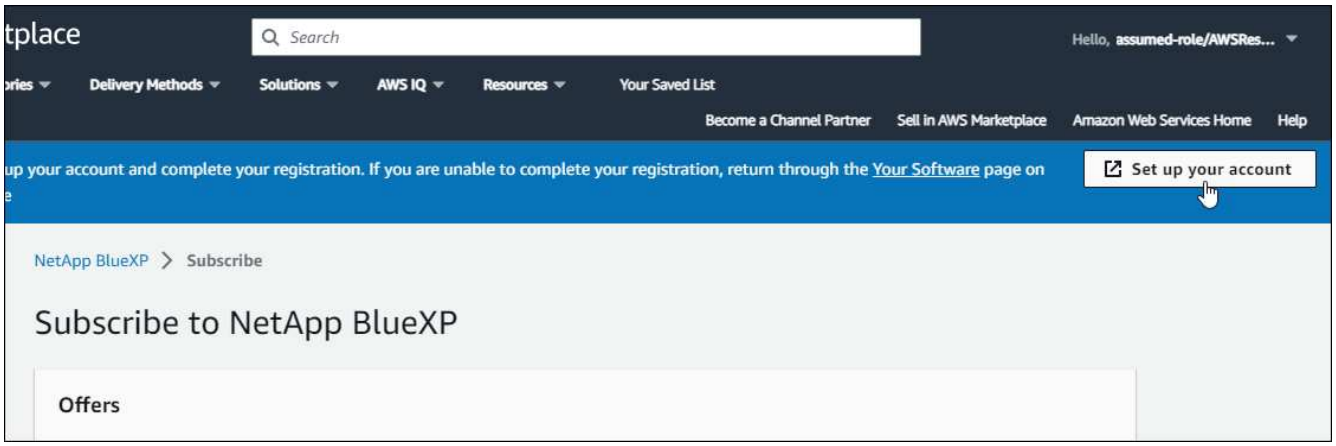
1. Gehen Sie zur digitalen Geldbörse, um zu bestätigen, dass Sie Ihr Abonnement nicht mit Ihrer BlueXP-Organisation oder Ihrem BlueXP-Konto verknüpft haben.
   a. Wählen Sie im Navigationsmenü **Governance > Digitale Geldbörse**.
   b. Wählen Sie **Abonnements**.
   c. Stellen Sie sicher, dass Ihr Abonnement nicht angezeigt wird.

      Es werden nur die Abonnements angezeigt, die mit der Organisation oder dem Konto verknüpft sind, das Sie gerade anzeigen. Wenn Ihr Abonnement nicht angezeigt wird, fahren Sie mit den folgenden Schritten fort.
2. Melden Sie sich an der AWS-Konsole an, und navigieren Sie zu **AWS Marketplace Subscriptions**.
3. Suchen Sie nach dem Abonnement für NetApp Intelligent Data Services.



4. Wählen Sie **Produkt einrichten**.

   Die Abonnementseite sollte in einem neuen Browser-Tab oder -Fenster geladen werden.
5. Wählen Sie **Konto einrichten**.



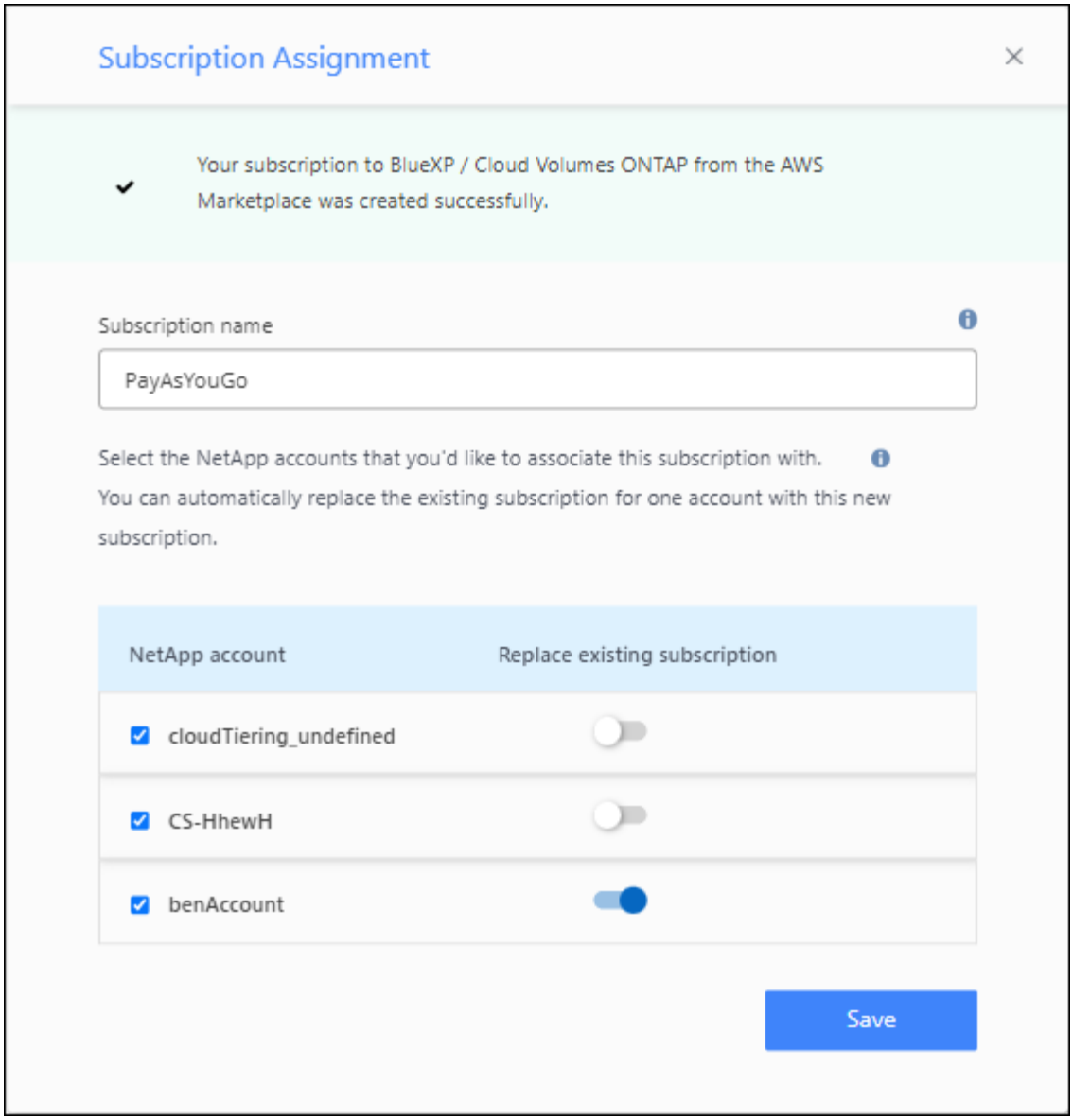
Die Seite **Subscription Assignment** auf netapp.com sollte in einem neuen Browser-Tab oder -Fenster geladen werden.

Beachten Sie, dass Sie möglicherweise zuerst zur Anmeldung bei BlueXP aufgefordert werden.

6. Auf der Seite **Subscription Assignment**:
   - Wählen Sie die BlueXP -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
   - Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

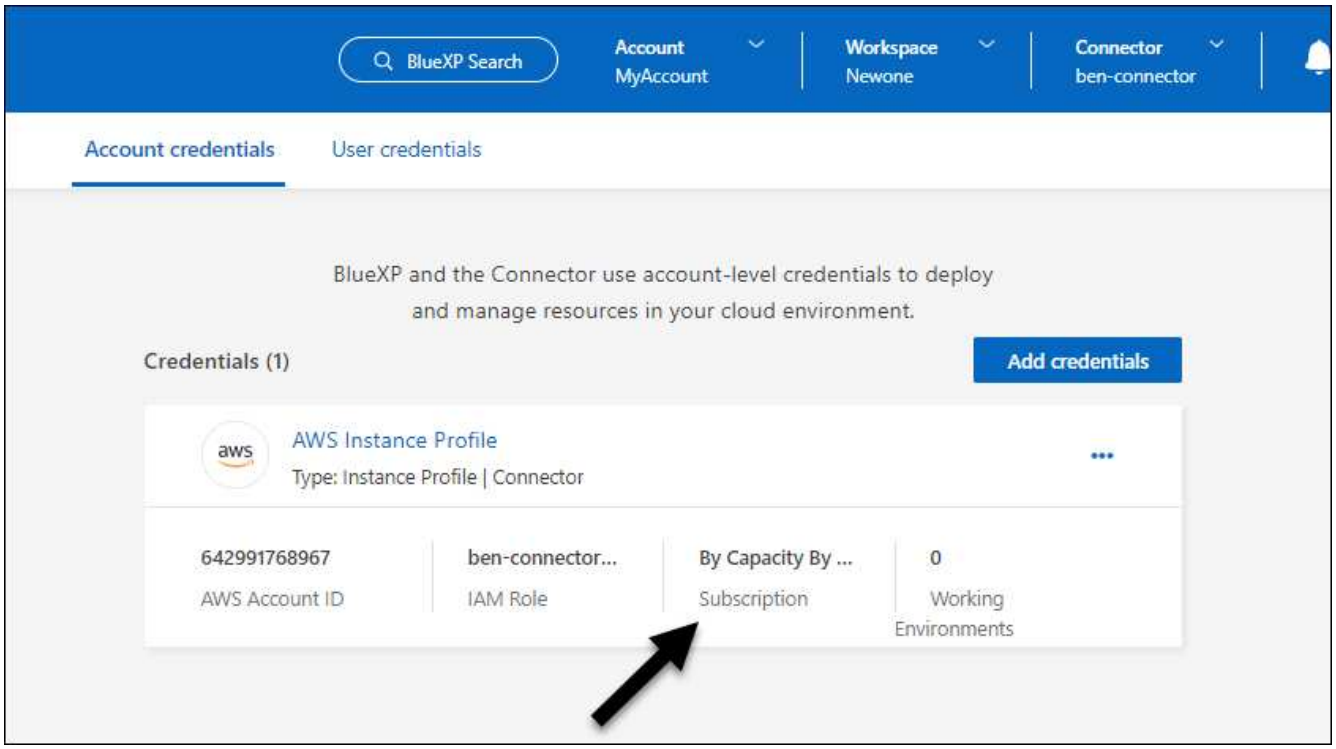
     BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

     Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.



7. Gehen Sie zur digitalen Geldbörse, um zu bestätigen, dass das Abonnement mit Ihrer Organisation oder Ihrem Konto verknüpft ist.
   a. Wählen Sie im Navigationsmenü **Governance > Digitale Geldbörse**.
   b. Wählen Sie **Abonnements**.
   c. Überprüfen Sie, ob Ihr Abonnement angezeigt wird.
8. Vergewissern Sie sich, dass das Abonnement mit Ihren AWS-Anmeldedaten verknüpft ist.
   a. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
   b. Überprüfen Sie auf der Seite **Unternehmensanmeldeinformationen** oder **Kontoanmeldeinformationen**, ob das Abonnement mit Ihren AWS-Anmeldeinformationen verknüpft ist.

      Hier ein Beispiel



Anmeldedaten bearbeiten

Bearbeiten Sie Ihre AWS-Anmeldeinformationen, indem Sie den Kontotyp ändern (AWS-Schlüssel oder Rolle übernehmen), den Namen bearbeiten oder die Anmeldeinformationen selbst aktualisieren (die Schlüssel oder die Rollen-ARN).

Sie können die Anmeldeinformationen für ein Instanzprofil nicht bearbeiten, das einer Connector-Instanz oder einer Amazon FSx for ONTAP-Instanz zugeordnet ist. Sie können die Anmeldeinformationen nur für eine FSx for ONTAP-Instanz umbenennen.

Schritte

1. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
2. Wählen Sie auf der Seite **Unternehmensanmeldeinformationen** oder **Kontoanmeldeinformationen** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann **Anwenden**.

Anmeldeinformationen löschen

Wenn Sie einen Satz Anmeldeinformationen nicht mehr benötigen, können Sie ihn löschen. Sie können nur Anmeldeinformationen löschen, die nicht mit einer Arbeitsumgebung verknüpft sind.

Sie können die Anmeldeinformationen für ein Instanzprofil nicht löschen, das einer Konnektor-Instanz zugeordnet ist.

Schritte

1. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
2. Wählen Sie auf der Seite **Unternehmensanmeldeinformationen** oder **Kontoanmeldeinformationen** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen**

löschen.

3. Wählen Sie **Löschen**, um zu bestätigen.

Azure

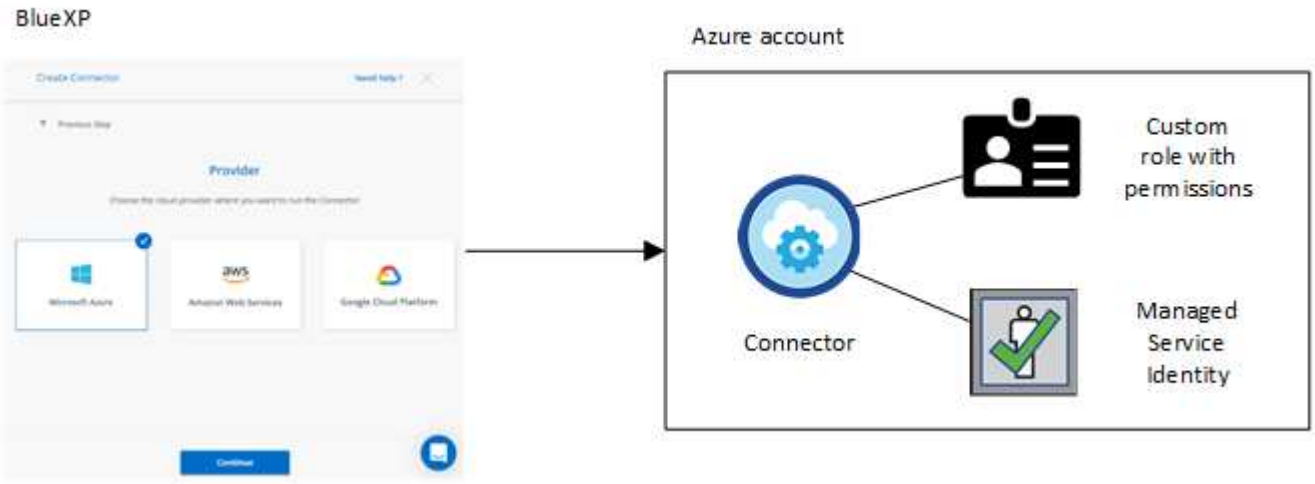
Erfahren Sie mehr über Azure-Anmeldeinformationen und Berechtigungen in BlueXP

Informieren Sie sich, wie BlueXP für Sie Azure Zugangsdaten verwendet, um Aktionen durchzuführen und wie diese Zugangsdaten mit Marketplace-Abonnements verknüpft sind. Das Verständnis dieser Details kann hilfreich sein, wenn Sie die Anmeldedaten für ein oder mehrere Azure-Abonnements verwalten. Beispielsweise könnte es hilfreich sein, wenn Sie mehr über Azure Zugangsdaten zu BlueXP erfahren möchten.

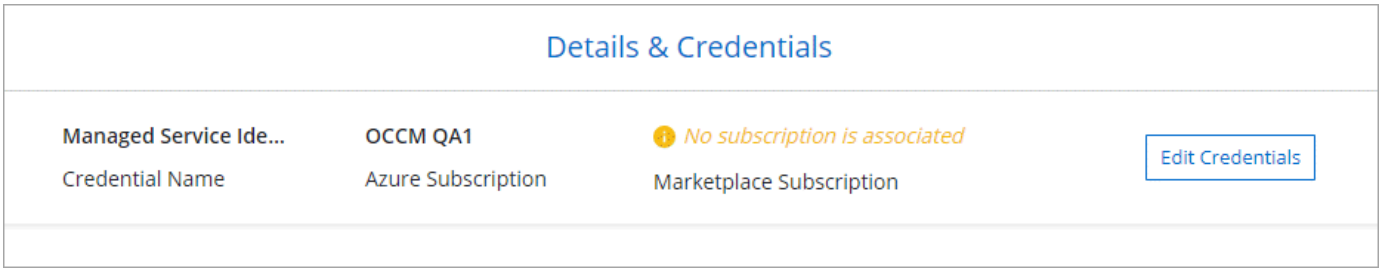
Erste Azure Zugangsdaten

Wenn Sie einen Connector von BlueXP bereitstellen, müssen Sie ein Azure-Konto oder einen Service-Principal verwenden, der über die Berechtigungen zum Bereitstellen der virtuellen Connector-Maschine verfügt. Die erforderlichen Berechtigungen sind im aufgeführt"Connector-Implementierungsrichtlinie für Azure".

Wenn BlueXP die virtuelle Connector-Maschine in Azure bereitstellt, wird ein auf der virtuellen Maschine aktiviert "Vom System zugewiesene verwaltete Identität", eine benutzerdefinierte Rolle erstellt und der virtuellen Maschine zugewiesen. Diese Rolle bietet BlueXP die Berechtigungen, die für das Management von Ressourcen und Prozessen innerhalb des Azure Abonnements erforderlich sind. "Überprüfen Sie, wie BlueXP die Berechtigungen verwendet".



Wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen, wählt BlueXP standardmäßig diese Azure Zugangsdaten aus:



Alle Cloud Volumes ONTAP Systeme können über die ersten Azure Zugangsdaten implementiert oder

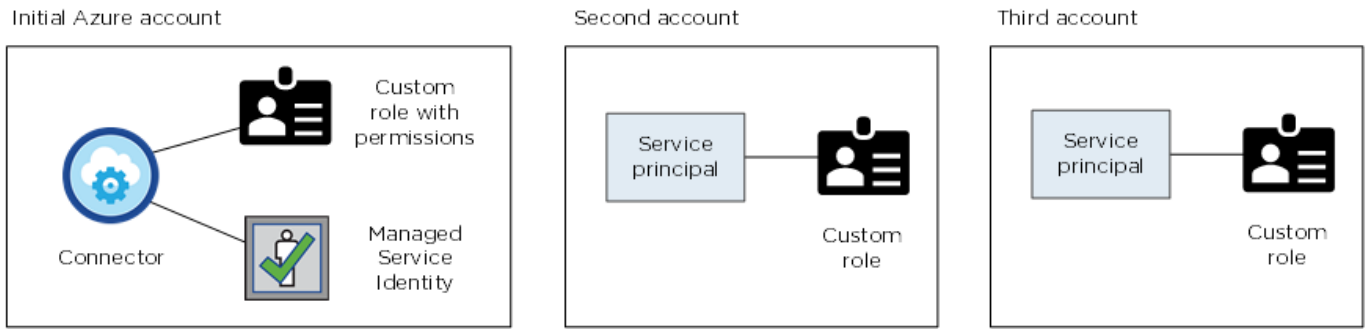
zusätzliche Anmeldedaten hinzugefügt werden.

Zusätzliche Azure-Abonnements für eine gemanagte Identität

Die der Konnektor-VM zugewiesene, vom System zugewiesene verwaltete Identität ist mit dem Abonnement verknüpft, in dem Sie den Connector gestartet haben. Wenn Sie ein anderes Azure Abonnement auswählen möchten, müssen Sie es ausführen "Verknüpfen Sie die verwaltete Identität mit diesen Abonnements".

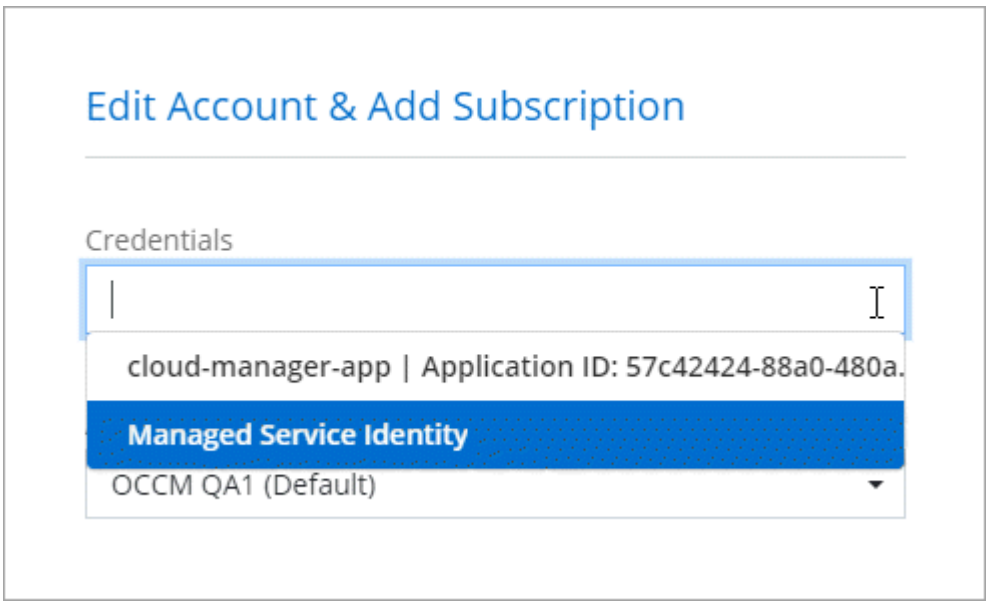
Zusätzliche Azure Zugangsdaten

Wenn Sie unterschiedliche Azure-Anmeldedaten für BlueXP verwenden möchten, müssen Sie die erforderlichen Berechtigungen bis erteilen "Erstellen und Einrichten eines Dienstprincipals in Microsoft Entra ID" Für jedes Azure Konto. Das folgende Bild zeigt zwei zusätzliche Konten, die jeweils mit einer Dienstprinzipal- und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:



Das würden Sie dann tun "Fügen Sie die Kontoanmeldeinformationen zu BlueXP hinzu" Durch Angabe von Details zum AD-Dienstprinzipal.

Sie können beispielsweise beim Erstellen einer neuen Cloud Volumes ONTAP-Arbeitsumgebung zwischen den Anmeldedaten wechseln:



Anmeldedaten und Abonnements für den Marktplatz

Die Zugangsdaten, die Sie zu einem Connector hinzufügen, müssen mit einem Azure Marketplace Abonnement verbunden sein, sodass Sie für Cloud Volumes ONTAP einen Stundensatz (PAYGO) oder über einen Jahresvertrag zahlen und andere BlueXP Services nutzen können.

"Lesen Sie, wie Sie ein Azure-Abonnement zuordnen".

Beachten Sie Folgendes zu Azure Zugangsdaten und Marketplace-Abonnements:

- Sie können nur ein Azure Marketplace Abonnement mit einem Satz von Azure Zugangsdaten verknüpfen
- Sie können ein bestehendes Marketplace-Abonnement durch ein neues Abonnement ersetzen

Häufig gestellte Fragen

Die folgende Frage bezieht sich auf Anmeldeinformationen und Abonnements.

Kann ich das Azure Marketplace Abonnement für Cloud Volumes ONTAP-Arbeitsumgebungen ändern?

Ja, können Sie. Mit Änderung des Abonnements für Azure Marketplace für bestimmte Azure Zugangsdaten werden alle bestehenden und neuen Cloud Volumes ONTAP-Arbeitsumgebungen mit dem neuen Abonnement abgerechnet.

"Lesen Sie, wie Sie ein Azure-Abonnement zuordnen".

Kann ich mehrere Azure Zugangsdaten mit jeweils unterschiedlichen Marketplace-Abonnements hinzufügen?

Alle Azure Zugangsdaten, die zum selben Azure Abonnement gehören, werden mit demselben Azure Marketplace Abonnement verknüpft.

Wenn Sie mehrere Azure-Anmeldeinformationen haben, die zu verschiedenen Azure-Abonnements gehören, können diese Anmeldeinformationen demselben Azure Marketplace Abonnement oder verschiedenen Marketplace-Abonnements zugeordnet werden.

Kann ich vorhandene Cloud Volumes ONTAP-Arbeitsumgebungen auf ein anderes Azure Abonnement verschieben?

Nein, es ist nicht möglich, die Azure Ressourcen, die Ihrer Cloud Volumes ONTAP-Arbeitsumgebung zugeordnet sind, in ein anderes Azure Abonnement zu verschieben.

Wie funktionieren Anmeldeinformationen für Marktplatzbereitstellungen und lokale Bereitstellungen?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Connector beschrieben, der aus BlueXP stammt. Sie können einen Connector auch in Azure über den Azure Marketplace implementieren und die Connector-Software auf Ihrem eigenen Linux-Host installieren.

Wenn Sie den Marketplace verwenden, können Sie Berechtigungen bereitstellen, indem Sie der Connector-VM und einer vom System zugewiesenen verwalteten Identität eine benutzerdefinierte Rolle zuweisen oder ein Microsoft Entra-Dienstprincipal verwenden.

Für On-Premises-Bereitstellungen können Sie keine verwaltete Identität für den Connector einrichten, aber Sie können Berechtigungen mithilfe eines Dienstprincipals bereitstellen.

Weitere Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- Standardmodus
  - "Richten Sie Berechtigungen für eine Azure Marketplace-Implementierung ein"
  - "Einrichten von Berechtigungen für lokale Bereitstellungen"

- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

Azure Zugangsdaten und Marketplace-Abonnements für BlueXP managen

Hinzufügen und Managen von Azure-Anmeldeinformationen, um zu ermöglichen, dass BlueXP über die erforderlichen Berechtigungen zum Implementieren und Managen von Cloud-Ressourcen in Ihren Azure Abonnements verfügt. Wenn Sie mehrere Azure Marketplace-Abonnements verwalten, können Sie jedes davon auf der Seite „Anmeldeinformationen“ verschiedenen Azure Zugangsdaten zuweisen.

Folgen Sie den Schritten auf dieser Seite, wenn Sie mehrere Azure Zugangsdaten oder mehrere Azure Marketplace Abonnements für Cloud Volumes ONTAP verwenden möchten.

Überblick

Es gibt zwei Möglichkeiten, in BlueXP zusätzliche Azure-Abonnements und Anmeldedaten hinzuzufügen.

1. Verknüpfen Sie zusätzliche Azure-Abonnements mit der von Azure verwalteten Identität.
2. Wenn Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten bereitstellen möchten, erteilen Sie Azure Berechtigungen unter Verwendung eines Service-Principal und fügen dessen Zugangsdaten BlueXP hinzu.

Zuordnen zusätzlicher Azure-Abonnements zu einer gemanagten Identität

Mit BlueXP können Sie die Azure Zugangsdaten und das Azure Abonnement auswählen, in dem Sie Cloud Volumes ONTAP bereitstellen möchten. Sie können kein anderes Azure-Abonnement für das verwaltete Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "Verwaltete Identität" Mit diesen Abonnements.

Über diese Aufgabe

Eine verwaltete Identität ist "Zunächst das Azure-Konto" Wenn Sie einen Connector von BlueXP bereitstellen. Wenn Sie den Connector bereitgestellt haben, hat BlueXP die Rolle BlueXP Operator erstellt und der virtuellen Connector-Maschine zugewiesen.

Schritte

1. Melden Sie sich beim Azure Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Wählen Sie **Access Control (IAM)**.
   a. Wählen Sie **Hinzufügen** > **Rollenzuweisung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **BlueXP Operator** aus.

        BlueXP Operator ist der Standardname, der in der Connector-Richtlinie angegeben ist. Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

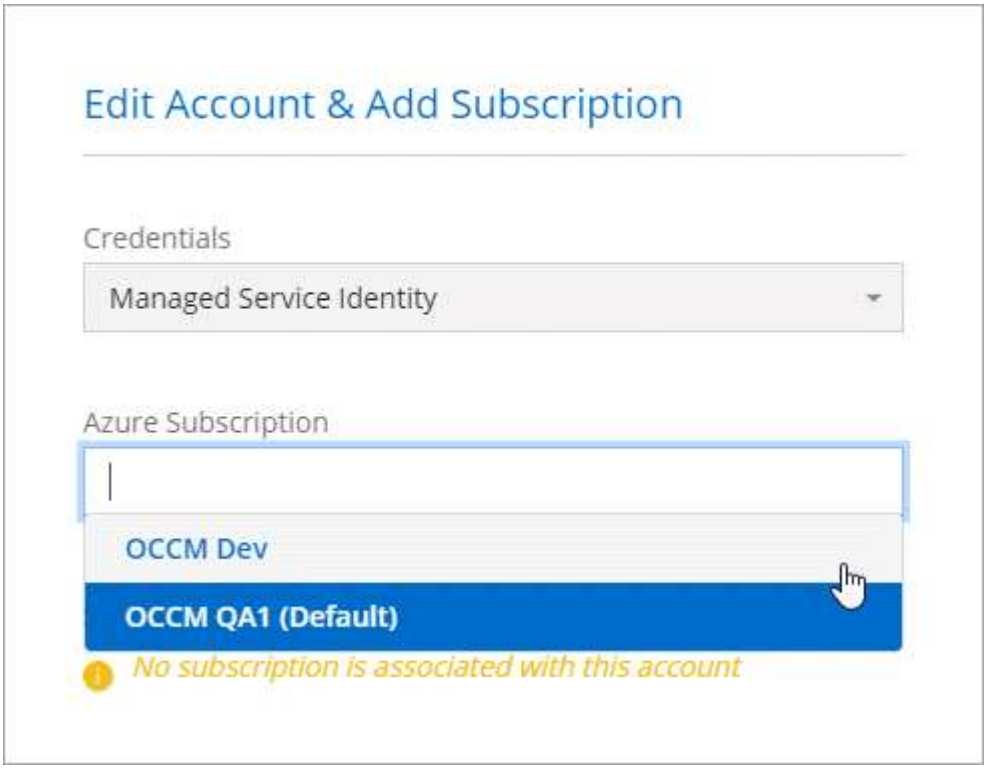
      - Weisen Sie einer **virtuellen Maschine** Zugriff zu.
      - Wählen Sie das Abonnement aus, in dem die virtuelle Connector-Maschine erstellt wurde.

- Wählen Sie die virtuelle Verbindungsmaschine aus.
- Wählen Sie **Speichern**.

4. Wiederholen Sie diese Schritte für weitere Abonnements.

Ergebnis

Wenn Sie eine neue Arbeitsumgebung erstellen, sollten Sie nun über mehrere Azure-Abonnements für das verwaltete Identitätsprofil verfügen.



Zusätzliche Azure Zugangsdaten zu BlueXP hinzufügen

Wenn Sie einen Connector von BlueXP bereitstellen, aktiviert BlueXP eine vom System zugewiesene verwaltete Identität auf der virtuellen Maschine, die über die erforderlichen Berechtigungen verfügt. BlueXP wählt diese Azure-Anmeldedaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen.

Ein erster Satz von Anmeldeinformationen wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. "Informationen zu Azure Zugangsdaten und Berechtigungen".

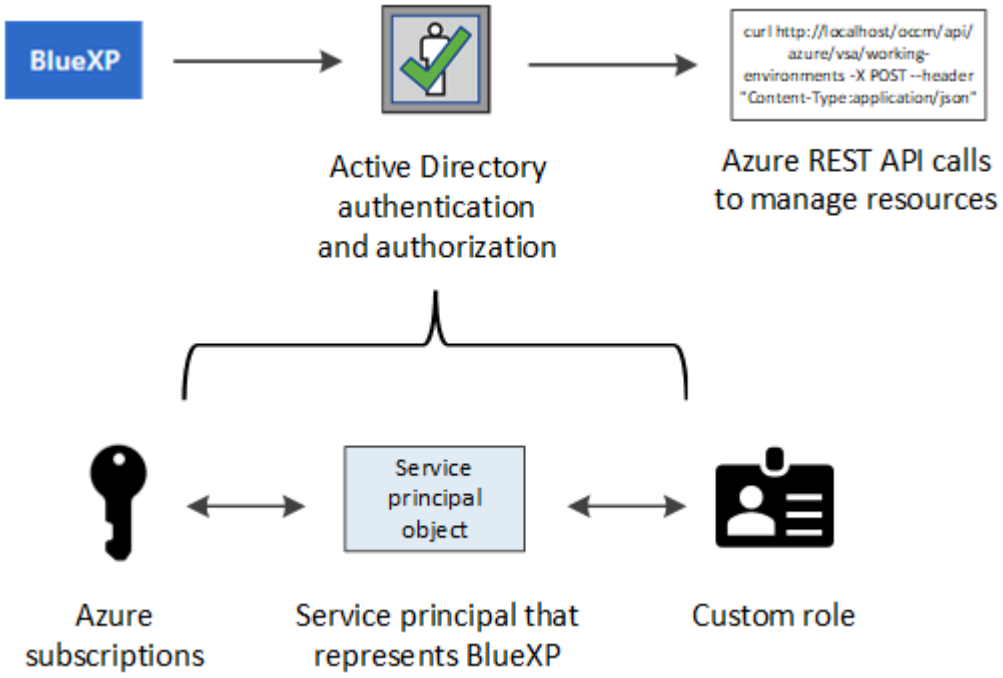
Wenn Sie Cloud Volumes ONTAP mit *different* Azure-Anmeldeinformationen bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie für jedes Azure-Konto einen Dienstprinzipal in der Microsoft Entra-ID erstellen und einrichten. Anschließend können Sie die neuen Anmeldeinformationen zu BlueXP hinzufügen.

Erteilen Sie Azure Berechtigungen mithilfe eines Service-Prinzipals

Für Aktionen in Azure benötigt BlueXP Berechtigungen. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie in der Microsoft Entra-ID einen Service-Principal erstellen und einrichten und die für BlueXP erforderlichen Azure-Zugangsdaten erhalten.

Über diese Aufgabe

Die folgende Abbildung zeigt, wie BlueXP Berechtigungen zur Durchführung von Operationen in Azure erhält. Ein Service-Principal-Objekt, das an ein oder mehrere Azure-Abonnements gebunden ist, repräsentiert BlueXP in der Microsoft Entra ID und wird einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen erlaubt.



Schritte

1. Erstellen Sie eine Microsoft Entra-Anwendung.
2. Anwendung einer Rolle zuweisen.
3. Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu.
4. Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab.
5. Erstellen Sie einen Clientschlüssel.

Erstellen Sie eine Microsoft Entra-Anwendung

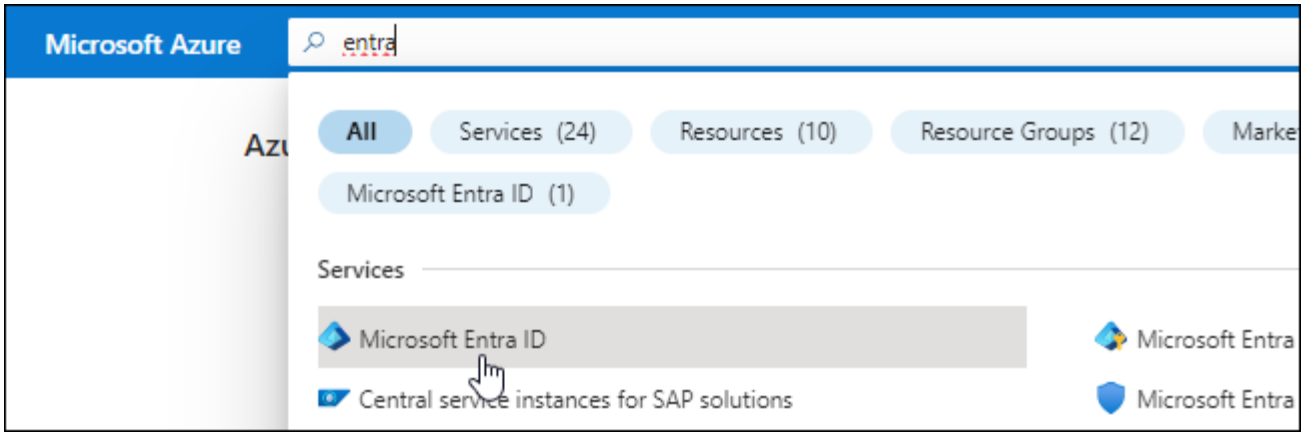
Erstellen Sie ein Microsoft Entra-Applikations- und Serviceprinzip, das BlueXP für die rollenbasierte Zugriffssteuerung verwenden kann.

Schritte

1. Stellen Sie sicher, dass Sie in Azure über die Berechtigungen zum Erstellen einer Active Directory-Anwendung und zum Zuweisen der Anwendung zu einer Rolle verfügen.

   Weitere Informationen finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen"

2. Öffnen Sie im Azure-Portal den Dienst **Microsoft Entra ID**.



3. Wählen Sie im Menü **App-Registrierungen**.
4. Wählen Sie **Neue Registrierung**.
5. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (jeder kann mit BlueXP verwendet werden).
   - **Redirect URI**: Sie können dieses Feld leer lassen.
6. Wählen Sie **Registrieren**.

   Sie haben die AD-Anwendung und den Service-Principal erstellt.

Ergebnis

Sie haben die AD-Anwendung und den Service-Principal erstellt.

Anwendung einer Rolle zuweisen

Sie müssen den Service-Principal an ein oder mehrere Azure-Abonnements binden und ihm die benutzerdefinierte Rolle „BlueXP Operator“ zuweisen, damit BlueXP über Berechtigungen in Azure verfügt.

Schritte

1. Erstellen einer benutzerdefinierten Rolle:

   Beachten Sie, dass Sie eine benutzerdefinierte Azure-Rolle über das Azure-Portal, Azure PowerShell, Azure CLI oder REST-API erstellen können. Die folgenden Schritte zeigen, wie Sie die Rolle mithilfe der Azure-CLI erstellen. Wenn Sie eine andere Methode verwenden möchten, finden Sie weitere Informationen unter "Azure-Dokumentation"

   a. Kopieren Sie den Inhalt des "Benutzerdefinierte Rollenberechtigungen für den Konnektor" Und speichern Sie sie in einer JSON-Datei.

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP Systeme erstellen.

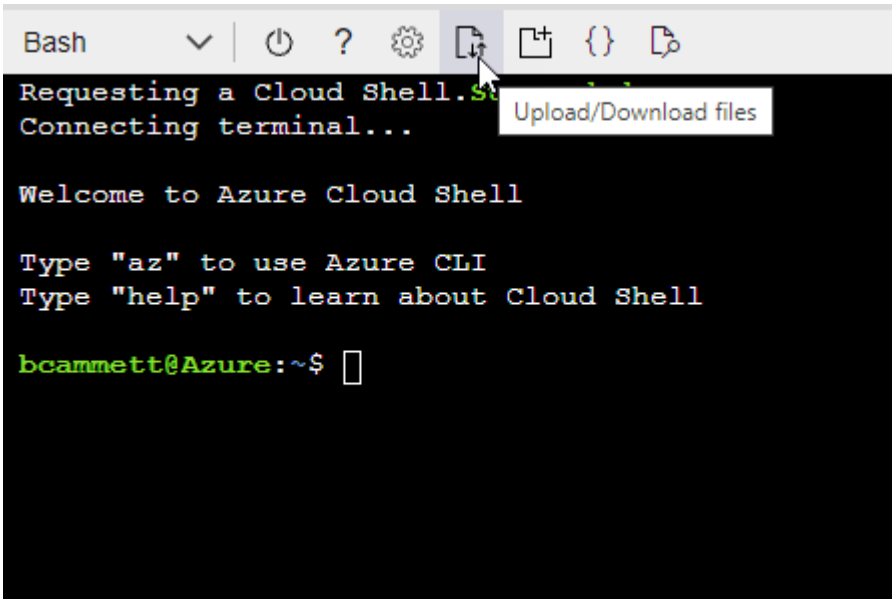
      Beispiel

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

c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

In den folgenden Schritten wird beschrieben, wie die Rolle mithilfe von Bash in Azure Cloud Shell erstellt wird.

- Starten "Azure Cloud Shell" Und wählen Sie die Bash-Umgebung.
- Laden Sie die JSON-Datei hoch.



- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

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

Sie sollten nun eine benutzerdefinierte Rolle namens BlueXP Operator haben, die Sie der virtuellen Connector-Maschine zuweisen können.

2. Applikation der Rolle zuweisen:

a. Öffnen Sie im Azure-Portal den Service **Abonnements**.

b. Wählen Sie das Abonnement aus.

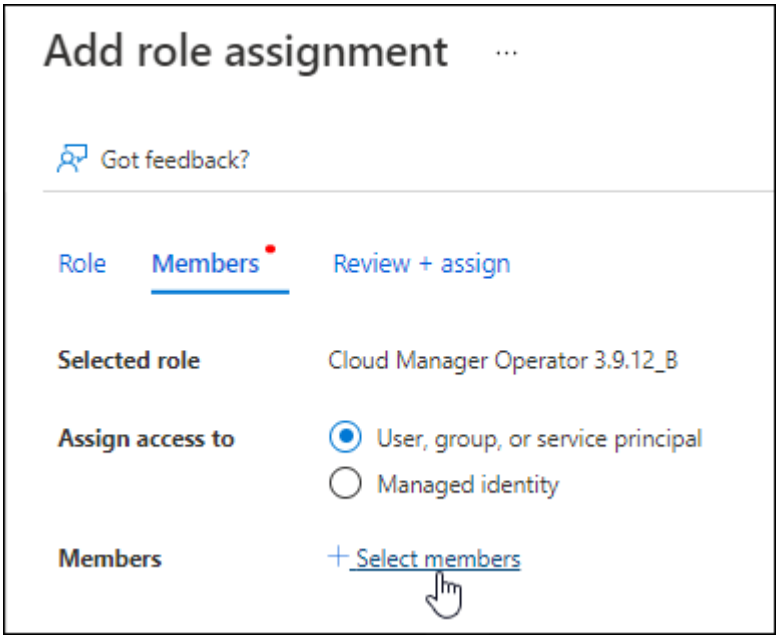
c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.

e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

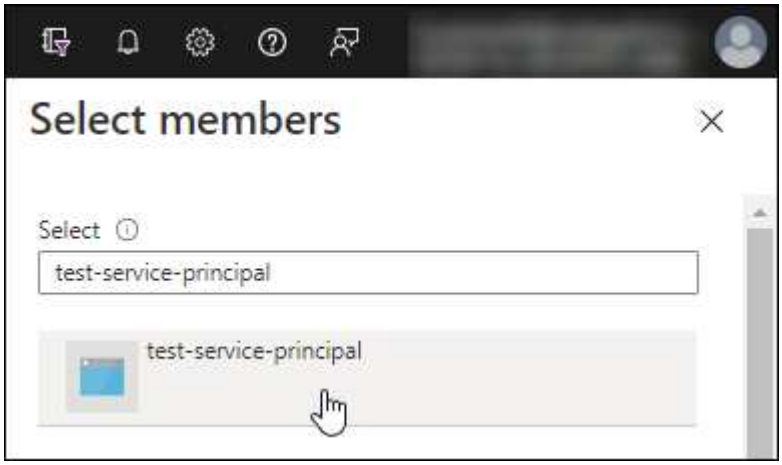
- **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.

- Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

  Hier ein Beispiel:



- Wählen Sie die Anwendung aus und wählen Sie **Select**.
- Wählen Sie **Weiter**.

f. Wählen Sie **Überprüfen + Zuweisen**.

   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

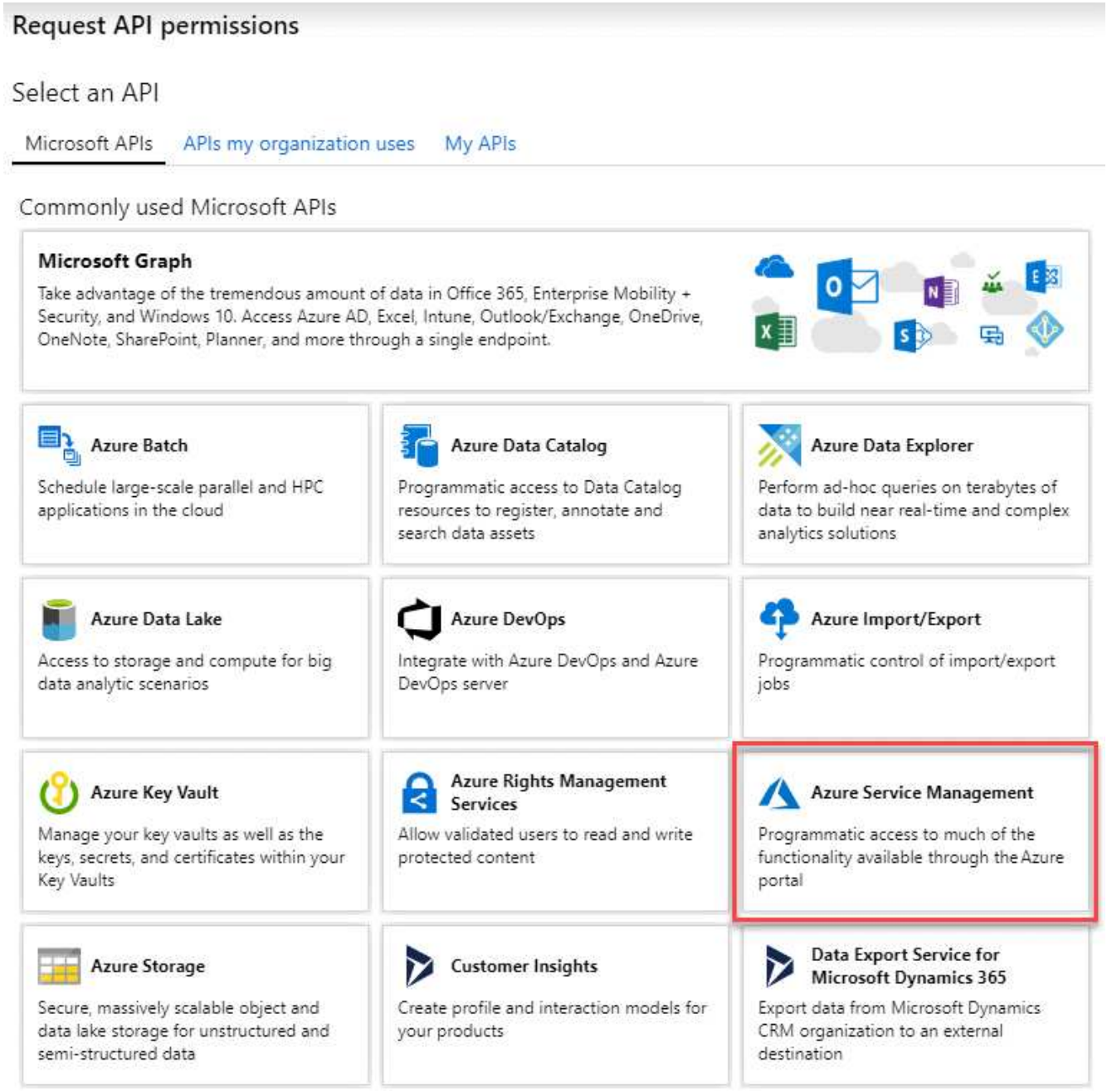
Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Prinzipal an jedes dieser Subscriptions binden. Mit BlueXP können Sie das Abonnement auswählen, das Sie bei der Bereitstellung von Cloud Volumes ONTAP verwenden möchten.

Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

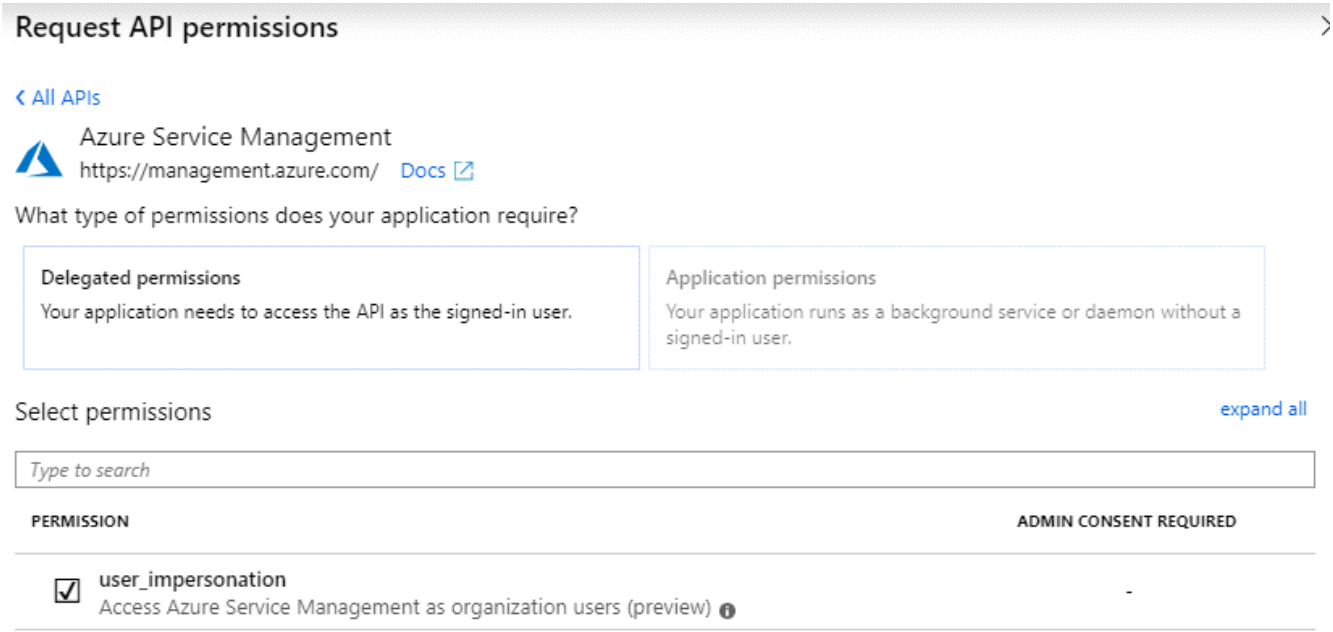
Der Service-Principal muss über die Berechtigungen „Windows Azure Service Management API“ verfügen.

Schritte

1. Wählen Sie im **Microsoft Entra ID**-Dienst **App-Registrierungen** aus und wählen Sie die Anwendung aus.
2. Wählen Sie **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft APIs Azure Service Management** aus.



4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.

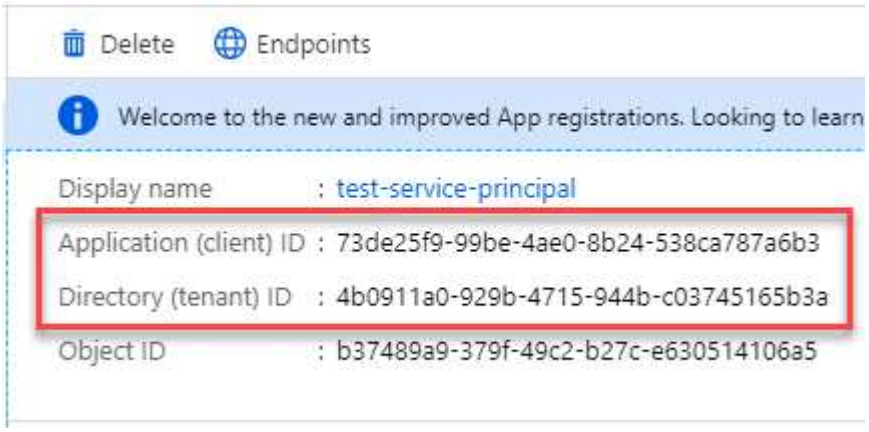


Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab

Wenn Sie das Azure-Konto zu BlueXP hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. BlueXP verwendet die IDs, um sich programmatisch anzumelden.

Schritte

1. Wählen Sie im **Microsoft Entra ID**-Dienst **App-Registrierungen** aus und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Application (Client) ID** und die **Directory (Tenant) ID**.



Wenn Sie das Azure-Konto zu BlueXP hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. BlueXP verwendet die IDs, um sich programmatisch anzumelden.

Erstellen Sie einen Clientschlüssel

Sie müssen einen Client Secret erstellen und BlueXP dann den Wert des Geheimnisses bereitstellen, damit BlueXP ihn zur Authentifizierung mit Microsoft Entra ID verwenden kann.

Schritte

1. Öffnen Sie den Dienst **Microsoft Entra ID**.
2. Wählen Sie **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Wählen Sie **Zertifikate & Geheimnisse > Neues Kundengeheimnis**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Wählen Sie **Hinzufügen**.
6. Kopieren Sie den Wert des Clientgeheimnisses.

Jetzt haben Sie einen Client-Schlüssel, den BlueXP zur Authentifizierung mit Microsoft Entra ID verwenden kann.

Ergebnis

Ihr Service-Principal ist jetzt eingerichtet und Sie sollten die Anwendungs- (Client-)ID, die Verzeichnis- (Mandanten-)ID und den Wert des Clientgeheimnisses kopiert haben. Sie müssen diese Informationen in BlueXP eingeben, wenn Sie ein Azure-Konto hinzufügen.

Zugangsdaten zu BlueXP hinzufügen

Nachdem Sie ein Azure-Konto mit den erforderlichen Berechtigungen angegeben haben, können Sie die Anmeldedaten für dieses Konto bei BlueXP hinzufügen. Durch diesen Schritt können Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten starten.

Bevor Sie beginnen

Falls Sie diese Zugangsdaten gerade bei Ihrem Cloud-Provider erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie BlueXP die Anmeldeinformationen hinzufügen.

Bevor Sie beginnen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "Erfahren Sie, wie Sie einen Konnektor erstellen".

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.

2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten im Assistenten.

a. **Anmeldeort**: Wählen Sie **Microsoft Azure > Connector**.

b. **Credentials definieren**: Geben Sie Informationen über den Microsoft Entra-Dienst-Prinzipal ein, der die erforderlichen Berechtigungen gewährt:

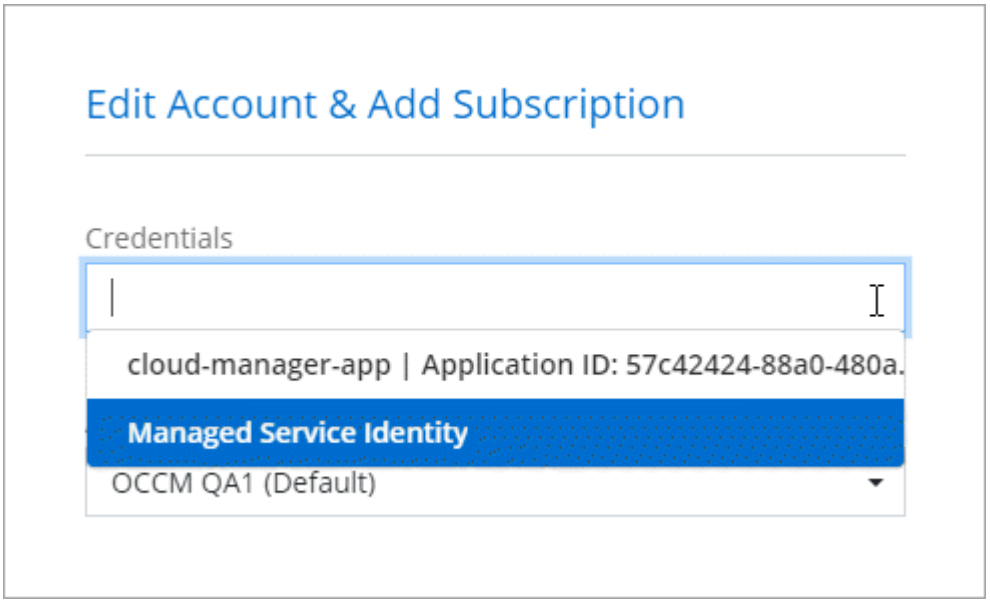
   - Anwendungs-ID (Client)
   - ID des Verzeichnisses (Mandant)
   - Client-Schlüssel

c. **Marketplace-Abonnement**: Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.

d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

Auf der Seite Details und Anmeldeinformationen können Sie nun zu verschiedenen Anmeldeinformationen wechseln "Beim Erstellen einer neuen Arbeitsumgebung"



Vorhandene Anmeldedaten verwalten

Verwalten Sie die Azure-Anmeldedaten, die Sie BlueXP bereits hinzugefügt haben, indem Sie ein Marketplace-Abonnement zuordnen, Anmeldedaten bearbeiten und löschen.

Azure Marketplace Abonnement mit Anmeldedaten verknüpfen

Nachdem Sie Ihre Azure Zugangsdaten zu BlueXP hinzugefügt haben, können Sie diesen Anmeldedaten ein Azure Marketplace Abonnement zuordnen. Mit dem Abonnement können Sie ein Pay-as-you-go Cloud Volumes ONTAP System erstellen und andere BlueXP Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein Azure Marketplace-Abonnement verknüpfen können, nachdem Sie BlueXP bereits die Zugangsdaten hinzugefügt haben:

- Sie haben ein Abonnement nicht zugeordnet, wenn Sie die Anmeldeinformationen zu BlueXP hinzugefügt haben.
- Sie möchten das Abonnement für Azure Marketplace ändern, das mit den Azure-Anmeldedaten verknüpft ist.

Durch den Austausch des aktuellen Marketplace-Abonnements durch ein neues Abonnement wird das Marketplace-Abonnement für alle bestehenden Cloud Volumes ONTAP Arbeitsumgebungen und alle neuen Arbeitsumgebungen geändert.

Bevor Sie beginnen

Sie müssen einen Connector erstellen, bevor Sie die BlueXP-Einstellungen ändern können. I "Erfahren Sie, wie Sie einen Konnektor erstellen" .

Schritte

1. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
2. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen und dann **Abonnement konfigurieren**.

   Sie müssen Anmeldeinformationen auswählen, die einem Connector zugeordnet sind. Sie können kein Marketplace-Abonnement mit Anmeldedaten verknüpfen, die mit BlueXP verknüpft sind.

3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie das Abonnement aus der Down-Liste aus und wählen Sie **Konfigurieren**.
4. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Weiter** und befolgen Sie die Schritte im Azure Marketplace:

   a. Melden Sie sich bei Ihrem Azure-Konto an, wenn Sie dazu aufgefordert werden.
   b. Wählen Sie **Abonnieren**.
   c. Füllen Sie das Formular aus und wählen Sie **Abonnieren**.
   d. Wählen Sie nach Abschluss des Abonnements **Konto jetzt konfigurieren** aus.

      Sie werden zu BlueXP weitergeleitet.

   e. Auf der Seite **Subscription Assignment**:

      - Wählen Sie die BlueXP -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
      - Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

        BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

      Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.

      - Wählen Sie **Speichern**.

        Im folgenden Video sehen Sie, wie Sie im Azure Marketplace abonnieren:

Abonnieren Sie NetApp Intelligent Services vom Azure Marketplace

Anmeldedaten bearbeiten

Bearbeiten Sie Ihre Azure-Anmeldedaten in BlueXP, indem Sie die Details zu Ihren Azure-Serviceanmeldeinformationen ändern. Sie müssen beispielsweise den Clientschlüssel aktualisieren, wenn ein neues Geheimnis für die Service-Hauptanwendung erstellt wurde.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie auf der Seite **Unternehmensanmeldeinformationen** oder **Kontoanmeldeinformationen** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann **Anwenden**.

Anmeldeinformationen löschen

Wenn Sie keine Anmeldedaten mehr benötigen, können Sie diese aus BlueXP löschen. Sie können nur Anmeldeinformationen löschen, die nicht mit einer Arbeitsumgebung verknüpft sind.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie auf der Seite **Unternehmensanmeldeinformationen** oder **Kontoanmeldeinformationen** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Anmeldeinformationen löschen**.
3. Wählen Sie **Löschen**, um zu bestätigen.

Google Cloud

Mehr über Google Cloud-Projekte und -Berechtigungen erfahren

Erfahren Sie, wie BlueXP für Sie Aktionen mit Google Cloud Credentials durchführt und diese Zugangsdaten mit Marketplace-Abonnements verknüpft. Diese Details zu verstehen, kann hilfreich sein, wenn Sie die Anmeldeinformationen für ein oder mehrere Google Cloud-Projekte verwalten. Vielleicht möchten Sie mehr über das Servicekonto erfahren, das mit der Connector-VM verbunden ist.

Projekt und Berechtigungen für BlueXP

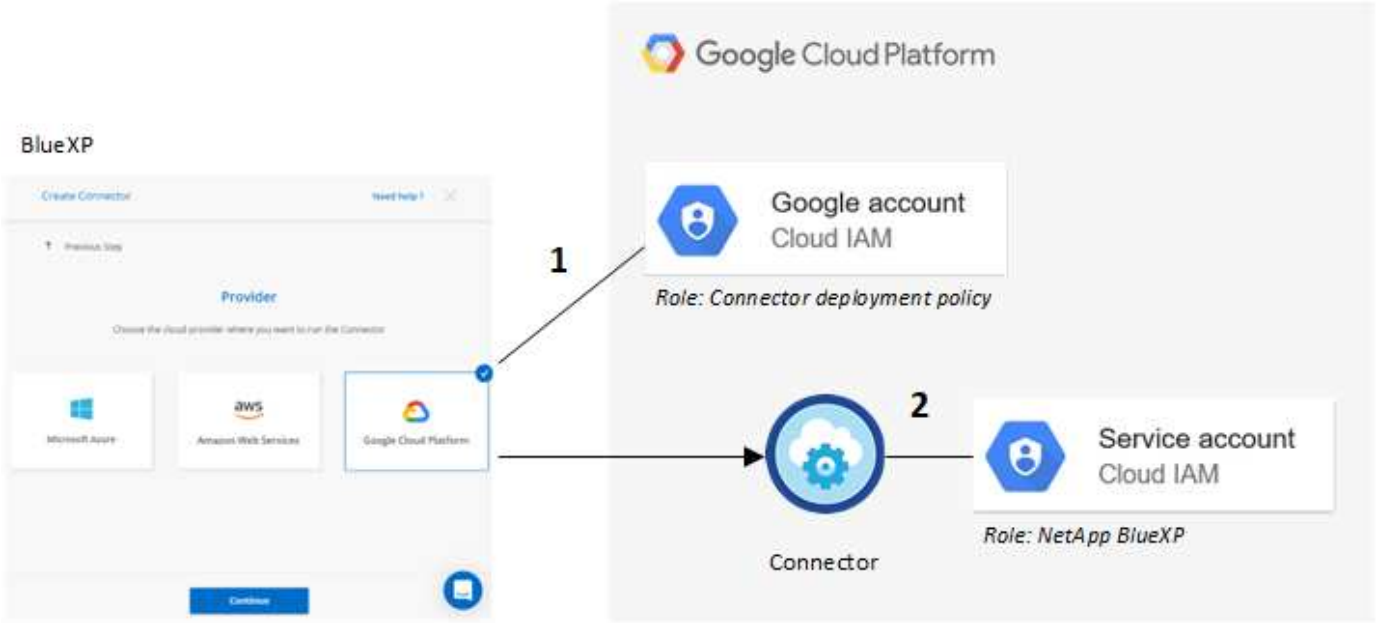
Bevor Sie BlueXP zum Managen von Ressourcen in Ihrem Google Cloud-Projekt verwenden können, müssen Sie zunächst einen Connector implementieren. Der Connector kann nicht vor Ort oder bei einem anderen Cloud-Provider ausgeführt werden.

Zwei Berechtigungsgruppen müssen vorhanden sein, bevor Sie einen Connector direkt von BlueXP bereitstellen:

1. Sie müssen einen Connector mit einem Google-Konto bereitstellen, das über Berechtigungen zum Starten der Connector VM-Instanz von BlueXP verfügt.
2. Bei der Bereitstellung des Connectors werden Sie aufgefordert, ein auszuwählen "Servicekonto" Für die VM-Instanz. BlueXP erhält Berechtigungen über das Servicekonto, um Cloud Volumes ONTAP Systeme zu erstellen und zu managen, Backups mit BlueXP Backup und Recovery zu managen usw. Berechtigungen

werden durch Hinzufügen einer benutzerdefinierten Rolle an das Servicekonto bereitgestellt.

Das folgende Bild zeigt die in den Nummern 1 und 2 oben beschriebenen Berechtigungsanforderungen:



Weitere Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- "Richten Sie Google Cloud-Berechtigungen für den Standardmodus ein"
- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

Anmeldedaten und Abonnements für den Marktplatz

Wenn Sie einen Connector in Google Cloud implementieren, erstellt BlueXP im Projekt, in dem sich der Connector befindet, einen StandardSatz an Anmeldeinformationen für das Google Cloud Servicekonto. Diese Anmeldedaten müssen mit einem Google Cloud Marketplace Abonnement verbunden sein, sodass Sie für Cloud Volumes ONTAP einen Stundensatz (PAYGO) zahlen und andere BlueXP Services nutzen können.

"Erfahren Sie, wie Sie ein Google Cloud Marketplace Abonnement verknüpfen".

Beachten Sie Folgendes über Google Cloud-Anmeldedaten und Marketplace-Abonnements:

- Einem Connector kann nur ein Satz Google Cloud-Anmeldedaten zugeordnet werden
- Sie können den Anmeldedaten nur ein Google Cloud Marketplace-Abonnement zuweisen
- Sie können ein bestehendes Marketplace-Abonnement durch ein neues Abonnement ersetzen

Projekt für Cloud Volumes ONTAP

Cloud Volumes ONTAP kann im selben Projekt wie der Connector oder in einem anderen Projekt residieren. Um Cloud Volumes ONTAP in einem anderen Projekt bereitzustellen, müssen Sie zunächst das Connector-Servicekonto und die Rolle zu diesem Projekt hinzufügen.

- "Erfahren Sie, wie Sie das Service-Konto einrichten"
- "Erfahren Sie, wie Sie Cloud Volumes ONTAP in Google Cloud implementieren und ein Projekt auswählen"

Managen Sie Google Cloud-Anmeldedaten und -Abonnements für BlueXP

Sie können die Google Cloud-Anmeldedaten verwalten, die mit der VM-Instanz Connector verknüpft sind, indem Sie ein Marketplace-Abonnement zuordnen und den Abonnementprozess beheben. Beide Aufgaben stellen sicher, dass Sie Ihr Marktplatz-Abonnement zum Bezahlen von Datendiensten verwenden können.

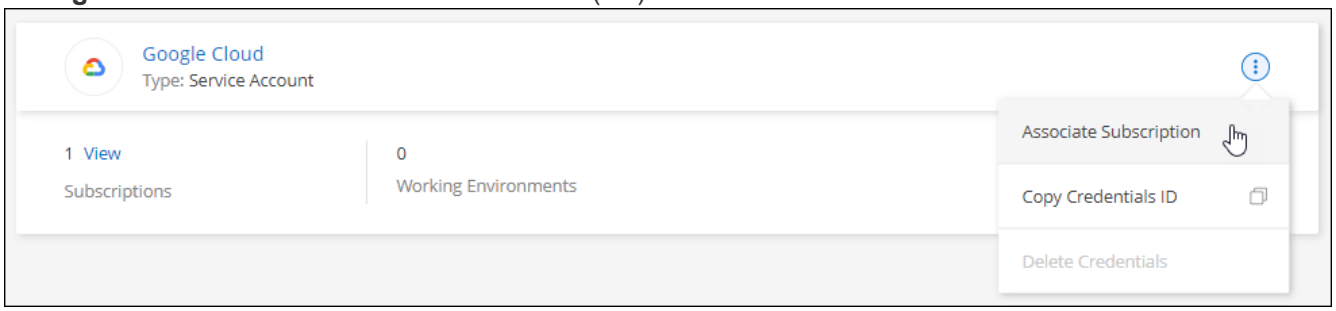
Verbinden Sie ein Marketplace-Abonnement mit Google Cloud-Anmeldedaten

Wenn Sie einen Connector in Google Cloud bereitstellen, erstellt BlueXP einen Standardsatz von Anmeldeinformationen, die der Connector-VM-Instanz zugeordnet sind. Sie können jederzeit das mit diesen Anmeldedaten verbundene Abonnement von Google Cloud Marketplace ändern. Mit dem Abonnement können Sie ein Cloud Volumes ONTAP-System mit nutzungsbasierter Abrechnung erstellen und andere Datendienste nutzen.

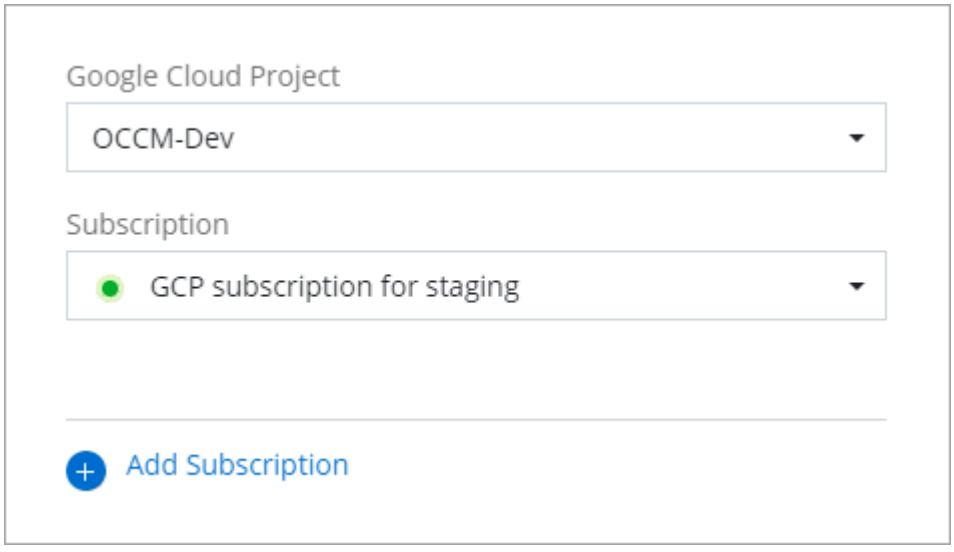
Durch den Austausch des aktuellen Marketplace-Abonnements durch ein neues Abonnement wird das Marketplace-Abonnement für alle bestehenden Cloud Volumes ONTAP Arbeitsumgebungen und alle neuen Arbeitsumgebungen geändert.

Schritte

1. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
2. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen und dann **Abonnement konfigurieren**. +neuer Screenshot erforderlich (TS)



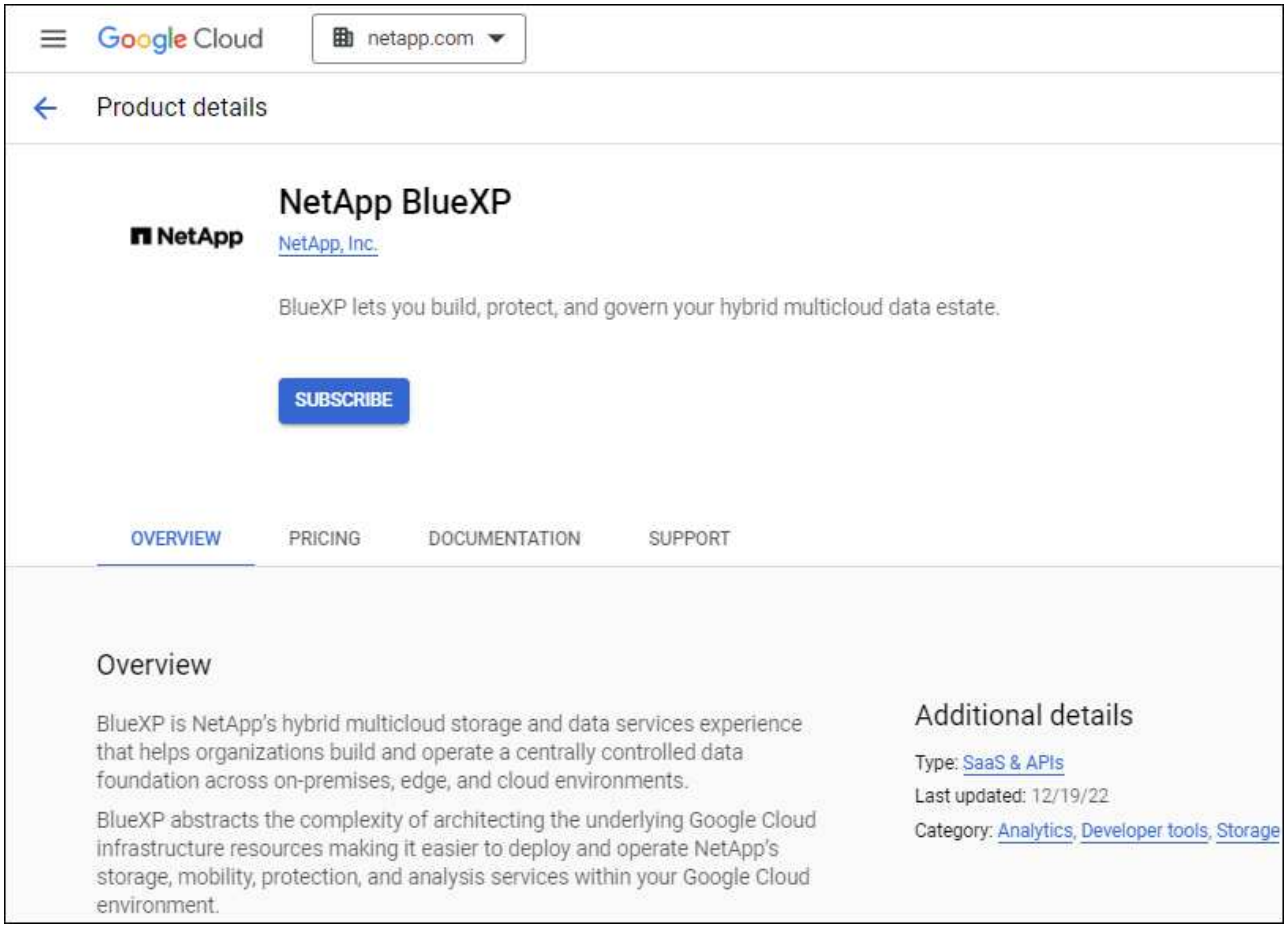
3. Um ein bestehendes Abonnement mit den ausgewählten Anmeldeinformationen zu konfigurieren, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Dropdown-Liste aus, und wählen Sie dann **Konfigurieren** aus.



4. Wenn Sie noch kein Abonnement besitzen, wählen Sie **Abonnement hinzufügen > Weiter** und folgen Sie den Schritten im Google Cloud Marketplace.

   Bevor Sie die folgenden Schritte durchführen, stellen Sie sicher, dass Sie sowohl Billing Admin-Berechtigungen in Ihrem Google Cloud-Konto als auch BlueXP-Login haben.

   a. Nachdem Sie weitergeleitet wurden auf die "NetApp Intelligent Services-Seite im Google Cloud Marketplace" , stellen Sie sicher, dass im oberen Navigationsmenü das richtige Projekt ausgewählt ist.



   b. Wählen Sie **Abonnieren**.

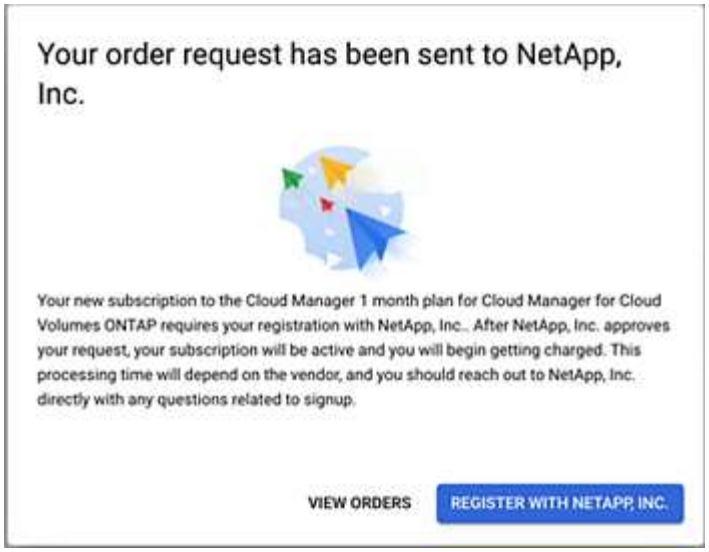
   c. Wählen Sie das entsprechende Rechnungskonto aus und stimmen Sie den allgemeinen Geschäftsbedingungen zu.

   d. Wählen Sie **Abonnieren**.

      Dieser Schritt sendet Ihre Transferanfrage an NetApp.

   e. Wählen Sie im Popup-Dialogfeld **Registrierung bei NetApp, Inc.** aus

      Dieser Schritt muss abgeschlossen sein, um das Google Cloud-Abonnement mit Ihrer-Organisation oder Ihrem BlueXP -Konto zu verknüpfen. Der Vorgang der Verknüpfung eines Abonnements ist erst abgeschlossen, wenn Sie von dieser Seite umgeleitet und dann bei BlueXP angemeldet sind.



f. Führen Sie die Schritte auf der Seite **Subscription Assignment** aus:

> Wenn ein Mitarbeiter Ihres Unternehmens bereits über Ihr Rechnungskonto das NetApp BlueXP Abonnement abonniert hat, werden Sie weitergeleitet "Die Cloud Volumes ONTAP-Seite auf der BlueXP-Website" Stattdessen. Sollte dies nicht unerwartet sein, wenden Sie sich an Ihr NetApp Vertriebsteam. Google ermöglicht nur ein Abonnement pro Google-Abrechnungskonto.

- Wählen Sie die BlueXP -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
- Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

  BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

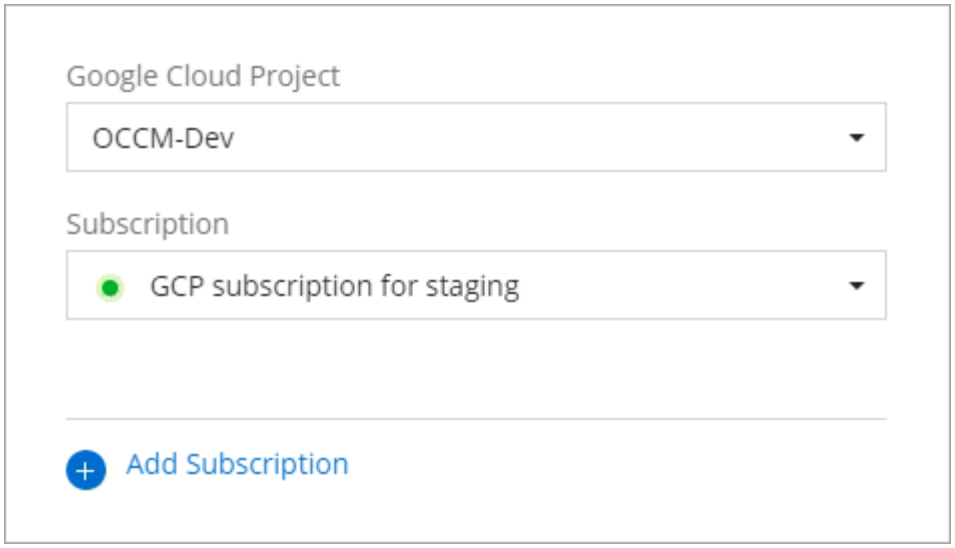
Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.

- Wählen Sie **Speichern**.

  Im folgenden Video sehen Sie, wie Sie sich für den Google Cloud Marketplace anmelden können:

Abonnieren Sie BlueXP über den Google Cloud Marketplace

a. Navigieren Sie nach Abschluss dieses Vorgangs zur Seite Anmeldeinformationen in BlueXP, und wählen Sie dieses neue Abonnement aus.

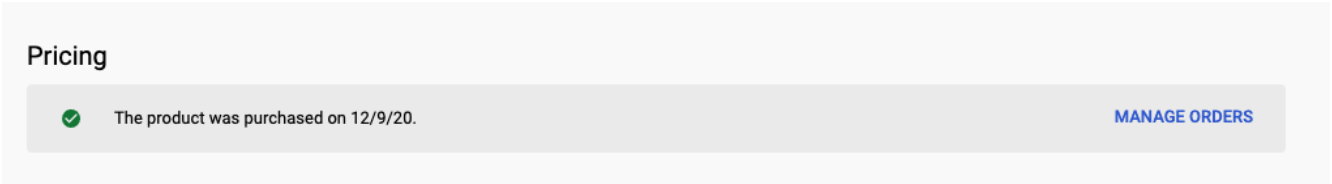


Fehlerbehebung bei der Marketplace-Subscription

Manchmal kann das Abonnieren von NetApp Intelligent Services über den Google Cloud Marketplace aufgrund falscher Berechtigungen oder aufgrund des versehentlichen Nichtbefolgens der Weiterleitung zur BlueXP-Website fragmentiert werden. Wenn dies geschieht, führen Sie die folgenden Schritte aus, um den Abonnementprozess abzuschließen.

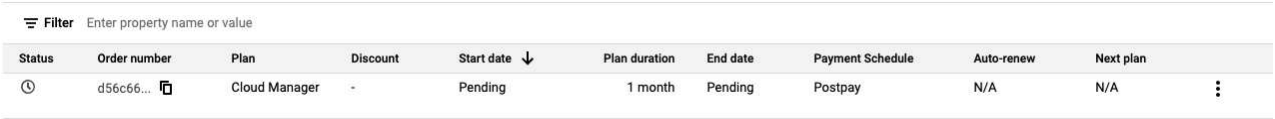
Schritte

1. Navigieren Sie zum "Seite zu NetApp BlueXP im Google Cloud Marketplace" Um den Status der Bestellung zu überprüfen. Wenn auf der Seite **auf Anbieter verwalten** steht, scrollen Sie nach unten und wählen Sie **Bestellungen verwalten**.



   - Wenn der Auftrag ein grünes Häkchen anzeigt und dies unerwartet ist, kann bereits ein anderer Mitarbeiter des Unternehmens, der dasselbe Rechnungskonto verwendet, abonniert werden. Wenn das unerwartete vorbereitet ist oder wenn Sie die Details zu diesem Abonnement benötigen, wenden Sie sich an Ihr NetApp Vertriebsteam.

   - Wenn der Auftrag einen Clock- und **Ausstehend**-Status anzeigt, gehen Sie zurück zur Marktplatzseite und wählen Sie **auf Anbieter verwalten**, um den Prozess wie oben beschrieben abzuschließen.



NSS-Anmeldeinformationen verwalten, die mit BlueXP verknüpft sind

Ordnen Sie Ihrer BlueXP -Organisation ein NetApp Support Site-Konto zu, um wichtige Workflows für Cloud Volumes ONTAP zu aktivieren. Diese NSS-Anmeldeinformationen sind der gesamten BlueXP Organisation zugeordnet.

BlueXP unterstützt zudem die Zuordnung eines NSS-Kontos pro BlueXP -Benutzerkonto. "Erfahren Sie, wie Sie Anmeldedaten auf Benutzerebene verwalten".

- "Weitere Informationen zu BlueXP Implementierungsmodi"
- "Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "

Überblick

Um in BlueXP die folgenden Aufgaben zu ermöglichen, ist es erforderlich, die Zugangsdaten der NetApp Support Website mit der angegebenen Seriennummer Ihres BlueXP Kontos zu verknüpfen:

- Implementierung von Cloud Volumes ONTAP unter Verwendung von BYOL (Bring-Your-Own-License)

  Die Bereitstellung Ihres NSS-Kontos ist erforderlich, damit BlueXP Ihren Lizenzschlüssel hochladen und das Abonnement für den von Ihnen erworbenen Zeitraum aktivieren kann. Dies schließt automatische Updates für Vertragsverlängerungen ein.

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen

  Die Bereitstellung Ihres NSS Kontos ist erforderlich, um Support für Ihr System zu aktivieren und Zugang zu den technischen Support-Ressourcen von NetApp zu erhalten.

- Aktualisieren der Cloud Volumes ONTAP Software auf die neueste Version

Diese Anmeldedaten sind mit Ihrer spezifischen Seriennummer Ihres BlueXP -Kontos verknüpft. Benutzer, die der-Organisation oder dem BlueXP -Konto angehören, können über **Support > NSS-Verwaltung** auf diese Anmeldedaten zugreifen.

Fügen Sie ein NSS-Konto hinzu

Sie können Ihre Konten für die NetApp Support-Website zur Verwendung mit BlueXP über das Support Dashboard in BlueXP hinzufügen und managen.

Wenn Sie Ihr NSS-Konto hinzugefügt haben, kann BlueXP diese Informationen für Bereiche wie Lizenzdownloads, Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen verwenden.

Sie können Ihrer BlueXP -Organisation mehrere NSS-Konten zuordnen. Sie können jedoch keine Kunden- und Partnerkonten innerhalb derselben Organisation haben.

NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsservices, die speziell auf Support und Lizenzierung zugeschnitten sind.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.
2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. Wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite umgeleitet zu werden.

4. Geben Sie auf der Anmeldeseite Ihre NetApp registrierte E-Mail-Adresse und das Kennwort an.

   Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern.

   Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet ist. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen ••• Menü.

   - Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option ••• Menü.

     Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Eine Benachrichtigung wird gesendet, um Sie darüber zu informieren.

Was kommt als Nächstes?

Benutzer können jetzt das Konto beim Erstellen neuer Cloud Volumes ONTAP-Systeme und bei der Registrierung vorhandener Cloud Volumes ONTAP-Systeme auswählen.

- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Cloud Volumes ONTAP in Google Cloud wird gestartet"
- "Registrieren von Pay-as-you-go-Systemen"

NSS-Anmeldeinformationen aktualisieren

Aus Sicherheitsgründen müssen Sie Ihre NSS-Anmeldeinformationen alle 90 Tage aktualisieren. Sie werden im BlueXP -Benachrichtigungscenter benachrichtigt, wenn Ihre NSS-Anmeldeinformationen abgelaufen sind. "Erfahren Sie mehr über das Benachrichtigungscenter".

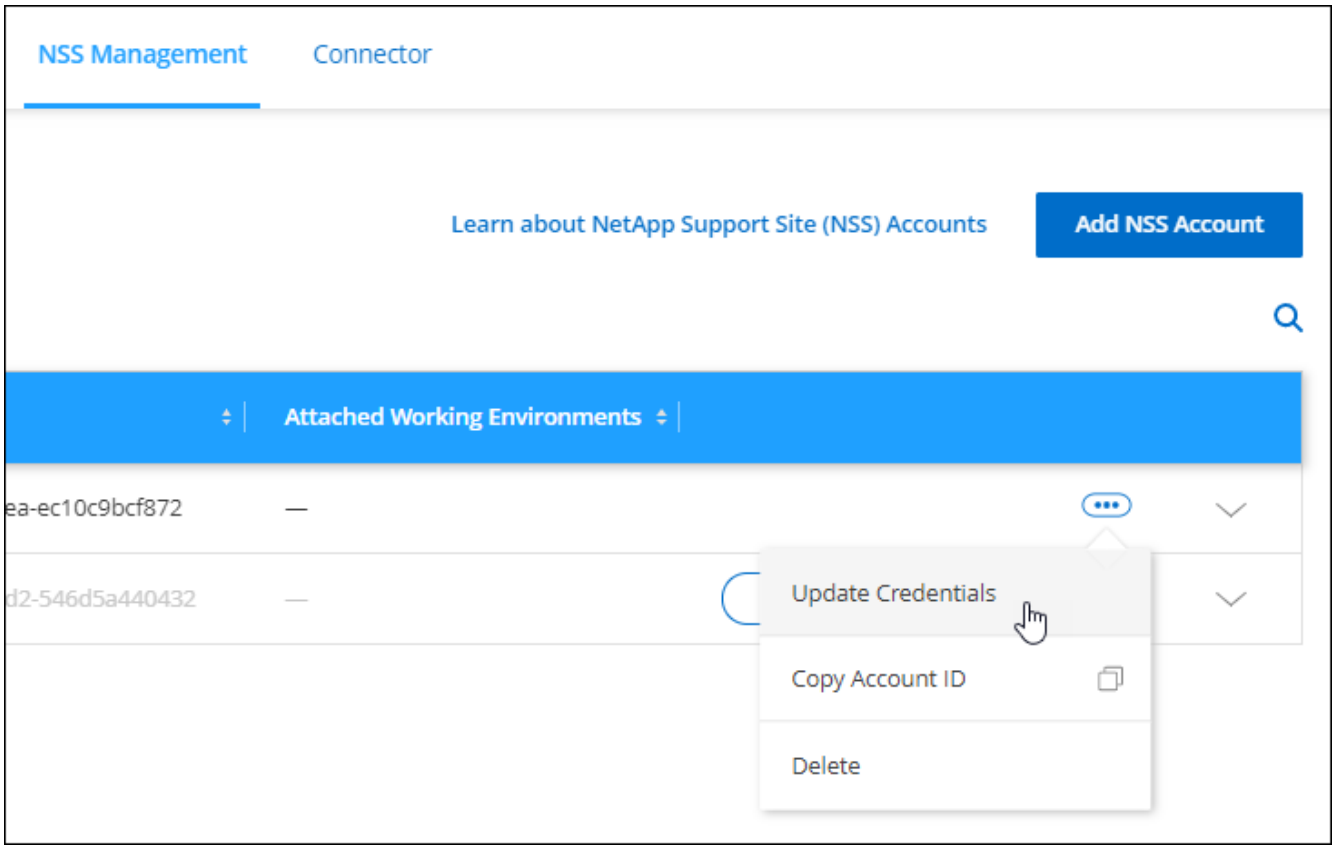
Abgelaufene Anmeldeinformationen können Folgendes stören, sind aber nicht beschränkt auf:

- Lizenz-Updates in Digital Wallet, d. h. Sie können nicht die neu erworbene Kapazität nutzen.
- Möglichkeit, Support-Fälle einzureichen und zu verfolgen

Darüber hinaus können Sie die NSS-Anmeldeinformationen, die Ihrer Organisation zugeordnet sind, aktualisieren, wenn Sie das NSS-Konto Ihrer BlueXP -Organisation ändern möchten. Wenn beispielsweise die Person, die mit Ihrem NSS-Konto verknüpft ist, Ihr Unternehmen verlassen hat.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.
2. Wählen Sie **NSS Management**.
3. Wählen Sie für das NSS-Konto, das Sie aktualisieren möchten, aus ••• Und wählen Sie dann **Anmeldeinformationen aktualisieren**.



4. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite umgeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsservices im Zusammenhang mit Support und Lizenzierung.

5. Geben Sie auf der Anmeldeseite Ihre NetApp registrierte E-Mail-Adresse und das Kennwort an.

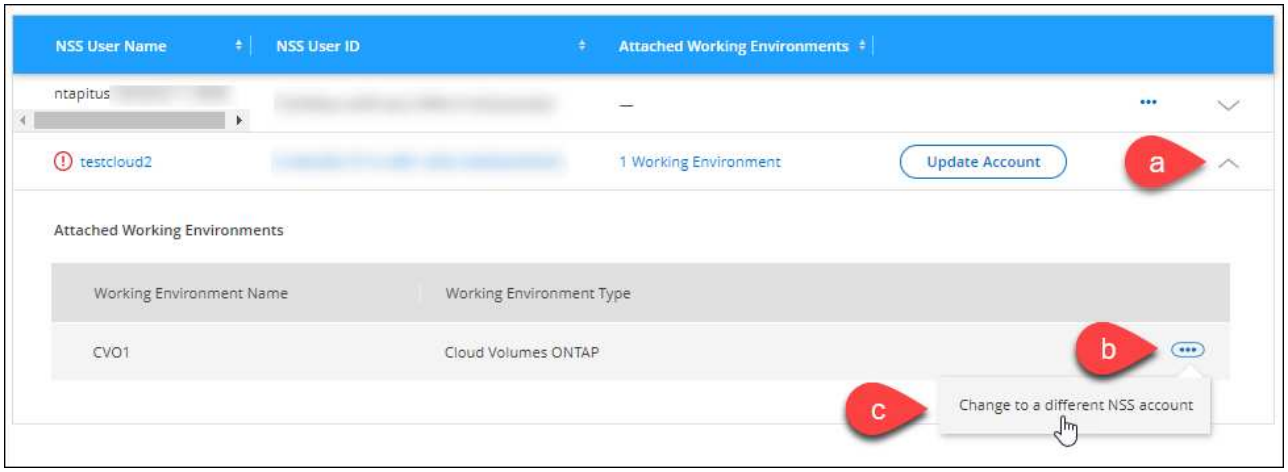
Verbinden Sie eine Arbeitsumgebung mit einem anderen NSS-Konto

Wenn Ihr Unternehmen über mehrere NetApp Support Site Accounts verfügt, können Sie ändern, welches Konto einem Cloud Volumes ONTAP System zugeordnet ist.

Sie müssen das Konto zunächst mit BlueXP verknüpft haben.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.
2. Wählen Sie **NSS Management**.
3. Führen Sie die folgenden Schritte aus, um das NSS-Konto zu ändern:
   a. Erweitern Sie die Zeile für den NetApp Support Site Account, dem die Arbeitsumgebung derzeit zugeordnet ist.
   b. Wählen Sie für die Arbeitsumgebung, für die Sie die Zuordnung ändern möchten, aus •••
   c. Wählen Sie **Ändern Sie auf ein anderes NSS-Konto**.



d. Wählen Sie das Konto aus und wählen Sie dann **Speichern**.

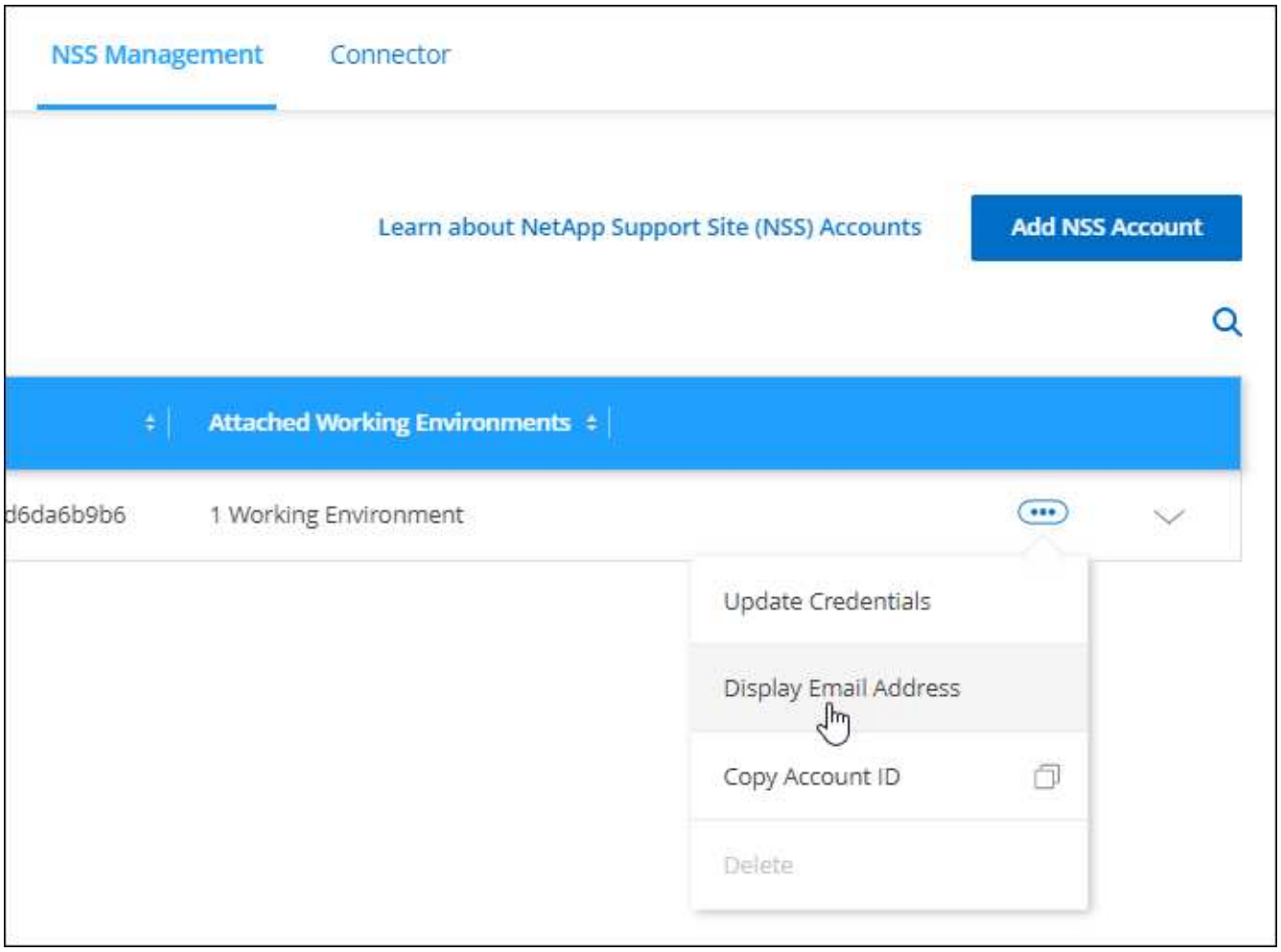
Zeigen Sie die E-Mail-Adresse für ein NSS-Konto an

Aus Sicherheitsgründen wird die E-Mail-Adresse, die einem NSS-Konto zugeordnet ist, standardmäßig nicht angezeigt. Sie können die E-Mail-Adresse und den zugehörigen Benutzernamen für ein NSS-Konto anzeigen.

Wenn Sie die NSS-Verwaltungsseite aufrufen, generiert BlueXP für jedes Konto in der Tabelle ein Token. Dieses Token enthält Informationen zur zugehörigen E-Mail-Adresse. Das Token wird entfernt, wenn Sie die Seite verlassen. Die Informationen werden niemals zwischengespeichert, wodurch Ihre Privatsphäre geschützt wird.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.
2. Wählen Sie **NSS Management**.
3. Wählen Sie für das NSS-Konto, das Sie aktualisieren möchten ••• , und wählen Sie dann **E-Mail-Adresse anzeigen** aus. Sie können die Schaltfläche Kopieren verwenden, um die E-Mail-Adresse zu kopieren.



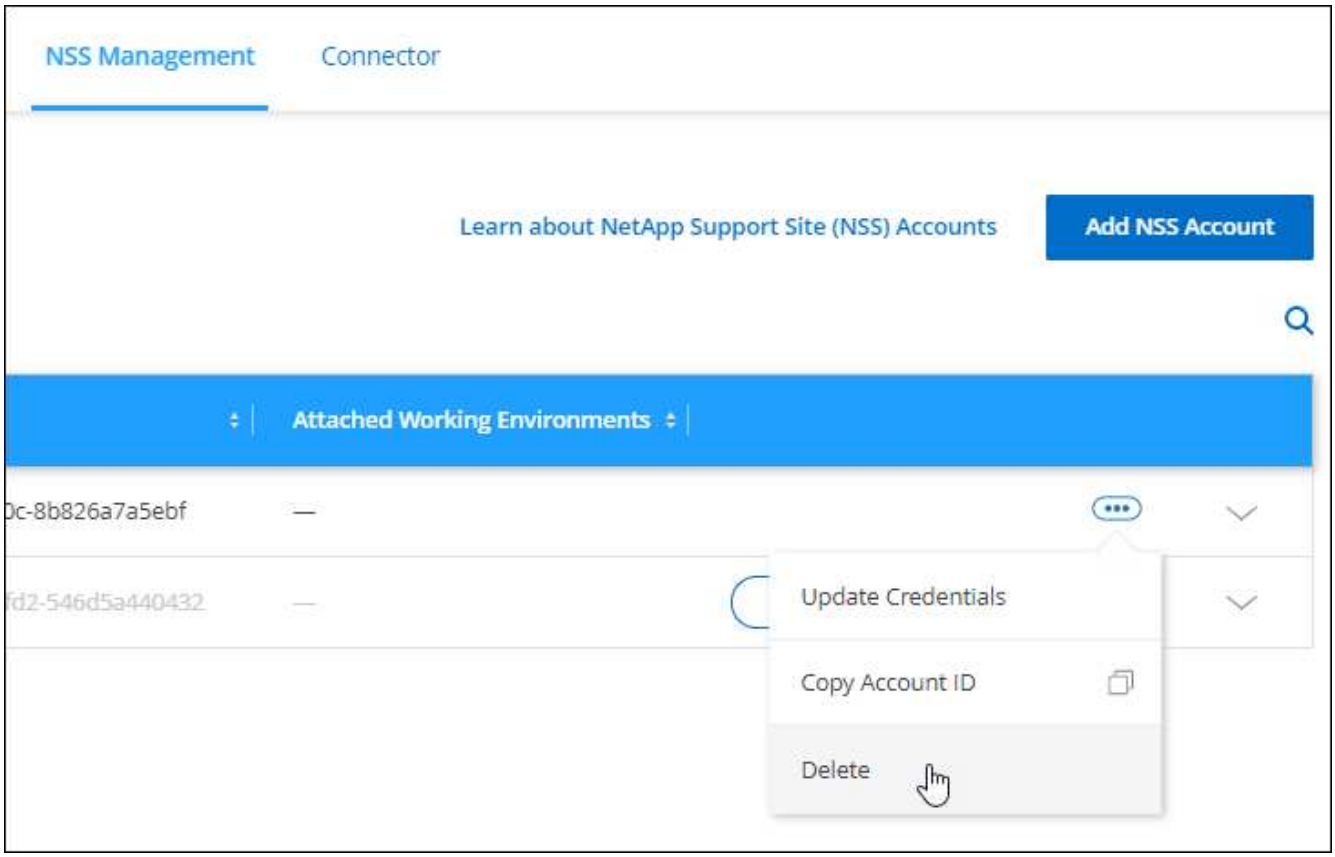
Entfernen Sie ein NSS-Konto

Löschen Sie alle NSS-Konten, die Sie nicht mehr mit BlueXP verwenden möchten.

Sie können kein Konto löschen, das derzeit mit einer Cloud Volumes ONTAP-Arbeitsumgebung verknüpft ist. Sie müssen zuerst zu Verbinden Sie die Arbeitsumgebungen mit einem anderen NSS-Konto.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.
2. Wählen Sie **NSS Management**.
3. Wählen Sie für das NSS-Konto, das Sie löschen möchten, aus ••• Und wählen Sie dann **Löschen**.



4. Wählen Sie **Löschen**, um zu bestätigen.

Managen Sie die mit Ihren BlueXP Anmeldedaten verbundenen Zugangsdaten

Je nach den Aktionen, die Sie in BlueXP durchgeführt haben, können Sie Ihren BlueXP Benutzeranmeldeinformationen zur ONTAP und zur NetApp Support Website (NSS) zugeordnet haben. Sie können diese Anmeldedaten in BlueXP anzeigen und managen, nachdem Sie sie verknüpft haben. Wenn Sie beispielsweise das Passwort für diese Anmeldedaten ändern, müssen Sie das Passwort in BlueXP aktualisieren.

ONTAP Referenzen

Benutzer benötigen ONTAP-Administratoranmeldeinformationen, um ONTAP-Cluster in BlueXP zu erkennen. Der Zugriff auf ONTAP System Manager hängt jedoch davon ab, ob Sie einen Connector verwenden.

Ohne Steckverbinder

Die Benutzer werden aufgefordert, ihre ONTAP-Anmeldedaten einzugeben, um auf den ONTAP System Manager für das Cluster zuzugreifen. Benutzer können diese Anmeldeinformationen in BlueXP speichern, was bedeutet, dass sie nicht jedes Mal aufgefordert werden, sie einzugeben. Benutzeranmeldeinformationen sind nur für den jeweiligen Benutzer sichtbar und können über die Seite Benutzeranmeldeinformationen verwaltet werden.

Mit einem Connector

Standardmäßig werden Benutzer nicht aufgefordert, ihre ONTAP-Anmeldedaten für den Zugriff auf ONTAP System Manager einzugeben. Ein BlueXP -Administrator (mit der Administratorrolle des Unternehmens) kann BlueXP jedoch so konfigurieren, dass Benutzer aufgefordert werden, ihre ONTAP-Anmeldedaten einzugeben. Wenn diese Einstellung aktiviert ist, müssen Benutzer jedes Mal ihre ONTAP-Anmeldeinformationen eingeben.

"Weitere Informationen ."

NSS-Anmeldeinformationen

Die NSS-Zugangsdaten für Ihre BlueXP Anmeldung ermöglichen die Support-Registrierung, das Fallmanagement und den Zugriff auf Digital Advisor.

- Wenn Sie **Support > Ressourcen** aufrufen und sich für den Support registrieren, werden Sie aufgefordert, Ihre NSS-Anmeldedaten mit Ihrem BlueXP Login zu verknüpfen.

  Dadurch wird Ihre Organisation bzw. Ihr Konto für den Support registriert und der Supportanspruch aktiviert. Nur ein Benutzer in Ihrer BlueXP Organisation oder Ihrem Account muss ein NetApp Support Site Konto mit seinem BlueXP Login verknüpfen, um sich für Support zu registrieren und die Support-Berechtigung zu aktivieren. Nachdem dies abgeschlossen ist, zeigt die Seite **Ressourcen** an, dass Ihr Konto für Support registriert ist.

  "Erfahren Sie, wie Sie sich für Support registrieren"

- Wenn Sie auf **Support > Case Management** zugreifen, werden Sie aufgefordert, Ihre NSS-Anmeldedaten einzugeben, sofern Sie dies noch nicht getan haben. Auf dieser Seite können Sie die Support-Fälle erstellen und verwalten, die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpft sind.
- Wenn Sie in BlueXP auf Digital Advisor zugreifen, werden Sie aufgefordert, sich bei Digital Advisor anzumelden, indem Sie Ihre NSS-Anmeldedaten eingeben.

Beachten Sie Folgendes zu dem NSS-Konto bei Ihrer BlueXP Anmeldung:

- Das Konto wird auf Benutzerebene verwaltet, was bedeutet, dass es von anderen Benutzern, die sich anmelden, nicht angezeigt wird.
- Digital Advisor und Support-Case-Management können nur ein NSS-Konto pro Benutzer zugeordnet werden.
- Wenn Sie versuchen, ein NetApp-Support-Site-Konto mit einer Cloud Volumes ONTAP-Arbeitsumgebung zu verknüpfen, können Sie nur aus den NSS-Konten auswählen, die der BlueXP -Organisation oder dem Konto hinzugefügt wurden, in dem Sie Mitglied sind.

  Die Zugangsdaten für NSS Konten unterscheiden sich von dem NSS-Konto, das mit Ihrer BlueXP Anmeldung verknüpft ist. Mit den Anmeldeinformationen auf NSS-Kontoebene können Sie Cloud Volumes ONTAP mit BYOL bereitstellen, PAYGO-Systeme registrieren und die Software aktualisieren.

  "Erfahren Sie mehr über die Verwendung von NSS-Anmeldeinformationen mit Ihrer-Organisation oder Ihrem BlueXP -Konto".

Verwalten Sie Ihre Benutzeranmeldeinformationen

Verwalten Sie Ihre Benutzeranmeldeinformationen, indem Sie den Benutzernamen und das Kennwort aktualisieren oder die Anmeldeinformationen löschen.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wenn Sie noch keine Anmeldedaten für den Benutzer haben, können Sie **Add NSS Credentials** auswählen, um Ihr NetApp Support Site Konto hinzuzufügen.

4. Verwalten Sie vorhandene Anmeldeinformationen, indem Sie im Menü „Aktionen“ die folgenden Optionen auswählen:
   - **Zugangsdaten aktualisieren**: Aktualisieren Sie den Benutzernamen und das Passwort für das Konto.
   - **Zugangsdaten löschen**: Entfernen Sie das Konto, das Ihrem BlueXP Benutzerkonto zugeordnet ist.

Ergebnis

BlueXP aktualisiert Ihre Anmeldeinformationen und Sie sehen die Änderungen, wenn Sie auf den ONTAP-Cluster, den digitalen Berater oder die Fallmanagement-Seite zugreifen.

Monitoring des BlueXP -Betriebs

Sie können den Status der Operationen überwachen, die BlueXP durchführt, um zu sehen, ob Probleme auftreten, die Sie beheben müssen. Sie können den Status in der Zeitleiste oder im Benachrichtigungscenter anzeigen oder Benachrichtigungen an Ihre E-Mail senden lassen.

Die Tabelle vergleicht die Timeline und das Benachrichtigungscenter, um ihre Funktionen hervorzuheben.

Notification Center	Zeitachse
Zeigt den allgemeinen Status von Ereignissen und Aktionen an	Enthält Details zu jedem Ereignis oder jeder Aktion zur weiteren Untersuchung
Zeigt den Status der aktuellen Anmeldesitzung an (die Informationen werden nach der Abmeldung nicht im Benachrichtigungscenter angezeigt)	Behält den Status des letzten Monats bei
Zeigt nur Aktionen an, die in der Benutzeroberfläche initiiert wurden	Zeigt alle Aktionen der UI oder der APIs an
Zeigt benutzerinitiierte Aktionen an	Zeigt alle Aktionen an, ob vom Benutzer initiiert oder vom System initiiert
Ergebnisse nach Bedeutung filtern	Filtern nach Dienst, Aktion, Benutzer, Status und mehr
Ermöglicht die E-Mail-Benachrichtigung an Benutzer und andere Personen	Keine E-Mail-Funktion

Überwachen Sie die Benutzeraktivität über den BlueXP -Zeitplan

Die Zeitleiste zeigt die Aktionen, die Benutzer zur Verwaltung Ihrer Organisation oder Ihres Kontos ausgeführt haben. Dazu gehören Verwaltungsaktionen wie das Zuordnen von Benutzern, das Erstellen von Arbeitsumgebungen, das Erstellen von Connectors und vieles mehr.

Mithilfe der Zeitleiste können Sie feststellen, wer eine Aktion ausgeführt hat und welchen Status sie hat.

Schritte

1. Wählen Sie oben rechts in der BlueXP -Konsole > **Zeitleiste** aus.
2. Verwenden Sie die Filter über der Tabelle, um zu ändern, welche Aktionen in der Tabelle angezeigt werden.

   Sie können zum Beispiel den Filter **Dienst** verwenden, um Aktionen anzuzeigen, die mit einem bestimmten

BlueXP -Dienst zusammenhängen, oder Sie können den Filter **Benutzer** verwenden, um Aktionen in Bezug auf ein bestimmtes Benutzerkonto anzuzeigen.

Laden Sie Überwachungsprotokolle aus der Zeitleiste herunter

Sie können die Audit-Protokolle der Zeitleiste in eine CSV-Datei herunterladen. So können Sie die Aktionen Ihrer Benutzer in Ihrer Organisation protokollieren. Die heruntergeladene CSV-Datei enthält alle verfügbaren Spalten der Zeitleiste, unabhängig davon, welche Sie in der Zeitleiste filtern oder anzeigen.

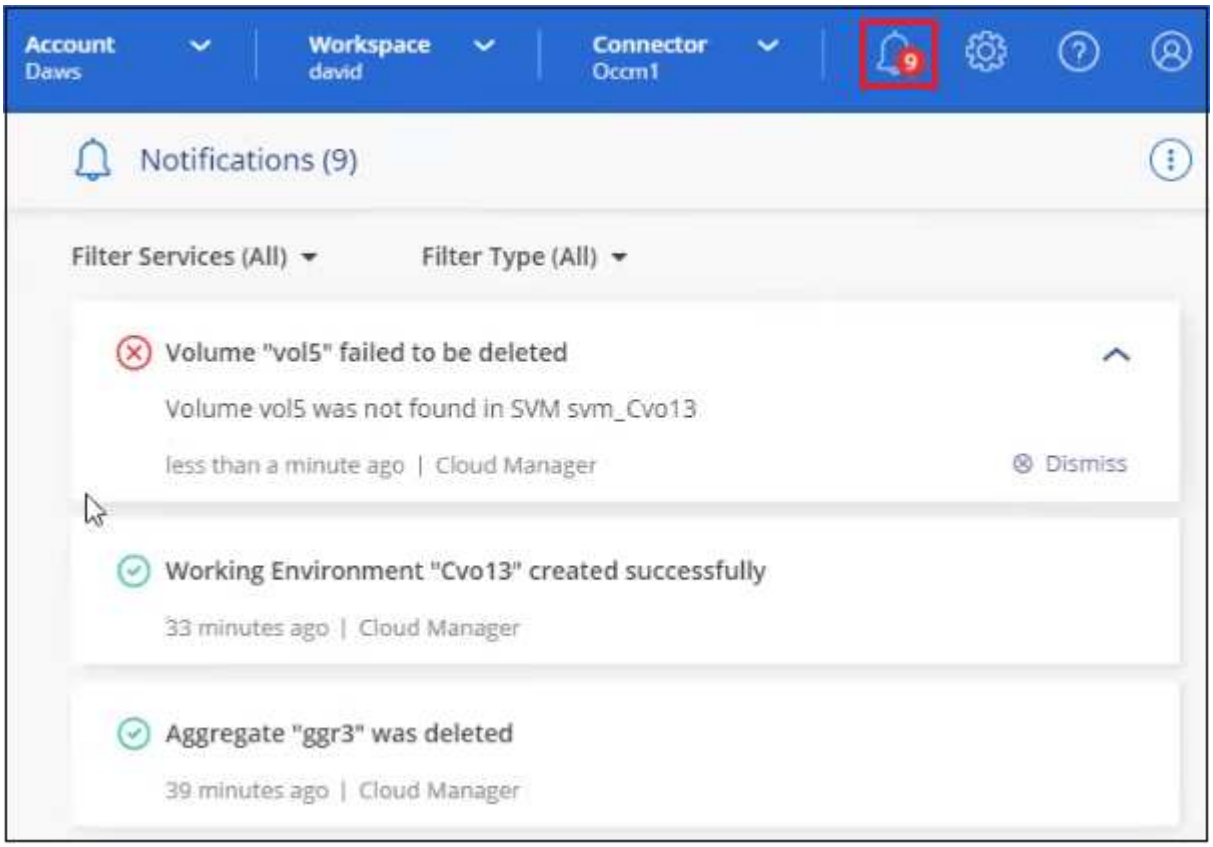
Schritte

1. Wählen Sie in der Timeline das Download-Symbol in der oberen rechten Ecke der Tabelle aus.

Überwachen Sie Aktivitäten mit dem Benachrichtigungscenter

Benachrichtigungen verfolgen den Fortschritt Ihrer BlueXP-Operationen, um den Erfolg zu überprüfen. Mit diesen können Sie den Status vieler BlueXP-Aktionen anzeigen, die Sie während Ihrer aktuellen Anmeldesitzung initiiert haben. Derzeit werden nicht alle BlueXP Services dem Benachrichtigungs-Center gemeldet.

Sie können die Benachrichtigungen anzeigen, indem Sie die Benachrichtigungsanzeige () In der Menüleiste. Die Farbe der kleinen Blase in der Glocke zeigt die Meldung mit dem höchsten Schweregrad an, die aktiv ist. Wenn Sie also eine rote Blase sehen, bedeutet dies, dass eine wichtige Benachrichtigung angezeigt wird, die Sie sich ansehen sollten.



Sie können BlueXP auch so konfigurieren, dass bestimmte Arten von Benachrichtigungen per E-Mail gesendet werden, sodass Sie über wichtige Systemaktivitäten informiert werden können, selbst wenn Sie nicht beim System angemeldet sind. E-Mails können an alle Benutzer gesendet werden, die Teil Ihrer BlueXP -Organisation oder Ihres Kontos sind, oder an alle anderen Empfänger, die bestimmte Arten von

Systemaktivitäten kennen müssen. Siehe Anleitung Einstellungen für E-Mail-Benachrichtigungen festlegen.

Vergleichen des Benachrichtigungscenters mit BlueXP -Warnmeldungen

Mit dem Benachrichtigungscenter können Sie den Status von Vorgängen anzeigen, die Sie von BlueXP initiiert haben, und Benachrichtigungen für bestimmte Arten von Systemaktivitäten einrichten. Gleichzeitig können Sie mit BlueXP -Warnmeldungen Probleme oder potenzielle Risiken in Ihrer ONTAP Storage-Umgebung in Bezug auf Kapazität, Verfügbarkeit, Performance, Schutz und Sicherheit anzeigen.

"Weitere Informationen zu BlueXP -Warnmeldungen"

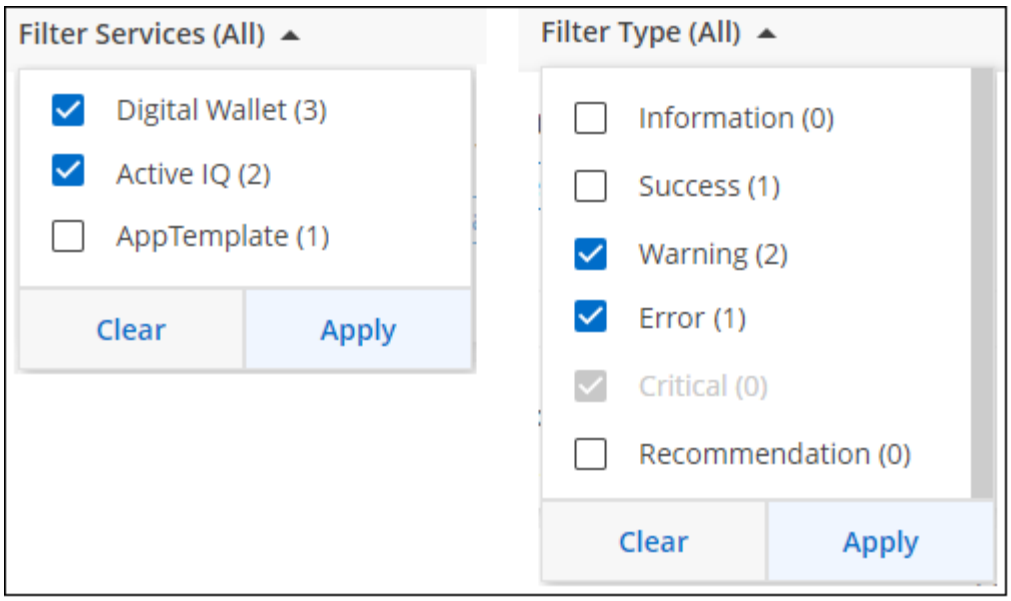
Benachrichtigungstypen

BlueXP klassifiziert Benachrichtigungen in die folgenden Kategorien:

Benachrichtigungstyp	Beschreibung
Kritisch	Ein Problem, das zu einer Serviceunterbrechung führen kann, wenn keine Korrekturmaßnahmen sofort ergriffen werden.
Fehler	Eine Aktion oder ein Prozess wurde mit einem Fehler beendet oder könnte zu einem Fehler führen, wenn keine Korrekturmaßnahmen ergriffen werden.
Warnung	Ein Problem, das Sie beachten sollten, um sicherzustellen, dass es den kritischen Schweregrad nicht erreicht. Benachrichtigungen dieses Schweregrades verursachen keine Serviceunterbrechungen und es sind möglicherweise keine sofortigen Korrekturmaßnahmen erforderlich.
Empfehlung	Eine Systemempfehlung für Sie, Maßnahmen zur Verbesserung des Systems oder eines bestimmten Dienstes zu ergreifen, zum Beispiel: Kostenersparnis, Vorschlag für neue Dienste, empfohlene Sicherheitskonfiguration, etc
Informationsdaten	Eine Meldung, die zusätzliche Informationen zu einer Aktion oder einem Prozess enthält.
Erfolg	Eine Aktion oder ein Prozess erfolgreich abgeschlossen.

Benachrichtigungen filtern

Standardmäßig werden alle aktiven Benachrichtigungen im Benachrichtigungscenter angezeigt. Sie können die Benachrichtigungen filtern, die Sie sehen, um nur die Benachrichtigungen anzuzeigen, die für Sie wichtig sind. Sie können nach BlueXP „Service“ und nach Benachrichtigung „Typ“ filtern.

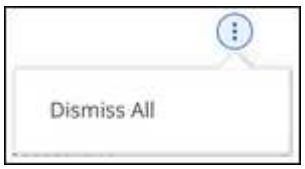


Wenn Sie beispielsweise nur „Fehler“ und „Warnung“ für BlueXP-Vorgänge sehen möchten, wählen Sie diese Einträge aus, und Sie werden nur die Arten von Benachrichtigungen sehen.

Benachrichtigungen schließen

Sie können Benachrichtigungen von der Seite entfernen, wenn Sie sie nicht mehr sehen müssen. Sie können Benachrichtigungen einzeln oder alle auf einmal ablehnen.

Um alle Benachrichtigungen zu schließen, wählen Sie im Benachrichtigungscenter aus ⋮ Und wählen Sie **Alle verwerfen**.



Um einzelne Benachrichtigungen zu schließen, bewegen Sie den Mauszeiger über die Benachrichtigung und wählen **Abweisen**.

Einstellungen für E-Mail-Benachrichtigungen festlegen

Sie können bestimmte Arten von Benachrichtigungen per E-Mail versenden, damit Sie über wichtige Systemaktivitäten informiert werden können, auch wenn Sie nicht bei BlueXP angemeldet sind. E-Mails können an alle Benutzer gesendet werden, die Teil Ihrer BlueXP -Organisation oder Ihres Kontos sind, oder an alle anderen Empfänger, die bestimmte Arten von Systemaktivitäten kennen müssen.

- BlueXP sendet E-Mail-Benachrichtigungen für den Connector, die digitale Geldbörse, das Kopieren und Synchronisieren sowie das Sichern und Wiederherstellen.
- Das Senden von E-Mail-Benachrichtigungen wird nicht unterstützt, wenn der Connector auf einer Website ohne Internetzugang installiert ist.

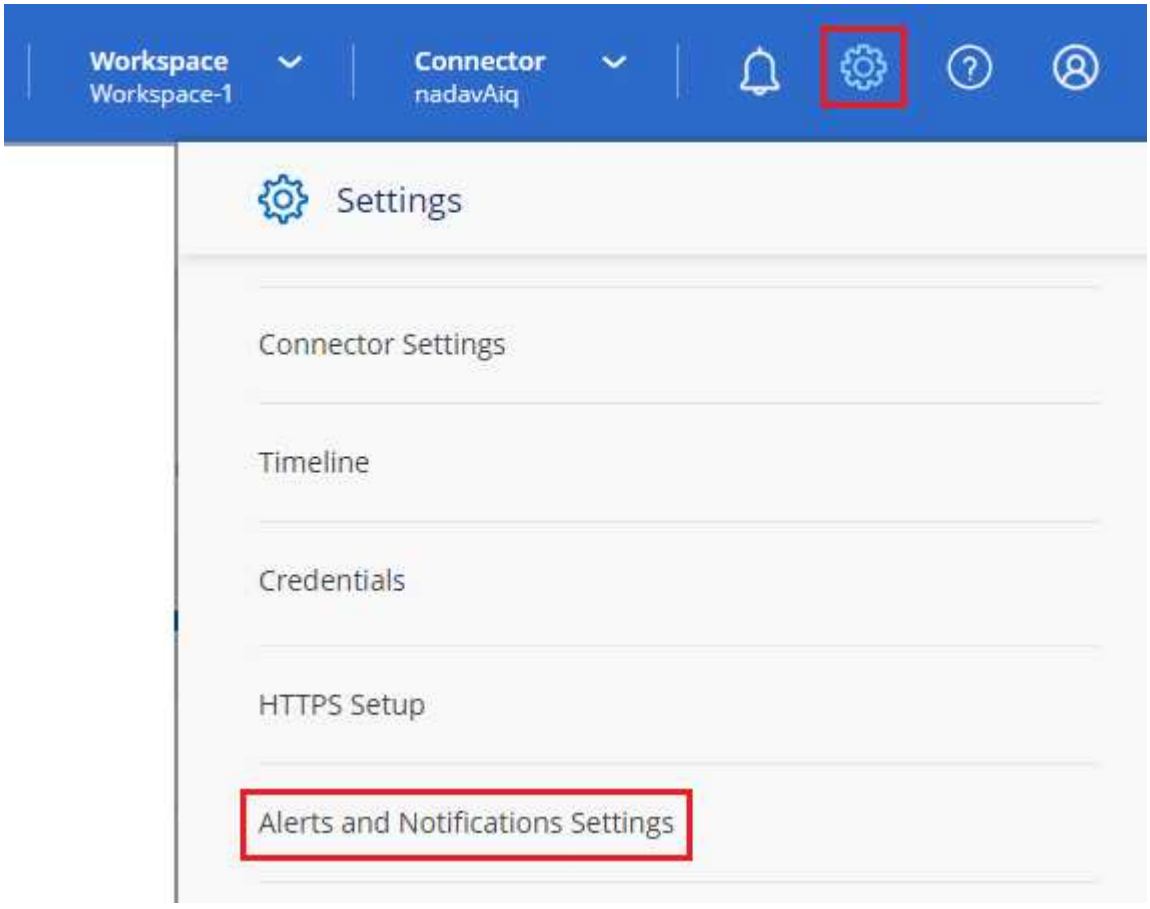
Die Filter, die Sie im Benachrichtigungscenter festlegen, bestimmen nicht, welche Arten von Benachrichtigungen Sie per E-Mail erhalten. Standardmäßig erhält jeder BlueXP -Administrator E-Mails für alle Benachrichtigungen zu „kritisch“ und „Empfehlung“. Diese Benachrichtigungen gelten für alle Services. Sie können keine Benachrichtigungen nur für bestimmte Services erhalten, z. B. Connectors oder BlueXP Backup und Recovery.

Alle anderen Benutzer und Empfänger sind so konfiguriert, dass sie keine Benachrichtigungs-E-Mails erhalten. Sie müssen daher die Benachrichtigungseinstellungen für weitere Benutzer konfigurieren.

Sie müssen über die Rolle des Organisationsadministrators verfügen, um die Benachrichtigungseinstellungen anzupassen.

Schritte

1. Wählen Sie in der BlueXP Menüleiste **Einstellungen > Einstellungen für Warnmeldungen und Benachrichtigungen** aus.

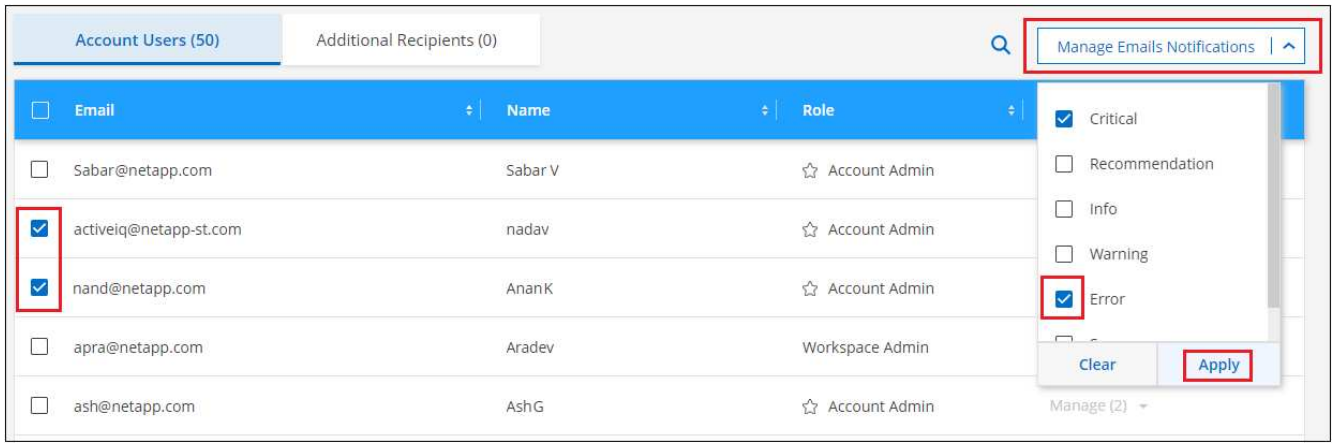


2. Wählen Sie einen oder mehrere Benutzer entweder auf der Registerkarte *Users* oder auf der Registerkarte *Additional Recipients* aus, und wählen Sie den Typ der zu sendenden Benachrichtigungen aus:

    ◦ Um Änderungen für einen einzelnen Benutzer vorzunehmen, wählen Sie das Menü in der Spalte Benachrichtigungen für diesen Benutzer aus, überprüfen Sie die zu sendenden

Benachrichtigungstypen und wählen Sie **Anwenden** aus.

- Um Änderungen für mehrere Benutzer vorzunehmen, aktivieren Sie das Kontrollkästchen für jeden Benutzer, wählen Sie **E-Mail-Benachrichtigungen verwalten**, aktivieren Sie die zu sendenden Benachrichtigungstypen und wählen Sie **Anwenden** aus.

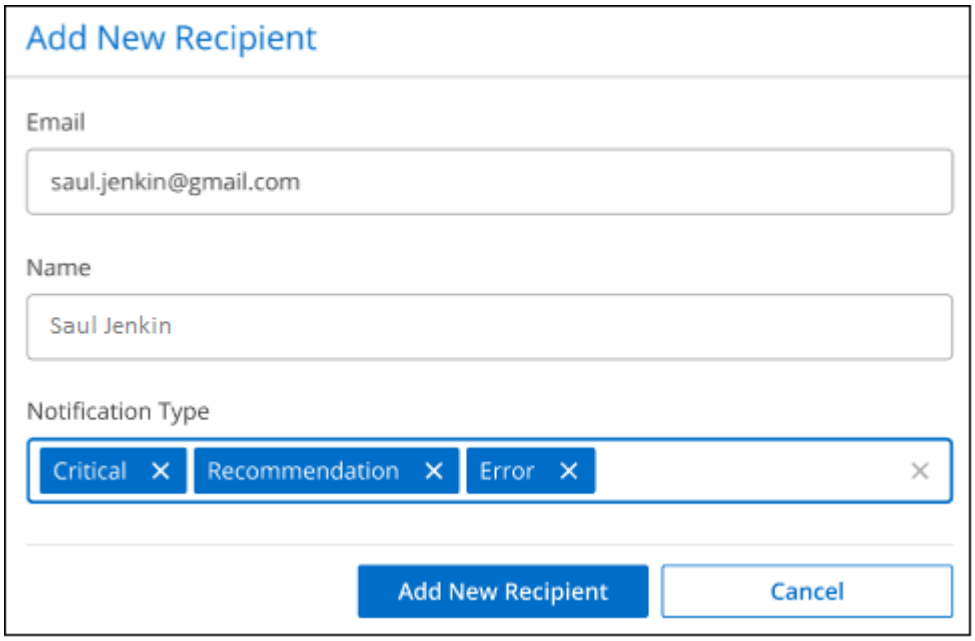


Fügen Sie weitere E-Mail-Empfänger hinzu

Die Benutzer, die auf der Registerkarte „Benutzer“ angezeigt werden, werden automatisch aus den Benutzern in Ihrer Organisation oder Ihrem Konto gefüllt. Sie können E-Mail-Adressen auf der Registerkarte „*Additional Recipients*“ für andere Personen oder Gruppen hinzufügen, die keinen Zugriff auf BlueXP haben, aber über bestimmte Arten von Warnungen und Benachrichtigungen benachrichtigt werden müssen.

Schritte

1. Wählen Sie auf der Seite Einstellungen für Warnmeldungen und Benachrichtigungen die Option **Neue Empfänger hinzufügen** aus.



2. Geben Sie den Namen und die E-Mail-Adresse ein, und wählen Sie die Benachrichtigungstypen aus, die der Empfänger erhalten soll, und wählen Sie **Neuen Empfänger hinzufügen**.