Administrar BlueXP

BlueXP setup and administration

NetApp
August 21, 2025

This PDF was generated from https://docs.netapp.com/es-es/bluexp-setup-admin/concept-identity-and-access-management.html on August 21, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Administrar BlueXP . . . 1
- Gestión de identidades y accesos . . . 1
  - Obtenga más información sobre la gestión de identidades y accesos de BlueXP . . . 1
  - Comience a utilizar la gestión de acceso e identidad de BlueXP . . . 8
  - Organiza tus recursos en BlueXP IAM con carpetas y proyectos . . . 9
  - Agregar miembros de BlueXP y cuentas de servicio . . . 14
  - Use roles para gestionar el acceso de usuarios a los recursos . . . 19
  - Gestione la jerarquía de recursos de su organización de BlueXP . . . 21
  - Asociar un conector BlueXP a otras carpetas y proyectos . . . 23
  - Cambiar entre Organizaciones, Proyectos y Conectores de BlueXP . . . 25
  - ID de organización y proyecto . . . 27
  - Supervise o audite la actividad de IAM desde la línea de tiempo de BlueXP . . . 28
  - Roles de acceso de BlueXP . . . 29
- federación de identidades . . . 42
  - Active el inicio de sesión único mediante la federación de identidades con BlueXP . . . 42
  - Verificación de dominio . . . 44
  - Configurar federaciones . . . 45
  - Administrar federaciones en BLueXP . . . 53
  - Importa tu federación a BlueXP . . . 55
- Conectores . . . 56
  - Mantener la VM Connector y el sistema operativo . . . 56
  - Instale un certificado firmado por CA para acceder a la consola basada en web . . . 58
  - Configure un conector para que utilice un servidor proxy . . . 61
  - Requiere el uso de IMDSv2 en instancias de Amazon EC2 . . . 68
  - Gestionar actualizaciones de conectores . . . 70
  - Trabaje con varios conectores . . . 72
  - Localice y solucione los problemas del conector . . . 74
  - Desinstale y retire el conector . . . 76
  - Configuración predeterminada del conector . . . 78
  - Aplicar permisos de ONTAP para la vista avanzada de ONTAP (ONTAP System Manager) . . . 80
- Credenciales y suscripciones . . . 81
  - AWS . . . 81
  - Azure . . . 95
  - Google Cloud . . . 109
  - Permite gestionar las credenciales de NSS asociadas con BlueXP . . . 115
  - Administre las credenciales asociadas con su inicio de sesión de BlueXP . . . 120
- Supervise las operaciones de BlueXP . . . 122
  - Audite la actividad del usuario desde la línea de tiempo de BlueXP . . . 122
  - Supervise las actividades mediante el Centro de notificaciones . . . 123

Administrar BlueXP

Gestión de identidades y accesos

Obtenga más información sobre la gestión de identidades y accesos de BlueXP

La gestión de identidades y accesos (IAM) de BlueXP le permite organizar y controlar el acceso a sus recursos de NetApp. Puede organizar sus recursos de acuerdo con la jerarquía de su organización. Por ejemplo, puede organizar recursos por ubicación geográfica, sitio o unidad de negocio. A continuación, puede asignar roles de IAM a miembros de partes específicas de la jerarquía, lo que impide el acceso a recursos en otras partes de la jerarquía.

- "Obtenga más información sobre los modos de implementación de BlueXP"

Cómo funciona BlueXP IAM

BlueXP IAM permite otorgar acceso a recursos asignando roles de acceso a usuarios a partes específicas de la jerarquía. Por ejemplo, a un miembro se le puede asignar el rol de administrador de carpeta o de proyecto para un proyecto con cinco recursos.

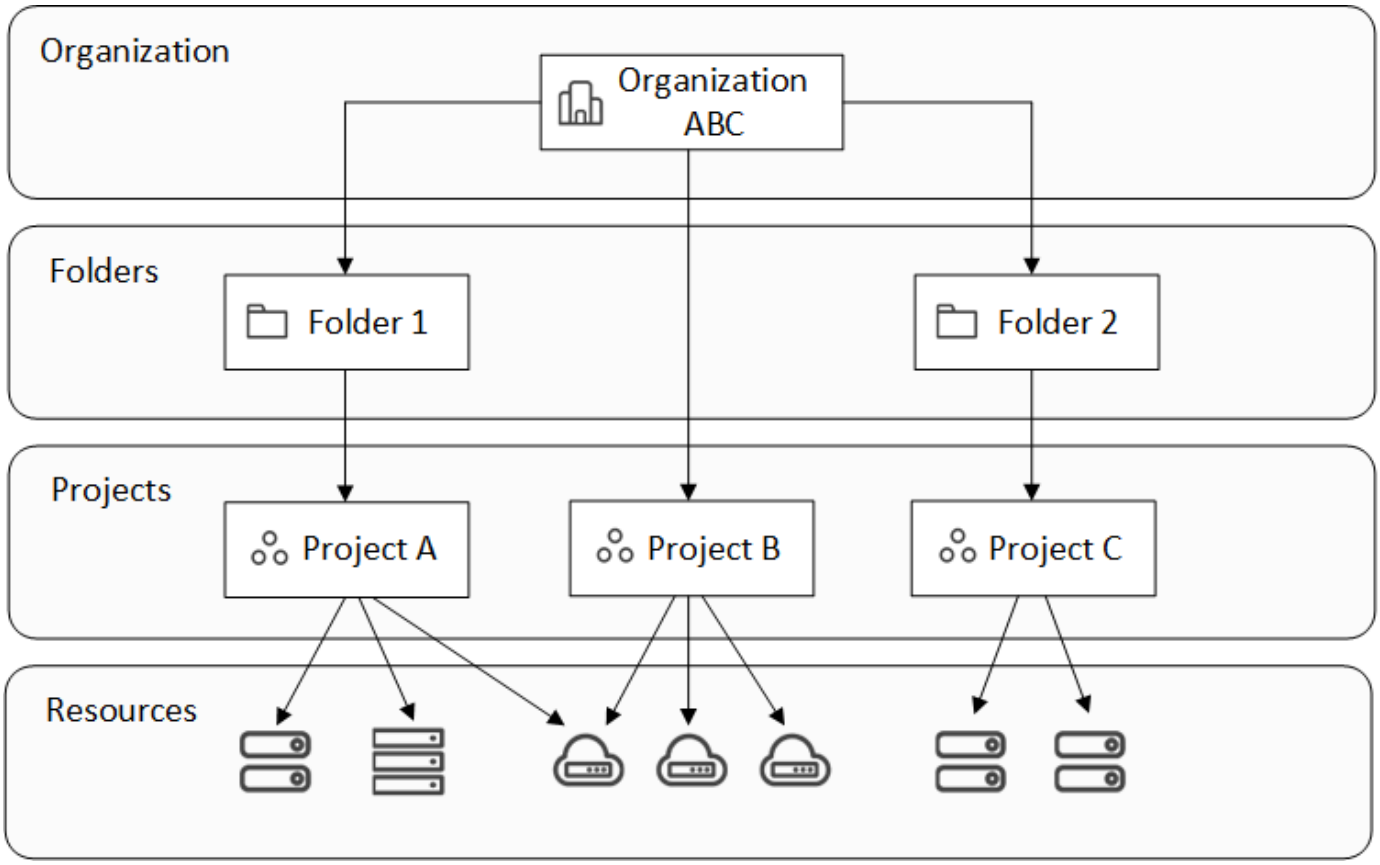
Al utilizar BlueXP IAM, gestionará los siguientes componentes:

- La organización
- Carpetas
- Proyectos
- Recursos
- Miembros
- Roles y permisos
- Conectores

Los recursos de BlueXP se organizan jerárquicamente:

- La organización es la parte superior de la jerarquía.
- Las carpetas son hijos de la organización o de otra carpeta.
- Los proyectos son hijos de la organización o de una carpeta.
- Los recursos están asociados a una o más carpetas o proyectos.

La siguiente imagen ilustra esta jerarquía en un nivel básico.



Organización

Una *ORGANIZATION* es el nivel superior del sistema IAM de BlueXP y, por lo general, representa a su empresa. La organización consta de carpetas, proyectos, miembros, roles y recursos. Los conectores están asociados a proyectos específicos de la organización.

Carpetas

A *FOLDER* le permite agrupar proyectos relacionados y separarlos de otros proyectos de la organización. Por ejemplo, una carpeta puede representar una ubicación geográfica (UE o EE.UU. Este), un sitio (Londres o Toronto) o una unidad de negocio (ingeniería o marketing).

Los archivos antiguos pueden contener proyectos, otras carpetas o ambos. La creación de carpetas es opcional.

Proyectos

Un *project* representa un espacio de trabajo en BlueXP al que los miembros de la organización acceden desde el lienzo de BlueXP para gestionar los recursos. Por ejemplo, un proyecto puede incluir un sistema Cloud Volumes ONTAP, un clúster de ONTAP en las instalaciones o un sistema de archivos FSx para ONTAP.

Una organización puede tener uno o varios proyectos. Un proyecto puede residir directamente debajo de la organización o dentro de una carpeta.

Recursos

Un *RESOURCE* es un entorno de trabajo que ha creado o detectado en BlueXP .

Al crear o detectar un recurso, el recurso se asocia al proyecto seleccionado actualmente. Ese puede ser el

único proyecto al que desea asociar este recurso. Pero puede optar por asociar el recurso con proyectos adicionales en su organización.

Por ejemplo, puede asociar un sistema Cloud Volumes ONTAP a un proyecto adicional o a todos los proyectos de la organización. La forma en que se asocia un recurso depende de las necesidades de su organización.

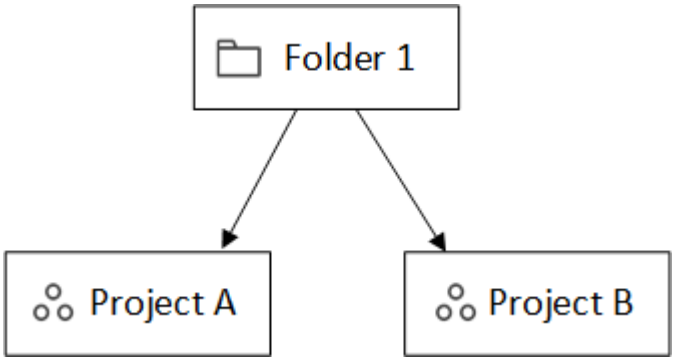
> También puede asociar un conector a otra carpeta o proyecto de su organización. Obtenga más información sobre el uso de conectores con BlueXP IAM.

Cuándo asociar un recurso a una carpeta

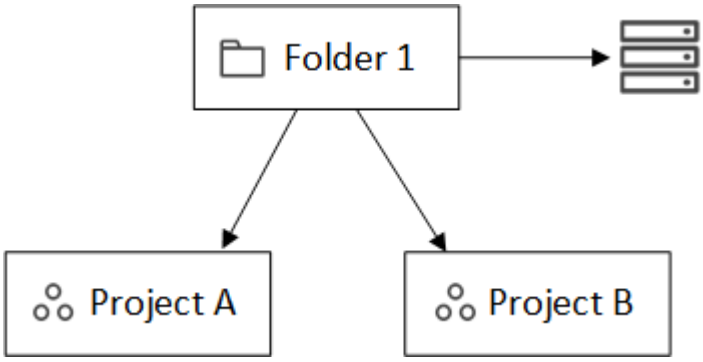
También tiene la opción de asociar un recurso a una carpeta, pero esto es opcional y satisface las necesidades de un caso de uso específico.

Un *administrador de la organización* puede asociar un recurso con una carpeta para permitir que un *administrador de carpeta o proyecto* vincule ese recurso con los proyectos apropiados en la carpeta.

Por ejemplo, supongamos que tiene una carpeta que contiene dos proyectos:

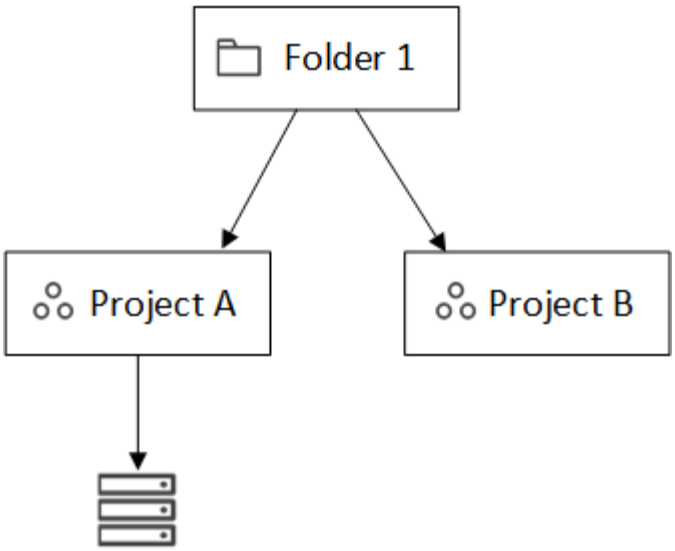


Organization admin puede asociar un recurso a la carpeta:



Asociar un recurso a una carpeta no lo hace accesible a todos los proyectos; solo el administrador de la carpeta o del proyecto puede verlo. El administrador de la carpeta o del proyecto decide qué proyectos pueden acceder a él y lo asocia con los proyectos correspondientes.

En este ejemplo, el administrador asocia el recurso con el Proyecto A:



Los miembros que tienen permisos para el proyecto A ahora pueden acceder al recurso.

Miembros

Los miembros de su organización son cuentas de usuario o cuentas de servicio. Una cuenta de servicio suele ser utilizada por una aplicación para completar tareas especificadas sin intervención humana.

Cada organización incluye al menos un usuario con el rol *Administrador de la organización* (BlueXP asigna automáticamente este rol al usuario que crea la organización). Puede agregar otros miembros a la organización y asignar diferentes permisos en diferentes niveles de la jerarquía de recursos.

Roles y permisos

En BlueXP IAM, no otorga permisos directamente a los miembros de la organización. En su lugar, debe otorgar a cada miembro un rol. Un rol contiene un juego de permisos que permite a un miembro realizar acciones específicas en un nivel específico de la jerarquía de recursos.

Otorgar permisos en un nivel de jerarquía específico restringe el acceso a los recursos que un miembro necesita y los servicios que puede usar con esos recursos.

Donde puede asignar roles en la jerarquía

Cuando asocia un miembro a un rol, debe seleccionar toda la organización, una carpeta específica o un proyecto específico. El rol que seleccione otorga permisos de miembro a los recursos de la parte seleccionada de la jerarquía.

Herencia de roles

Al asignar un rol, el rol se hereda por la jerarquía de la organización:

Organización
: Otorgarle a un miembro un rol de acceso a nivel de organización le otorga permisos para todas las carpetas, proyectos y recursos.

Carpetas
: Cuando se otorga un rol de acceso a nivel de carpeta, todas las carpetas, proyectos y recursos de la carpeta heredan ese rol.

Por ejemplo, si asigna un rol en el nivel de carpeta y esa carpeta tiene tres proyectos, el miembro tendrá permisos para esos tres proyectos y cualquier recurso asociado.

Proyectos

Cuando se otorga un rol de acceso a nivel de proyecto, todos los recursos asociados con ese proyecto heredan ese rol.

Varios roles

Puede asignar a cada miembro de la organización un rol en diferentes niveles de la jerarquía de la organización. Puede ser el mismo rol o un rol diferente. Por ejemplo, puede asignar un rol de miembro A para el proyecto 1 y el proyecto 2. También puede asignar un rol de miembro A para el proyecto 1 y el rol B para el proyecto 2.

Acceda a roles

BlueXP admite varios roles predefinidos que puede asignar a los miembros de la organización.

"Obtenga más información sobre los roles de acceso".

Conectores

Cuando un *Organization admin* crea un conector, BlueXP asocia automáticamente ese conector con la organización y el proyecto seleccionado actualmente. *Organization admin* tiene acceso automáticamente a ese conector desde cualquier lugar de la organización. Pero si tiene otros miembros en la organización con roles diferentes, esos miembros solo podrán acceder a ese conector desde el proyecto en el que se creó, a menos que asocie ese conector con otros proyectos.

Pon un conector a disposición de otro proyecto en estos casos:

- Desea permitir que los miembros de la organización utilicen un conector existente para crear o detectar entornos de trabajo adicionales en otro proyecto
- Ha asociado un recurso existente a otro proyecto y ese recurso lo gestiona un conector

  Si se descubre un recurso que asocia con un proyecto adicional mediante un conector BlueXP, también deberá asociar el conector con el proyecto con el que ahora está asociado el recurso. De lo contrario, el conector y su recurso asociado no serán accesibles desde el lienzo de BlueXP para los miembros que no tengan el rol de *Administrador de la organización*.

Puede crear una asociación desde la página **Conectores** en BlueXP IAM:

- Asociar un conector a un proyecto

  Al asociar un conector a un proyecto, se puede acceder a dicho conector desde el lienzo de BlueXP al visualizar el proyecto.

- Asociar un conector a una carpeta

  La asociación de un conector a una carpeta no hace que ese conector sea accesible automáticamente desde todos los proyectos de la carpeta. Los miembros de la organización no pueden acceder a un conector desde un proyecto hasta que no asocie el conector a ese proyecto específico.

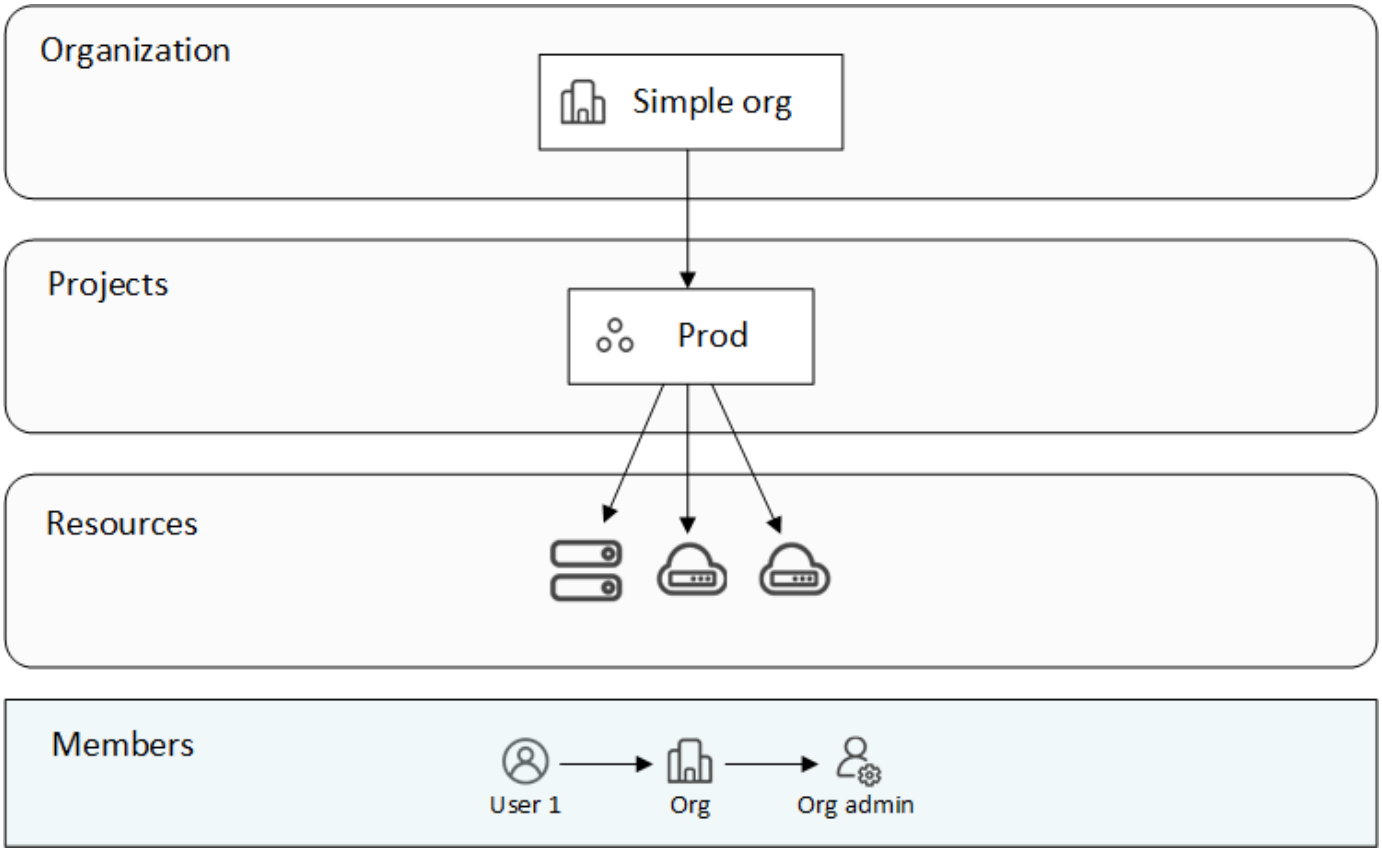
  Un *Organization admin* puede asociar un Connector a una carpeta para que *Folder o project admin* pueda tomar la decisión de asociar ese Connector a los proyectos apropiados que residen en la carpeta.

Ejemplos de IAM

Estos ejemplos demuestran cómo podría configurar su organización.

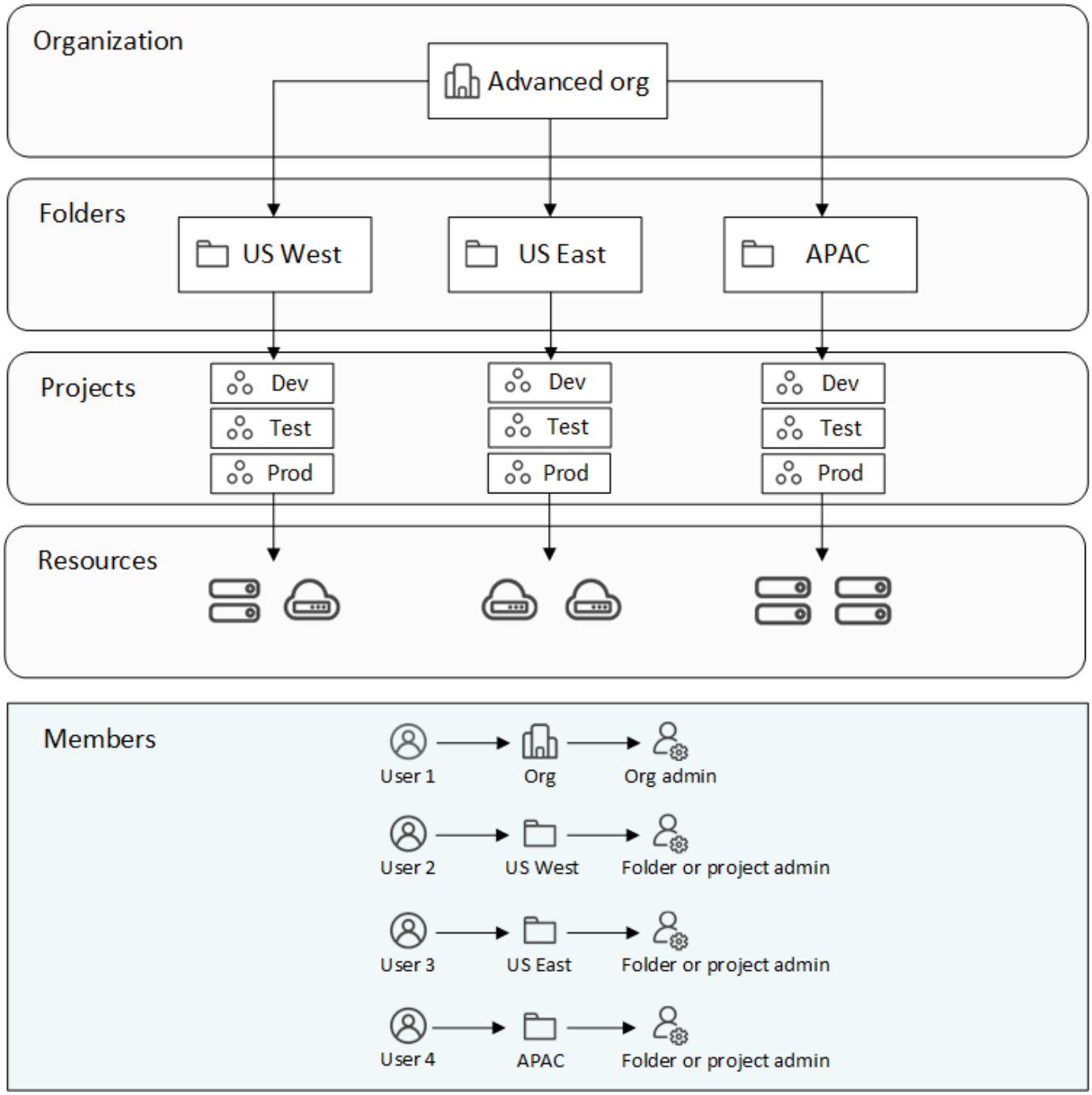
Organización sencilla

El siguiente diagrama muestra un ejemplo sencillo de una organización que utiliza el proyecto predeterminado y ninguna carpeta. Un solo miembro gestiona toda la organización.



Organización avanzada

El siguiente diagrama muestra una organización que utiliza carpetas para organizar los proyectos para cada ubicación geográfica de la empresa. Cada proyecto tiene su propio conjunto de recursos asociados. Los miembros incluyen un administrador de la organización y un administrador para cada carpeta de la organización.



Qué puede hacer con IAM de BlueXP

En los siguientes ejemplos se describe cómo utilizar IAM para gestionar su organización de BlueXP :

- Otorgue roles específicos a miembros específicos para que solo puedan completar las tareas necesarias.
- Modificar los permisos de los miembros porque han movido departamentos o porque tienen responsabilidades adicionales.
- Eliminar un usuario que abandonó la empresa.
- Agregue carpetas o proyectos a la jerarquía porque una nueva unidad de negocio ha agregado almacenamiento NetApp.
- Asocie un recurso a otro proyecto porque ese recurso tiene capacidad que otro equipo puede utilizar.

- Ver los recursos a los que puede acceder un miembro.
- Ver los miembros y recursos asociados a un proyecto específico.

A continuación, ¿dónde ir

- "Comience a usar BlueXP IAM"
- "Organiza tus recursos en BlueXP con carpetas y proyectos"
- "Gestionar miembros de BlueXP y sus permisos"
- "Gestione la jerarquía de recursos de su organización de BlueXP "
- "Asociar conectores a carpetas y proyectos"
- "Cambiar entre proyectos y organizaciones de BlueXP "
- "Cambie el nombre de su organización de BlueXP "
- "Supervisar o auditar la actividad de IAM"
- "Roles de acceso de BlueXP"
- "Obtenga más información sobre la API para IAM de BlueXP "

Comience a utilizar la gestión de acceso e identidad de BlueXP

Cuando te registras en BlueXP , se te pedirá que crees una nueva organización. La organización incluye un miembro (un administrador de organización) y un proyecto por defecto. Para configurar la administración de identidades y accesos (IAM) de BlueXP para satisfacer las necesidades de su empresa, deberá personalizar la jerarquía de su organización, agregar miembros adicionales, agregar o detectar recursos y asociar dichos recursos en su jerarquía.

Debe tener permisos de administrador de la organización* para administrar toda la organización desde BlueXP IAM. Si tiene permisos de administrador de carpeta o proyecto*, solo puede administrar las carpetas y proyectos para los que tenga permisos.

Siga estos pasos para configurar una nueva organización de BlueXP . El orden en el que realice estos pasos puede ser diferente, dependiendo de las necesidades de su organización.

1 **Edite el proyecto por defecto o agréguelo a la jerarquía de la organización**

Utilice el proyecto predeterminado o cree proyectos y carpetas adicionales que coincidan con la jerarquía de su negocio.

"Aprenda a organizar sus recursos con carpetas y proyectos".

2 **Asocie miembros a su organización**

Si varias personas de su empresa necesitan acceder a BlueXP, asocie sus cuentas de usuario con su organización y asigne los permisos necesarios. También tiene la opción de agregar cuentas de servicio a su organización.

"Aprenda a administrar miembros y sus permisos".

3 Añadir o detectar recursos

Agregue o descubra recursos en BlueXP como entornos de trabajo. Los miembros de la organización gestionan un entorno de trabajo, que representa un sistema de almacenamiento, desde un proyecto.

Aprenda a crear o descubrir recursos:

- "Amazon FSX para ONTAP de NetApp"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Sistemas E-Series"
- "Clústeres de ONTAP en las instalaciones"
- "StorageGRID"

4 Asociar recursos a proyectos adicionales

Al crear o detectar un recurso en BlueXP , dicho recurso se asocia automáticamente al proyecto seleccionado al crear o detectar el entorno de trabajo. Si desea que ese recurso esté disponible para otro proyecto de su organización, deberá crear una asociación entre ellos. Si un conector administra el recurso, asocie el conector con el proyecto respectivo.

- "Aprenda a gestionar la jerarquía de recursos de su organización".
- "Aprenda a asociar un conector a una carpeta o proyecto".

Información relacionada

- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "
- "Obtenga más información sobre la API para IAM de BlueXP "

Organiza tus recursos en BlueXP IAM con carpetas y proyectos

La gestión de identidades y accesos (IAM) de BlueXP le permite organizar sus recursos de NetApp mediante proyectos y carpetas. Un *project* representa un espacio de trabajo en BlueXP al que acceden los miembros de la organización para gestionar *resources* (por ejemplo, un sistema Cloud Volumes ONTAP). A *folder* agrupa proyectos relacionados juntos. Después de organizar los recursos en carpetas y proyectos, puede otorgar acceso granular a los recursos proporcionando a los miembros de la organización permisos para carpetas y proyectos específicos.

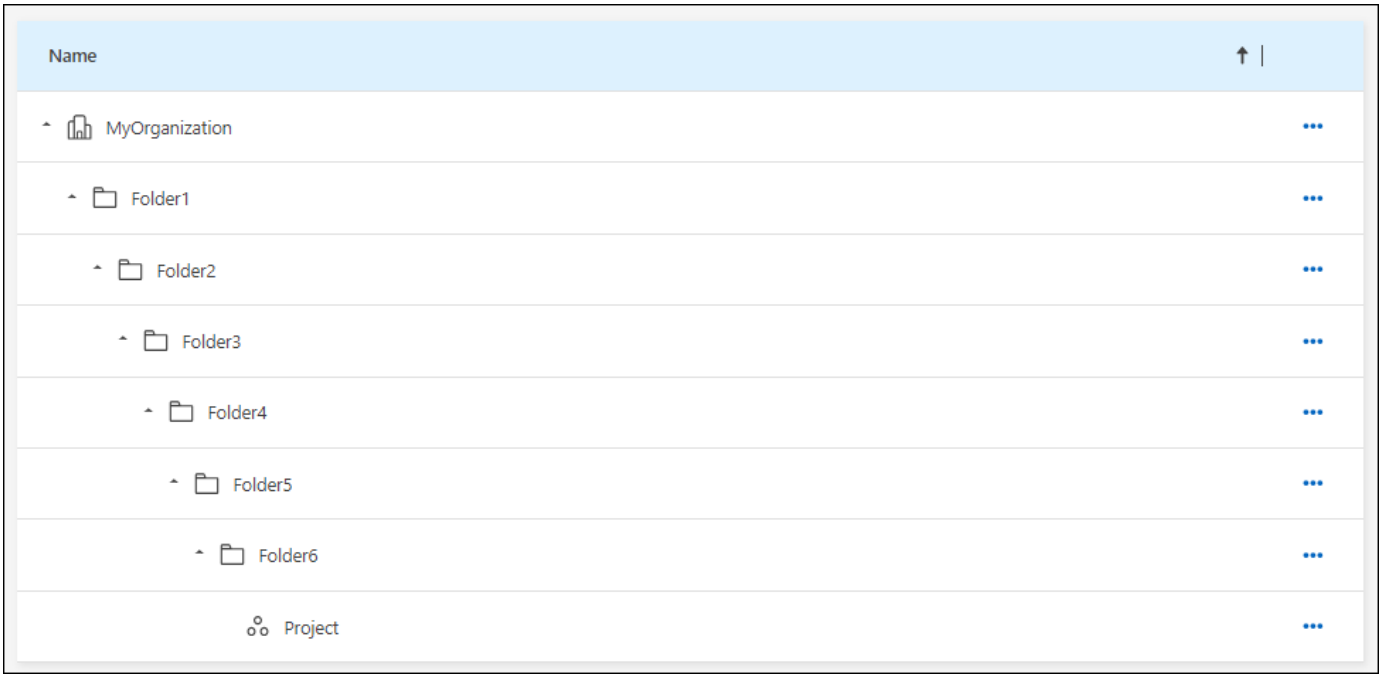
Agregue una carpeta o un proyecto

Cuando crea su organización BlueXP , incluye un solo proyecto. Puede crear proyectos adicionales para gestionar los recursos de su organización. Opcionalmente, puede crear carpetas para agrupar proyectos relacionados.

Acerca de esta tarea

La jerarquía de recursos de su organización puede tener hasta 7 niveles, con carpetas anidadas en el séptimo nivel.

La siguiente imagen ilustra la profundidad máxima de la jerarquía de recursos de la organización:



Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione > **Gestión de identidades y acceso**.
2. En la página **Organización**, selecciona **Añadir carpeta o proyecto**.
3. Seleccione **Carpeta** o **Proyecto**.
4. Proporcione detalles sobre la carpeta o el proyecto:
   - **Nombre y ubicación**: Introduce un nombre y elige una ubicación en la jerarquía para la carpeta o proyecto. Una carpeta o proyecto puede residir directamente debajo de la organización o dentro de una carpeta.
   - **Recursos**: Seleccione los recursos que desea asociar a esta carpeta o proyecto.

     Puede seleccionar recursos asociados con la carpeta o proyecto principal: todos los recursos para una organización principal o recursos específicos de la carpeta para una carpeta principal.

     "Descubra cuándo puede asociar un recurso a una carpeta".
   - **Acceso**: Vea los miembros que tendrán acceso a la carpeta o proyecto en función de los permisos existentes ya definidos en su jerarquía de recursos.

     Si es necesario, seleccione **Agregar un miembro** para especificar miembros adicionales de la organización que deben tener acceso a la carpeta o el proyecto y, a continuación, seleccione un rol. Un rol define los permisos que tienen los miembros para la carpeta o el proyecto.

   "Obtenga información sobre los roles predefinidos de IAM".
5. Seleccione **Agregar**.

Obtenga el ID de un proyecto

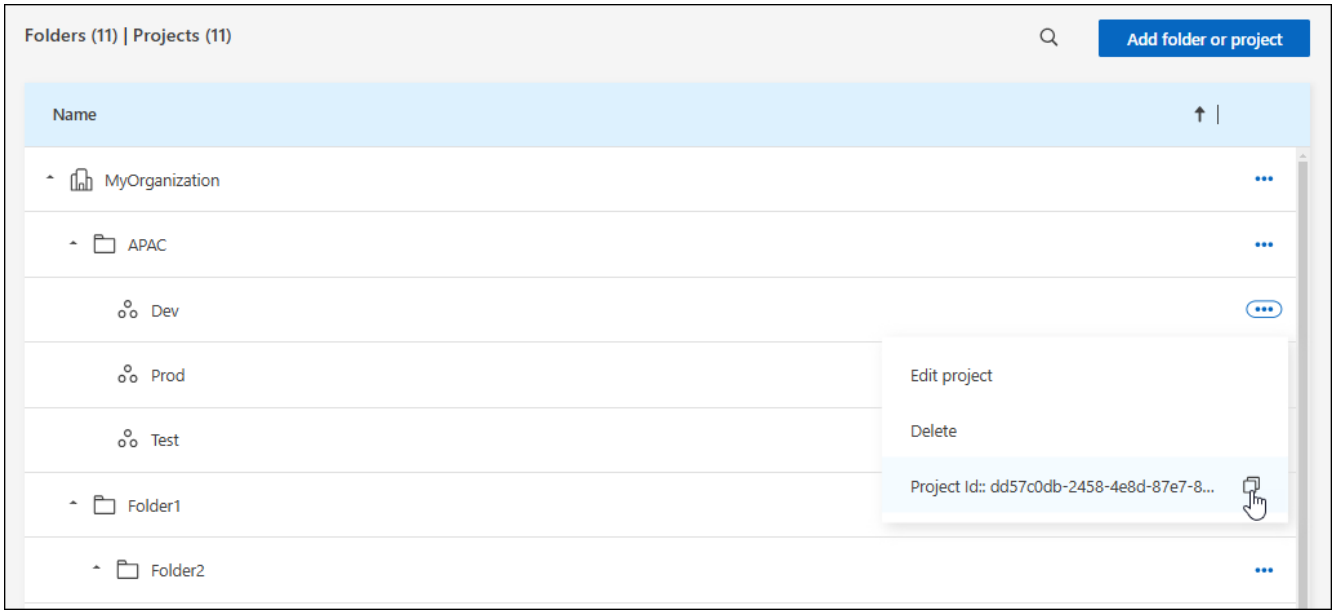
Si usas la API de BlueXP , es posible que necesites obtener el ID de un proyecto. Por ejemplo, al crear un entorno de trabajo Cloud Volumes ONTAP.

Pasos

1. Desde la página **Organización**, navega a un proyecto en la tabla y selecciona •••

   El sistema muestra el ID del proyecto.

2. Para copiar el ID, seleccione el botón Copiar.



Cambiar el nombre de una carpeta o proyecto

Si es necesario, puede cambiar el nombre de sus carpetas y proyectos.

Pasos

1. Desde la página **Organización**, navega a un proyecto o carpeta de la tabla, selecciona ••• y luego selecciona **Editar carpeta** o **Editar proyecto**.
2. En la página **Editar**, introduce un nuevo nombre y selecciona **Aplicar**.

Eliminar una carpeta o un proyecto

Puede eliminar las carpetas y los proyectos que ya no necesite.

Antes de empezar

- La carpeta o el proyecto no deben tener ningún recurso asociado. Aprende a desasociar recursos.
- Una carpeta no debe contener subcarpetas ni proyectos. Primero debe eliminar esas carpetas y proyectos.

Pasos

1. Desde la página **Organización**, navega a un proyecto o carpeta de la tabla, selecciona ••• y luego selecciona **Eliminar**.

2. Confirme que desea eliminar la carpeta o el proyecto.

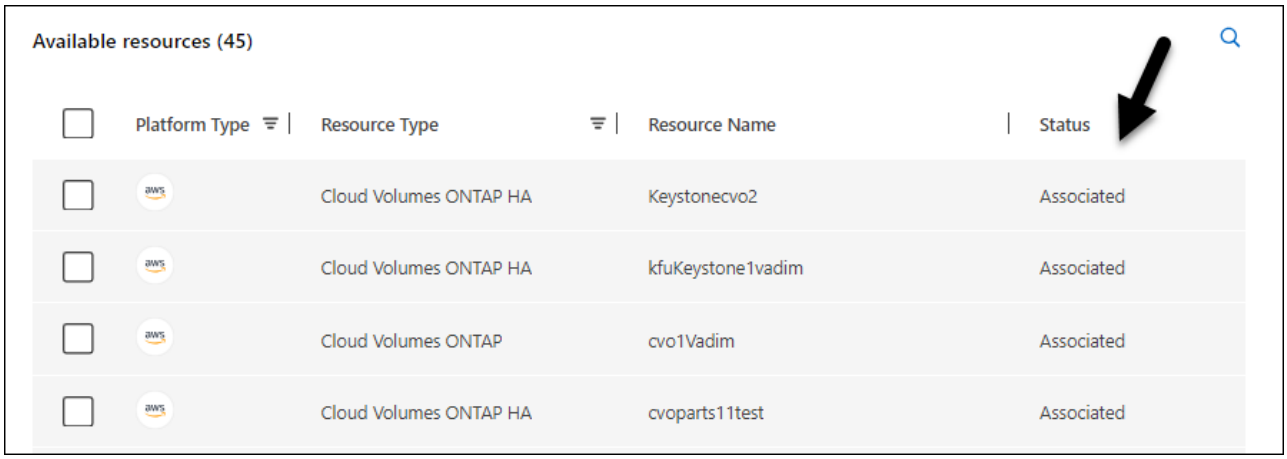
Ver los recursos asociados a una carpeta o proyecto

Para verificar que los recursos están organizados correctamente y son accesibles para los miembros correctos de su organización, puede ver qué recursos y miembros están asociados a una carpeta o proyecto.

Pasos

1. Desde la página **Organización**, navega a un proyecto o carpeta de la tabla, selecciona ••• y luego selecciona **Editar carpeta** o **Editar proyecto**.

2. En la página **Editar**, puede ver detalles sobre la carpeta o proyecto seleccionado ampliando las secciones **Recursos** o **Acceso**.
   - Selecciona **Recursos** para ver los recursos asociados. En la tabla, la columna **Status** identifica los recursos asociados a la carpeta o proyecto.



Modificar los recursos asociados a una carpeta o proyecto

Los miembros con permisos para una carpeta o proyecto pueden acceder a sus recursos asociados.

Antes de empezar

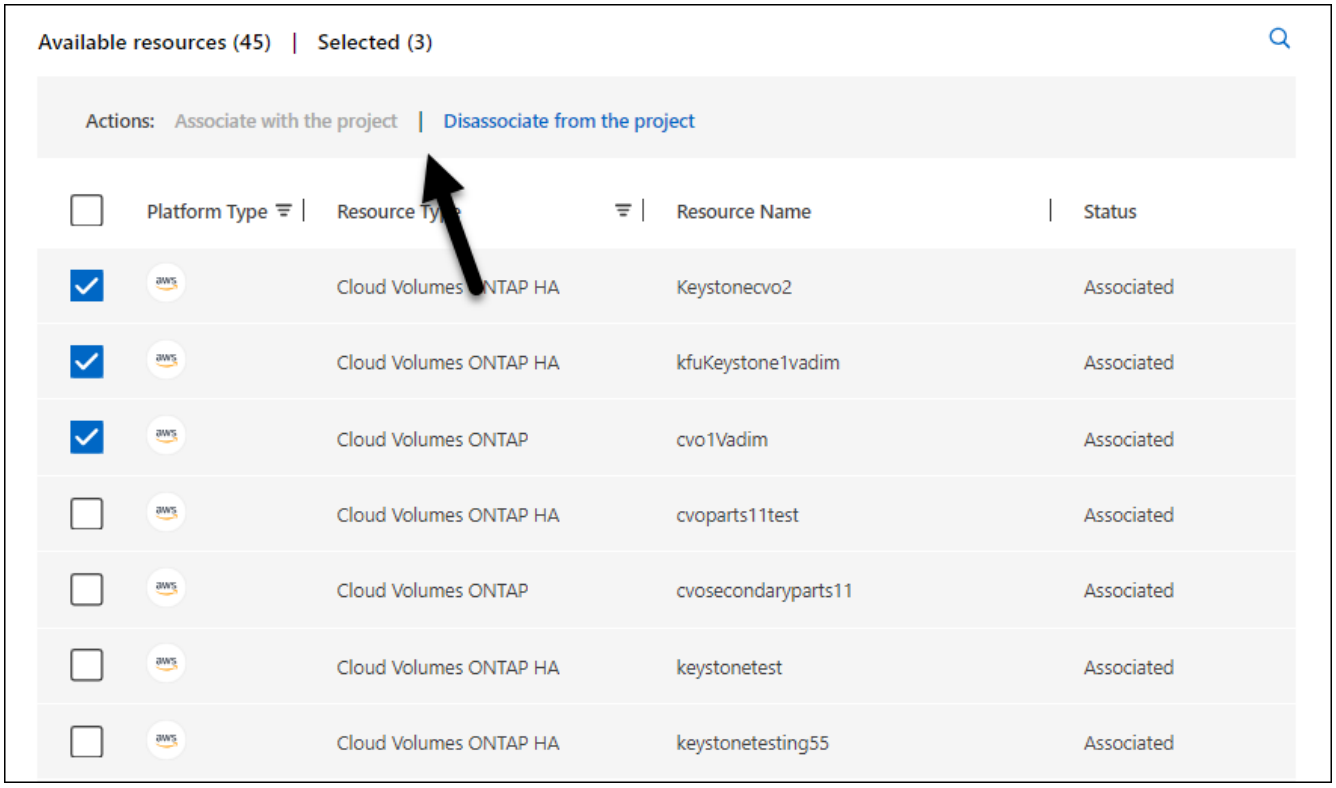
"Descubra cuándo puede asociar un recurso a una carpeta".

Pasos

1. Desde la página **Organización**, navega a un proyecto o carpeta de la tabla, selecciona ••• y luego selecciona **Editar carpeta** o **Editar proyecto**.
2. En la página **Editar**, selecciona **Recursos**.

   En la tabla, la columna **Status** identifica los recursos asociados a la carpeta o proyecto.

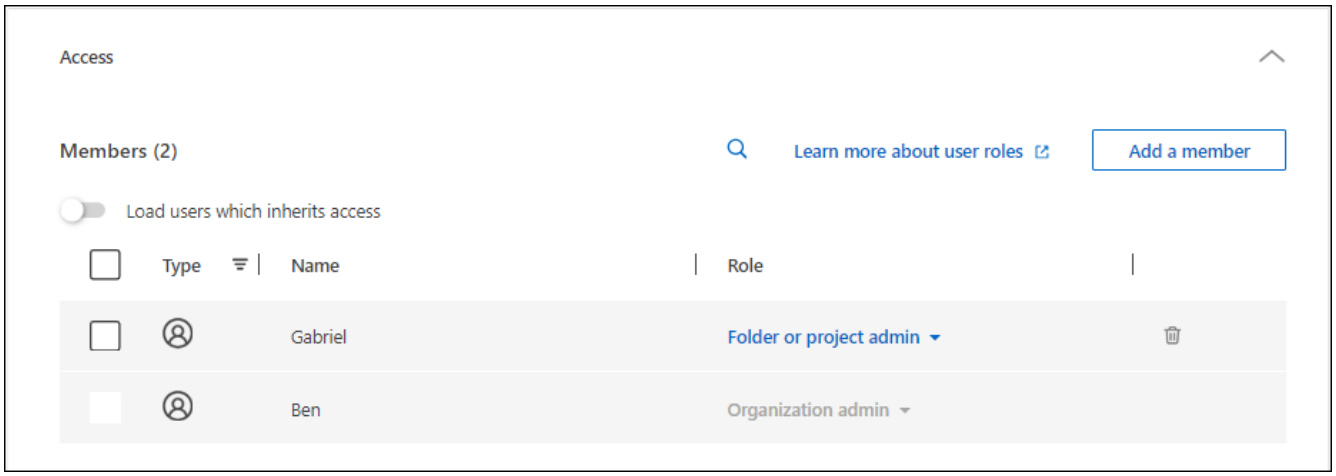
3. Seleccione los recursos que desea asociar o desasociar.
4. Dependiendo de los recursos que haya seleccionado, seleccione **Asociar con el proyecto** o **Desasociar del proyecto**.



5. Seleccione **Aplicar**

Ver miembros asociados a una carpeta o proyecto

- Seleccione **Acceso** para ver los miembros que tienen acceso a la carpeta o proyecto.



Modificar el acceso de miembro a una carpeta o proyecto

Modificar el acceso de los miembros para garantizar que los miembros correctos puedan acceder a los recursos asociados.

El acceso de miembros proporcionado en un nivel de jerarquía superior no se puede cambiar en niveles inferiores. Debe cambiar a esa parte de la jerarquía y actualizar los permisos del miembro allí. Como alternativa, puede "Gestione los permisos desde la página Miembros".

"Obtenga más información sobre la herencia de roles".

Pasos

1. Desde la página **Organización**, navega a un proyecto o carpeta de la tabla, selecciona ••• y luego selecciona **Editar carpeta** o **Editar proyecto**.
2. En la página **Editar**, selecciona **Acceso** para ver la lista de miembros que tienen acceso a la carpeta o proyecto seleccionado.
3. Modificar acceso de miembros:
   - **Agregar un miembro**: Seleccione el miembro que desea agregar a la carpeta o proyecto y asígnele un rol.
   - **Cambiar el rol de un miembro**: Para cualquier miembro que tenga un rol distinto del Administrador de la Organización, seleccione su rol existente y luego elija un nuevo rol.
   - * Eliminar acceso de miembro*: Para los miembros que tienen un rol definido en la carpeta o proyecto para el que está viendo, puede eliminar su acceso.
4. Seleccione **aplicar**.

Información relacionada

- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "
- "Comience a usar BlueXP IAM"
- "Obtenga más información sobre la API para IAM de BlueXP "

Agregar miembros de BlueXP y cuentas de servicio

La gestión de identidades y accesos (IAM) de BlueXP permite agregar miembros a la organización y asignarles uno o más roles en la jerarquía de recursos. Un *role* contiene un juego de permisos que permite a un miembro realizar acciones específicas en un nivel específico de la jerarquía de recursos. Puede asociar nuevas cuentas de usuario y cuentas de servicio, administrar roles de miembros y más.

> Asegúrese de que dos miembros tengan el rol de administrador de la organización para evitar perder el acceso a su organización BlueXP.

Para administrar usuarios y sus permisos, debe tener asignado uno de los siguientes roles:

- Administrador de la organización

  Los usuarios con este rol pueden gestionar todos los miembros

- Administrador de carpetas o proyectos

  Los usuarios con este rol pueden administrar únicamente a los miembros de una carpeta o proyecto designado

```
_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].
```

Agregue miembros a su organización

Puede agregar dos tipos de miembros a su organización: una cuenta de usuario y una cuenta de servicio. Las aplicaciones utilizan una cuenta de servicio para realizar tareas a través de la API de BlueXP sin intervención humana. Generalmente, una persona utiliza una cuenta de usuario para iniciar sesión en BlueXP y administrar recursos.

Los usuarios deben registrarse en BlueXP antes de ser agregados a una organización o asignarles un rol. Sin embargo, puedes crear cuentas de servicio directamente desde BlueXP.

Para administrar usuarios y sus permisos, debe tener la función **Administrador de organización** o la función **Carpeta o administrador de proyecto**. Recuerde que los usuarios con la función **Folder o project admin** solo pueden administrar miembros para la carpeta o proyectos de los que tienen permisos de administrador.

Cuenta de usuario

Pasos

1. Dirigir al usuario a visitar "Sitio web de NetApp BlueXP" Para registrarse.

   Una vez que los usuarios se registran, completan la página **Registrarse**, revisan su correo electrónico e inician sesión. Si BlueXP solicita a los usuarios que creen una organización, la cierran y le notifican la creación de su cuenta. Luego puede agregar el usuario a su organización BlueXP existente.

   "Descubra cómo registrarse en BlueXP ".

2. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
3. Selecciona **Miembros**.
4. Selecciona **Añadir un miembro**.
5. Para agregar el miembro, complete los pasos del cuadro de diálogo:
   - **Tipo de entidad**: Mantener **Usuario** seleccionado.
   - **Correo electrónico del usuario**: Introduzca la dirección de correo electrónico del usuario que está asociada con el inicio de sesión de BlueXP que creó.
   - **Seleccione una organización, carpeta o proyecto**: Elija el nivel de su jerarquía de recursos para el que el miembro debe tener permisos.

     Tenga en cuenta lo siguiente:

     - Solo puede seleccionar entre las carpetas y proyectos para los que tiene permisos de administrador.
     - Al seleccionar una organización o carpeta, se otorgan al miembro permisos sobre todo su contenido.
   - **Seleccione una categoría** y luego seleccione un **rol** que le proporcione al miembro permisos para los recursos asociados a la organización, carpeta o proyecto que seleccionó.
     - Si seleccionó una carpeta o un proyecto, puede elegir entre cualquier función que no sea **Administrador de la organización**.

       "Obtenga más información sobre los roles de acceso".
   - **Agregar rol**: Si desea proporcionar acceso a carpetas o proyectos adicionales dentro de su organización o otorgar al usuario permisos adicionales en el área seleccionada, seleccione **Agregar rol**, especifique otra carpeta o proyecto o una categoría de rol diferente y luego elija un rol.
6. Seleccione **Agregar**.

   NetApp BlueXP envía al usuario un correo electrónico con información sobre cómo acceder a BlueXP.

Cuenta de servicio

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y**

acceso.

2. Selecciona **Miembros**.
3. Selecciona **Añadir un miembro**.
4. Para agregar el miembro, complete los pasos del cuadro de diálogo:
   - **Tipo de entidad**: Selecciona **Cuenta de servicio**.
   - **Nombre de la cuenta de servicio**: Introduzca un nombre para la cuenta de servicio.
   - **Seleccione una organización, carpeta o proyecto**: Elija el nivel de su jerarquía de recursos para el que el miembro debe tener permisos.

     Tenga en cuenta lo siguiente:

     - Solo puede seleccionar entre las carpetas y proyectos para los que tiene permisos de administrador.
     - Al seleccionar una organización o carpeta, se otorgan al miembro permisos sobre todo su contenido.
   - **Seleccione una categoría** y luego seleccione un **Rol** que proporcione al miembro permisos para los recursos asociados con la organización, carpeta o proyecto que usted seleccionó.
     - Si seleccionó una carpeta o un proyecto, puede elegir entre cualquier función que no sea **Administrador de la organización**.

       "Obtenga información sobre los roles predefinidos de IAM".
   - **Agregar rol**: Si desea proporcionar acceso a carpetas o proyectos adicionales dentro de su organización o otorgar al usuario permisos adicionales en el área seleccionada, seleccione **Agregar rol**, especifique otra carpeta o proyecto o una categoría de rol diferente y luego elija un rol.
5. Descargue o copie el ID de cliente y el secreto de cliente.

   BlueXP muestra el secreto del cliente solo una vez. Cópielo o descárguelo y guárdelo de forma segura. Tenga en cuenta que puede volver a crear el ID y el secreto del cliente más adelante según sea necesario.
6. Seleccione **Cerrar**.

Ver miembros de la organización

Puede ver una lista de todos los miembros de su organización de BlueXP . Para comprender qué recursos y permisos están disponibles para un miembro, puede ver los roles asignados al miembro en diferentes niveles de la jerarquía de recursos de la organización. "Aprenda a usar los roles para controlar el acceso a los recursos de BlueXP ."

Puede ver las cuentas de usuario y las cuentas de servicio desde la página **Miembros**.

> También puede ver todos los miembros asociados a una carpeta o proyecto específico. "Leer más".

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione > **Gestión de identidades y**

acceso.

2. Selecciona **Miembros**.

   La tabla **Miembros** enumera los miembros de su organización.

3. Desde la página **Miembros**, navega a un miembro de la tabla, selecciona ••• y luego selecciona **Ver detalles**.

Eliminar un miembro de la organización

Es posible que necesites eliminar a un miembro de tu organización (por ejemplo, si abandona tu empresa).

Al eliminar un miembro se eliminan sus permisos, pero se conservan sus cuentas del sitio de soporte de BlueXP y NetApp .

Pasos

1. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• luego seleccione **Eliminar usuario**.
2. Confirme que desea eliminar el miembro de su organización.

Vuelva a crear las credenciales para una cuenta de servicio

Cree nuevas credenciales si las pierde o cuando sea necesario actualizar las credenciales de seguridad.

Acerca de esta tarea

Al volver a crear las credenciales, elimina las credenciales existentes para la cuenta de servicio y crea otras nuevas. No puedes utilizar las credenciales anteriores.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Selecciona **Miembros**.
3. En la tabla **Miembros**, navega a una cuenta de servicio, selecciona ••• y luego selecciona **recrear secretos**.
4. Selecciona **Volver a crear**.
5. Descargue o copie el ID de cliente y el secreto de cliente.

   BlueXP muestra el secreto del cliente solo una vez. Cópielo o descárguelo y guárdelo de forma segura.

Administrar la autenticación multifactor (MFA) de un usuario

Si un usuario pierde el acceso a su dispositivo MFA, puede eliminar o deshabilitar su configuración MFA.

Si elimina la configuración de MFA, el usuario deberá volver a configurarla al iniciar sesión en BlueXP. Si solo ha perdido el acceso a su dispositivo con MFA temporalmente, puede usar el código de recuperación que guardó al configurar la MFA para iniciar sesión en BlueXP.

Si no tienen su código de recuperación, deshabilite temporalmente MFA para permitir el inicio de sesión. Cuando deshabilita MFA para un usuario, esta se deshabilita solo durante ocho horas y luego se vuelve a habilitar automáticamente. Al usuario se le permite un inicio de sesión durante ese tiempo sin MFA. Después

de las ocho horas, el usuario deberá utilizar MFA para iniciar sesión en BlueXP.

> Debe tener una dirección de correo electrónico en el mismo dominio que el usuario afectado para administrar la autenticación multifactor de ese usuario.

Pasos

1. En la parte superior derecha de la consola, seleccione ⚙ > **Gestión de identidad y acceso**.
2. Selecciona **Miembros**.

   Los miembros de tu organización aparecen en la tabla **Miembros**.

3. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Administrar autenticación multifactor**.
4. Elija si desea eliminar o deshabilitar la configuración de MFA del usuario.

Información relacionada

- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "
- "Comience a usar BlueXP IAM"
- "Roles de IAM predefinidos de BlueXP "
- "Obtenga más información sobre la API para IAM de BlueXP "

Use roles para gestionar el acceso de usuarios a los recursos

Dentro de BlueXP, puedes asignar roles a los usuarios según lo que necesiten hacer y dónde.

Los usuarios con el rol de **Administrador de la organización** o **Administrador de carpeta o proyecto** tienen la responsabilidad de asignar roles a otros usuarios. Puede asignar roles de acceso por proyecto o carpeta. Por ejemplo, puede asignar a un usuario el rol de administrador de protección contra ransomware para un proyecto y el rol de administrador de SnapCenter para un proyecto diferente. Como alternativa, si un usuario necesita el rol de administrador de Clasificación para todos los proyectos dentro de una carpeta específica, puede otorgarle este rol a nivel de carpeta.

Utilice roles de acceso para asignar acceso a los recursos de almacenamiento según las tareas específicas que los usuarios deben realizar. Por ejemplo, si un usuario necesita interactuar con servicios de protección contra ransomware, debe tener un rol de acceso que incluya permisos de visualización o administración para el servicio de protección contra ransomware del proyecto para el que se le otorga dicho rol.

Asigne roles a los usuarios según su estrategia de IAM para mejorar la seguridad. Los roles de IAM garantizan que los usuarios tengan solo el acceso que necesitan.

> Recuerde que no puede otorgar acceso directo a los recursos. Asignar recursos a los proyectos primero. Considere la posibilidad de configurar la jerarquía de recursos antes de asignar el acceso de los usuarios. "Aprenda a organizar sus recursos en BlueXP IAM con carpetas y proyectos."

Ver roles asignados a un miembro

Cuando agrega un miembro a su organización, se le solicita que le asigne un rol. Puede verificar los roles que están asignados actualmente.

Si tiene el rol *Folder o project admin*, la página muestra todos los miembros de la organización. Sin embargo, solo puede ver y gestionar los permisos de miembros para las carpetas y proyectos para los que tiene permisos. "Obtenga más información sobre las acciones que puede completar una *Carpeta o un proyecto admin*".

1. Desde la página **Miembros**, navega a un miembro de la tabla, selecciona ••• y luego selecciona **Ver detalles**.
2. En la tabla, expanda la fila correspondiente para la organización, carpeta o proyecto en el que desee ver el rol asignado del miembro y seleccione **Ver** en la columna **Rol**.

Agregar un rol de acceso a un miembro

Normalmente, se asigna un rol al agregar un miembro a su organización, pero puede actualizarlo en cualquier momento eliminando o agregando roles.

Puede asignar a un usuario un rol de acceso para su organización, carpeta o proyecto.

Los miembros pueden tener varios roles dentro del mismo proyecto y en diferentes proyectos. Por ejemplo, las organizaciones más pequeñas pueden asignar todos los roles de acceso disponibles al mismo usuario, mientras que las organizaciones más grandes pueden asignar usuarios a tareas más especializadas. Como alternativa, también podría asignar a un usuario el rol de administrador de protección contra ransomware para una organización. En ese ejemplo, el usuario podría realizar tareas de protección frente al ransomware en todos los proyectos de su organización.

Su estrategia de roles de acceso debe estar alineada con la forma en que ha organizado sus recursos de NetApp.

> No se puede asignar ningún rol adicional a un miembro que tenga asignado el rol de administrador de la organización. Ya tienen permisos en toda la organización. A un miembro con el rol de carpeta o proyecto no se le puede asignar ningún otro rol dentro de la carpeta o proyecto en el que ya tenga ese rol. Ambos roles proporcionan acceso a todos los servicios dentro del alcance que están asignados.

Pasos

1. Desde la página **Miembros**, navega a un miembro de la tabla, selecciona ••• y luego selecciona **Agregar un rol**.
2. Para agregar un rol, complete los pasos del cuadro de diálogo:
   - **Seleccione una organización, carpeta o proyecto**: Elija el nivel de su jerarquía de recursos para el que el miembro debe tener permisos.

     Si selecciona la organización o una carpeta, el miembro tendrá permisos para todo lo que reside en la organización o carpeta.

   - **Seleccionar una categoría**: Elija una categoría de rol. "Obtenga más información sobre los roles de acceso".
   - Seleccione un **rol**: Elija un rol que proporcione al miembro permisos para los recursos asociados a la organización, carpeta o proyecto que seleccionó.

"Obtenga más información sobre los roles de acceso". * **Agregar rol**: Si desea proporcionar acceso a carpetas o proyectos adicionales dentro de su organización, seleccione **Agregar rol**, especifique otra carpeta o proyecto o categoría de rol, y luego seleccione una categoría de rol y un rol correspondiente.

1. Selecciona **Añadir nuevos roles**.

Cambiar el rol asignado de un miembro

Puede cambiar los roles asignados a un miembro si necesita ajustar el acceso de un usuario.

> Los usuarios deben tener al menos un rol asignado. No se pueden eliminar todos los roles de un usuario. Si necesita eliminar todos los roles, debe eliminar al usuario de su organización.

Pasos

1. Desde la página **Miembros**, navega a un miembro de la tabla, selecciona ••• y luego selecciona **Ver detalles**.
2. En la tabla, expanda la fila correspondiente para la organización, carpeta o proyecto en el que desee cambiar el rol asignado del miembro y seleccione **Ver** en la columna **Rol** para ver los roles asignados a este miembro.
3. Puede cambiar un rol existente para un miembro o eliminar un rol.
   a. Para cambiar el rol de un miembro, seleccione **Cambiar** junto al rol que desea cambiar. Sólo puede cambiar este rol a un rol dentro de la misma categoría de rol. Por ejemplo, puede cambiar de un rol de servicio de datos a otro. Confirme el cambio.
   b. Para anular la asignación del rol de un miembro, seleccione junto al rol para anular la asignación del rol respectivo al miembro. Se le pedirá que confirme la eliminación.

Gestione la jerarquía de recursos de su organización de BlueXP

Cuando asocia un miembro a su organización, proporciona permisos a nivel de organización, carpeta o proyecto. Para asegurarse de que esos miembros tienen permisos para acceder a los recursos correctos, deberá gestionar la jerarquía de recursos de su organización asociando recursos a proyectos y carpetas específicos. Un *resource* es un recurso de almacenamiento que BlueXP ya gestiona o conoce.

Ver los recursos de su organización

Puede ver los recursos descubiertos y no descubiertos asociados con su organización. Los recursos no descubiertos son recursos de almacenamiento identificados por el asesor digital pero que no se agregan como entornos de trabajo.

> La página de recursos de IAM excluye los recursos de Amazon FSx for NetApp ONTAP porque no se pueden asociar con una función de IAM. Vea estos recursos en su lienzo respectivo o desde las cargas de trabajo.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione > **Gestión de identidades y acceso**.
2. Selecciona **Recursos** para ver la página Recursos.

3. Selecciona **Búsqueda avanzada y filtrado**.
4. Utilice cualquiera de las opciones disponibles para encontrar el recurso que está buscando:
   - **Buscar por nombre de recurso**: Ingrese una cadena de texto y seleccione **Agregar**.
   - **Plataforma**: Selecciona una o más plataformas, como Amazon Web Services.
   - **Recursos**: Selecciona uno o más recursos, como Cloud Volumes ONTAP.
   - **Organización, carpeta o proyecto**: Seleccione toda la organización, una carpeta específica o un proyecto específico.
5. Selecciona **Buscar**.

Asociar un recurso a carpetas y proyectos

Asociar un recurso a una carpeta o proyecto para que esté disponible.

Antes de empezar

Debe comprender cómo funciona la asociación de recursos. "Obtenga información sobre los recursos, incluido cuándo asociar un recurso a una carpeta".

Pasos

1. Desde la página **Recursos**, navegue a un recurso de la tabla, seleccione ••• y luego seleccione **Asociar a carpetas o proyectos**.
2. Seleccione una carpeta o proyecto y luego seleccione **Aceptar**.
3. Para asociar una carpeta o proyecto adicional, seleccione **Agregar carpeta o proyecto** y, a continuación, seleccione la carpeta o el proyecto.

   Tenga en cuenta que solo puede seleccionar entre las carpetas y proyectos para los que tiene permisos de administrador.

4. Seleccione **Asociar recursos**.
   - Si asoció el recurso a proyectos, los miembros que tienen permisos para esos proyectos ahora tienen la capacidad de acceder al recurso en BlueXP .
   - Si ha asociado el recurso a una carpeta, una *Carpeta o un proyecto admin* puede acceder al recurso desde BlueXP IAM. "Obtenga información sobre cómo asociar un recurso a una carpeta".

Después de terminar

Si descubre un recurso utilizando un conector BlueXP , asocie el conector con el proyecto para otorgarle acceso. De lo contrario, los miembros que no tengan el rol de *administrador de la organización* no podrán acceder al conector ni a su recurso asociado desde el lienzo de BlueXP .

"Aprenda a asociar un conector a una carpeta o proyecto".

Ver las carpetas y los proyectos asociados a un recurso

Para identificar dónde está disponible un recurso en la jerarquía de la organización, puede ver las carpetas y los proyectos asociados a ese recurso.

> Si necesita determinar qué miembros de la organización tienen acceso al recurso, puede "ver los miembros que tienen acceso a las carpetas y proyectos asociados al recurso".

Pasos

1. Desde la página **Recursos**, navega a un recurso de la tabla, selecciona ••• y luego selecciona **Ver detalles**.

El siguiente ejemplo muestra un recurso asociado a un proyecto.

Si necesita determinar qué miembros de la organización tienen acceso al recurso, puede "ver los miembros que tienen acceso a las carpetas y proyectos asociados al recurso".

Eliminar un recurso de una carpeta o proyecto

Para eliminar un recurso de una carpeta o proyecto, debe eliminar la asociación entre la carpeta o proyecto y el recurso. Eliminar la asociación impide que los miembros administren el recurso en la carpeta o el proyecto.

Si desea eliminar un recurso detectado de toda la organización, debe eliminar el entorno de trabajo del lienzo de BlueXP .

Pasos

1. Desde la página **Recursos**, navega a un recurso de la tabla, selecciona ••• y luego selecciona **Ver detalles**.
2. Para la carpeta o proyecto para el que desea eliminar el recurso, seleccione 🗑
3. Confirme que desea eliminar la asociación seleccionando **Eliminar**.

Información relacionada

- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "
- "Comience a usar BlueXP IAM"
- "Obtenga más información sobre la API para IAM de BlueXP "

Asociar un conector BlueXP a otras carpetas y proyectos

```
 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.
.Antes de empezar
Debe entender cómo funciona la asociación Connector.
xref:{relative_path}concept-identity-and-access-management.html#associate-
connectors["Obtenga información sobre el uso de conectores con BlueXP
IAM"].
```

Acerca de esta tarea

- Cuando una *Carpeta o un proyecto admin* ve la página **Conectores**, la página muestra todos los Conectores de la organización. Sin embargo, un miembro con este rol solo puede ver y asociar conectores con las carpetas y proyectos para los que tienen permisos. "Obtenga más información sobre las acciones que puede completar una *Carpeta o un proyecto admin*".

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Seleccione **Conectores**.
3. En la tabla, busque el conector que desea asociar.

   Utilice la búsqueda sobre la tabla para encontrar un conector específico o filtrar la tabla por jerarquía de recursos.

4. Para ver las carpetas y proyectos vinculados al Conector, seleccione ••• y luego seleccione **Ver detalles**.

   BlueXP muestra detalles sobre las carpetas y proyectos a los que está asociado el conector.

5. Seleccione **Asociar a carpeta o proyecto**.
6. Seleccione una carpeta o proyecto y luego seleccione **Aceptar**.
7. Para asociar el Conector a una carpeta o proyecto adicional, seleccione **Agregar una carpeta o proyecto** y, a continuación, seleccione la carpeta o proyecto.
8. Seleccione **Associate Connector**.

Después de terminar

Si desea asociar los recursos que gestiona Connector con las mismas carpetas y proyectos, puede hacerlo desde la página Recursos.

"Aprenda a asociar un recurso a carpetas y proyectos".

Información relacionada

- "Obtenga más información sobre los conectores BlueXP "
- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "

- "Comience a usar BlueXP IAM"
- "Obtenga más información sobre la API para IAM de BlueXP "

Cambiar entre Organizaciones, Proyectos y Conectores de BlueXP

Puede pertenecer a varias organizaciones de BlueXP o tener permisos para acceder a varios proyectos o conectores dentro de una organización de BlueXP . Cuando sea necesario, puede cambiar fácilmente entre organizaciones, proyectos y conectores para acceder a los recursos asociados a esa organización, proyecto o conector.

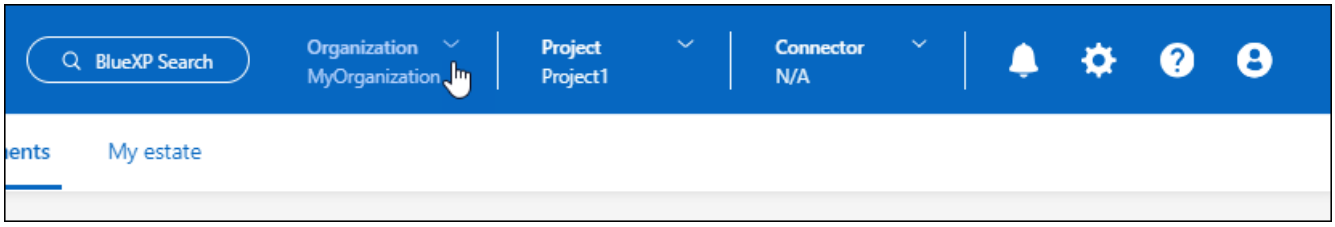
Puede pertenecer a varias organizaciones si se le invitó a unirse a otra organización o si creó una organización adicional usted mismo. Puede crear una organización adicional mediante la API. "Aprende a crear una nueva organización"

Cambiar entre organizaciones

Si es miembro de varias organizaciones, puede alternar entre ellas en cualquier momento.

Pasos

1. En la parte superior de BlueXP , selecciona **Organización**.



2. Seleccione otra organización y luego seleccione **Cambiar**.

Resultado

BlueXP cambia a la organización seleccionada y muestra los recursos asociados a esa organización.

Cambiar entre proyectos

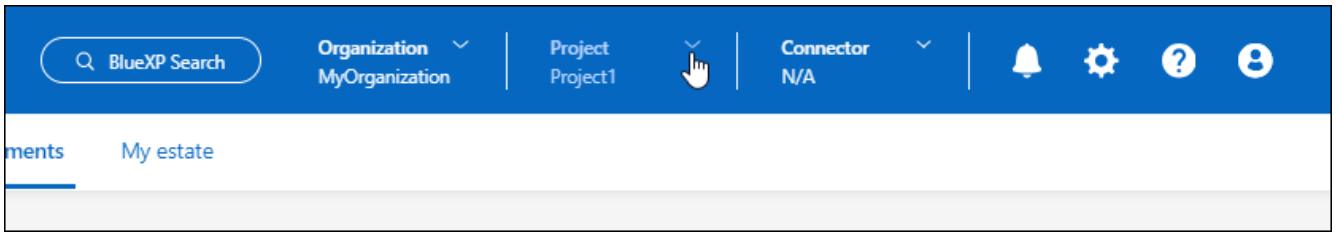
Si su organización incluye varios proyectos y tiene acceso a ellos, puede alternar entre ellos en cualquier momento.

Antes de empezar

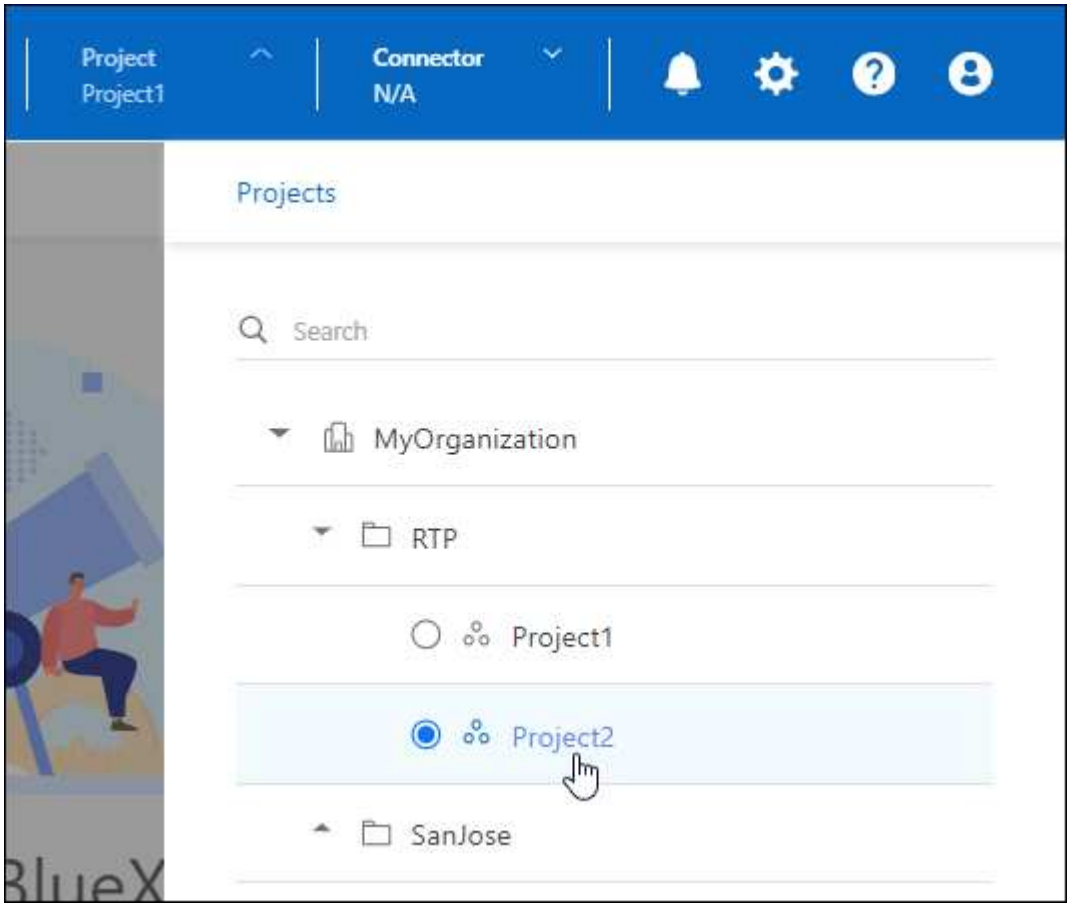
Debe estar en cualquier página de la consola de BlueXP , excepto en las páginas de gestión de acceso e identidad (IAM) de BlueXP . No puede cambiar a otro proyecto al ver cualquiera de las páginas de IAM.

Pasos

1. En la parte superior de BlueXP , selecciona **Proyecto**.



2. Navegue por las carpetas y proyectos de su organización, seleccione el proyecto que desee y, a continuación, seleccione * Cambiar *.



Resultado

BlueXP cambia al proyecto seleccionado y muestra los recursos asociados a ese proyecto.

Cambiar entre conectores

Si tiene varios conectores, puede alternar entre ellos para ver los entornos de trabajo asociados a un conector específico.

Pasos

1. En la parte superior de BlueXP , selecciona **Conector**.
2. Seleccione Otro conector y luego seleccione **Switch**.

Resultado

BlueXP actualiza y muestra los entornos de trabajo asociados al conector seleccionado.

Información relacionada

"Asociar conectores a carpetas y proyectos".

Información relacionada

- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "
- "Comience a usar BlueXP IAM"
- "Obtenga más información sobre la API para IAM de BlueXP "

ID de organización y proyecto

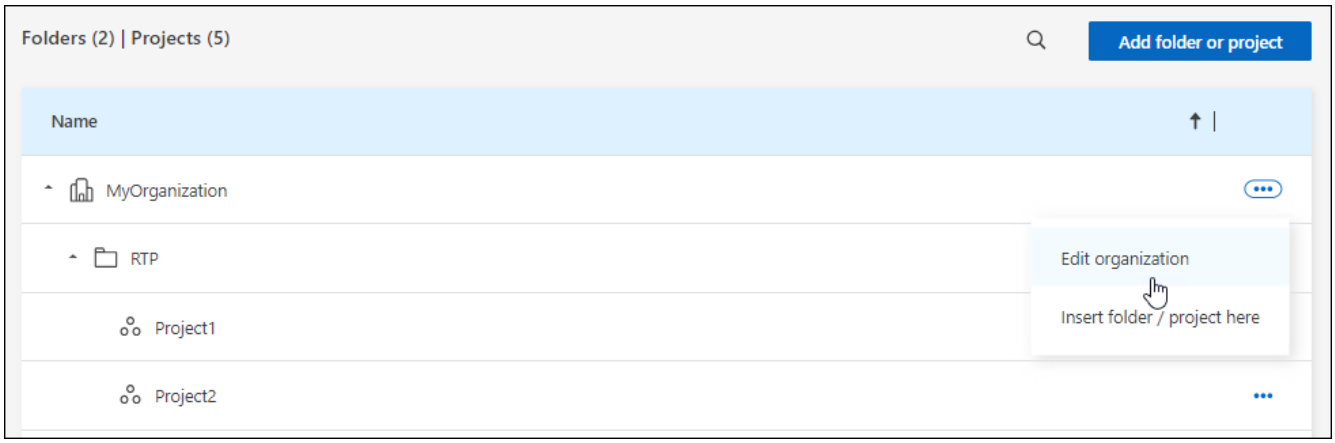
Su organización BlueXP tiene un nombre y un ID. Puede elegir un nombre para que su organización ayude a identificarlo en la implementación de BlueXP . Es posible que también necesite recuperar el identificador de organización para determinadas integraciones.

Cambie el nombre de su organización

Puede cambiar el nombre de su organización en BlueXP . Esto resulta útil si presta soporte a más de una organización dentro de la puesta en marcha de BlueXP .

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Desde la página **Organización**, navega a la primera fila de la tabla, selecciona ••• y luego selecciona **Editar organización**.



3. Introduzca un nuevo nombre de organización y seleccione **Aplicar**.

Obtenga el ID de organización

El identificador de organización se utiliza para determinadas integraciones con BlueXP .

Puede ver el identificador de organización en la página Organizaciones y copiarlo en el portapapeles según sus necesidades.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙ > **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Organización** para ver la página **Organización**.
3. En la página **Organización**, busca el ID de tu organización en la barra de resumen y cópialo en el portapapeles. Puede guardarlo para usarlo más adelante o copiarlo directamente donde necesite usarlo.

Obtenga el ID de un proyecto

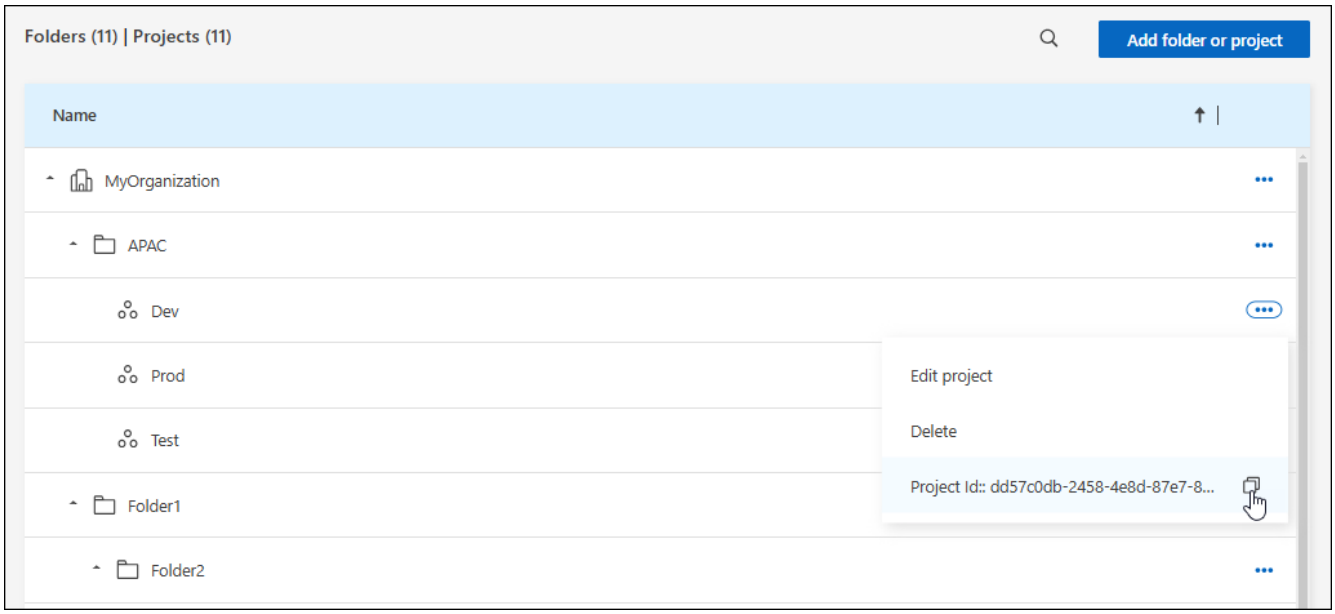
Si usas la API de BlueXP , es posible que necesites obtener el ID de un proyecto. Por ejemplo, al crear un entorno de trabajo Cloud Volumes ONTAP.

Pasos

1. Desde la página **Organización**, navega a un proyecto en la tabla y selecciona •••

   Aparece el ID de proyecto.

2. Para copiar el ID, seleccione el botón Copiar.



Información relacionada

- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "
- "Comience a usar BlueXP IAM"
- "Obtenga más información sobre la API para IAM de BlueXP "

Supervise o audite la actividad de IAM desde la línea de tiempo de BlueXP

Si necesita supervisar o auditar una acción que se ha completado desde la gestión de identidades y acceso (IAM) de BlueXP , puede ver los detalles en la línea de tiempo de BlueXP . Por ejemplo, puede que desee verificar quién ha agregado un miembro a una organización o si un proyecto se ha eliminado correctamente.

Pasos

1. En la parte superior derecha de la consola BlueXP , selecciona ⚙ > **Línea de tiempo**.
2. En los filtros, seleccione **Servicio** y luego seleccione **Artenza**.
3. Utilice cualquiera de los demás filtros para cambiar las acciones que se muestran en la tabla.

   Por ejemplo, puedes usar el filtro **Usuario** para mostrar acciones relacionadas con una cuenta de usuario específica.

Resultado

Se actualiza la línea de tiempo para indicar las acciones de gestión completadas relacionadas con IAM de BlueXP .

Roles de acceso de BlueXP

Obtenga más información sobre los roles de acceso de BlueXP

La gestión de identidad y acceso (IAM) de BlueXP incluye roles predefinidos que puede asignar a los miembros de su organización en diferentes niveles de su jerarquía de recursos. Antes de asignar estos roles, debe comprender los permisos que incluye cada rol. Las funciones se incluyen en las siguientes categorías: Plataforma, aplicación y servicio de datos.

Funciones de la plataforma

Los roles de plataforma otorgan todos los permisos de administración de BlueXP , incluyendo la asignación de roles y la adición de usuarios. Los roles de plataforma proporcionan acceso a todos los servicios y aplicaciones de datos de BlueXP . BlueXP IAM incluye dos roles de plataforma: administrador de la organización y administrador de carpeta o proyecto. La principal diferencia entre los dos roles de la plataforma IAM de BlueXP es Scope.

Función de la plataforma	Responsabilidades
"Administrador de la organización"	Permite a un usuario acceso sin restricciones a todos los proyectos y carpetas dentro de una organización, agregar miembros a cualquier proyecto o carpeta, así como realizar cualquier tarea de BlueXP y utilizar cualquier servicio de datos que no tenga un rol explícito asociado. Los usuarios con este rol organizan y administran su organización BlueXP . Crean carpetas y proyectos, asignan roles, agregan usuarios y pueden administrar todos los entornos de trabajo, si tienen las credenciales para hacerlo. Este es el único rol de acceso que puede crear conectores.
"Administrador de carpetas o proyectos"	Permite al usuario acceder sin restricciones a proyectos y carpetas específicos a los que están asignados. Puede agregar miembros a carpetas o proyectos que administran, así como realizar cualquier tarea de BlueXP y utilizar cualquier servicio de datos o aplicación en recursos dentro de la carpeta o proyecto que se les asigna. Los administradores de carpetas o proyectos no pueden crear conectores.
"Administración de la federación"	Permite a un usuario crear y administrar federaciones con BlueXP, lo que habilita el inicio de sesión único (SSO).

Función de la plataforma	Responsabilidades
"Visor de la Federación"	Permite a un usuario ver las federaciones existentes con BlueXP. No se pueden crear ni administrar federaciones

Funciones de la aplicación

A continuación se muestra una lista de roles en la categoría de aplicación. Cada rol otorga permisos específicos dentro de su ámbito designado. Los usuarios que no tengan el rol de aplicación o un rol de plataforma necesarios no podrán acceder a la aplicación.

Rol de la aplicación	Responsabilidades
"Administrador de Google Cloud NetApp Volumes"	Los usuarios con la función Google Cloud NetApp Volumes pueden descubrir y administrar Google Cloud NetApp Volumes.
"Administrador de Keystone"	Los usuarios con el rol de administrador de Keystone pueden crear solicitudes de servicio. Permite a los usuarios supervisar y ver información de consumo, activos e administrativa dentro del inquilino de Keystone al que acceden.
"Visor de Keystone"	Los usuarios con el rol de visor de Keystone NO PUEDEN crear solicitudes de servicio. Permite a los usuarios supervisar y ver información de consumo, activos e administrativa dentro del inquilino de Keystone al que acceden.
Rol de configuración del mediador de ONTAP	Las cuentas de servicio con el rol de configuración de Mediador de ONTAP pueden crear solicitudes de servicio. Este rol es necesario en una cuenta de servicio para configurar una instancia de "Mediador de la nube de ONTAP" .
"Analista de soporte de operaciones"	Proporciona acceso a alertas y herramientas de monitoreo y la capacidad de ingresar y administrar casos de soporte.
"Administrador de almacenamiento"	Administre funciones de gobernanza y estado del almacenamiento, detecte recursos de almacenamiento, y modifique y elimine los entornos de trabajo existentes.
"Visor de almacenamiento"	Vea las funciones de estado y gobernanza del almacenamiento, y también vea los recursos de almacenamiento detectados previamente. No se pueden detectar, modificar ni eliminar los entornos de trabajo de almacenamiento existentes.
"Especialista en salud de sistemas"	Administre las funciones de almacenamiento y estado y gobernanza, todos los permisos del administrador de almacenamiento, excepto no puede modificar ni eliminar los entornos de trabajo existentes.

Roles de servicio de datos

A continuación se muestra una lista de roles en la categoría de servicio de datos. Cada rol otorga permisos específicos dentro de su ámbito designado. Los usuarios que no tengan el rol de servicio de datos o un rol de plataforma necesarios no podrán acceder al servicio de datos.

Rol del servicio de datos	Responsabilidades
"Superadministrador de copias de seguridad y recuperación"	Realizar cualquier acción en el servicio de copia de seguridad y recuperación.

Rol del servicio de datos	Responsabilidades
"Administrador de copias de seguridad y recuperación"	Realice copias de seguridad en instantáneas locales, replique en almacenamiento secundario y realice copias de seguridad en almacenamiento de objetos.
"Administrador de restauración de copias de seguridad y recuperación"	Restaurar cargas de trabajo en el servicio de copia de seguridad y recuperación.
"Administrador de clones de copia de seguridad y recuperación"	Clonar aplicaciones y datos en el servicio de Backup y recuperación.
"Visor de copias de seguridad y recuperación"	Ver información de copia de seguridad y recuperación.
"Administración de recuperación ante desastres"	Realizar cualquier acción en el servicio de recuperación ante desastres.
"Administrador de conmutación por error de recuperación ante desastres"	Realizar conmutaciones por error y migraciones.
"Administrador de aplicaciones de recuperación ante desastres"	Cree planes de replicación, modifique planes de replicación e inicie conmutaciones por error de prueba.
"Visor de recuperación ante desastres"	Ver sólo información.
Visor de clasificación	Proporciona la capacidad de ver los resultados del escaneo de BlueXP classification . Los usuarios con este rol pueden ver información de cumplimiento y generar informes para los recursos a los que tienen permiso para acceder. Estos usuarios no pueden activar o desactivar el análisis de volúmenes, bloques o esquemas de base de datos. La clasificación no tiene un rol de visor.
"Administrador de protección frente a ransomware"	Gestiona acciones en las pestañas Proteger, Alerts, Recover, Settings e Reports del servicio de protección contra ransomware.
"Visor de protección contra ransomware"	Ver datos de carga de trabajo, ver datos de alerta, descargar datos de recuperación y descargar informes en el servicio de protección contra ransomware.
Administrador de SnapCenter	Ofrece la posibilidad de realizar backups de snapshots de clústeres de ONTAP en las instalaciones mediante backup y recuperación de datos de BlueXP en aplicaciones. Un miembro que tenga este rol puede completar las siguientes acciones en BlueXP: * Completar cualquier acción desde Copia de seguridad y recuperación > Aplicaciones * Administrar todos los entornos de trabajo en los proyectos y carpetas para los que tiene permisos * Usar todos los servicios de BlueXP SnapCenter no tiene un rol de espectador.

Enlaces relacionados

- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "
- "Comience a usar BlueXP IAM"

- "Gestionar miembros de BlueXP y sus permisos"
- "Obtenga más información sobre la API para IAM de BlueXP "

Funciones de acceso a la plataforma BlueXP

Asignar roles de plataforma a los usuarios para otorgar permisos para realizar tareas de administración en BlueXP, asignar roles, agregar usuarios, crear conectores y administrar federaciones.

Ejemplo de roles de organización en BlueXP para una organización multinacional grande

XYZ Corporation organiza el acceso al almacenamiento de datos por región (América del Norte, Europa y Asia-Pacífico), proporcionando control regional con supervisión centralizada.

El **administrador de la organización** en BlueXP de XYZ Corporation crea una organización inicial y carpetas separadas para cada región. El administrador de carpeta o proyecto de cada región organiza los proyectos (con los recursos asociados) dentro de la carpeta de la región.

Los administradores regionales con el rol de **Administrador de carpeta o proyecto** administran activamente sus carpetas agregando recursos y usuarios. Estos administradores regionales también pueden agregar, eliminar o cambiar el nombre de las carpetas y los proyectos que administran. El **administrador de la organización** hereda los permisos para cualquier recurso nuevo, lo que mantiene la visibilidad del uso del almacenamiento en toda la organización.

Dentro de la misma organización, a un usuario se le asigna el rol de **administrador de federación** para administrar la federación de la organización con su IdP corporativo. Este usuario puede agregar o eliminar organizaciones federadas, pero no puede administrar usuarios ni recursos dentro de la organización. El **Administrador de la organización** asigna a un usuario el rol de **Visor de la federación** para verificar el estado de la federación y ver las organizaciones federadas.

Las siguientes tablas indican las acciones que cada rol de la plataforma BlueXP puede realizar.

Roles de administración de la organización

Tarea	Administrador de la organización	Administrador de carpetas o proyectos
Crear conectores	Sí	No
Crear, modificar o suprimir entornos de trabajo (añadir o detectar nuevos recursos mediante el lienzo de BlueXP)	Sí	Sí
Cree carpetas y proyectos, incluida la eliminación	Sí	No
Cambie el nombre de las carpetas y proyectos existentes	Sí	Sí
Asigne roles y añada usuarios	Sí	Sí
Asociar recursos a carpetas y proyectos	Sí	Sí
Asociar conectores a carpetas y proyectos	Sí	No
Eliminar conectores de carpetas y proyectos	Sí	No

Tarea	Administrador de la organización	Administrador de carpetas o proyectos
Administrar conectores (editar certificados, configuración, etc.)	Sí	No
Gestione credenciales desde Configuración > Credenciales	Sí	Sí
Crear, administrar y visualizar federaciones	Sí	No
Regístrese para recibir soporte y enviar casos a través de BlueXP	Sí	Sí
Utilizar servicios de datos	Sí	Sí
Ver la línea de tiempo y las notificaciones de BlueXP	Sí	Sí

Roles de la federación

Tarea	Administración de la federación	Visor de la Federación
Crear una federación	Sí	No
Verificar un dominio	Sí	No
Agregar un dominio a una federación	Sí	No
Deshabilitar y eliminar federaciones	Sí	No
Federaciones de pruebas	Sí	No
Ver federaciones y sus detalles	Sí	Sí

Funciones de la aplicación

Roles de acceso de Keystone para BlueXP

Los roles de Keystone proporcionan acceso a las consolas de Keystone y permiten a los usuarios ver y gestionar su suscripción de Keystone. Existen dos roles de Keystone: El administrador de Keystone y el visor de Keystone. La principal diferencia entre los dos roles son las acciones que pueden tomar en Keystone. El rol de administrador de Keystone es el único rol que permite crear solicitudes de servicio o modificar suscripciones.

Ejemplo de roles de Keystone en BlueXP

XYZ Corporation tiene cuatro ingenieros de almacenamiento de diferentes departamentos que visualizan la información de suscripción de Keystone. Aunque todos estos usuarios necesitan supervisar la suscripción de Keystone, solo el jefe del equipo puede hacer solicitudes de servicio. A tres de los miembros del equipo se les da el rol **Keystone Viewer**, mientras que al jefe del equipo se le da el rol **Keystone admin** para que haya un punto de control sobre las solicitudes de servicio para la empresa.

La siguiente tabla indica las acciones que puede realizar cada rol Keystone.

Característica y acción	Administrador de Keystone	Visor de Keystone
Visualice las siguientes pestañas: Suscripción, Activos, Supervisión y Administración	Sí	Sí
Página de suscripción de Keystone:		
Ver suscripciones	Sí	Sí
Modificar o renovar suscripciones	Sí	No
Página de activos de Keystone:		
Consulta de activos	Sí	Sí
Gestionar activos	Sí	No
Página de alertas de Keystone:		
Ver las alertas	Sí	No
Gestionar alertas	Sí	No
Crear alertas para sí mismo	Sí	Sí
Cartera digital:		
Puede ver la cartera digital	Sí	Sí
Página de informes de Keystone:		
Descargar informes	Sí	Sí
Gestionar informes	Sí	Sí
Crear informes para sí mismo	Sí	Sí
Solicitudes de servicio:		
Crear solicitudes de servicio	Sí	No
Consulta de solicitudes de servicio creadas por cualquier usuario de la organización	Sí	Sí

Rol de acceso de analista de soporte operativo para BlueXP

Puede asignar el siguiente rol a los usuarios para brindarles acceso a alertas y monitoreo. Los usuarios con este rol también pueden abrir casos de soporte.

Analista de soporte operativo

Tarea	Puede realizar
Administre sus propias credenciales de usuario desde Configuración > Credenciales	Sí
Ver los recursos detectados	Sí
Regístrese para recibir soporte y enviar casos a través de BlueXP	Sí
Ver la línea de tiempo y las notificaciones de BlueXP	Sí
Ver, descargar y configurar alertas	Sí

Roles de acceso a almacenamiento para BlueXP

Es posible asignar los siguientes roles a los usuarios para proporcionarles acceso a las funciones de gestión del almacenamiento en BlueXP que se asocian con los recursos de almacenamiento compatibles. Puede asignar a los usuarios un rol administrativo para administrar el almacenamiento o un rol de espectador para monitorear.

Estos roles no están disponibles desde la API de asociación de BlueXP.

Los administradores pueden asignar roles de almacenamiento a los usuarios para los siguientes recursos y funciones de almacenamiento:

Recursos de almacenamiento:

- Clústeres de ONTAP en las instalaciones
- StorageGRID
- E-Series

Servicios y características de BlueXP :

- Asesor digital
- Actualizaciones de software
- Eficiencia económica
- Sostenibilidad

Ejemplo de roles de almacenamiento en BlueXP

XYZ Corporation, una empresa multinacional, cuenta con un gran equipo de ingenieros de almacenamiento y administradores de almacenamiento. Permiten que este equipo administre los activos de almacenamiento para sus regiones mientras limita el acceso a las tareas principales de BlueXP, como la administración de usuarios, la creación de conectores y herramientas de costos como la billetera digital.

Dentro de un equipo de 12, dos usuarios reciben el rol **Storage Viewer**, que les permite monitorear los recursos de almacenamiento asociados con los proyectos de BlueXP a los que están asignados. A los nueve restantes se les da el rol de administrador de almacenamiento*, que incluye la capacidad de administrar actualizaciones de software, acceder al Administrador del sistema de ONTAP a través de BlueXP , así como

descubrir recursos de almacenamiento (agregar entornos de trabajo). A una persona del equipo se le asigna el rol de **Especialista en salud del sistema** para que pueda administrar el estado de los recursos de almacenamiento en su región, pero no modificar ni eliminar ningún entorno de trabajo. Esta persona también puede realizar actualizaciones de software en los recursos de almacenamiento para los proyectos asignados.

La organización tiene dos usuarios adicionales con la función **Administrador de organización** que pueden administrar todos los aspectos de BlueXP , incluyendo la administración de usuarios, la creación de conectores y herramientas de administración de costos como la cartera digital, así como varios usuarios con la función **Carpeta o administrador de proyectos** que pueden realizar tareas de administración de BlueXP para las carpetas y proyectos a los que están asignados.

La siguiente tabla muestra las acciones que realiza cada rol de almacenamiento de BlueXP.

Característica y acción	Administrador de almacenamiento	Especialista en salud de sistemas	Visor de almacenamiento
Canvas:			
Descubrir nuevos recursos (crear un nuevo entorno de trabajo)	Sí	Sí	No
Ver los recursos detectados	Sí	Sí	No
Eliminar entornos de trabajo	Sí	No	No
Modificar entornos de trabajo	Sí	No	No
Crear conector	No	No	No
Asesor digital			
Ver todas las páginas y funciones	Sí	Sí	Sí
Cartera digital			
Ver todas las páginas y funciones	No	No	No
Actualizaciones de software			
Ver página de destino y recomendaciones	Sí	Sí	Sí
Revisar las recomendaciones de versiones potenciales y las ventajas clave	Sí	Sí	Sí
Vea los detalles de actualización de un clúster	Sí	Sí	Sí
Ejecute las comprobaciones previas a la actualización y descargue el plan de actualización	Sí	Sí	Sí
Instale las actualizaciones de software	Sí	Sí	No
Eficiencia económica			

Característica y acción	Administrador de almacenamiento	Especialista en salud de sistemas	Visor de almacenamiento
Revisar el estado de planificación de la capacidad	Sí	Sí	Sí
Elija la siguiente acción (práctica recomendada, nivel)	Sí	No	No
Organice en niveles los datos fríos en el almacenamiento en cloud y libere almacenamiento	Sí	Sí	No
Configurar recordatorios	Sí	Sí	Sí
Sostenibilidad			
Vea el panel y las recomendaciones	Sí	Sí	Sí
Descargar datos de informes	Sí	Sí	Sí
Edite el porcentaje de mitigación de carbono	Sí	Sí	No
Corrija las recomendaciones	Sí	Sí	No
Aplazar las recomendaciones	Sí	Sí	No
Acceso al administrador del sistema			
Puede introducir credenciales	Sí	Sí	No
Credenciales			
Credenciales de usuario	Sí	Sí	No

Roles de servicios de datos

Funciones de BlueXP backup and recovery

Puede asignar los siguientes roles a los usuarios para brindarles acceso al servicio de copia de seguridad y recuperación de BlueXP. Estos roles le ofrecen la flexibilidad de asignar a los usuarios un rol específico para las tareas que deben realizar en su organización. La forma de asignar roles depende de su negocio y de sus prácticas de gestión del almacenamiento.

La copia de seguridad y la recuperación utilizan los siguientes roles:

- **Superadministrador de copias de seguridad y recuperación**: realiza cualquier acción.
- **Administrador de copias de seguridad y recuperación**: realiza copias de seguridad en instantáneas locales, replica en almacenamiento secundario y realiza copias de seguridad en almacenamiento de objetos.

- **Administrador de restauración de copias de seguridad y recuperación**: Restaurar cargas de trabajo.
- **Administrador de clones de copia de seguridad y recuperación**: Clonar aplicaciones y datos.
- **Visor de copias de seguridad y recuperación**: vea información de copias de seguridad y recuperación.

La siguiente tabla indica las acciones que puede realizar cada rol.

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de backups	Restaurar administrador	Administrador clon	Visionador
Agregar, editar o eliminar hosts	Sí	No	No	No	No
Instalar complementos	Sí	No	No	No	No
Agregar credenciales (host, instancia, vCenter)	Sí	No	No	No	No
Ver panel y todas las pestañas	Sí	Sí	Sí	Sí	Sí
Inicie una prueba gratuita	Sí	No	No	No	No
Inicie la detección de las cargas de trabajo	No	Sí	Sí	Sí	No
Ver información de la licencia	Sí	Sí	Sí	Sí	Sí
Activar licencia	Sí	No	No	No	No
Ver anfitriones	Sí	Sí	Sí	Sí	Sí
Horarios:					
Activar horarios	Sí	Sí	Sí	Sí	No
Suspender horarios	Sí	Sí	Sí	Sí	No
Políticas y protección:					
Ver planes de protección	Sí	Sí	Sí	Sí	Sí
Crear, modificar o eliminar planes de protección	Sí	Sí	No	No	No
Restaurar cargas de trabajo	Sí	No	Sí	No	No
Crear, dividir o eliminar clones	Sí	No	No	Sí	No

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de backups	Restaurar administrador	Administrador clon	Visionador
Crear, modificar o eliminar una política	Sí	Sí	No	No	No
Informes:					
Ver informes	Sí	Sí	Sí	Sí	Sí
Crear informes	Sí	Sí	Sí	Sí	No
Eliminar informes	Sí	No	No	No	No
Importar desde SnapCenter y administrar el host:					
Ver datos importados de SnapCenter	Sí	Sí	Sí	Sí	Sí
Importar datos desde SnapCenter	Sí	Sí	No	No	No
Administrar (migrar) host	Sí	Sí	No	No	No
Configurar ajustes:					
Configure el directorio de registro	Sí	Sí	Sí	No	No
Asociar o eliminar credenciales de instancia	Sí	Sí	Sí	No	No
Cubos:					
Ver depósitos de almacenamiento	Sí	Sí	Sí	Sí	Sí
Crear, editar o eliminar depósitos de almacenamiento	Sí	Sí	No	No	No

Funciones de BlueXP disaster recovery

Puede asignar los siguientes roles a los usuarios para brindarles acceso a la recuperación ante desastres dentro de BlueXP. Los roles de recuperación ante desastres le brindan la flexibilidad de asignar a los usuarios un rol específico para las tareas que necesitan realizar dentro de su organización. La forma de asignar roles depende de su propio negocio y de sus prácticas de gestión de almacenamiento.

La recuperación ante desastres utiliza los siguientes roles:

- **Administrador de recuperación ante desastres**: Realizar cualquier acción.
- **Administrador de conmutación por error de recuperación ante desastres**: realiza conmutaciones por error y migraciones.
- **Administrador de aplicaciones de recuperación ante desastres**: Crear planes de replicación. Modificar planes de replicación. Iniciar pruebas de conmutación por error.
- **Visor de recuperación ante desastres**: Ver solo información.

La siguiente tabla indica las acciones que puede realizar cada rol.

Característica y acción	Administración de recuperación ante desastres	Administrador de conmutación por error de recuperación ante desastres	Administrador de aplicaciones de recuperación ante desastres	Visor de recuperación ante desastres
Ver panel y todas las pestañas	Sí	Sí	Sí	Sí
Inicie una prueba gratuita	Sí	No	No	No
Inicie la detección de las cargas de trabajo	Sí	No	No	No
Ver información de la licencia	Sí	Sí	Sí	Sí
Activar licencia	Sí	No	Sí	No
En la pestaña Sitios:				
Ver sitios	Sí	Sí	Sí	Sí
Agregar, modificar o eliminar sitios	Sí	No	No	No
En la pestaña Planes de replicación:				
Ver planes de replicación	Sí	Sí	Sí	Sí
Ver detalles del plan de replicación	Sí	Sí	Sí	Sí
Crear o modificar planes de replicación	Sí	Sí	Sí	No
Crear informes	Sí	No	No	No
Ver instantáneas	Sí	Sí	Sí	Sí
Realizar pruebas de conmutación por error	Sí	Sí	Sí	No
Realizar conmutaciones por error	Sí	Sí	No	No

Característica y acción	Administración de recuperación ante desastres	Administrador de conmutación por error de recuperación ante desastres	Administrador de aplicaciones de recuperación ante desastres	Visor de recuperación ante desastres
Realizar conmutaciones por error	Sí	Sí	No	No
Realizar migraciones	Sí	Sí	No	No
En la pestaña Grupos de recursos:				
Ver grupos de recursos	Sí	Sí	Sí	Sí
Crear, modificar o eliminar grupos de recursos	Sí	No	Sí	No
En la pestaña Monitoreo de trabajos:				
Ver trabajos	Sí	No	Sí	Sí
Cancelar trabajos	Sí	Sí	Sí	No

Roles de acceso de protección contra ransomware para BlueXP

Los roles de ransomware brindan a los usuarios acceso al servicio de protección contra ransomware. Los dos roles son el administrador de protección contra ransomware y el visor de protección contra ransomware. La principal diferencia entre los dos roles son las acciones que pueden tomar en la protección contra ransomware.

La siguiente tabla muestra las acciones que cada rol de protección contra ransomware BlueXP puede realizar.

Característica y acción	Administrador de protección frente a ransomware	Visor de protección contra ransomware
Ver panel y todas las pestañas	Sí	Sí
Inicie una prueba gratuita	Sí	No
Detectar cargas de trabajo	Sí	No
En la pestaña Proteger:		
Agregar, modificar o eliminar políticas	Sí	No
Proteja las cargas de trabajo	Sí	No
Identificar los datos confidenciales	Sí	No

Característica y acción	Administrador de protección frente a ransomware	Visor de protección contra ransomware
Editar la protección de cargas de trabajo	Sí	No
Ver detalles de la carga de trabajo	Sí	Sí
Descargar datos	Sí	Sí
En la pestaña Alertas:		
Ver detalles de alerta	Sí	Sí
Editar el estado del incidente	Sí	No
Ver detalles del incidente	Sí	Sí
Obtener una lista completa de archivos afectados	Sí	No
Descargar datos de alertas	Sí	Sí
En la pestaña Recuperar:		
Descargar archivos afectados	Sí	No
Restaure la carga de trabajo	Sí	No
Descargar datos de recuperación	Sí	Sí
Descargar informes	Sí	Sí
En la pestaña Configuración:		
Agregue o modifique destinos de copia de seguridad	Sí	No
Agregue o modifique destinos de SIEM	Sí	No
En la pestaña Informes:		
Descargar informes	Sí	Sí

federación de identidades

Active el inicio de sesión único mediante la federación de identidades con BlueXP

El inicio de sesión único (federación) simplifica el proceso de inicio de sesión y mejora la seguridad al permitir que los usuarios inicien sesión en BlueXP con sus credenciales

corporativas. Puede habilitar el inicio de sesión único (SSO) con su proveedor de identidad (IdP) o a través del sitio web de soporte de NetApp .

Rol requerido

Administrador de la organización, Administrador de la federación, Visor de la federación. "Obtenga más información sobre los roles de acceso."

Federación de identidades con el sitio de soporte de NetApp

Cuando se federa con el Sitio de soporte de NetApp , los usuarios pueden iniciar sesión con las mismas credenciales para acceder a BlueXP que utiliza para el Sitio de soporte de NetApp , Active IQ Digital Advisor y otras aplicaciones asociadas con su cuenta del Sitio de soporte de NetApp . Después de configurar la federación, cualquier usuario nuevo que cree una cuenta del sitio de soporte de NetApp también podrá acceder a BlueXP.

> Si se federa con el sitio de soporte de NetApp , no podrá hacerlo también con su proveedor de gestión de identidades corporativas. Elija la opción que mejor se adapte a su organización.

Pasos

1. Descargue y complete el "Formulario de solicitud de federación de NetApp" .
2. Envíe el formulario a la dirección de correo electrónico especificada en el formulario.

   El equipo de soporte de NetApp revisa y procesa su solicitud.

Configurar una conexión federada con su proveedor de identidad

Puede configurar una conexión federada con su proveedor de identidad para habilitar el inicio de sesión único (SSO) en BlueXP. El proceso implica configurar su proveedor de identidad para que confíe en NetApp como proveedor de servicios y, a continuación, crear la conexión en BlueXP.

> Si anteriormente configuró la federación usando NetApp Cloud Central (una aplicación externa a BlueXP), necesitará importar su federación usando la página de Federación de BlueXP para poder administrarla dentro de BlueXP."Aprenda cómo importar su federación."

Proveedores de identidades compatibles

NetApp admite los siguientes protocolos y proveedores de identidad para la federación:

Protocolos

- Proveedores de identidad del lenguaje de marcado de aserción de seguridad (SAML)
- Servicios de federación de Active Directory (AD FS)

proveedores de identidad

- ID de Microsoft Entra
- PingFederate

Federación con flujo de trabajo de BlueXP

NetApp solo admite el SSO iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para que confíe en NetApp como proveedor de servicios. Después, puede crear una conexión en BlueXP que utilice la configuración del proveedor de identidad.

Puedes federar con tu dominio de correo electrónico o con un dominio diferente de tu propiedad. Para federar con un dominio diferente a tu dominio de correo electrónico, primero verifica que eres el propietario del dominio.

1. **Verifique su dominio (si no utiliza su dominio de correo electrónico)**

Para federarse con un dominio diferente a su dominio de correo electrónico, verifique que sea su propietario. Puede federar su dominio de correo electrónico sin realizar pasos adicionales.

2. **Configure su IdP para confiar en NetApp como proveedor de servicios**

Configure su proveedor de identidad para que confíe en NetApp creando una nueva aplicación y proporcionando la información necesaria, como la URL de ACS, el ID de entidad u otra información de credenciales. La información del proveedor de servicios varía según el proveedor de identidad, por lo que consulte la documentación de su proveedor de identidad específico para obtener más detalles. Necesitará trabajar con el administrador de su IdP para completar este paso.

3. **Crear la conexión federada en BlueXP**

Para crear la conexión, debe proporcionar la información necesaria de su proveedor de identidad, como la URL o el archivo de metadatos SAML. Esta información se utiliza para establecer la relación de confianza entre BlueXP y su proveedor de identidad. La información que proporciones dependerá del IdP que estés utilizando. Por ejemplo, si utiliza Microsoft Entra ID, deberá proporcionar el ID de cliente, el secreto y el dominio.

4. **Pon a prueba tu federación en BlueXP**

Pruebe su conexión federada antes de habilitarla. La página de Federación en BlueXP proporciona una opción de prueba que le permite verificar que su usuario de prueba pueda autenticarse correctamente. Si la prueba es exitosa, puedes habilitar la conexión.

5. **Habilite su conexión en BlueXP**

Después de habilitar la conexión, los usuarios pueden iniciar sesión en BlueXP utilizando sus credenciales corporativas.

Revise el tema de su respectivo protocolo o IdP para comenzar:

- "Configurar una conexión federada con AD FS"
- "Configurar una conexión federada con Microsoft Entra ID"
- "Configurar una conexión federada con PingFederate"
- "Configurar una conexión federada con un proveedor de identidad SAML"

Verificación de dominio

Verifique el dominio de correo electrónico para su conexión federada

Si desea federarse con un dominio diferente a su dominio de correo electrónico, primero

debe verificar que es el propietario del dominio. Solo puede usar dominios verificados para la federación.

Roles requeridos

Administrador de la organización o administrador de la federación. "Obtenga más información sobre los roles de acceso."

Para verificar su dominio, agregue un registro TXT a la configuración DNS. Este registro se utiliza para demostrar que usted es el propietario del dominio y permite que BlueXP confíe en él para la federación. Es posible que deba coordinar con su administrador de TI o de red para completar este paso.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione > **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione **Configurar nueva federación**.
4. Seleccione **Verificar propiedad del dominio**.
5. Ingrese el dominio que desea verificar y seleccione **Continuar**.
6. Copie el registro TXT que se proporciona.
7. Acceda a la configuración DNS de su dominio y configure el valor TXT proporcionado como registro TXT. Consulte con su administrador de TI o de red si es necesario.
8. Después de agregar el registro TXT, regrese a BlueXP y seleccione **Verificar**.

Configurar federaciones

Federar BlueXP con los Servicios de federación de Active Directory (AD FS)

Federe sus Servicios de Federación de Active Directory (AD FS) con BlueXP para habilitar el inicio de sesión único (SSO) en BlueXP. Esto permite a los usuarios iniciar sesión en BlueXP con sus credenciales corporativas.

Roles requeridos

Se requiere un administrador de la organización o de la federación para crear y administrar federaciones. El visor de federaciones puede ver la página de la federación. "Obtenga más información sobre los roles de acceso."

> Puede federarse con su proveedor de identidades corporativo o con el sitio de soporte de NetApp . NetApp recomienda elegir uno u otro, pero no ambos.

NetApp solo admite el SSO iniciado por el proveedor de servicios (SP). Primero, configure el proveedor de identidad para que confíe en BlueXP como proveedor de servicios. A continuación, cree una conexión en BlueXP con la configuración de su proveedor de identidad.

Puede configurar la federación con su servidor AD FS para habilitar el inicio de sesión único (SSO) en BlueXP. El proceso implica configurar AD FS para que confíe en BlueXP como proveedor de servicios y, a continuación, crear la conexión en BlueXP.

Antes de empezar

- Se requiere una cuenta de IdP con privilegios administrativos. Coordínese con el administrador de su IdP para completar los pasos.
- Identifique el dominio que desea usar para la federación. Puede usar su dominio de correo electrónico o uno diferente de su propiedad. Si desea usar un dominio distinto a su dominio de correo electrónico, primero debe verificarlo en BlueXP. Puede hacerlo siguiendo los pasos de la sección "Verifique su dominio en BlueXP" tema.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione > **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione **Configurar nueva federación**.
4. Introduzca los detalles de su dominio:
   a. Elige si quieres usar un dominio verificado o tu dominio de correo electrónico. El dominio de correo electrónico es el asociado a la cuenta con la que iniciaste sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
5. Seleccione **Siguiente**.
6. Para su método de conexión, elija **Protocolo** y luego seleccione **Servicios de federación de Active Directory (AD FS)**.
7. Seleccione **Siguiente**.
8. Cree una relación de confianza de usuario autenticado en su servidor AD FS. Puede usar PowerShell o configurarla manualmente en su servidor AD FS. Consulte la documentación de AD FS para obtener más información sobre cómo crear una relación de confianza de usuario autenticado.
   a. Cree la confianza mediante PowerShell utilizando el siguiente script:

```
(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. Como alternativa, puede crear la confianza manualmente en la consola de administración de AD FS. Utilice los siguientes valores de BlueXP al crear la confianza:
      - Al crear el identificador de confianza, utilice el valor **YOUR_TENANT**: `netapp-cloud-account`
      - Cuando seleccione **Habilitar soporte para WS-Federation**, utilice el valor **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`
   c. Después de crear la confianza, copie la URL de metadatos de su servidor AD FS o descargue el archivo de metadatos de federación. Necesitará esta URL o archivo para completar la conexión en BlueXP.

   NetApp recomienda utilizar la URL de metadatos para permitir que BlueXP recupere automáticamente la última configuración de AD FS. Si descarga el archivo de metadatos de federación, deberá actualizarlo manualmente en BlueXP cada vez que se produzcan cambios en la configuración de AD FS.

9. Regrese a BlueXP y seleccione **Siguiente** para crear la conexión.
10. Cree la conexión con AD FS.
    a. Ingrese la **URL de AD FS** que copió de su servidor de AD FS en el paso anterior o cargue el archivo de metadatos de federación que descargó de su servidor de AD FS.
11. Seleccione **Crear conexión**. La creación de la conexión puede tardar unos segundos.
12. Seleccione **Siguiente**.
13. Seleccione **Probar conexión** para probar su conexión. Accederá a la página de inicio de sesión de su servidor IdP. Inicie sesión con sus credenciales de IdP para completar la prueba y vuelva a BlueXP para habilitar la conexión.
14. Seleccione **Siguiente**.
15. En la página **Habilitar federación**, revise los detalles de la federación y luego seleccione **Habilitar federación**.
16. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios pueden iniciar sesión en BlueXP usando sus credenciales corporativas.

Federar BlueXP con Microsoft Entra ID

Conéctese con su proveedor de IdP de Microsoft Entra ID para habilitar el inicio de sesión único (SSO) en BlueXP. Esto permite a los usuarios iniciar sesión con sus credenciales corporativas.

Roles requeridos

Se requiere un administrador de la organización o de la federación para crear y administrar federaciones. El visor de federaciones puede ver la página de la federación. "Obtenga más información sobre los roles de acceso."

> Puede federarse con su proveedor de identidades corporativo o con el sitio de soporte de NetApp . NetApp recomienda elegir uno u otro, pero no ambos.

NetApp solo admite el SSO iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para que confíe en NetApp como proveedor de servicios. Después, puede crear una conexión en BlueXP que utilice la configuración del proveedor de identidad.

Puede configurar una conexión federada con Microsoft Entra ID para habilitar el inicio de sesión único (SSO) en BlueXP. El proceso implica configurar su Microsoft Entra ID para que confíe en BlueXP como proveedor de servicios y, a continuación, crear la conexión en BlueXP.

Antes de empezar

- Se requiere una cuenta de IdP con privilegios administrativos. Coordínese con el administrador de su IdP para completar los pasos.
- Identifique el dominio que desea usar para la federación. Puede usar su dominio de correo electrónico o uno diferente de su propiedad. Si desea usar un dominio distinto a su dominio de correo electrónico, primero debe verificarlo en BlueXP. Puede hacerlo siguiendo los pasos de la sección "Verifique su dominio en BlueXP" tema.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione > **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione **Configurar nueva federación**.

Detalles del dominio

1. Introduzca los detalles de su dominio:
   a. Elige si quieres usar un dominio verificado o tu dominio de correo electrónico. El dominio de correo electrónico es el asociado a la cuenta con la que iniciaste sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
2. Seleccione **Siguiente**.

Método de conexión

1. Para su método de conexión, elija **Proveedor** y luego seleccione **Microsoft Entra ID**.
2. Seleccione **Siguiente**.

Instrucciones de configuración

1. Configure su ID de Microsoft Entra para que confíe en NetApp como proveedor de servicios. Debe realizar este paso en su servidor de ID de Microsoft Entra.
   a. Utilice los siguientes valores al registrar su aplicación Microsoft Entra ID para confiar en BlueXP:
      - Para la **URL de redirección**, utilice `https://services.cloud.netapp.com`
      - Para la **URL de respuesta**, utilice `https://netapp-cloud-account.auth0.com/login/callback`
   b. Cree un secreto de cliente para su aplicación Microsoft Entra ID. Deberá proporcionar el ID de cliente, el secreto de cliente y el nombre de dominio de Entra ID para completar la federación.
2. Regrese a BlueXP y seleccione **Siguiente** para crear la conexión.

Crear conexión

1. Crear la conexión con Microsoft Entra ID
   a. Ingrese el ID de cliente y el secreto de cliente que creó en el paso anterior.
   b. Introduzca el nombre de dominio de Microsoft Entra ID.
2. Seleccione **Crear conexión**. El sistema creará la conexión en unos segundos.

Probar y habilitar la conexión

1. Seleccione **Siguiente**.
2. Seleccione **Probar conexión** para probar su conexión. Accederá a la página de inicio de sesión de su servidor IdP. Inicie sesión con sus credenciales de IdP para completar la prueba y vuelva a BlueXP para habilitar la conexión.
3. Seleccione **Siguiente**.

4. En la página **Habilitar federación**, revise los detalles de la federación y luego seleccione **Habilitar federación**.
5. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios pueden iniciar sesión en BlueXP usando sus credenciales corporativas.

Federar BlueXP con PingFederate

Conéctese con su proveedor de IdP de PingFederate para habilitar el inicio de sesión único (SSO) en BlueXP. Esto permite a los usuarios iniciar sesión con sus credenciales corporativas.

Roles requeridos

Se requiere un administrador de la organización o de la federación para crear y administrar federaciones. El visor de federaciones puede ver la página de la federación. "Obtenga más información sobre los roles de acceso."

> Puede federarse con su proveedor de identidades corporativo o con el sitio de soporte de NetApp . NetApp recomienda elegir uno u otro, pero no ambos.

NetApp solo admite el SSO iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para que confíe en NetApp como proveedor de servicios. Después, puede crear una conexión en BlueXP que utilice la configuración del proveedor de identidad.

Puede configurar una conexión federada con PingFederate para habilitar el inicio de sesión único (SSO) en BlueXP. El proceso implica configurar su servidor PingFederate para que confíe en BlueXP como proveedor de servicios y luego crear la conexión en BlueXP.

Antes de empezar

- Se requiere una cuenta de IdP con privilegios administrativos. Coordínese con el administrador de su IdP para completar los pasos.
- Identifique el dominio que desea usar para la federación. Puede usar su dominio de correo electrónico o uno diferente de su propiedad. Si desea usar un dominio distinto a su dominio de correo electrónico, primero debe verificarlo en BlueXP. Puede hacerlo siguiendo los pasos de la sección "Verifique su dominio en BlueXP" tema.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione **Configurar nueva federación**.
4. Introduzca los detalles de su dominio:
   a. Elige si quieres usar un dominio verificado o tu dominio de correo electrónico. El dominio de correo electrónico es el asociado a la cuenta con la que iniciaste sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
5. Seleccione **Siguiente**.

6. Para su método de conexión, elija **Proveedor** y luego seleccione **PingFederate**.
7. Seleccione **Siguiente**.
8. Configure su servidor PingFederate para que confíe en NetApp como proveedor de servicios. Debe realizar este paso en su servidor PingFederate.
   a. Utilice los siguientes valores al configurar PingFederate para que confíe en BlueXP:
      - Para la **URL de respuesta** o la **URL del servicio de consumidor de afirmaciones (ACS)**, utilice `https://netapp-cloud-account.auth0.com/login/callback`
      - Para la **URL de cierre de sesión**, utilice `https://netapp-cloud-account.auth0.com/logout`
      - Para **ID de audiencia/entidad**, utilice `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` donde <fed-domain-name-pingfederate> es el nombre de dominio de la federación. Por ejemplo, si su dominio es `example.com` , el ID de audiencia/entidad sería `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Copia la URL del servidor PingFederate. La necesitarás para crear la conexión en BlueXP.
   c. Descargue el certificado X.509 de su servidor PingFederate. Debe estar en formato PEM codificado en Base64 (.pem, .crt, .cer).
9. Regrese a BlueXP y seleccione **Siguiente** para crear la conexión.
10. Crea la conexión con PingFederate
    a. Ingrese la URL del servidor PingFederate que copió en el paso anterior.
    b. Cargue el certificado de firma X.509. El certificado debe estar en formato PEM, CER o CRT.
11. Seleccione **Crear conexión**. El sistema creará la conexión en unos segundos.
12. Seleccione **Siguiente**.
13. Seleccione **Probar conexión** para probar su conexión. Accederá a la página de inicio de sesión de su servidor IdP. Inicie sesión con sus credenciales de IdP para completar la prueba y vuelva a BlueXP para habilitar la conexión.
14. Seleccione **Siguiente**.
15. En la página **Habilitar federación**, revise los detalles de la federación y luego seleccione **Habilitar federación**.
16. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios pueden iniciar sesión en BlueXP usando sus credenciales corporativas.

Federarse con un proveedor de identidad SAML

Conéctese con su proveedor de IdP SAML 2.0 para habilitar el inicio de sesión único (SSO) en BlueXP. Esto permite a los usuarios iniciar sesión con sus credenciales corporativas.

Rol requerido

Administrador de la organización. "Obtenga más información sobre los roles de acceso."

> Puede federarse con su proveedor de identidades corporativo o con el sitio de soporte de NetApp . No puede federarse con ambos.

NetApp solo admite el SSO iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para que confíe en NetApp como proveedor de servicios. Después, puede crear una conexión en BlueXP que utilice la configuración del proveedor de identidad.

Puede configurar una conexión federada con su proveedor de SAML 2.0 para habilitar el inicio de sesión único (SSO) en BlueXP. El proceso implica configurar su proveedor para que confíe en NetApp como proveedor de servicios y, a continuación, crear la conexión en BlueXP.

Antes de empezar

- Se requiere una cuenta de IdP con privilegios administrativos. Coordínese con el administrador de su IdP para completar los pasos.
- Identifique el dominio que desea usar para la federación. Puede usar su dominio de correo electrónico o uno diferente de su propiedad. Si desea usar un dominio distinto a su dominio de correo electrónico, primero debe verificarlo en BlueXP. Puede hacerlo siguiendo los pasos de la sección "Verifique su dominio en BlueXP" tema.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione **Configurar nueva federación**.
4. Introduzca los detalles de su dominio:
   a. Elige si quieres usar un dominio verificado o tu dominio de correo electrónico. El dominio de correo electrónico es el asociado a la cuenta con la que iniciaste sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
5. Seleccione **Siguiente**.
6. Para su método de conexión, elija **Protocolo** y luego seleccione **Proveedor de identidad SAML**.
7. Seleccione **Siguiente**.
8. Configure su proveedor de identidad SAML para que confíe en NetApp como proveedor de servicios. Debe realizar este paso en el servidor de su proveedor SAML.
   a. Asegúrese de que su IdP tenga el atributo `email` Establecido en la dirección de correo electrónico del usuario. Esto es necesario para que BlueXP identifique correctamente a los usuarios:

```
<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. Utilice los siguientes valores al registrar su aplicación SAML con BlueXP:
   - Para la **URL de respuesta** o la **URL del servicio de consumidor de afirmaciones (ACS)**, utilice `https://netapp-cloud-account.auth0.com/login/callback`
   - Para la **URL de cierre de sesión**, utilice `https://netapp-cloud-account.auth0.com/logout`
   - Para **ID de audiencia/entidad**, utilice `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` Donde <fed-domain-name-saml> es el nombre de dominio que desea usar para la federación. Por ejemplo, si su dominio es `example.com` , el ID de audiencia/entidad sería `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
c. Después de crear la confianza, copie los siguientes valores de su servidor de proveedor SAML:
   - URL de inicio de sesión
   - URL de cierre de sesión (opcional)
d. Descargue el certificado X.509 del servidor de su proveedor SAML. Debe estar en formato PEM, CER o CRT.

9. Regrese a BlueXP y seleccione **Siguiente** para crear la conexión.
10. Crea la conexión con SAML.
    a. Introduzca la **URL de inicio de sesión** de su servidor SAML.
    b. Cargue el certificado X.509 que descargó de su servidor de proveedor SAML.
    c. Opcionalmente, ingrese la **URL de cierre de sesión** de su servidor SAML.
11. Seleccione **Crear conexión**. El sistema creará la conexión en unos segundos.
12. Seleccione **Siguiente**.
13. Seleccione **Probar conexión** para probar su conexión. Accederá a la página de inicio de sesión de su servidor IdP. Inicie sesión con sus credenciales de IdP para completar la prueba y vuelva a BlueXP para habilitar la conexión.
14. Seleccione **Siguiente**.
15. En la página **Habilitar federación**, revise los detalles de la federación y luego seleccione **Habilitar federación**.
16. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios pueden iniciar sesión en BlueXP usando sus credenciales

corporativas.

Administrar federaciones en BLueXP

Puedes administrar tu federación en BlueXP. Puedes desactivarla, actualizar las credenciales caducadas y desactivarla si ya no la necesitas.

> Si anteriormente configuró la federación usando NetApp Cloud Central (una aplicación externa a BlueXP), necesitará importar su federación usando la página de Federación de BlueXP para poder administrarla dentro de BlueXP."Aprenda a importar su federación"

También puede agregar un dominio verificado a una federación existente, lo que le permite utilizar múltiples dominios para su conexión federada.

> Los eventos de gestión de la federación, como la habilitación, deshabilitación y actualización de las federaciones, se muestran en la línea de tiempo. "Obtenga más información sobre las operaciones de monitoreo en BlueXP."

Roles requeridos

Se requiere un administrador de la organización o de la federación para crear y administrar federaciones. El visor de federaciones puede ver la página de la federación. "Obtenga más información sobre los roles de acceso."

Habilitar una federación

Si ha creado una federación, pero no está habilitada, puede habilitarla a través de la pestaña "Federación" en BlueXP. Al habilitar una federación, los usuarios asociados a ella podrán iniciar sesión en BlueXP con sus credenciales corporativas. Debe haber creado la federación y haberla probado correctamente antes de habilitarla.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones ••• junto a la federación que desea habilitar y seleccione **Habilitar**.

Agregar un dominio verificado a una federación existente

Puede agregar un dominio verificado a una federación existente en BlueXP para usar múltiples dominios con el mismo proveedor de identidad (IdP).

Debe haber verificado el dominio en BlueXP antes de poder agregarlo a una federación. Si aún no lo ha hecho, puede hacerlo siguiendo los pasos de "Verifique su dominio en BlueXP" .

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones ⋮ Junto a la federación a la que desea agregar un dominio verificado,

seleccione **Actualizar dominios**. El cuadro de diálogo **Actualizar dominios** muestra el dominio ya asociado a esta federación.

4. Seleccione un dominio verificado de la lista de dominios disponibles.
5. Seleccione **Actualizar**. Puede tomar hasta 30 segundos para que los usuarios del nuevo dominio tengan acceso federado a BlueXP.

Actualización de una conexión federada que está a punto de expirar

Puede actualizar los detalles de una federación en BlueXP. Por ejemplo, deberá actualizar la federación si las credenciales, como un certificado o un secreto de cliente, caducan. Cuando sea necesario, actualice la fecha de notificación para recordarle que debe actualizar la conexión antes de que caduque.

> Actualice BlueXP antes de actualizar su IdP para evitar problemas de inicio de sesión. Mantenga la sesión iniciada en BlueXP durante el proceso.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione > **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones (tres puntos verticales) junto a la federación que desea actualizar y seleccione **Actualizar federación**.
4. Actualice los detalles de la federación según sea necesario.
5. Seleccione **Actualizar**.

Probar una federación existente

Si tiene problemas con una federación existente, puede probar la conexión para comprobar su correcto funcionamiento. Esto le ayudará a identificar y solucionar cualquier problema con la federación.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione > **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones ⋮ junto a la federación a la que desea agregar un dominio verificado y seleccione **Probar conexión**.
4. Seleccione **Prueba**. Se le solicitará que inicie sesión con sus credenciales corporativas. Si la conexión es correcta, se le redirigirá a la consola de BlueXP . Si la conexión falla, verá un mensaje de error que indica el problema con la federación.
5. Seleccione **Listo** para regresar a la pestaña **Federación**.

Deshabilitar una federación

Si ya no necesita una federación, puede desactivarla. Esto impide que los usuarios asociados a ella inicien sesión en BlueXP con sus credenciales corporativas. Puede reactivarla más adelante si es necesario.

Debes desactivar una federación antes de eliminarla. Por ejemplo, si vas a dar de baja el IdP en favor de otro IdP o si ya no quieres usar la federación. Esto te permitirá volver a activarla más adelante si es necesario.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones ⋮ junto a la federación a la que desea agregar un dominio verificado y seleccione **Deshabilitar**.

Eliminar una federación

Si ya no necesita una federación, puede eliminarla. Esto elimina la federación de BlueXP e impide que los usuarios asociados a ella inicien sesión en BlueXP con sus credenciales corporativas. Por ejemplo, si el IdP se está desmantelando o si la federación ya no es necesaria. Tras eliminar una federación, no podrá recuperarla. Debe crear una nueva.

> Debes deshabilitar una federación antes de eliminarla. No es posible recuperarla después de eliminarla.

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones ⋮ junto a la federación a la que desea agregar un dominio verificado y seleccione **Eliminar**.

Importa tu federación a BlueXP

Si previamente ha configurado la federación a través de NetApp Cloud Central (una aplicación externa a BlueXP), la página Federación le solicitará que importe su conexión federada existente a BlueXP para administrarla en la nueva interfaz. Esto le permite aprovechar las últimas mejoras sin tener que recrear sus conexiones federadas.

Los clientes que ya hayan configurado conexiones federadas con BlueXP pueden importarlas a la nueva interfaz. Esto les permite administrar sus conexiones federadas en la nueva página Federaciones sin tener que volver a crearlas.

> Después de importar su federación existente, puede administrarla desde la página Federaciones. "Obtenga más información sobre la gestión de federaciones."

Rol requerido

Administrador de la organización o administrador de la federación. "Obtenga más información sobre los roles de acceso."

Pasos

1. En la parte superior derecha de la consola de BlueXP , seleccione ⚙> **Gestión de identidades y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione **Importar federación**.

Conectores

Mantener la VM Connector y el sistema operativo

El mantenimiento del sistema operativo en el host del Conector es responsabilidad del cliente. Por ejemplo, debe aplicar actualizaciones de seguridad al sistema operativo del host del Conector siguiendo los procedimientos estándar de su empresa para la distribución de sistemas operativos.

Si tiene un conector existente, debe tener en cuenta "Cambios en los sistemas operativos Linux admitidos".

Parches del sistema operativo y el conector

Aplicar parches de seguridad del sistema operativo sin detener los servicios del host del conector.

Tipo de máquina virtual o instancia

Si crea un conector desde BlueXP, se implementará una instancia de máquina virtual en su proveedor de nube con una configuración predeterminada. Después de crear el conector, no cambie a una instancia de máquina virtual más pequeña con menos CPU o RAM.

La siguiente tabla enumera los requisitos de CPU y RAM:

CPU
: 8 núcleos o 8 vCPU

RAM
: 32GB

"Obtenga información sobre la configuración predeterminada para el conector".

Monitorear el conector

BlueXP le notifica cuando la máquina virtual del conector presenta problemas, incluyendo problemas de espacio en disco, RAM y CPU. Supervise estas notificaciones en el Centro de notificaciones de BlueXP o configure notificaciones por correo electrónico. Los aumentos ocasionales en el uso de espacio en disco, memoria o CPU son normales, pero si ocurren con frecuencia, debe tomar medidas para solucionarlos.

BlueXP le notifica cuando un recurso del Conector (CPU, RAM o espacio en disco) supera el 90 % de su capacidad total durante 30 minutos consecutivos. Posteriormente, si el uso del recurso cae por debajo de ese umbral, la notificación se muestra como resuelta (verde) en el Centro de notificaciones.

Trabaje con el soporte de NetApp si tiene preguntas sobre cómo modificar su máquina virtual Connector.

"Leer más."

Notificación	Es necesario actuar
El espacio en disco es demasiado alto	"Revise el artículo de la base de conocimientos de NetApp".
El uso de la CPU es demasiado alto	Aumente el tamaño de la CPU de la máquina virtual del conector en su hiperescalador o en su entorno local, según dónde la haya instalado. Como alternativa, cree conectores adicionales y distribuya la carga de trabajo entre varios. El uso de RAM puede variar según su entorno, las cargas de trabajo de ONTAP , la cantidad de sistemas Cloud Volumes ONTAP y los servicios de datos que utilice.
El uso de RAM es demasiado alto	Aumente la RAM de la máquina virtual del conector en su hiperescalador o en las instalaciones locales, según dónde la haya instalado. Como alternativa, cree conectores adicionales y distribuya la carga de trabajo entre varios. El uso de RAM puede variar según su entorno, las cargas de trabajo de ONTAP , la cantidad de sistemas Cloud Volumes ONTAP y los servicios de datos que utilice.

Parada e inicio de Connector VM

Si es necesario, detenga e inicie la máquina virtual Connector mediante la consola de su proveedor de nube o los procedimientos locales estándar.

"Tenga en cuenta que el conector debe estar operativo en todo momento".

Conéctese a la máquina virtual de Linux

Si necesita conectarse a la máquina virtual Linux en la que se ejecuta el conector, utilice las opciones de conectividad de su proveedor de nube.

AWS

Al crear la instancia del Conector en AWS, proporcione una clave de acceso y una clave secreta de AWS. Es posible usar este par de claves para SSH a la instancia. Use el nombre de usuario "ubuntu" para la instancia EC2 Linux. Para los Conectores creados antes de mayo de 2023, use el nombre de usuario "ec2-user".

"AWS Docs: Conéctese a su instancia de Linux"

Azure

Cuando crea la máquina virtual del conector en Azure, especifica un nombre de usuario y elige autenticarse con una contraseña o una clave pública SSH. Utilice el método de autenticación que ha elegido para conectarse a la máquina virtual.

"Azure Docs: SSH en su máquina virtual"

Google Cloud

No puede especificar un método de autenticación al crear un conector en Google Cloud. Sin embargo, puede conectarse a la instancia de VM de Linux mediante Google Cloud Console o Google Cloud CLI (gcloud).

"Google Cloud Docs: Conexión a equipos virtuales Linux"

Cambiar la dirección IP de un conector

Puede cambiar las direcciones IP internas y públicas de la instancia del Conector asignada por su proveedor de nube si es necesario.

Pasos

1. Siga las instrucciones del proveedor de cloud para cambiar la dirección IP local o la dirección IP pública (o ambas) de la instancia de Connector.
2. Reinicie la instancia del Conector para registrar una nueva dirección IP pública con BlueXP.
3. Si cambió la dirección IP privada, actualice la ubicación de copia de seguridad de los archivos de configuración de Cloud Volumes ONTAP para que las copias de seguridad se envíen a la nueva dirección IP privada del conector.

   Actualice la ubicación de la copia de seguridad para cada sistema Cloud Volumes ONTAP .

   a. En la interfaz de línea de comandos de Cloud Volumes ONTAP, establezca el nivel de privilegio en advanced:

   ```
   set -privilege advanced
   ```

   b. Ejecute el siguiente comando para mostrar el destino de backup actual:

   ```
   system configuration backup settings show
   ```

   c. Ejecute el siguiente comando para actualizar la dirección IP del destino de copia de seguridad:

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

Editar los URI de un conector

Puede agregar y eliminar el Identificador uniforme de recursos (URI) para un conector.

Pasos

1. Seleccione la lista desplegable **conector** del encabezado BlueXP.
2. Seleccione **gestionar conectores**.
3. Expande la barra **URI del conector** para ver los URI del conector.
4. Agregue y elimine URIs y, a continuación, seleccione **aplicar**.

Instale un certificado firmado por CA para acceder a la consola basada en web

Cuando se utiliza BlueXP en modo restringido o en modo privado, se puede acceder a la interfaz de usuario desde la máquina virtual de Connector que se implementa en la

región de nube o en las instalaciones. De forma predeterminada, BlueXP utiliza un certificado SSL autofirmado para proporcionar acceso HTTPS seguro a la consola basada en web que se ejecuta en el conector. Si así lo requiere su empresa, puede instalar un certificado firmado por una entidad de certificación (CA), la cual ofrece mejor protección de seguridad que un certificado autofirmado. Después de instalar el certificado, BlueXP utiliza el certificado firmado por CA cuando los usuarios acceden a la consola basada en web.

Antes de empezar

Debe crear un conector para poder cambiar la configuración de BlueXP. "Aprenda a crear un conector".

Instale un certificado HTTPS

Instale un certificado firmado por una CA para obtener acceso seguro a la consola basada en web que se ejecuta en el conector.

Acerca de esta tarea

Puede instalar el certificado mediante una de las siguientes opciones:

- Genere una solicitud de firma de certificación (CSR) en BlueXP , envíe la solicitud de certificación a una CA y, a continuación, instale el certificado firmado por CA en el conector.

  El par de claves que BlueXP utiliza para generar la CSR se almacena internamente en el conector. BlueXP recupera automáticamente el mismo par de claves (clave privada) al instalar el certificado en el conector.

- Instale un certificado firmado por CA que ya tenga.

  Con esta opción, la CSR no se genera a través de BlueXP . Se genera la CSR por separado y se almacena la clave privada externamente. Usted proporciona a BlueXP la clave privada al instalar el certificado.

Pasos

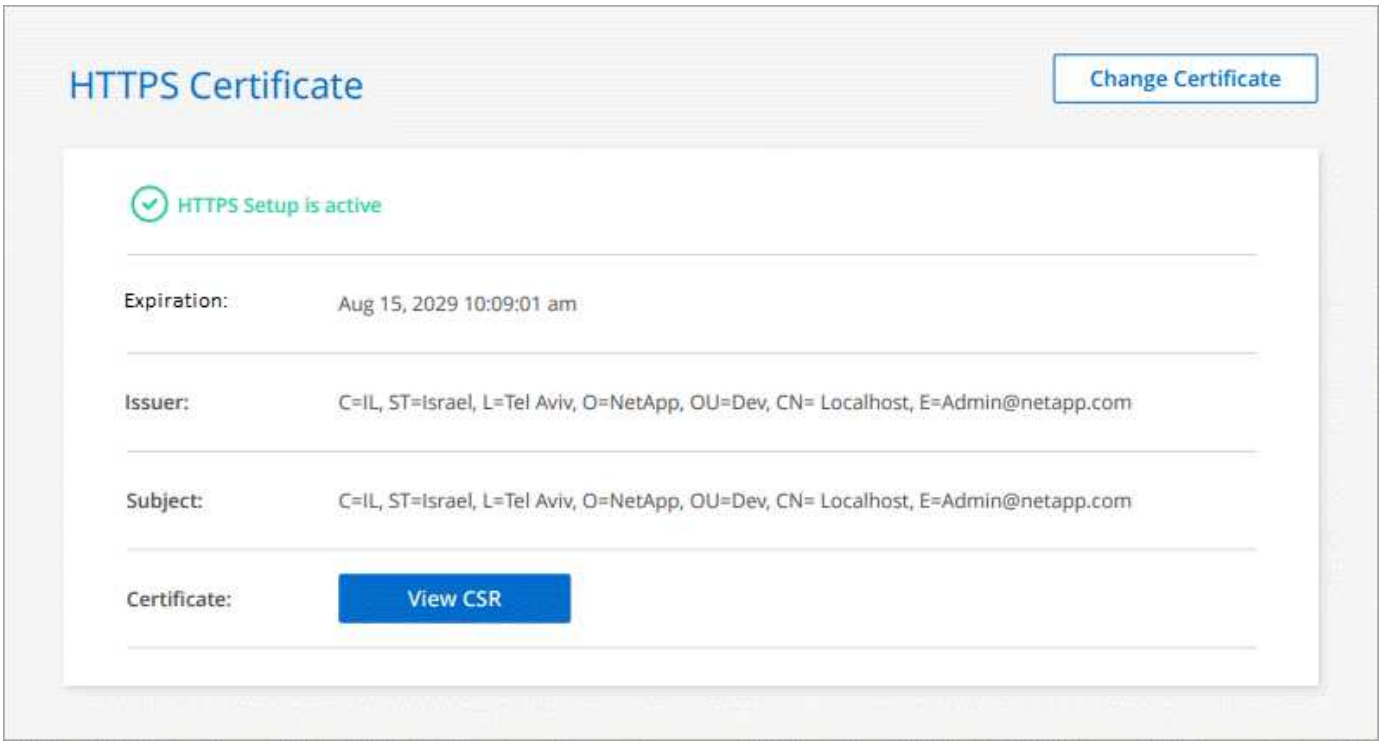
1. En la parte superior derecha de la consola BlueXP, seleccione el icono Configuración y seleccione **Configuración HTTPS**.

2. En la página HTTPS Setup, instale un certificado generando una solicitud de firma de certificación (CSR) o instalando su propio certificado firmado por una CA:

Opción	Descripción
Genere una CSR	a. Introduzca el nombre de host o DNS del host del conector (su nombre común) y, a continuación, seleccione **generar CSR**. BlueXP muestra una solicitud de firma de certificado. b. Utilice la CSR para enviar una solicitud de certificado SSL a una CA. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64. c. Cargue el archivo de certificado y, a continuación, seleccione **instalar**.
Instale su propio certificado firmado por CA	a. Seleccione **instalar certificado firmado por CA**. b. Cargue el archivo de certificado y la clave privada y, a continuación, seleccione **instalar**. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.

Resultado

Ahora BlueXP utiliza el certificado firmado por CA para proporcionar acceso HTTPS seguro. La siguiente imagen muestra un conector configurado para un acceso seguro:



Renueve el certificado HTTPS de BlueXP

Debe renovar el certificado HTTPS de BlueXP antes de que caduque para garantizar un acceso seguro a la consola BlueXP. Si no renueva el certificado antes de que caduque, aparece una advertencia cuando los

usuarios acceden a la consola Web mediante HTTPS.

Pasos

1. En la parte superior derecha de la consola BlueXP, seleccione el icono Configuración y seleccione **Configuración HTTPS**.

   Se muestra información sobre el certificado BlueXP, incluida la fecha de caducidad.

2. Seleccione **Cambiar certificado** y siga los pasos para generar una CSR o instalar su propio certificado firmado por CA.

Resultado

BlueXP utiliza el nuevo certificado firmado por CA para proporcionar acceso HTTPS seguro.

Configure un conector para que utilice un servidor proxy

Si las directivas de la empresa requieren que utilice un servidor proxy para todas las comunicaciones a Internet, deberá configurar los conectores para que utilicen ese servidor proxy. Si no configuró un conector para que utilice un servidor proxy durante la instalación, puede configurar el conector para que utilice ese servidor proxy en cualquier momento.

El servidor proxy del conector permite el acceso saliente a Internet sin una IP pública o una puerta de enlace NAT. El servidor proxy proporciona conectividad saliente solo para el Conector, no para los sistemas Cloud Volumes ONTAP.

Si los sistemas Cloud Volumes ONTAP carecen de acceso a Internet saliente, BlueXP los configura para utilizar el servidor proxy del Conector. Debe asegurarse de que el grupo de seguridad del Conector permita conexiones entrantes a través del puerto 3128. Abra este puerto después de implementar el conector.

Si el conector en sí no tiene una conexión a Internet saliente, los sistemas Cloud Volumes ONTAP no pueden usar el servidor proxy configurado.

Configuraciones admitidas

- Los servidores proxy transparentes son compatibles con los conectores que sirven a sistemas Cloud Volumes ONTAP . Si utiliza servicios de BlueXP con Cloud Volumes ONTAP, cree un conector dedicado para Cloud Volumes ONTAP donde pueda usar un servidor proxy transparente.
- Los servidores proxy explícitos son compatibles con todos los conectores, incluidos aquellos que administran sistemas Cloud Volumes ONTAP y aquellos que administran servicios BlueXP .
- HTTP y HTTPS.
- El servidor proxy puede residir en la nube o en su red.

> Una vez configurado un proxy, no se puede cambiar el tipo. Si necesita cambiarlo, elimine el conector y agregue uno nuevo con el nuevo tipo de proxy.

Habilitar un proxy explícito en un conector

Cuando configura un conector para utilizar un servidor proxy, ese conector y los sistemas Cloud Volumes ONTAP que administra (incluidos los mediadores ha), todos utilizan el servidor proxy.

Esta operación reinicia el Conector. Verifique que el conector esté inactivo antes de continuar.

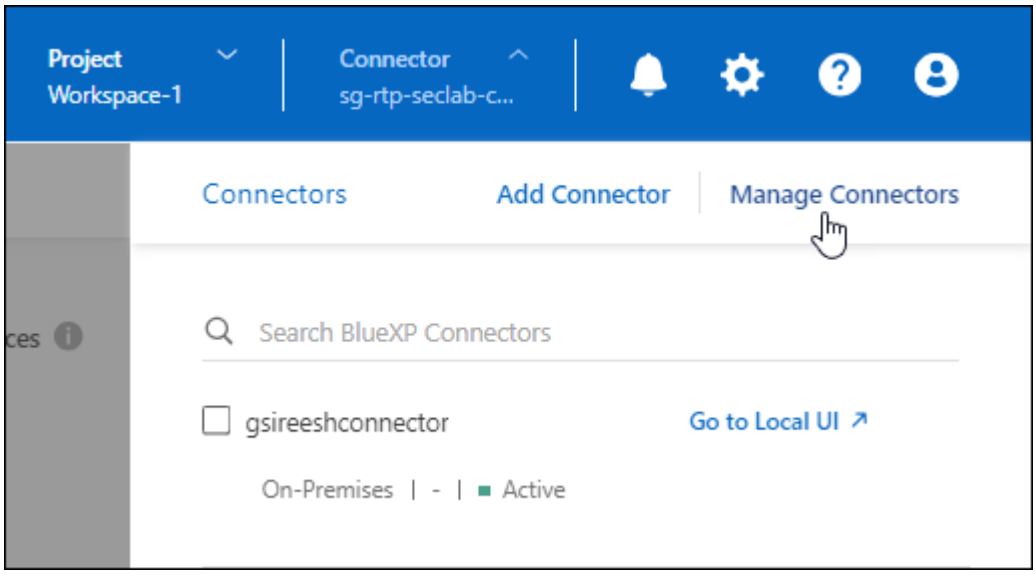
Pasos

1. Navega a la página **Edit BlueXP Connector**.

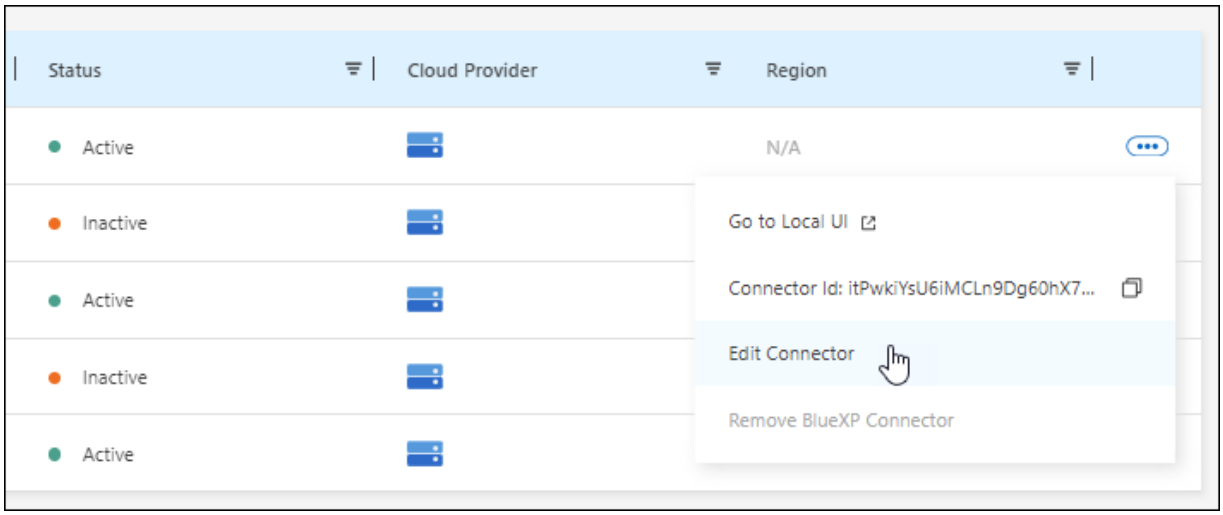
Modo estándar

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **gestionar conectores**.



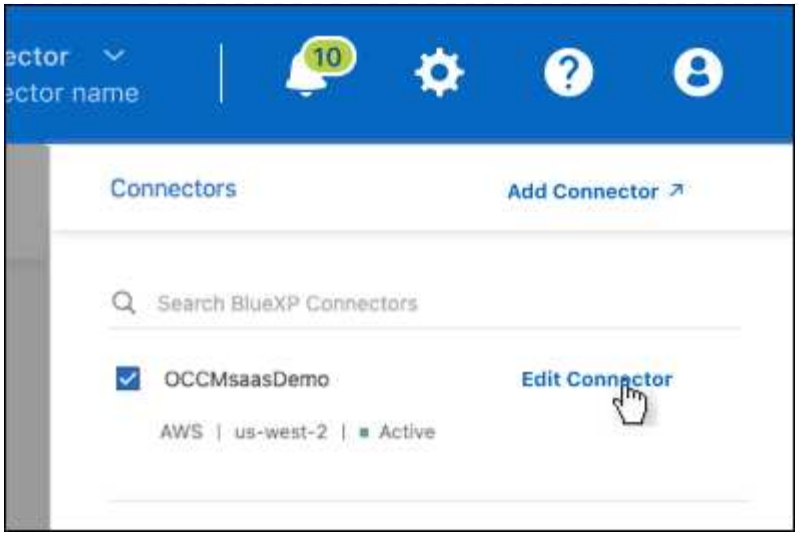
c. Seleccione el menú de acción de un conector y seleccione **Editar conector**.



Modo restringido o privado

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **Editar conector**.



2. Seleccione **Configuración de proxy HTTP**.
3. Seleccione **Proxy explícito** en el campo Tipo de configuración.
4. Seleccione **Activar proxy**.
5. Especifique el servidor con la sintaxis http://address:port o. https://address:port
6. Especifique un nombre de usuario y una contraseña si el servidor necesita autenticación básica.

   Tenga en cuenta lo siguiente:

   - El usuario puede ser un usuario local o un usuario de dominio.
   - Para un usuario de dominio, debe introducir el código ASCII para \ de la siguiente manera: Domain-name%92user-name

     Por ejemplo: netapp%92proxy

   - BlueXP no admite contraseñas que incluyan el carácter @.
7. Seleccione **Guardar**.

Habilitar un proxy transparente en un conector

Solo Cloud Volumes ONTAP admite el uso de un proxy transparente en el Conector. Si utiliza servicios de BlueXP además de Cloud Volumes ONTAP, debe crear un Conector independiente para los servicios de datos o para Cloud Volumes ONTAP.

Antes de habilitar un proxy transparente, asegúrese de que se cumplan los siguientes requisitos:

- El conector se instala en la misma red que el servidor proxy transparente.
- La inspección TLS está habilitada en el servidor proxy.
- Tienes un certificado en formato PEM que coincide con el utilizado en el servidor proxy transparente.
- No utilice el Conector para ningún servicio de datos de NetApp que no sea Cloud Volumes ONTAP.

Para configurar un conector existente para que utilice un servidor proxy transparente, utilice la herramienta de

mantenimiento del conector que está disponible a través de la línea de comandos en el host del conector.

Al configurar un servidor proxy, el Conector se reinicia. Verifique que el Conector esté inactivo antes de continuar.

Pasos

Asegúrese de tener un archivo de certificado en formato PEM para el servidor proxy. Si no tiene un certificado, contacte con su administrador de red para obtener uno.

1. Abra una interfaz de línea de comandos en el host del conector.
2. Navegue hasta el directorio de la herramienta de mantenimiento del conector: `/opt/application/netapp/service-manager-2/connector-maint-console`
3. Ejecute el siguiente comando para habilitar el proxy transparente, donde `/home/ubuntu/<certificate-file>.pem` es el directorio y el nombre del archivo de certificado que tiene para el servidor proxy:

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

   Asegúrese de que el archivo del certificado esté en formato PEM y resida en el mismo directorio que el comando o especifique la ruta completa al archivo del certificado.

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

Modificar el proxy transparente para el conector

Puede actualizar el servidor proxy transparente existente de un conector mediante el `proxy update` comando o elimine el servidor proxy transparente mediante el uso del `proxy remove` Comando. Para obtener más información, revise la documentación de "Consola de mantenimiento del conector" .

> Una vez configurado un proxy, no se puede cambiar el tipo. Si necesita cambiarlo, elimine el conector y agregue uno nuevo con el nuevo tipo de proxy.

Actualice el proxy del conector si pierde el acceso a Internet

Si cambia la configuración del proxy de su red, su Conector podría perder el acceso a internet. Por ejemplo, si alguien cambia la contraseña del servidor proxy o actualiza el certificado. En este caso, deberá acceder a la interfaz de usuario directamente desde el host del Conector y actualizar la configuración. Asegúrese de tener acceso de red al host del Conector y de poder iniciar sesión en la interfaz de usuario de BlueXP .

Habilite el tráfico de API directo

Si ha configurado un conector para utilizar un servidor proxy, puede habilitar el tráfico API directo en el conector para enviar llamadas API directamente a servicios de proveedores de cloud sin pasar por el proxy. Los conectores que se ejecutan en AWS, Azure o Google Cloud admiten esta opción.

Si deshabilita Azure Private Links con Cloud Volumes ONTAP y usa puntos de conexión de servicio, habilite el tráfico de API directo. De lo contrario, el tráfico no se enrutará correctamente.

"Obtenga más información sobre el uso de un enlace privado de Azure o extremos de servicio con Cloud Volumes ONTAP"

Pasos

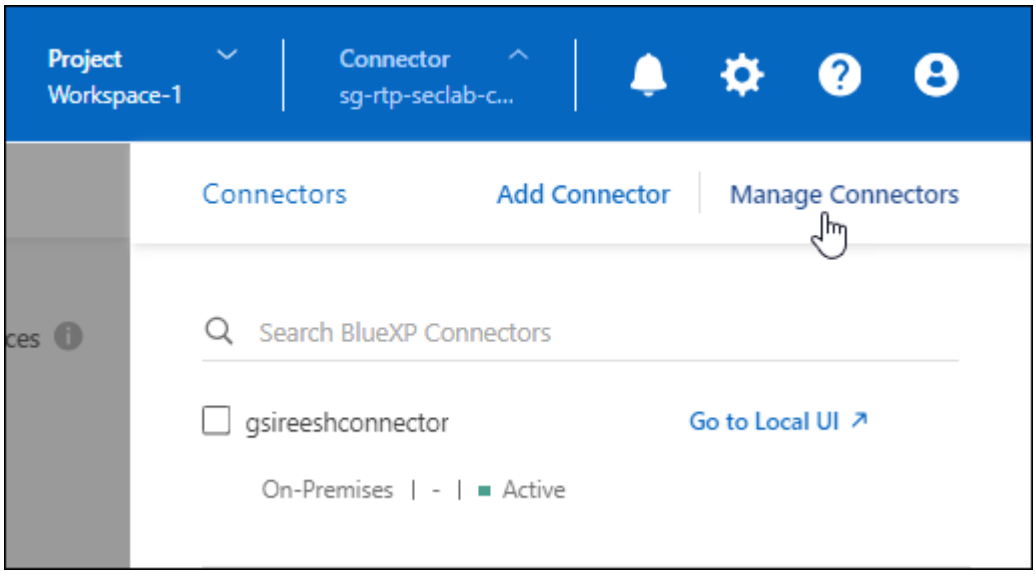
1. Navega a la página **Edit BlueXP Connector**:

   La navegación depende del modo de BlueXP. En el modo estándar, acceda a la interfaz desde el sitio web de SaaS. En el modo restringido o privado, acceda localmente desde el host del Conector.

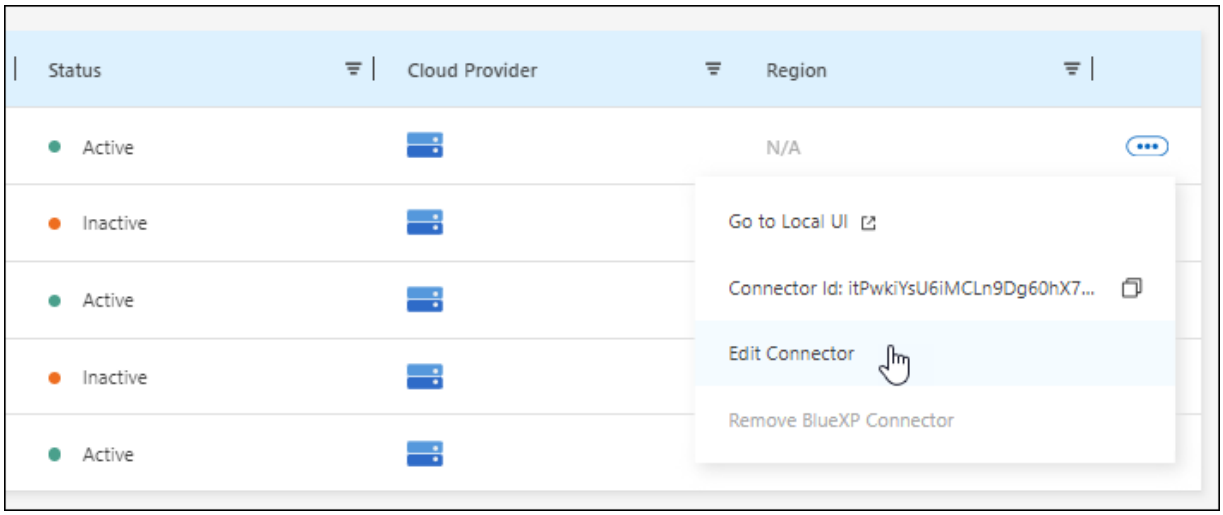
Modo estándar

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **gestionar conectores**.



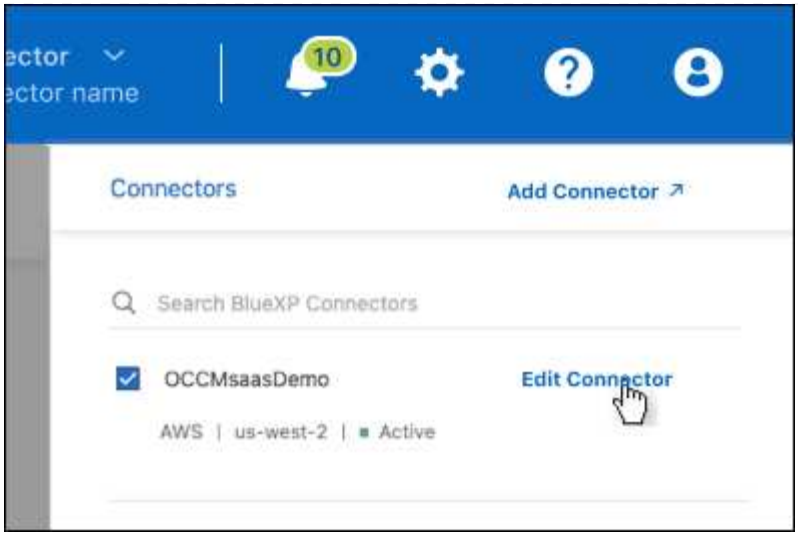
c. Seleccione el menú de acción de un conector y seleccione **Editar conector**.



Modo restringido o privado

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **Editar conector**.



2. Selecciona **Soporte Direct API Traffic**.
3. Seleccione la casilla de verificación para activar la opción y, a continuación, seleccione **Guardar**.

Requiere el uso de IMDSv2 en instancias de Amazon EC2

BlueXP admite el servicio de metadatos de la instancia de Amazon EC2 versión 2 (IMDSv2) con Connector y con Cloud Volumes ONTAP (incluido el mediador para puestas en marcha de alta disponibilidad). En la mayoría de los casos, IMDSv2 se configura automáticamente en instancias de EC2 nuevas. IMDSv1 se activó antes de marzo de 2024. Si las directivas de seguridad lo requieren, es posible que deba configurar manualmente IMDSv2 en las instancias de EC2.

Antes de empezar

- La versión del conector debe ser 3.9.38 o posterior.
- Cloud Volumes ONTAP debe ejecutar una de las siguientes versiones:
  - 9.12.1 P2 (o cualquier parche posterior)
  - 9.13.0 P4 (o cualquier parche posterior)
  - 9.13.1 o cualquier versión posterior a esta versión
- Este cambio requiere que reinicie las instancias de Cloud Volumes ONTAP.
- Estos pasos requieren el uso de la CLI de AWS porque debe cambiar el límite de saltos de respuesta a 3.

Acerca de esta tarea

IMDSv2 proporciona protección mejorada contra vulnerabilidades. "Obtenga más información sobre IMDSv2 en el blog de seguridad de AWS"

El servicio de metadatos de instancia (IMDS) se activa de la siguiente forma en las instancias EC2:

- Para nuevas puestas en marcha de Connector de BlueXP o mediante "Guiones Terraform", IMDSv2 está activado por defecto en la instancia EC2.
- Si inicia una nueva instancia de EC2 en AWS y, a continuación, instala manualmente el software Connector, también se habilita IMDSv2 de forma predeterminada.

- Si inicia Connector desde AWS Marketplace, IMDSv1 está habilitado de forma predeterminada. Puede configurar manualmente IMDSv2 en la instancia de EC2.
- Para los conectores existentes, IMDSv1 sigue siendo compatible, pero puede configurar manualmente IMDSv2 en la instancia EC2 si lo prefiere.
- Para Cloud Volumes ONTAP, IMDSv1 se habilita de forma predeterminada en las instancias nuevas y existentes. Puede configurar manualmente IMDSv2 en las instancias EC2 si lo prefiere.

Pasos

1. Requerir el uso de IMDSv2 en la instancia de conector:

   a. Conéctese a la máquina virtual de Linux para el conector.

      Al crear la instancia de Connector en AWS, proporcionó una clave de acceso y una clave secreta de AWS. Es posible usar este par de claves para SSH a la instancia. El nombre de usuario para la instancia de Linux EC2 es ubuntu (para los conectores creados antes de mayo de 2023, el nombre de usuario era EC2-user).

      "AWS Docs: Conéctese a su instancia de Linux"

   b. Instale la CLI de AWS.

      "AWS Docs: Instale o actualice a la última versión de la CLI de AWS"

   c. Utilice la `aws ec2 modify-instance-metadata-options` Comando para requerir el uso de IMDSv2 y para cambiar el límite de salto de respuesta PUT a 3.

      ejemplo

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

      La `http-tokens` El parámetro establece IMDSv2 en Necesario. Cuando `http-tokens` es necesario, también debe establecer `http-endpoint` para activarlo.

2. Requerir el uso de IMDSv2 en instancias de Cloud Volumes ONTAP:

   a. Vaya a la "Consola de Amazon EC2"

   b. En el panel de navegación, selecciona **Instancias**.

   c. Seleccione una instancia de Cloud Volumes ONTAP.

   d. Seleccione **Acciones > Configuración de instancia > Modificar opciones de metadatos de instancia**.

   e. En el cuadro de diálogo **Modificar opciones de metadatos de instancia**, seleccione lo siguiente:

      - Para **servicio de metadatos de instancia**, selecciona **Habilitar**.
      - Para **IMDSv2**, selecciona **Requerido**.

- Seleccione **Guardar**.

f. Repita estos pasos para otras instancias de Cloud Volumes ONTAP, incluido el mediador HA.

g. "Pare e inicie las instancias de Cloud Volumes ONTAP"

Resultado

La instancia de conector y las instancias de Cloud Volumes ONTAP ahora están configuradas para utilizar IMDSv2.

Gestionar actualizaciones de conectores

Cuando utiliza el modo estándar o el modo restringido, BlueXP actualiza automáticamente su Conector a la última versión, siempre que el Conector tenga acceso a Internet saliente para obtener la actualización del software. Si necesita administrar manualmente cuando se actualiza el conector, puede desactivar las actualizaciones automáticas para el modo estándar o el modo restringido.

> Al ejecutar BlueXP en modo privado, siempre debe actualizar el conector usted mismo.

Desactive las actualizaciones automáticas

La desactivación de la actualización automática del conector consta de dos pasos. En primer lugar, debe asegurarse de que su conector está en buen estado y actualizado. A continuación, editará un archivo de configuración para desactivar la función de actualización automática.

> Solo puede desactivar las actualizaciones automáticas si tiene la versión de conector 3.9.48 o superior.

Compruebe el estado del conector

Debe verificar que el conector es estable y que todos los contenedores que se ejecutan en la VM del conector están en buen estado y en funcionamiento. Después de desactivar las actualizaciones automáticas, la VM del conector deja de buscar nuevos servicios o paquetes de actualización.

Utilice uno de los siguientes comandos para verificar el conector. Todos los servicios deben tener el estado *Running*. Si no es así, póngase en contacto con el soporte de NetApp antes de deshabilitar la actualización automática.

Docker

```
docker ps -a
```

Podman

```
podman ps -a
```

Desactive la actualización automática del conector

Para deshabilitar las actualizaciones automáticas, establezca el indicador *isUpgradeDisabled* en el archivo *com/opt/application/NetApp/service-manager-2/config.json*. De forma predeterminada, este indicador se

establece en falso y el conector se actualiza automáticamente. Puede definir este indicador en true para desactivar las actualizaciones automáticas. Debe estar familiarizado con la sintaxis JSON antes de completar este paso.

Para volver a habilitar la actualización automática, siga estos pasos y establezca el indicador *isUpgradeDisabled* en FALSE.

Pasos

1. Asegúrese de haber verificado que su conector está actualizado y en buen estado.
2. Cree una copia de seguridad del archivo */opt/application/NetApp/service-manager-2/config.json* para asegurarse de que puede revertir los cambios.
3. Edite el archivo */opt/application/NetApp/service-manager-2/config.json* y cambie el valor del indicador *isUpgradeDisabled* a true.

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

4. Guarde el archivo.
5. Reinicie el servicio del gestor de servicios 2 ejecutando el siguiente comando:

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

6. Ejecute el siguiente comando y compruebe que el estado del conector se muestra como *active(running)*: _

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

Actualice el conector

El conector debe reiniciarse durante el proceso de actualización para que la consola basada en Web no esté disponible durante la actualización.

Pasos

1. Descargue el software del conector de "Sitio de soporte de NetApp".

   Asegúrese de descargar el instalador fuera de línea para redes privadas sin acceso a Internet.

2. Copie el instalador en el host Linux.
3. Asigne permisos para ejecutar el script.

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

   Donde <version> es la versión del conector que ha descargado.

4. Ejecute el script de instalación:

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

Donde <version> es la versión del conector que ha descargado.

5. Una vez finalizada la actualización, puede verificar la versión del conector en **Ayuda > Soporte > conector**.

Trabaje con varios conectores

Si utilizas varios conectores, BlueXP te permite alternar entre esos conectores directamente desde la consola. También puede gestionar un único entorno de trabajo con varios conectores.

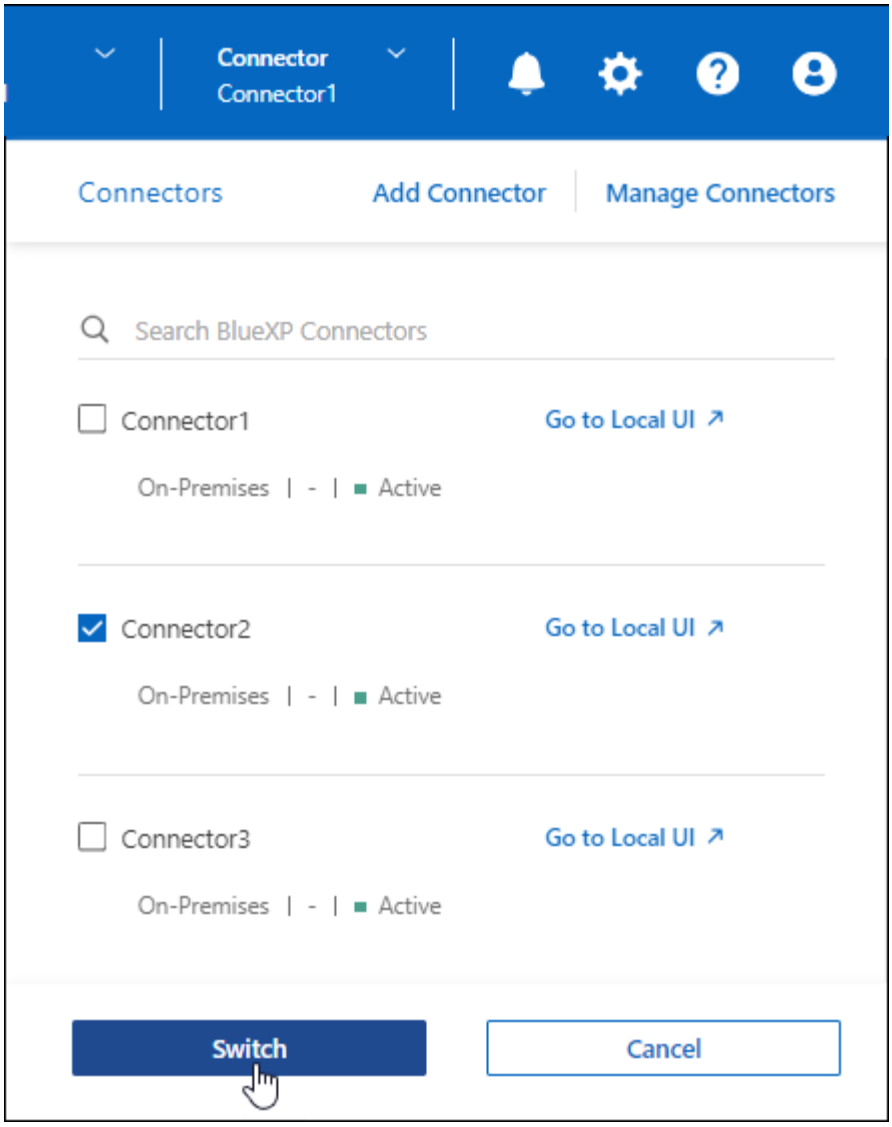
Cambiar entre conectores

Si tiene varios conectores, puede alternar entre ellos para ver los entornos de trabajo asociados a un conector específico.

Por ejemplo, digamos que trabaja en un entorno multicloud. Es posible que tenga un conector en AWS y otro en Google Cloud. Tendría que cambiar entre estos conectores para gestionar los sistemas Cloud Volumes ONTAP que se ejecutan en esas nubes.

Paso

1. Seleccione la lista desplegable **conector**, seleccione otro conector y, a continuación, seleccione **interruptor**.



Resultado

BlueXP actualiza y muestra los entornos de trabajo asociados al conector seleccionado.

Establezca una configuración de recuperación de desastres

Puede gestionar un entorno de trabajo con varios conectores al mismo tiempo para fines de recuperación ante desastres. Si se cae un conector, puede cambiar al otro conector para gestionar inmediatamente el entorno de trabajo.

Pasos

1. Cambie al otro conector que desee gestionar con el entorno de trabajo.
2. Detectar el entorno de trabajo existente.
   - "Agregue sistemas Cloud Volumes ONTAP existentes a BlueXP"
   - "Detectar clústeres de ONTAP"
3. Si gestiona un entorno de trabajo Cloud Volumes ONTAP, seleccione **Configuración > Configuración del conector** y establezca el Modo de gestión de capacidad en **Modo manual**.

   Para evitar problemas de contención, solo el conector principal debe configurarse en **Modo automático**.

"Obtenga más información sobre el modo de gestión de la capacidad"

Localice y solucione los problemas del conector

Para solucionar los problemas relacionados con el conector, puede trabajar con el soporte de NetApp que puede solicitar el ID del sistema, la versión del conector o los mensajes de AutoSupport más recientes. También puede ver la base de conocimientos de NetApp para solucionar los problemas por sí mismo.

Información relacionada

"Obtener ayuda del servicio de soporte de NetApp".

Busque el ID del sistema de un conector

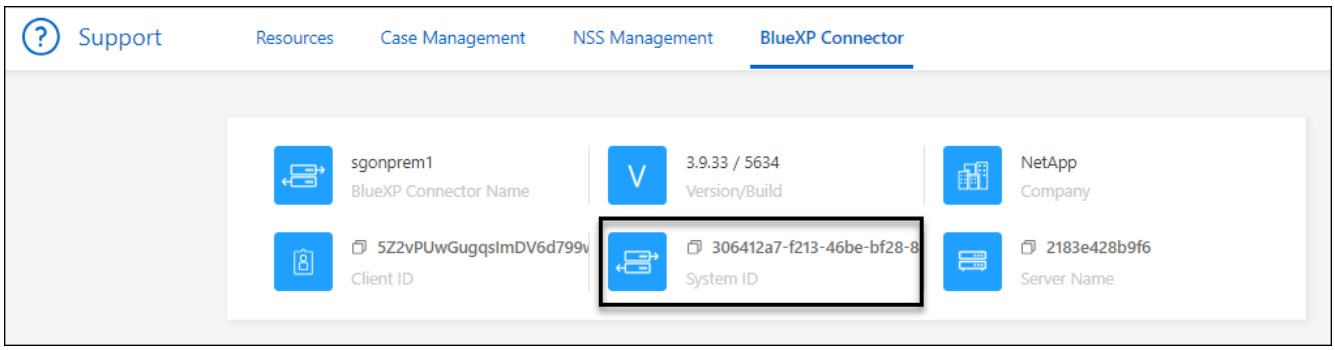
Para ayudarle a comenzar, su representante de NetApp puede pedirle el ID de sistema de su conector. El ID se utiliza normalmente para licencias y solución de problemas.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda.
2. Selecciona **Support > BlueXP Connector**.

   El ID del sistema aparece en la parte superior de la página.

   ejemplo



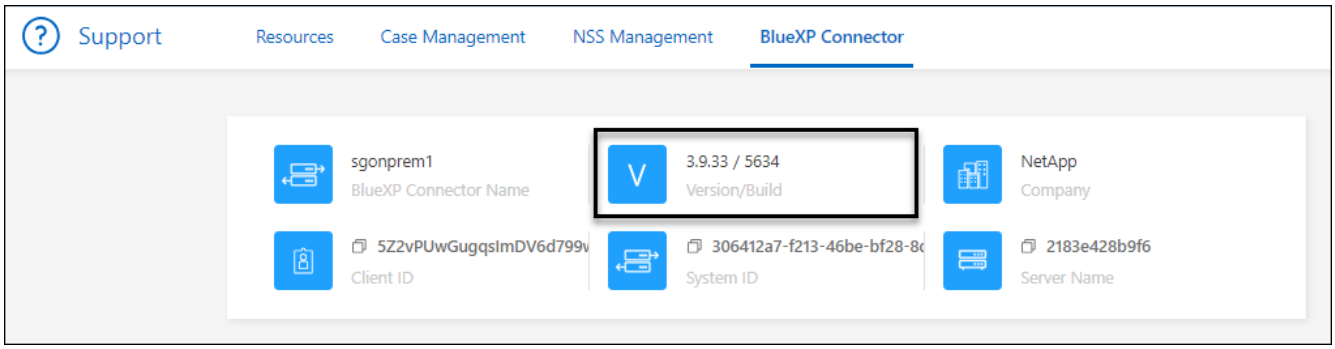
Ver la versión de un conector

Puede ver la versión de su conector para verificar que el conector se actualiza automáticamente a la última versión o porque necesita compartirlo con su representante de NetApp.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda.
2. Selecciona **Support > BlueXP Connector**.

   La versión se muestra en la parte superior de la página.

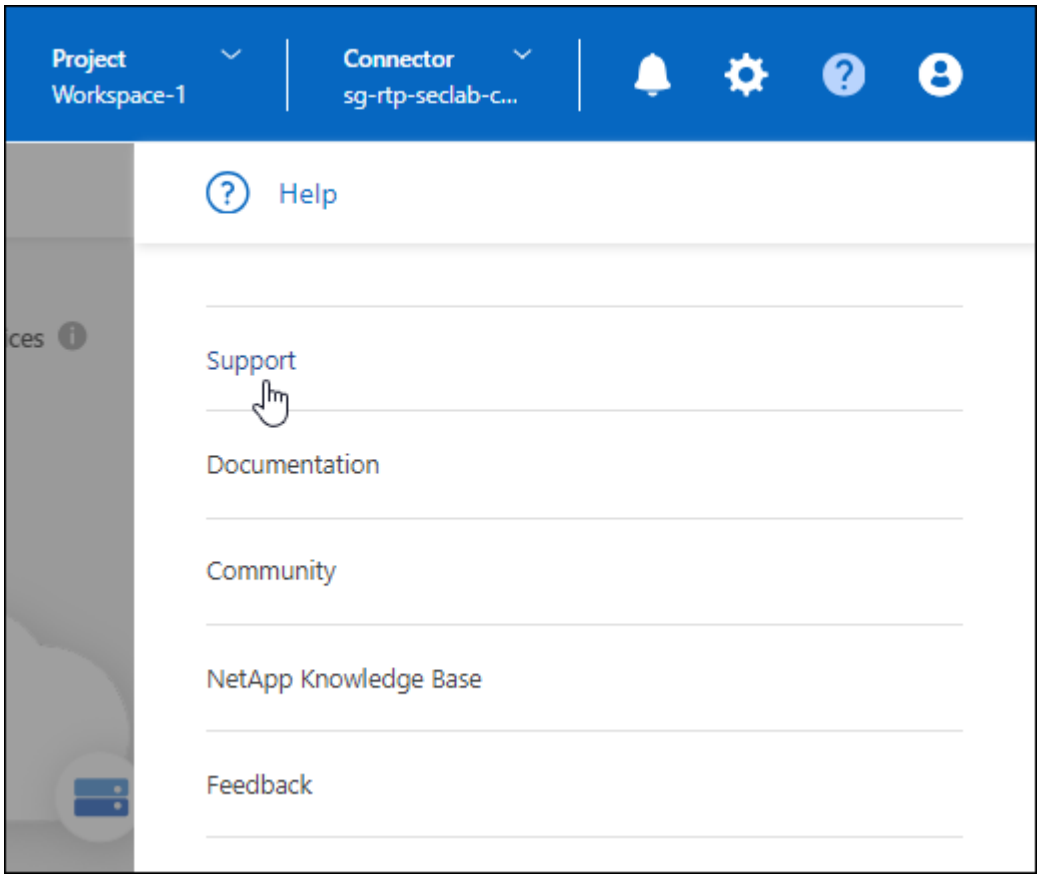


Descargar o enviar un mensaje de AutoSupport

Si tiene problemas, es posible que el personal de NetApp le solicite enviar un mensaje de AutoSupport al soporte de NetApp para la solución de problemas.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.

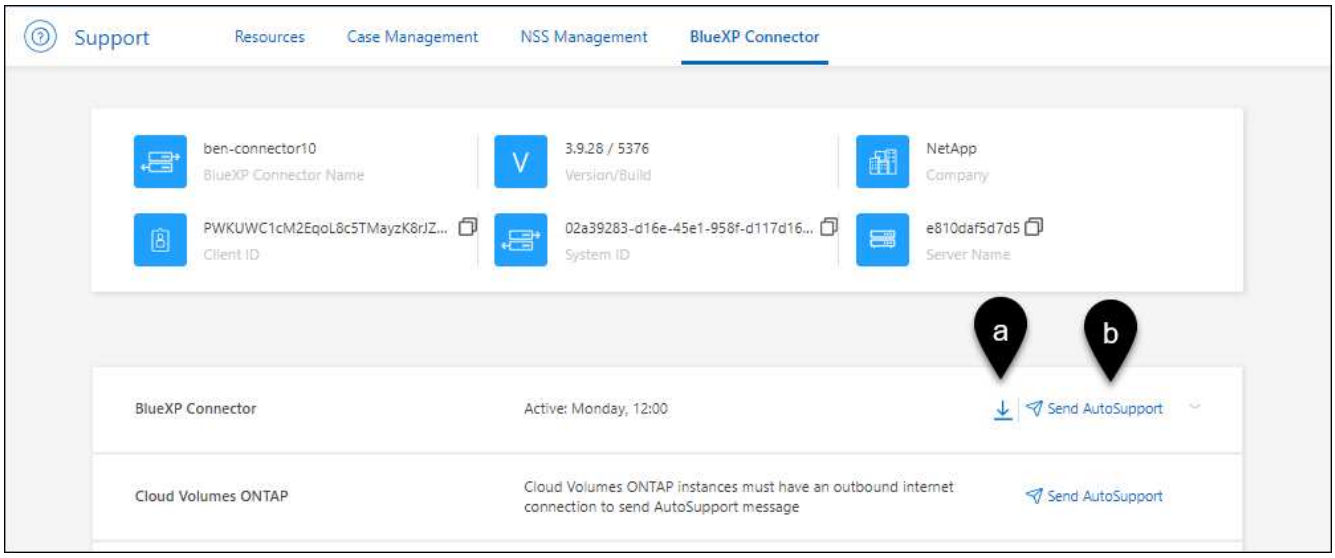


2. Seleccione **conector BlueXP**.
3. En función de cómo necesite enviar la información al soporte de NetApp, seleccione una de las siguientes opciones:

   a. Seleccione la opción para descargar el mensaje de AutoSupport en el equipo local. Luego, puede enviarlo al soporte de NetApp mediante un método preferido.

   b. Seleccione **Enviar AutoSupport** para enviar directamente el mensaje al soporte de NetApp.

BlueXP puede tardar hasta cinco horas en enviar mensajes de AutoSupport debido al equilibrio de carga. Para comunicaciones urgentes, descargue el archivo y envíelo manualmente.



Solucione los fallos de descarga al utilizar una puerta de enlace NAT de Google Cloud

El conector descarga automáticamente las actualizaciones de software de Cloud Volumes ONTAP. La descarga puede fallar si la configuración utiliza una puerta de enlace de NAT de Google Cloud. Puede corregir este problema limitando el número de partes en las que se divide la imagen de software. Este paso se debe completar mediante la API de BlueXP.

Paso

1. Envíe una solicitud PUT a /occm/config con el siguiente JSON como cuerpo:

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

   El valor para *maxDownloadSessions* puede ser 1 o cualquier entero mayor que 1. Si el valor es 1, la imagen descargada no se dividirá.

   Tenga en cuenta que 32 es un valor de ejemplo. El valor que debe utilizar depende de la configuración de NAT y del número de sesiones que puede tener simultáneamente.

"Obtenga más información acerca de la llamada a la API /occm/config"

Obtenga ayuda de la base de conocimientos de NetApp

"Ver la información para la solución de problemas creada por el equipo de soporte de NetApp".

Desinstale y retire el conector

Desinstale el software del conector para solucionar problemas o para quitar el software

del host de forma permanente. Los pasos que debe seguir dependen del modo de despliegue que esté utilizando. Cuando se ha eliminado un Connector de tu entorno, puedes eliminarlo de BlueXP.

"Obtenga más información sobre los modos de implementación de BlueXP".

Desinstale Connector cuando utilice el modo estándar o restringido

Si está utilizando el modo estándar o el modo restringido (en otras palabras, el host del Conector tiene conectividad saliente), debe seguir los pasos a continuación para desinstalar el software del Conector.

Pasos

1. Conéctese a la máquina virtual de Linux para el conector.
2. Desde el host Linux, ejecute el script de desinstalación:

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

   silent ejecuta la secuencia de comandos sin que se le solicite confirmación.

Desinstale Connector cuando utilice el modo privado

Si está utilizando el modo privado (donde el host del Conector no tiene conectividad saliente), siga los pasos a continuación para desinstalar el software del Conector.

Paso

1. Conéctese a la máquina virtual de Linux para el conector.
2. Desde el host Linux, ejecute los siguientes comandos:

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

3. Desde el host Linux, elimine los archivos de imágenes de contenedor antiguos y no utilizados para liberar espacio en el directorio /var para la reinstalación.

   Podman

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

   Docker

   ```
   docker system prune -a
   ```

Quitar conectores de BlueXP

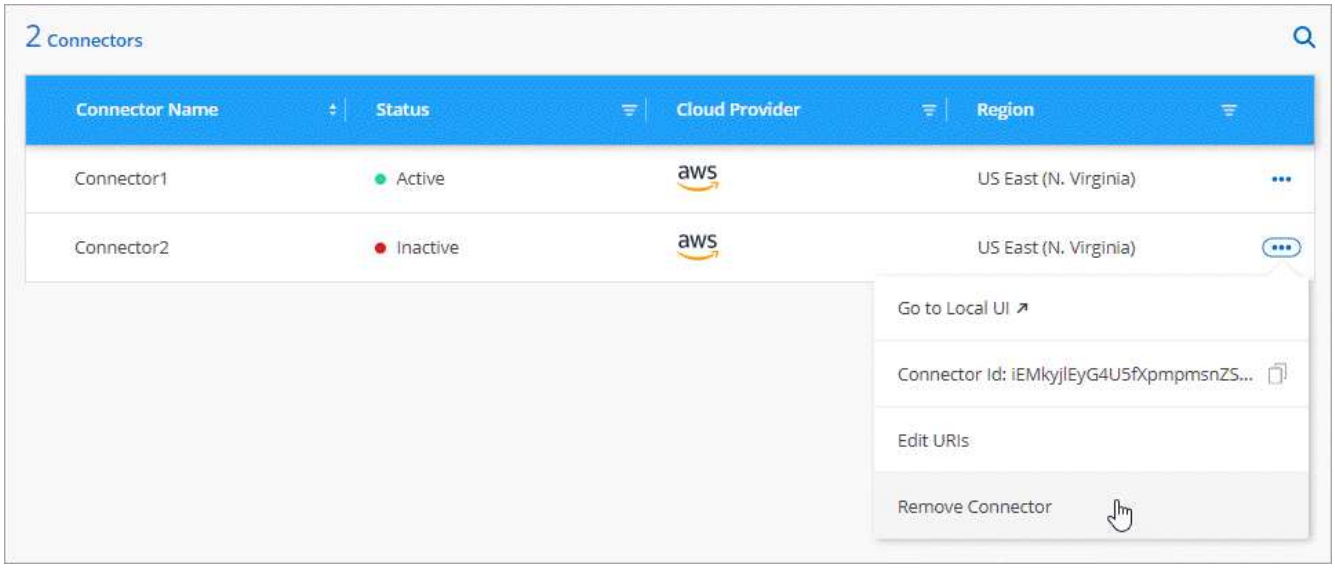
Si un conector está inactivo, puedes eliminarlo de la lista de conectores en BlueXP. Puede hacer esto si elimina la máquina virtual del Conector o si desinstala el software del Conector.

Tenga en cuenta lo siguiente sobre la extracción de un conector:

- Esta acción no elimina la máquina virtual.
- Esta acción no se puede revertir: una vez que elimines un conector, no podrás volver a agregarlo.

Pasos

1. Seleccione la lista desplegable **conector** del encabezado BlueXP.
2. Seleccione **gestionar conectores**.
3. Seleccione el menú de acción de un conector inactivo y seleccione **Quitar conector**.



4. Introduzca el nombre del conector que desea confirmar y, a continuación, seleccione **Quitar**.

Configuración predeterminada del conector

Es posible que desee obtener más información sobre la configuración del conector antes de implementarlo o si necesita solucionar cualquier problema.

Configuración predeterminada con acceso a Internet

Los siguientes detalles de configuración se aplican si ha implementado el conector desde BlueXP, desde el mercado del proveedor de la nube o si ha instalado manualmente el conector en un host Linux local que tenga acceso a Internet.

Detalles de AWS

Si implementó el conector desde BlueXP o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de instancia de EC2 es t3.2xlarge.
- El sistema operativo de la imagen es Ubuntu 22,04 LTS.

  El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.

- El nombre de usuario para la instancia de Linux EC2 es ubuntu (para los conectores creados antes de mayo de 2023, el nombre de usuario era EC2-user).
- El disco del sistema predeterminado es un disco gp2 de 100 GIB.

Detalles de Azure

Si implementó el conector desde BlueXP o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de máquina virtual es Standard_D8s_v3.
- El sistema operativo de la imagen es Ubuntu 22,04 LTS.

  El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El disco del sistema predeterminado es un disco SSD premium de 100 GIB.

Detalles de Google Cloud

Si implementó el Connector de BlueXP, tenga en cuenta lo siguiente:

- La instancia del equipo virtual es n2-standard-8.
- El sistema operativo de la imagen es Ubuntu 22,04 LTS.

  El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El disco del sistema predeterminado es un disco SSD persistente de 100 GIB.

Carpeta de instalación

La carpeta de instalación del conector se encuentra en la siguiente ubicación:

/opt/aplicación/netapp/cloudmanager

Archivos de registro

Los archivos de registro se encuentran en las siguientes carpetas:

- /opt/application/netapp/cloudmanager/log
  o.
- /opt/application/netapp/service-manager-2/logs (a partir de las nuevas instalaciones de 3.9.23)

  Los registros de estas carpetas proporcionan detalles sobre el conector.

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

  Los registros de esta carpeta proporcionan detalles sobre los servicios en la nube y el servicio BlueXP que se ejecuta en el conector.

Servicio de conectores

- El servicio BlueXP se llama occm.
- El servicio occm depende del servicio MySQL.

  Si el servicio MySQL está inactivo, entonces el servicio occm también está inactivo.

Puertos

El conector utiliza los siguientes puertos en el host Linux:

- 80 para acceso HTTP
- 443 para el acceso HTTPS

Configuración predeterminada sin acceso a Internet

La siguiente configuración se aplica si instaló manualmente el conector en un host Linux local que no tiene acceso a Internet. "Obtenga más información sobre esta opción de instalación".

- La carpeta de instalación del conector se encuentra en la siguiente ubicación:

  /opt/aplicación/netapp/ds

- Los archivos de registro se encuentran en las siguientes carpetas:

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

  Los registros de esta carpeta proporcionan detalles sobre las imágenes de conector y Docker.

- Todos los servicios se ejecutan en contenedores Docker

  Los servicios dependen del servicio docker Runtime que se esté ejecutando

- El conector utiliza los siguientes puertos en el host Linux:
  - 80 para acceso HTTP
  - 443 para el acceso HTTPS

Aplicar permisos de ONTAP para la vista avanzada de ONTAP (ONTAP System Manager)

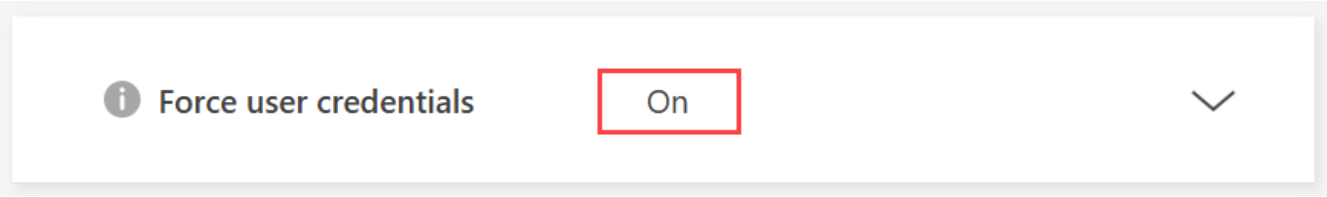
De forma predeterminada, las credenciales del Conector permiten a los usuarios acceder a la Vista Avanzada (Administrador del Sistema ONTAP). Puede solicitarles sus credenciales de ONTAP. Esto garantiza que los permisos ONTAP de un usuario se apliquen cuando funcionan con clústeres de ONTAP en clústeres en las instalaciones tanto de Cloud Volumes ONTAP como de ONTAP.

Debe tener el rol de administrador de la organización para editar la configuración del conector.

Pasos

1. Seleccione la lista desplegable **conector** del encabezado BlueXP.

2. Seleccione **gestionar conectores**.
3. Seleccione el menú de acción en la fila correspondiente al conector que desea editar.
4. Expanda la opción **Forzar credenciales**.
5. Seleccione la casilla de verificación para habilitar la opción **Forzar credenciales** y luego seleccione **Guardar**.
6. Compruebe si la opción **Forzar credenciales** está habilitada.



Credenciales y suscripciones

AWS

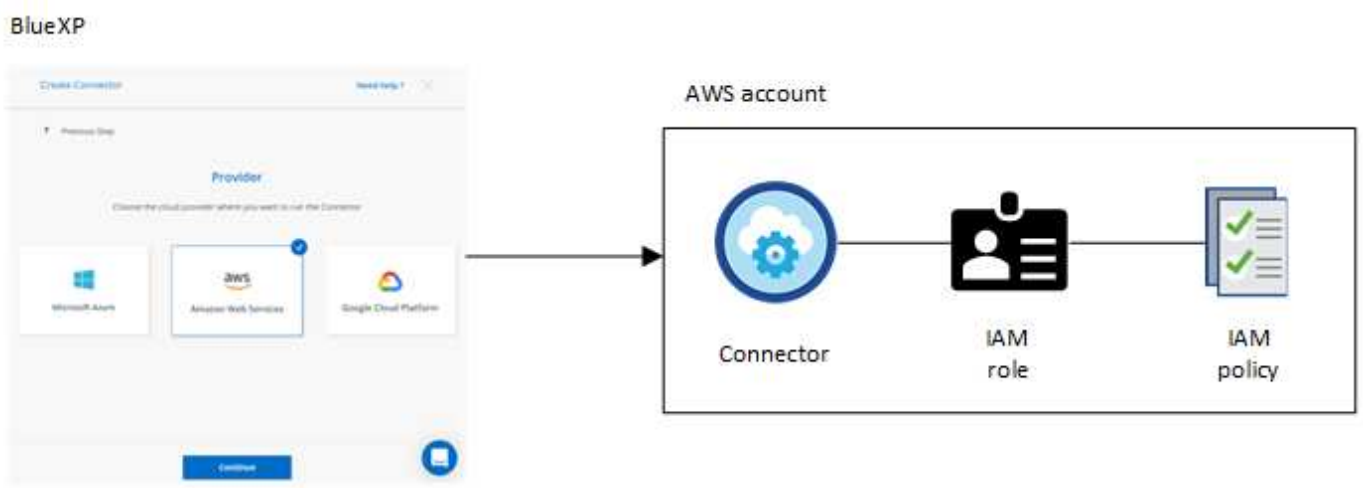
Obtenga información sobre las credenciales y permisos de AWS en BlueXP

Descubre cómo BlueXP utiliza las credenciales de AWS para realizar acciones en tu nombre y cómo esas credenciales están asociadas a las suscripciones del mercado. Comprender estos detalles puede resultar útil a la hora de gestionar las credenciales de una o más cuentas de AWS en BlueXP. Por ejemplo, quizás quieras saber cuándo añadir más credenciales de AWS a BlueXP.

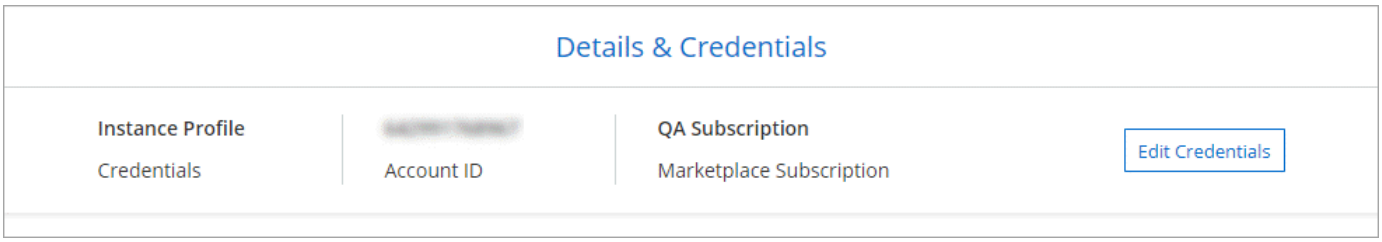
Credenciales iniciales de AWS

Al implantar un conector de BlueXP, debe proporcionar el ARN de una función de IAM o claves de acceso para un usuario de IAM. El método de autenticación que utilice debe tener los permisos necesarios para implementar la instancia de Connector en AWS. Los permisos necesarios se enumeran en la "La política de implementación de conectores para AWS".

Cuando BlueXP inicia la instancia de Connector en AWS, crea una función IAM y un perfil de instancia para la instancia. También adjunta una directiva que proporciona al conector permisos para administrar recursos y procesos dentro de esa cuenta de AWS. "Revise cómo BlueXP utiliza los permisos".



Si creas un nuevo entorno de trabajo para Cloud Volumes ONTAP, BlueXP selecciona estas credenciales de AWS de forma predeterminada:



Puede implementar todos sus sistemas Cloud Volumes ONTAP con las credenciales iniciales de AWS o bien añadir credenciales adicionales.

Credenciales adicionales de AWS

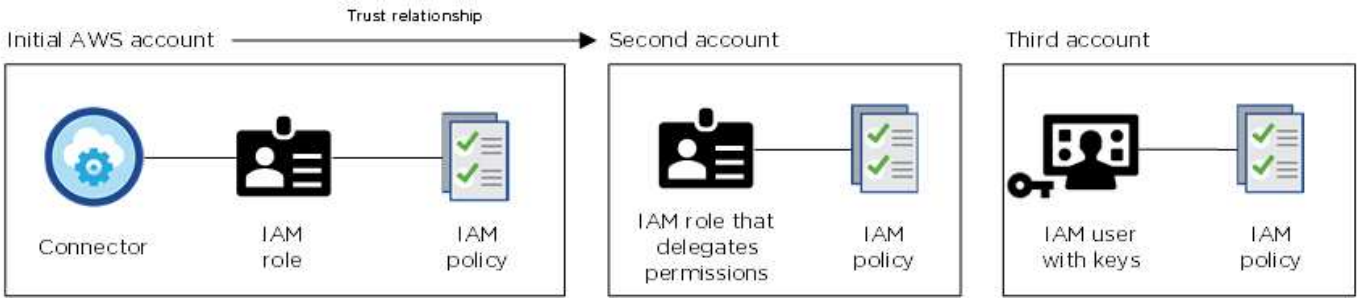
Puede añadir credenciales de AWS adicionales en BlueXP en los siguientes casos:

- Para utilizar su conector BlueXP existente con una cuenta de AWS adicional
- Para crear un nuevo conector en una cuenta de AWS específica
- Para crear y gestionar sistemas de archivos FSx para ONTAP

Revise las secciones siguientes para obtener más información.

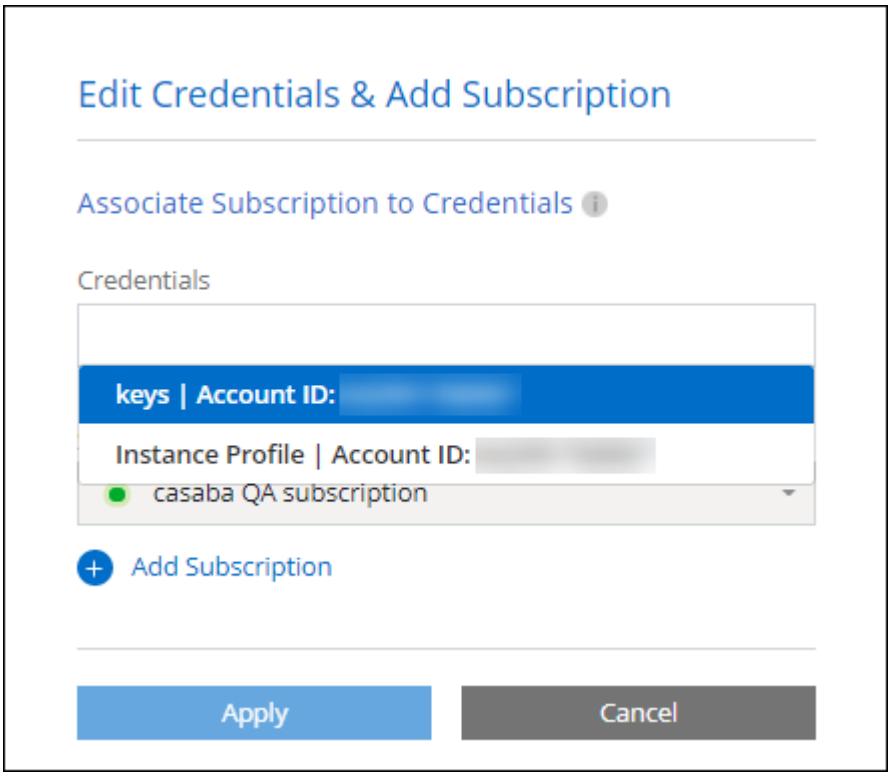
Agregue las credenciales de AWS para usar un conector con otra cuenta de AWS

Si desea usar BlueXP con cuentas adicionales de AWS, puede proporcionar claves de AWS para un usuario de IAM o el ARN de un rol en una cuenta de confianza. En la siguiente imagen se muestran dos cuentas adicionales, una que proporciona permisos a través de una función IAM en una cuenta de confianza y otra a través de las claves AWS de un usuario de IAM:



A continuación, se agregarían las credenciales de cuenta a BlueXP especificando el nombre de recurso de Amazon (ARN) del rol IAM o las claves de AWS del usuario de IAM.

Por ejemplo, es posible cambiar entre credenciales al crear un nuevo entorno de trabajo Cloud Volumes ONTAP:



"Aprenda a añadir credenciales de AWS a un conector existente."

Agregue las credenciales de AWS para crear un conector

Agregar nuevas credenciales de AWS a BlueXP proporciona los permisos necesarios para crear un conector.

"Aprenda a añadir credenciales de AWS a BlueXP para crear un conector"

Añade las credenciales de AWS para FSx para ONTAP

Añadir nuevas credenciales de AWS a BlueXP proporciona los permisos necesarios para crear y gestionar un entorno de trabajo de FSx para ONTAP.

"Aprenda a añadir credenciales de AWS a BlueXP para Amazon FSX para ONTAP"

Credenciales y suscripciones de Marketplace

Las credenciales que añadas a un conector deben estar asociadas a una suscripción de AWS Marketplace para que puedas pagar por Cloud Volumes ONTAP a una tarifa por hora (PAYGO) o a través de un contrato anual, así como para utilizar otros servicios de BlueXP.

"Aprenda a asociar una suscripción a AWS".

Tenga en cuenta lo siguiente acerca de las credenciales de AWS y las suscripciones al mercado:

- Solo se puede asociar una suscripción de AWS Marketplace a un conjunto de credenciales de AWS
- Puede reemplazar una suscripción existente de Marketplace por una nueva

PREGUNTAS FRECUENTES

Las siguientes preguntas están relacionadas con las credenciales y suscripciones.

¿Cómo puedo rotar mis credenciales de AWS de forma segura?

Como se describe en las secciones anteriores, BlueXP le permite proporcionar credenciales de AWS de varias formas: Un rol de IAM asociado a la instancia de Connector, asumiendo un rol de IAM en una cuenta de confianza o proporcionando claves de acceso de AWS.

Con las dos primeras opciones, BlueXP utiliza el Servicio de token de seguridad de AWS para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica, es automático y seguro.

Si proporciona a BlueXP claves de acceso de AWS, debe rotar las claves actualizándolas en BlueXP a intervalos regulares. Este es un proceso completamente manual.

¿Puedo cambiar la suscripción de AWS Marketplace para entornos de trabajo de Cloud Volumes ONTAP?

Sí, puedes. Al cambiar la suscripción de AWS Marketplace asociada a un conjunto de credenciales, todos los entornos de trabajo de Cloud Volumes ONTAP existentes y nuevos se cargarán con la nueva suscripción.

"Aprenda a asociar una suscripción a AWS".

¿Puedo añadir varias credenciales de AWS, cada una con diferentes suscripciones del mercado?

Todas las credenciales de AWS que pertenezcan a la misma cuenta de AWS se asociarán a la misma suscripción de AWS Marketplace.

Si tiene varias credenciales de AWS que pertenecen a diferentes cuentas de AWS, esas credenciales se pueden asociar con la misma suscripción de AWS Marketplace o con diferentes suscripciones.

¿Puedo mover entornos de trabajo existentes de Cloud Volumes ONTAP a otra cuenta de AWS?

No, no es posible mover los recursos de AWS asociados con su entorno de trabajo de Cloud Volumes ONTAP a una cuenta de AWS diferente.

¿Cómo funcionan las credenciales para las implementaciones del mercado y las implementaciones locales?

En las secciones anteriores se describe el método de implementación recomendado para el conector, que es

de BlueXP. También puede poner en marcha un conector en AWS desde AWS Marketplace y puede instalar manualmente el software del conector en su propio host Linux.

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Solo tiene que crear y configurar manualmente el rol IAM y, a continuación, proporcionar permisos para cualquier cuenta adicional.

En las implementaciones locales, no se puede configurar la función de IAM para el sistema BlueXP, pero se pueden proporcionar permisos con las claves de acceso de AWS.

Para aprender a configurar los permisos, consulte las siguientes páginas:

- Modo estándar
  - "Configure los permisos para una puesta en marcha de AWS Marketplace"
  - "Configurar permisos para implementaciones locales"
- "Configure los permisos para el modo restringido"
- "Configurar permisos para el modo privado"

Gestiona las credenciales y las suscripciones del mercado de AWS para BlueXP

Agregue y administre las credenciales de AWS para poder implementar y administrar recursos en la nube en sus cuentas de AWS desde BlueXP. Si administra varias suscripciones a AWS Marketplace, puede asignar cada una de ellas a diferentes credenciales de AWS desde la página Credentials.

Descripción general

Puede añadir credenciales de AWS a un conector existente o directamente a BlueXP:

- Agregue credenciales de AWS adicionales a un conector existente

  Agregue credenciales de AWS a un conector para administrar recursos en su entorno de nube. Aprenda a añadir credenciales de AWS a un conector.

- Añada las credenciales de AWS a BlueXP para crear un conector

  La adición de nuevas credenciales de AWS a BlueXP proporciona a BlueXP los permisos necesarios para crear un conector. Aprenda a añadir credenciales de AWS a BlueXP.

- Añada credenciales de AWS a BlueXP para FSX para ONTAP

  Agregue nuevas credenciales de AWS a BlueXP para crear y administrar FSx para ONTAP. "Aprenda a configurar permisos para FSX para ONTAP"

Cómo rotar credenciales

BlueXP le permite proporcionar credenciales de AWS de varias maneras: Una función IAM asociada a la instancia de Connector, asumiendo un rol IAM en una cuenta de confianza o proporcionando claves de acceso de AWS. "Obtenga más información acerca de las credenciales y permisos de AWS".

Con las dos primeras opciones, BlueXP utiliza el Servicio de token de seguridad de AWS para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica porque es automático y seguro.

Rote las claves de acceso de AWS periódicamente actualizándolas en BlueXP. Este proceso es manual.

Agregar credenciales adicionales a un conector

Añada credenciales de AWS adicionales a un conector para que tenga los permisos necesarios para gestionar recursos y procesos en su entorno de cloud público. Puede proporcionar el ARN de un rol IAM en otra cuenta o proporcionar claves de acceso de AWS.

Si acaba de empezar a utilizar BlueXP, "Descubra cómo BlueXP usa credenciales y permisos de AWS".

Conceder permisos

Proporcione los permisos necesarios antes de agregar credenciales de AWS a un conector. Estos permisos permiten que el conector administre recursos y procesos dentro de esa cuenta de AWS. Puede proporcionar los permisos con el ARN de un rol en una cuenta de confianza o con claves de AWS.

> Si implementó un conector desde BlueXP, BlueXP agregó automáticamente credenciales de AWS para la cuenta en la que implementó el conector. Esto garantiza que se cuente con los permisos necesarios para administrar los recursos. "Obtenga más información acerca de los permisos y credenciales de AWS".

opciones

- Conceda permisos asumiendo una función IAM en otra cuenta
- Conceda permisos proporcionando claves AWS

Conceda permisos asumiendo una función IAM en otra cuenta

Puede configurar una relación de confianza entre la cuenta AWS de origen en la que ha implementado la instancia de Connector y otras cuentas de AWS mediante los roles IAM. A continuación, debe proporcionar a BlueXP el ARN de las funciones de IAM de las cuentas de confianza.

Si el conector está instalado en las instalaciones, no puede utilizar este método de autenticación. Debe usar claves AWS.

Pasos

1. Vaya a la consola IAM de la cuenta de destino en la que desea proporcionar permisos al conector.
2. En Access Management, seleccione **roles > Crear función** y siga los pasos para crear la función.

   No olvide hacer lo siguiente:

   - En **Tipo de entidad de confianza**, seleccione **cuenta de AWS**.
   - Seleccione **otra cuenta de AWS** e introduzca el ID de la cuenta en la que reside la instancia de Connector.
   - Cree las directivas necesarias copiando y pegando el contenido de "Políticas de IAM para el conector".
3. Copie el rol ARN del rol IAM para que pueda pegarlo en BlueXP más adelante.

Resultado

La cuenta ahora tiene los permisos necesarios. Ahora puede agregar las credenciales a un conector.

Conceda permisos proporcionando claves AWS

Si desea proporcionar BlueXP con claves AWS para un usuario de IAM, debe conceder los permisos necesarios a ese usuario. La política IAM de BlueXP define las acciones y los recursos de AWS que BlueXP puede utilizar.

Debe utilizar este método de autenticación si el conector está instalado en las instalaciones. No se puede utilizar la función IAM.

Pasos

1. Desde la consola IAM, cree directivas copiando y pegando el contenido de "Políticas de IAM para el conector".

   "Documentación de AWS: Crear políticas de IAM"

2. Asocie las políticas a un rol de IAM o a un usuario de IAM.
   - "Documentación de AWS: Crear roles de IAM"
   - "Documentación de AWS: Adición y eliminación de políticas de IAM"

Resultado

La cuenta ahora tiene los permisos necesarios. Ahora puede agregar las credenciales a un conector.

Añada las credenciales

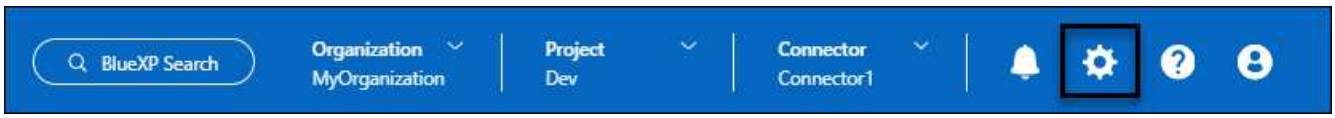
Después de proporcionar una cuenta de AWS con los permisos necesarios, puede agregar las credenciales de esa cuenta a un conector existente. Esto permite iniciar sistemas Cloud Volumes ONTAP en esa cuenta con el mismo conector.

Antes de empezar

Si acaba de crear estas credenciales en su proveedor de cloud, es posible que transcurran unos minutos hasta que estén disponibles para su uso. Espere unos minutos y luego agregue las credenciales.

Pasos

1. Utilice la barra de navegación superior para elegir el Conector al que desea agregar credenciales.
2. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.



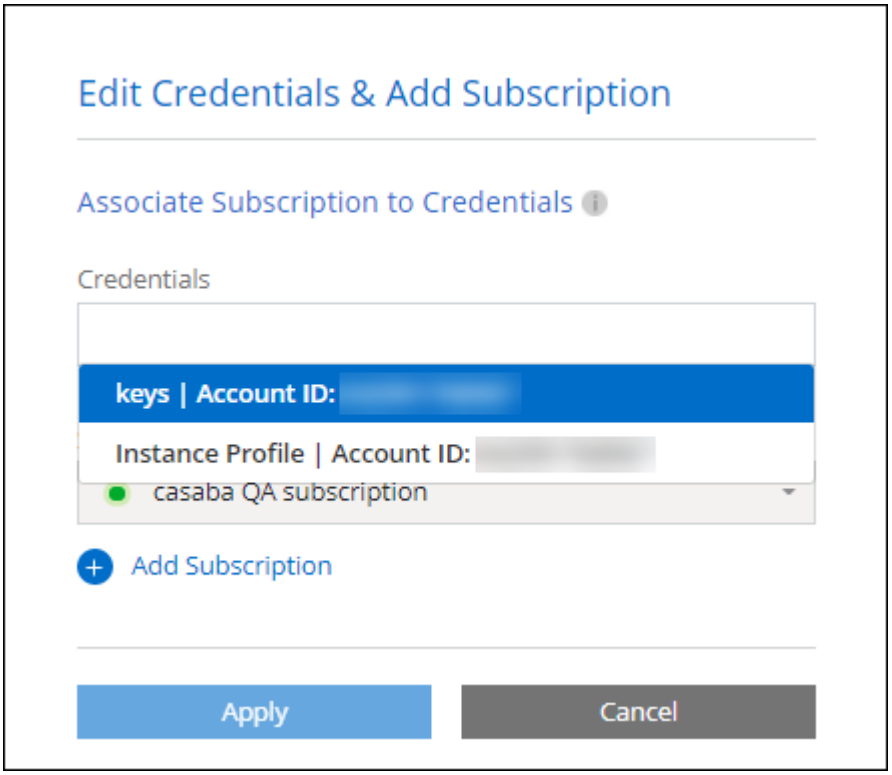
3. En la página **Credenciales de la organización** o **Credenciales de la cuenta**, selecciona **Añadir Credenciales** y sigue los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Servicios Web de Amazon > conector**.
   b. **Definir credenciales**: Proporcione el ARN (nombre de recurso de Amazon) de una función de IAM de confianza, o introduzca una clave de acceso de AWS y una clave secreta.
   c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

      Para pagar servicios a una tarifa por hora (PAYGO) o con un contrato anual, debe asociar las credenciales de AWS con su suscripción a AWS Marketplace.

d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

Ahora puede cambiar a un conjunto de credenciales diferente de la página Details y Credentials al crear un nuevo entorno de trabajo:



Agregar credenciales a BlueXP para crear un conector

Agregue credenciales de AWS proporcionando el ARN de una función de IAM que otorga los permisos necesarios para crear un conector. Puede elegir estas credenciales al crear un conector nuevo.

Configure el rol IAM

Configure un rol de IAM que permita a la capa de software como servicio (SaaS) de BlueXP asumir el rol.

Pasos

1. Vaya a la consola IAM de la cuenta de destino.
2. En Access Management, seleccione **roles > Crear función** y siga los pasos para crear la función.

   No olvide hacer lo siguiente:

   - En **Tipo de entidad de confianza**, seleccione **cuenta de AWS**.
   - Seleccione **otra cuenta de AWS** e introduzca el ID del SaaS BlueXP: 952013314444
   - Específicamente para Amazon FSx for NetApp ONTAP , edite la política **Relaciones de confianza** para incluir "AWS": "arn:aws:iam::952013314444:root".

     Por ejemplo, la política debería verse así:

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

+
Referirse a "Documentación de AWS Identity and Access Management (IAM)" para obtener más información sobre el acceso a recursos entre cuentas en IAM.

- Cree una directiva que incluya los permisos necesarios para crear un conector.
  - "Consulte los permisos necesarios para FSX para ONTAP"
  - "Ver la directiva de despliegue del conector"

3. Copie el rol ARN de la función IAM para que pueda pegarlo en BlueXP en el siguiente paso.

Resultado

El rol IAM ahora tiene los permisos necesarios. Ahora puede agregarla a BlueXP.

Añada las credenciales

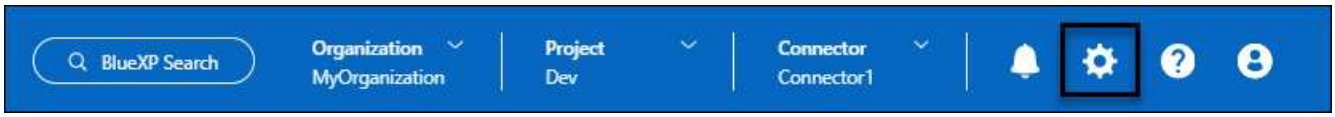
Después de proporcionar la función IAM con los permisos necesarios, agregue el rol ARN a BlueXP.

Antes de empezar

Si acaba de crear la función IAM, puede tardar unos minutos en estar disponible. Espere unos minutos antes de agregar las credenciales a BlueXP.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.



2. En la página **Credenciales de la organización** o **Credenciales de la cuenta**, selecciona **Añadir Credenciales** y sigue los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Servicios Web de Amazon > BlueXP**.
   b. **Definir credenciales**: Proporcionar el ARN (nombre de recurso de Amazon) de la función IAM.
   c. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Añada credenciales a BlueXP para Amazon FSX para ONTAP

Para obtener más información, consulte "Documentación de BlueXP para Amazon FSX para ONTAP"

Configure una suscripción a AWS

Después de agregar sus credenciales de AWS, puede configurar una suscripción a AWS Marketplace con ellas. Esta suscripción le permite pagar Cloud Volumes ONTAP por hora (PAYGO) o con un contrato anual, así como otros servicios de datos.

Hay dos escenarios en los que podrías configurar una suscripción a AWS Marketplace después de haber agregado las credenciales:

- No configuró una suscripción cuando agregó las credenciales inicialmente.
- Desea cambiar la suscripción de AWS Marketplace que está configurada para las credenciales de AWS.

  La sustitución de la suscripción actual del mercado por una nueva suscripción cambia la suscripción del mercado para cualquier entorno de trabajo existente de Cloud Volumes ONTAP y todos los nuevos entornos de trabajo.

Antes de empezar

Debe crear un conector antes de poder configurar una suscripción. "Aprenda a crear un conector".

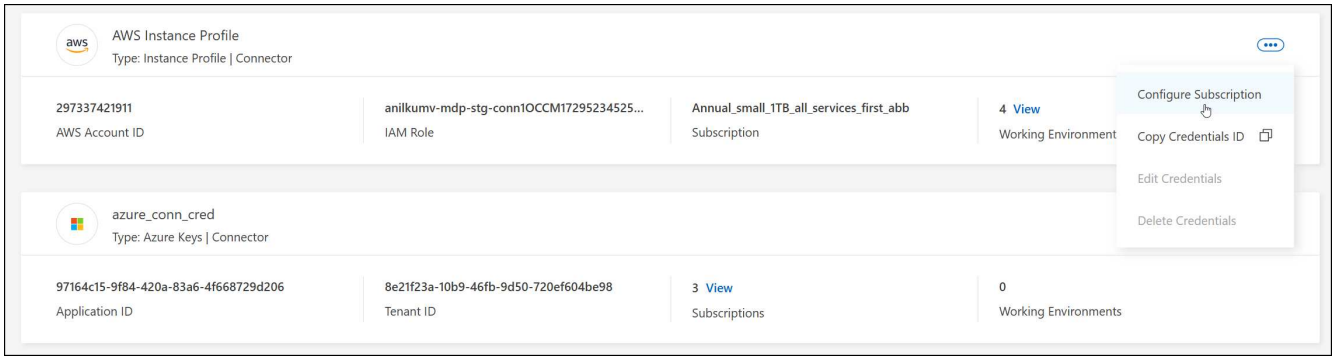
El siguiente vídeo muestra los pasos para suscribirse a NetApp Intelligent Services desde AWS Marketplace:

Suscríbase a NetApp Intelligent Services desde AWS Marketplace

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Configurar suscripción**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción de la lista desplegable y seleccione **Configurar**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos del AWS Marketplace:

   a. Seleccione **Ver opciones de compra**.

b. Seleccione **Suscribirse**.

c. Seleccione **Configurar su cuenta**.

   Se le redirigirá al sitio web de BlueXP.

d. Desde la página **asignación de suscripción**:

   - Seleccione las organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
   - En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

     BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

Asocie una suscripción existente a su organización o cuenta

Al suscribirse desde AWS Marketplace, el último paso del proceso es asociar la suscripción con su organización. Si no completó este paso, no podrá usar la suscripción con su organización ni cuenta.

- "Obtenga más información sobre los modos de implementación de BlueXP"
- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "

Siga los pasos a continuación si se suscribió a los servicios de datos inteligentes de NetApp desde AWS Marketplace, pero omitió el paso para asociar la suscripción con su cuenta.

Pasos

1. Vaya a la billetera digital para confirmar que no asoció su suscripción con su organización o cuenta de BlueXP.

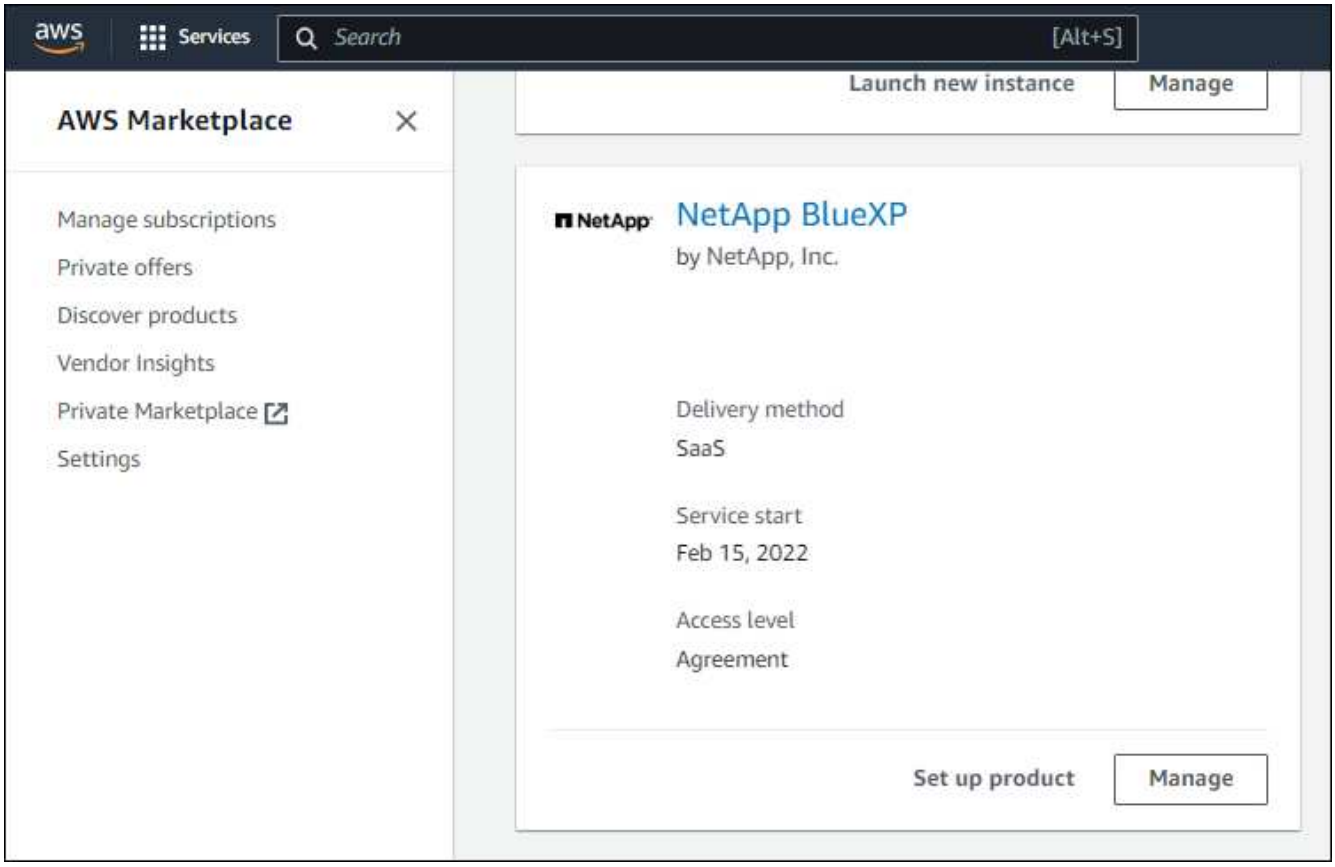
   a. Desde el menú de navegación, seleccione **Gobernanza > Billetera digital**.

   b. Seleccione **Suscripciones**.

   c. Verifica que tu suscripción no aparezca.

      Solo verá las suscripciones asociadas a la organización o cuenta que está visualizando en ese momento. Si no ve su suscripción, continúe con los siguientes pasos.

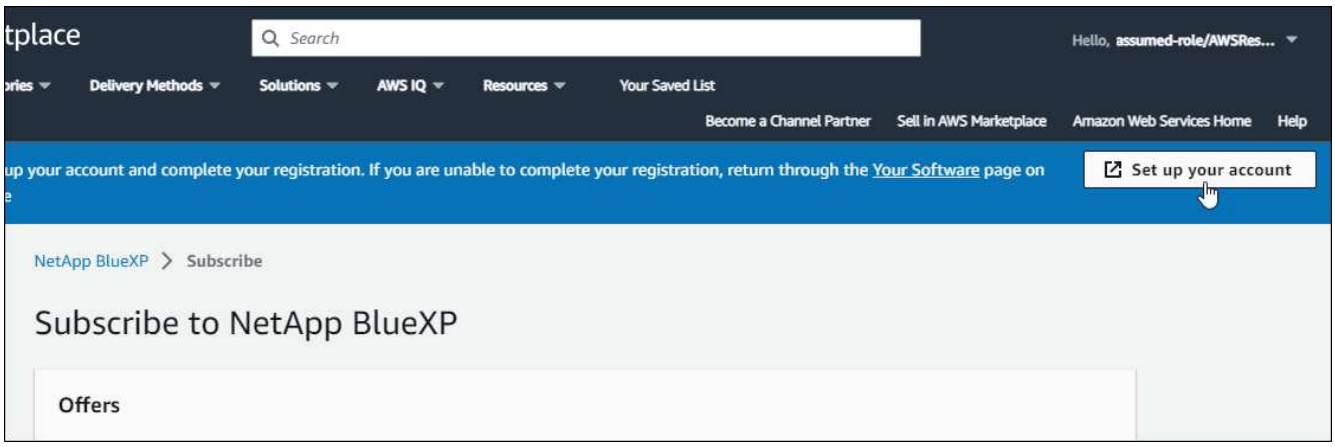
2. Inicie sesión en la consola de AWS y vaya a * Suscripciones de AWS Marketplace *.
3. Encuentre la suscripción a NetApp Intelligent Data Services.



4. Seleccione **Set up product**.

   La página de oferta de suscripción debe cargarse en una nueva pestaña o ventana del navegador.

5. Seleccione **Configurar su cuenta**.



   La página **Suscripción** en netapp.com debe cargarse en una nueva pestaña o ventana del navegador.

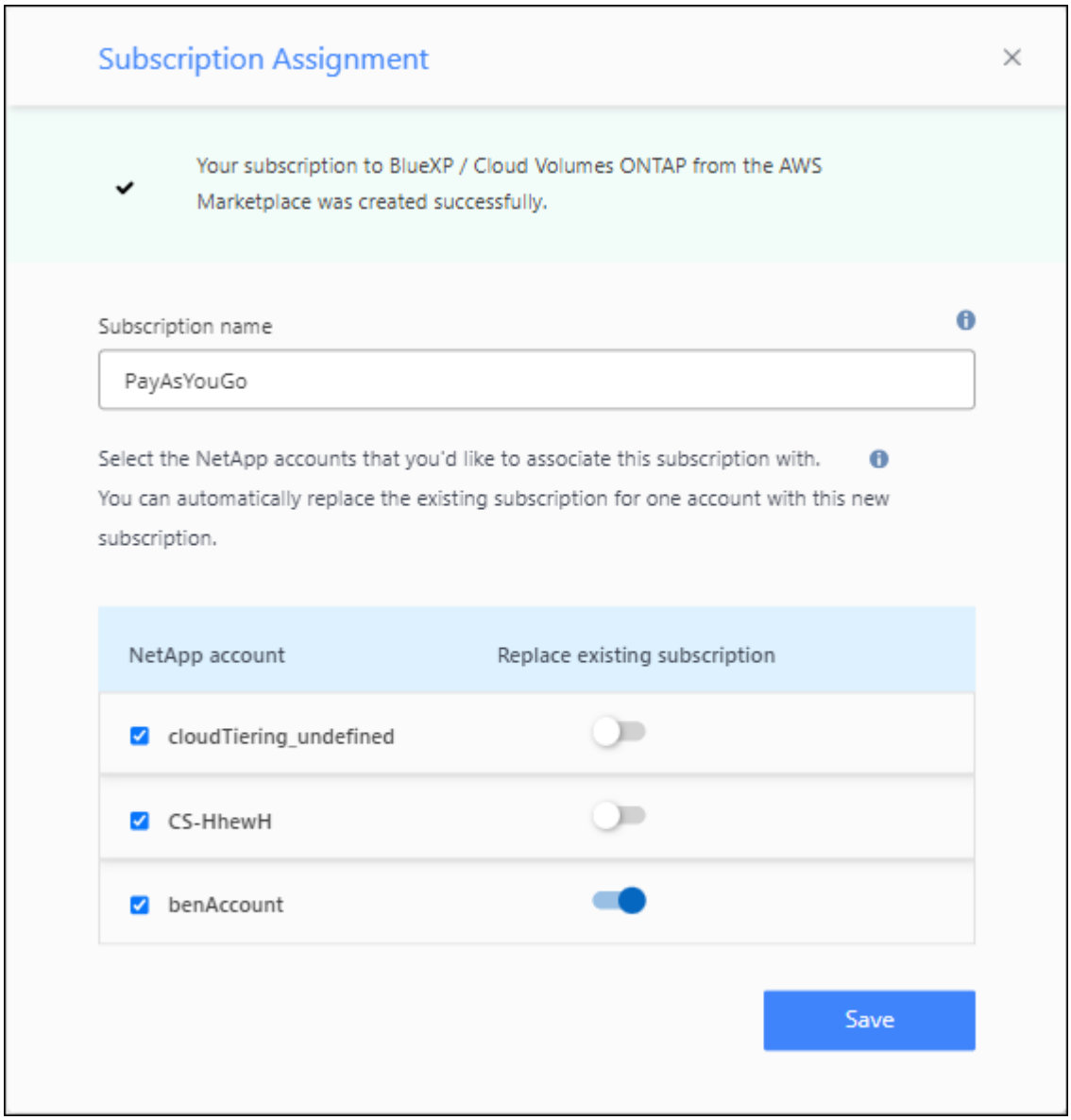
   Ten en cuenta que es posible que se te pida iniciar sesión en BlueXP primero.

6. Desde la página **asignación de suscripción**:

   - Seleccione las organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
   - En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

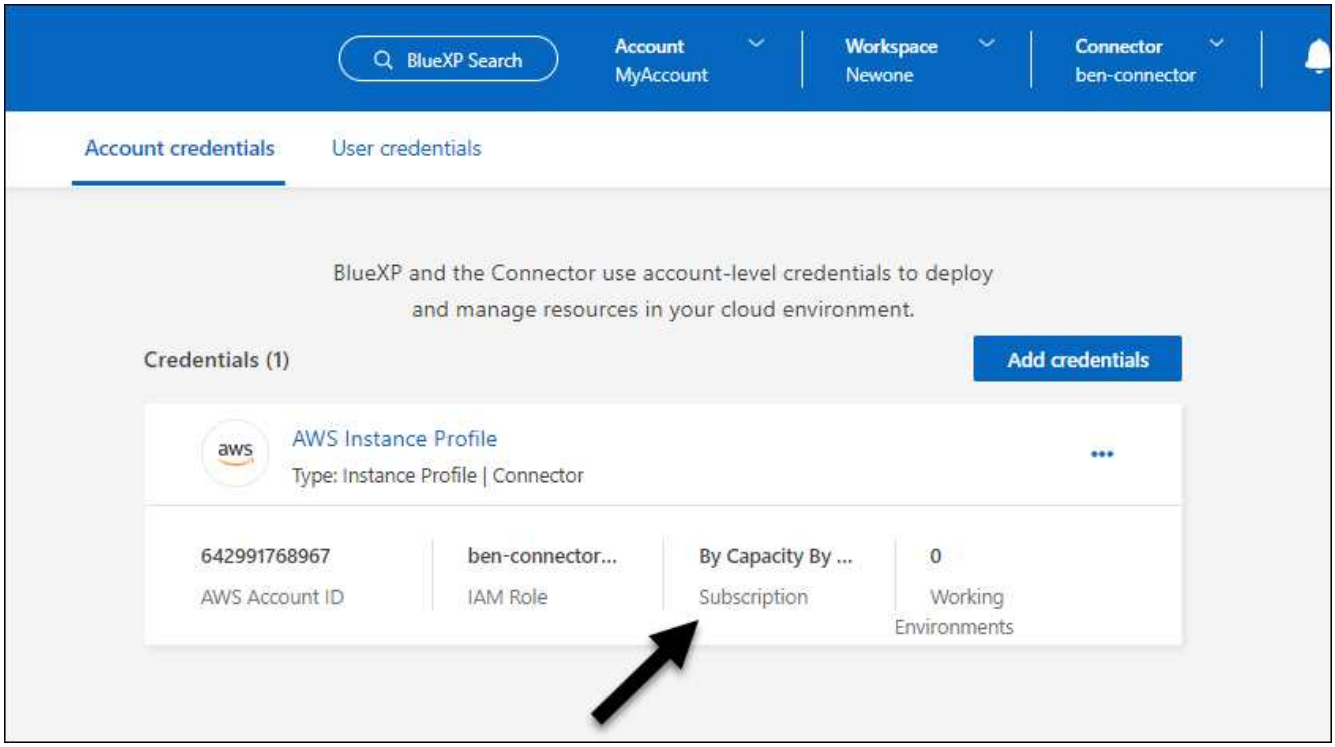
BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.



7. Vaya a la billetera digital para confirmar que la suscripción esté asociada a su organización o cuenta.
   a. Desde el menú de navegación, seleccione **Gobernanza > Billetera digital**.
   b. Seleccione **Suscripciones**.
   c. Verifica que aparezca tu suscripción.
8. Confirme que la suscripción está asociada a sus credenciales de AWS.
   a. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.
   b. En la página **Credenciales de la organización** o **Credenciales de la cuenta**, verifique que la suscripción esté asociada a sus credenciales de AWS.

Veamos un ejemplo.



Editar credenciales

Edite sus credenciales de AWS cambiando el tipo de cuenta (claves de AWS o asumir rol), editando el nombre o actualizando las credenciales en sí (las claves o el ARN del rol).

> No puede editar las credenciales de un perfil de instancia que esté asociado con una instancia de Connector o una instancia de Amazon FSx para ONTAP. Solo puede cambiar el nombre de las credenciales de una instancia de FSx para ONTAP.

Pasos

1. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.
2. En la página **Credenciales de la organización** o **Credenciales de la cuenta**, selecciona el menú de acción para un conjunto de credenciales y luego selecciona **Editar Credenciales**.
3. Realice los cambios necesarios y, a continuación, seleccione **aplicar**.

Eliminar credenciales

Si ya no necesita un conjunto de credenciales, puede eliminarlas. Sólo puede eliminar credenciales que no estén asociadas a un entorno de trabajo.

> No se pueden eliminar las credenciales de un perfil de instancia asociado a una instancia de conector.

Pasos

1. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.
2. En la página **Credenciales de la organización** o **Credenciales de la cuenta**, selecciona el menú de acción para un conjunto de credenciales y luego selecciona **Eliminar Credenciales**.

3. Seleccione **Eliminar** para confirmar.

Azure

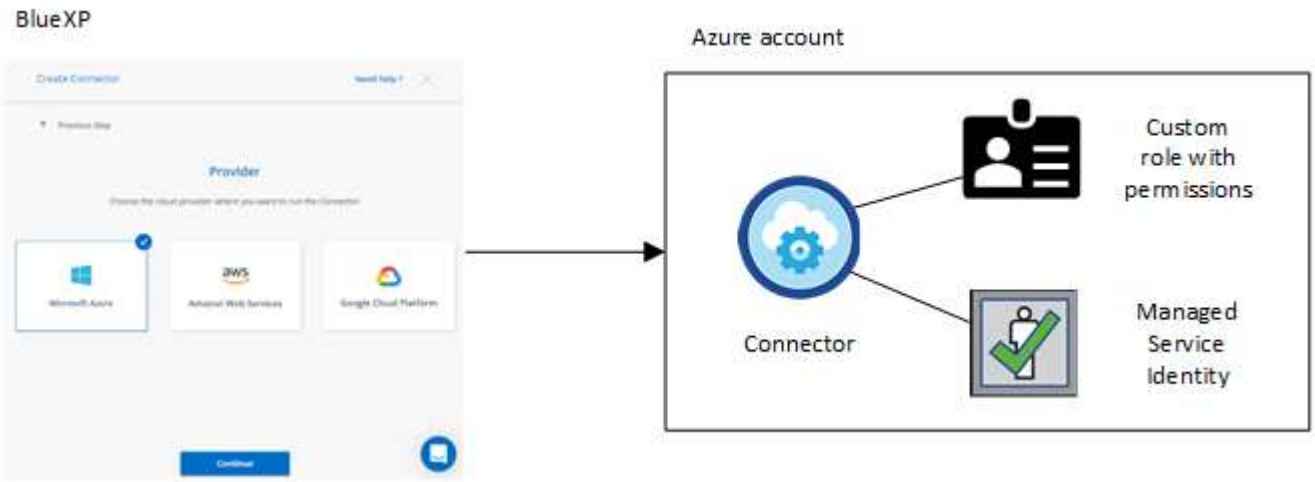
Obtenga información sobre las credenciales y los permisos de Azure en BlueXP

Descubre cómo BlueXP utiliza las credenciales de Azure para realizar acciones en tu nombre y cómo esas credenciales están asociadas a las suscripciones del mercado. Comprender estos detalles puede resultar útil cuando gestionas las credenciales de una o más suscripciones a Azure. Por ejemplo, quizás quieras saber cuándo añadir credenciales de Azure adicionales en BlueXP.

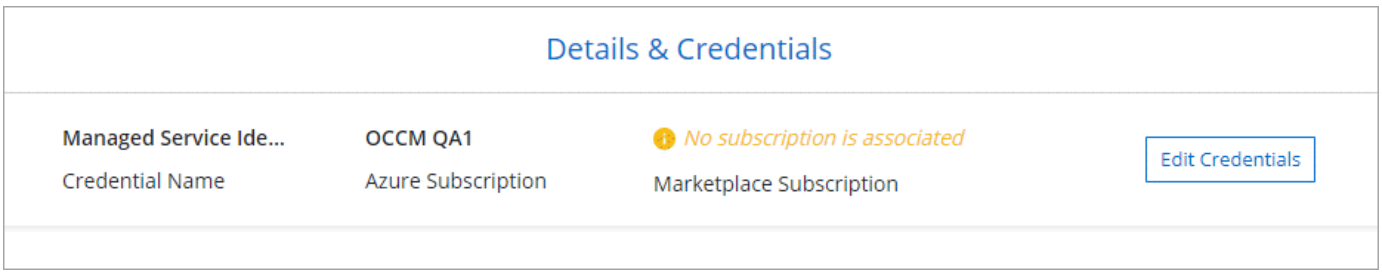
Credenciales iniciales de Azure

Al implementar un conector desde BlueXP, necesita utilizar una cuenta de Azure o una entidad de servicio con permisos para implementar la máquina virtual Connector. Los permisos necesarios se muestran en la "Política de implementación de conectores para Azure".

Cuando BlueXP implementa la máquina virtual Connector en Azure, habilita una en la máquina virtual, crea un "identidad administrada asignada por el sistema" rol personalizado y la asigna a la máquina virtual. La función proporciona a BlueXP los permisos necesarios para gestionar recursos y procesos dentro de esa suscripción a Azure. "Revise cómo BlueXP utiliza los permisos".



Si creas un nuevo entorno de trabajo para Cloud Volumes ONTAP, BlueXP selecciona estas credenciales de Azure de forma predeterminada:



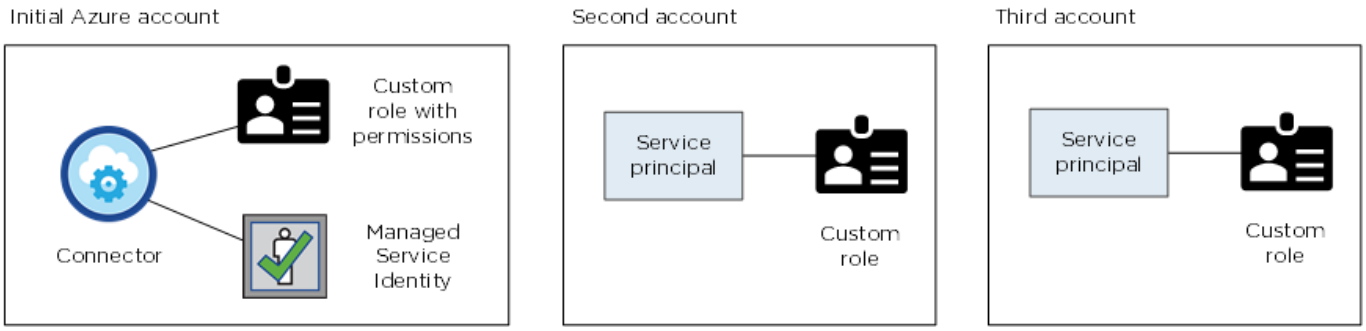
Puede poner en marcha todos los sistemas de Cloud Volumes ONTAP con las credenciales iniciales de Azure o bien añadir credenciales adicionales.

Suscripciones adicionales de Azure para una identidad gestionada

La identidad administrada asignada por el sistema asignada a la máquina virtual del conector está asociada a la suscripción en la que inició el conector. Si desea seleccionar una suscripción de Azure diferente, tendrá que hacerlo "asocie la identidad administrada a esas suscripciones".

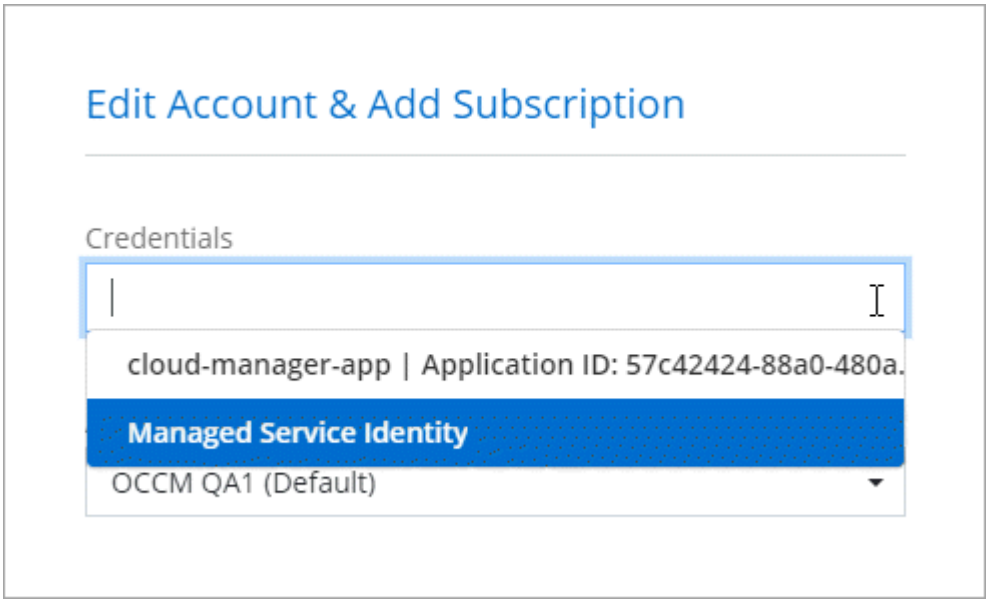
Credenciales adicionales de Azure

Si desea utilizar diferentes credenciales de Azure con BlueXP, debe conceder los permisos necesarios mediante "Creación y configuración de un principal de servicio en Microsoft Entra ID" Para cada cuenta de Azure. La siguiente imagen muestra dos cuentas adicionales, cada una configurada con una función personalizada y principal de servicio que proporciona permisos:



Entonces lo haría "Agregue las credenciales de cuenta a BlueXP" Proporcionando detalles acerca del director de servicio de AD.

Por ejemplo, es posible cambiar entre credenciales al crear un nuevo entorno de trabajo Cloud Volumes ONTAP:



Credenciales y suscripciones de Marketplace

Las credenciales que añadas a un conector deben estar asociadas a una suscripción a Azure Marketplace para que puedas pagar por Cloud Volumes ONTAP a una tarifa por hora (PAYGO) o a través de un contrato anual, y para utilizar otros servicios de BlueXP.

"Aprenda a asociar una suscripción a Azure".

Tenga en cuenta lo siguiente acerca de las credenciales de Azure y las suscripciones a Marketplace:

- Solo puede asociar una suscripción de Azure Marketplace a un conjunto de credenciales de Azure
- Puede reemplazar una suscripción existente de Marketplace por una nueva

PREGUNTAS FRECUENTES

La siguiente pregunta está relacionada con las credenciales y suscripciones.

¿Puedo cambiar la suscripción a Azure Marketplace para entornos de trabajo de Cloud Volumes ONTAP?

Sí, puedes. Al cambiar la suscripción de Azure Marketplace asociada a un conjunto de credenciales de Azure, todos los entornos de trabajo de Cloud Volumes ONTAP existentes y nuevos se cargarán con la nueva suscripción.

"Aprenda a asociar una suscripción a Azure".

¿Puedo agregar varias credenciales de Azure, cada una con diferentes suscripciones del mercado?

Todas las credenciales de Azure que pertenezcan a la misma suscripción de Azure se asociarán a la misma suscripción de Azure Marketplace.

Si tiene varias credenciales de Azure que pertenecen a diferentes suscripciones de Azure, esas credenciales se pueden asociar con la misma suscripción de Azure Marketplace o con diferentes suscripciones de Marketplace.

¿Puedo mover entornos de trabajo existentes de Cloud Volumes ONTAP a una suscripción diferente a Azure?

No, no es posible mover los recursos de Azure asociados con su entorno de trabajo de Cloud Volumes ONTAP a una suscripción de Azure diferente.

¿Cómo funcionan las credenciales para las implementaciones del mercado y las implementaciones locales?

En las secciones anteriores se describe el método de implementación recomendado para el conector, que es de BlueXP. También puede poner en marcha un conector en Azure desde Azure Marketplace y puede instalar el software del conector en su propio host Linux.

Si utiliza Marketplace, puede proporcionar permisos asignando un rol personalizado a la VM de Connector y a una identidad administrada asignada por el sistema, o puede usar un principal de servicio de Microsoft Entra.

Para implementaciones en las instalaciones, no puede configurar una identidad administrada para el conector, pero puede proporcionar permisos utilizando un director de servicio.

Para aprender a configurar los permisos, consulte las siguientes páginas:

- Modo estándar
  - "Configure los permisos para una puesta en marcha de Azure Marketplace"
  - "Configurar permisos para implementaciones locales"
- "Configure los permisos para el modo restringido"
- "Configurar permisos para el modo privado"

Gestiona las credenciales de Azure y las suscripciones al mercado para BlueXP

Añada y gestione credenciales de Azure para que BlueXP tenga los permisos que necesita para implementar y gestionar recursos cloud en sus suscripciones a Azure. Si gestiona varias suscripciones a Azure Marketplace, puede asignar cada una de ellas a diferentes credenciales de Azure desde la página Credentials.

Siga los pasos que se indican en esta página si necesita utilizar varias credenciales de Azure o varias suscripciones a Azure Marketplace para Cloud Volumes ONTAP.

Descripción general

Hay dos formas de añadir credenciales y suscripciones de Azure adicionales en BlueXP.

1. Asocie las suscripciones adicionales de Azure a la identidad gestionada de Azure.
2. Si desea implementar Cloud Volumes ONTAP con diferentes credenciales de Azure, conceda permisos de Azure con un servicio principal y añada sus credenciales a BlueXP.

Asocie suscripciones adicionales de Azure a una identidad gestionada

BlueXP le permite elegir las credenciales de Azure y la suscripción a Azure en la que desee poner en marcha Cloud Volumes ONTAP. No puede seleccionar una suscripción de Azure diferente para la gestionada perfil de identidad a menos que asocie el "identidad administrada" con estas suscripciones.

Acerca de esta tarea

Una identidad administrada es "La cuenta inicial de Azure" Al desplegar un conector desde BlueXP. Cuando implementó el conector, BlueXP creó la función de operador BlueXP y la asignó a la máquina virtual Connector.

Pasos

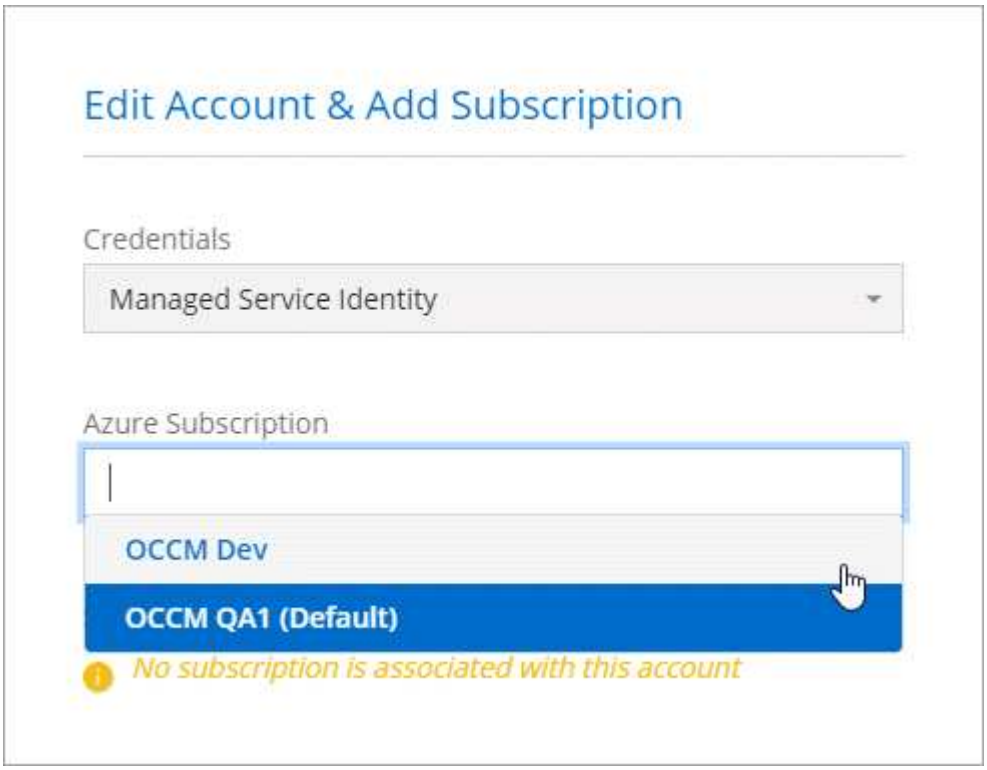
1. Inicie sesión en el portal de Azure.
2. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar Cloud Volumes ONTAP.
3. Seleccionar **Control de acceso (IAM)**.
   a. Seleccione **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos:
      - Seleccione el rol **operador de BlueXP**.

        BlueXP Operator es el nombre predeterminado que se proporciona en la directiva Connector. Si seleccionó otro nombre para el rol, seleccione ese nombre.

      - Asigne acceso a una **máquina virtual**.
      - Seleccione la suscripción en la que se creó la máquina virtual Connector.
      - Seleccione la máquina virtual conector.
      - Seleccione **Guardar**.
4. Repita estos pasos para suscripciones adicionales.

Resultado

Al crear un nuevo entorno de trabajo, ahora debe tener la posibilidad de seleccionar varias suscripciones de Azure para el perfil de identidad administrada.



Añada credenciales de Azure adicionales a BlueXP

Al implementar un conector desde BlueXP, BlueXP habilita una identidad administrada asignada por el sistema en la máquina virtual que tiene los permisos necesarios. BlueXP selecciona estas credenciales de Azure de forma predeterminada al crear un entorno de trabajo nuevo para Cloud Volumes ONTAP.

> No se agrega un conjunto inicial de credenciales si instaló manualmente el software Connector en un sistema existente. "Obtenga más información acerca de credenciales y permisos de Azure".

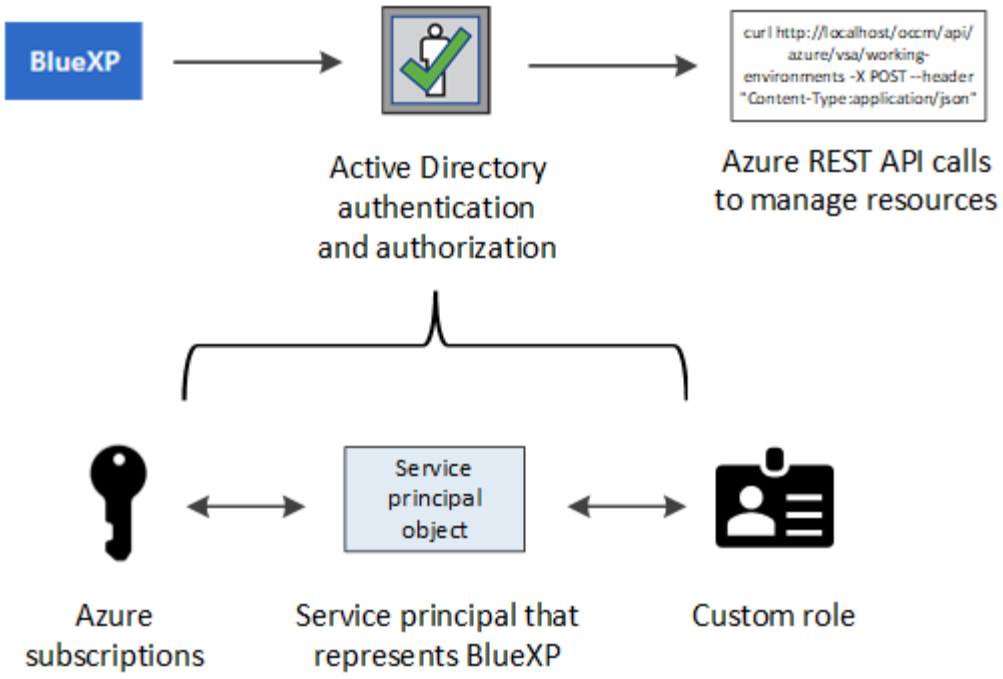
Si desea implementar Cloud Volumes ONTAP con credenciales *DIFERENTE* de Azure, debe otorgar los permisos necesarios creando y configurando un principal de servicio en Microsoft Entra ID para cada cuenta de Azure. A continuación, puede agregar las nuevas credenciales a BlueXP.

Conceda permisos de Azure con un director de servicio

BlueXP necesita permisos para realizar acciones en Azure. Puedes conceder los permisos necesarios a una cuenta de Azure creando y configurando un principal de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que necesita BlueXP.

Acerca de esta tarea

La siguiente imagen muestra cómo BlueXP obtiene permisos para realizar operaciones en Azure. Un objeto principal de servicio, vinculado a una o varias suscripciones de Azure, representa a BlueXP en Microsoft Entra ID y se asigna a un rol personalizado que permite los permisos requeridos.



Pasos

1. Cree una aplicación Microsoft Entra.
2. Asigne la aplicación a una función.
3. Añada permisos de API de administración de servicios de Windows Azure.
4. Obtener el ID de aplicación y el ID de directorio.
5. Cree un secreto de cliente.

Cree una aplicación Microsoft Entra

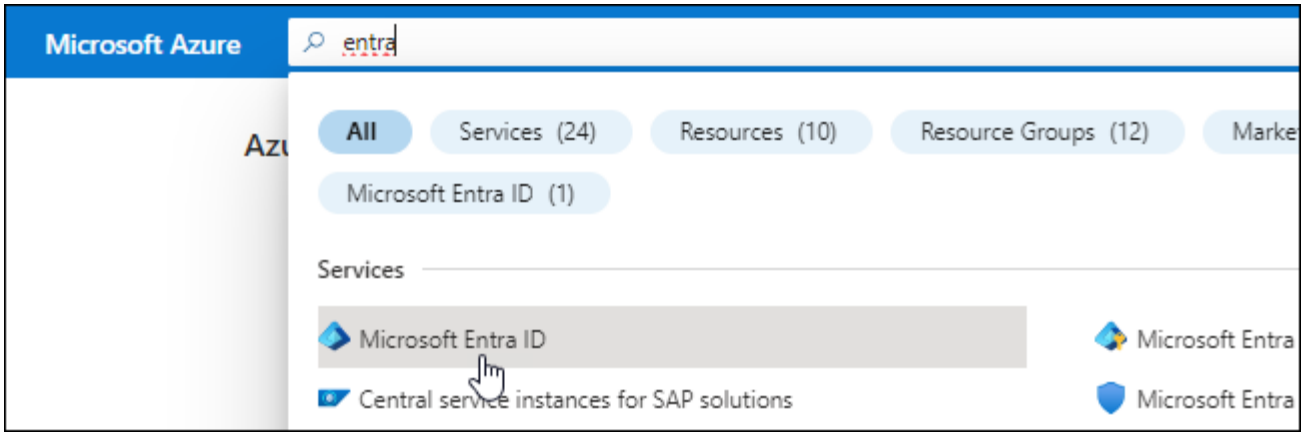
Crea una aplicación de Microsoft Entra y una entidad de servicio que BlueXP pueda utilizar para el control de acceso basado en roles.

Pasos

1. Asegúrese de tener permisos en Azure para crear una aplicación de Active Directory y para asignar la aplicación a un rol.

   Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios"

2. Desde el portal de Azure, abra el servicio **Microsoft Entra ID**.



3. En el menú, seleccione **App registrs**.
4. Seleccione **Nuevo registro**.
5. Especificar detalles acerca de la aplicación:
   - **Nombre**: Introduzca un nombre para la aplicación.
   - **Tipo de cuenta**: Seleccione un tipo de cuenta (cualquiera funcionará con BlueXP).
   - **Redirigir URI**: Puede dejar este campo en blanco.
6. Seleccione **Registrar**.

   Ha creado la aplicación AD y el director de servicio.

Resultado

Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

Debe enlazar el principal del servicio a una o más suscripciones de Azure y asignarle el rol de operador "BlueXP Operator" personalizado para que BlueXP tenga permisos en Azure.

Pasos

1. Crear un rol personalizado:

   Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

   a. Copie el contenido de "Permisos de función personalizada para el conector" Y guárdelos en un archivo JSON.

   b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

      Debe añadir el ID para cada suscripción de Azure desde la cual los usuarios crearán sistemas Cloud Volumes ONTAP.

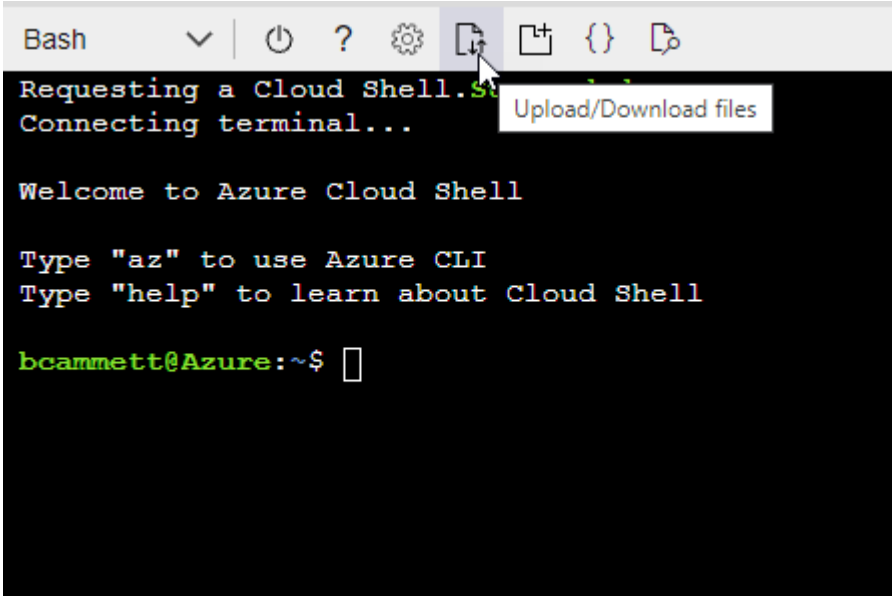
      ejemplo

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

c. Use el archivo JSON para crear una función personalizada en Azure.

En los pasos siguientes se describe cómo crear la función mediante Bash en Azure Cloud Shell.

- Comenzar "Shell de cloud de Azure" Y seleccione el entorno Bash.
- Cargue el archivo JSON.



- Use la interfaz de línea de comandos de Azure para crear el rol personalizado:

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

Ahora debe tener una función personalizada denominada operador BlueXP que puede asignar a la máquina virtual Connector.

2. Asigne la aplicación al rol:

a. En el portal de Azure, abra el servicio **Suscripciones**.

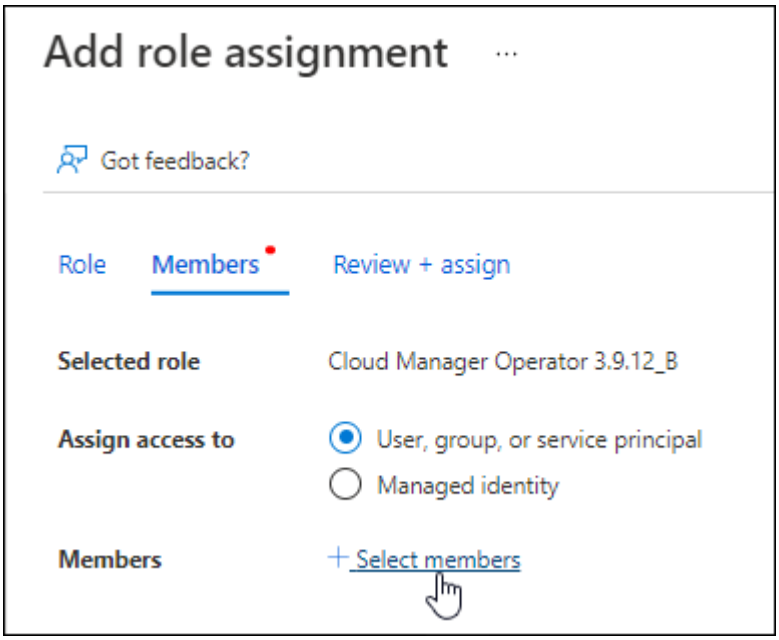
b. Seleccione la suscripción.

c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.

d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.

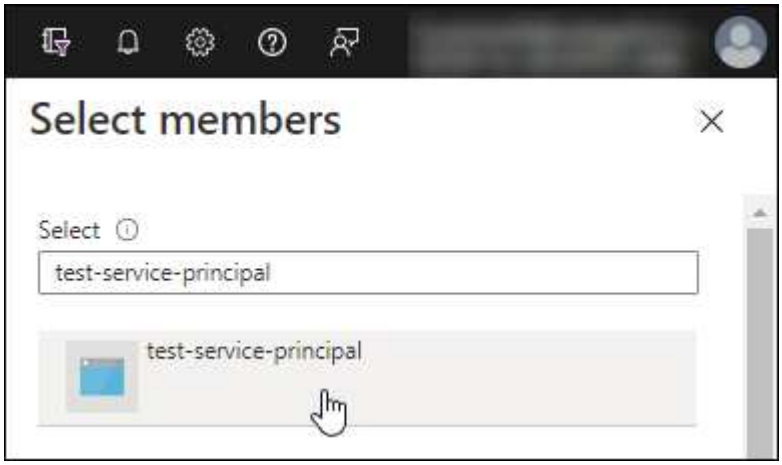
e. En la ficha **Miembros**, realice los siguientes pasos:

- Mantener seleccionado **Usuario, grupo o principal de servicio**.
- Seleccione **Seleccionar miembros**.



- Busque el nombre de la aplicación.

  Veamos un ejemplo:



- Seleccione la aplicación y seleccione **Seleccionar**.
- Seleccione **Siguiente**.

f. Seleccione **revisar + asignar**.

El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

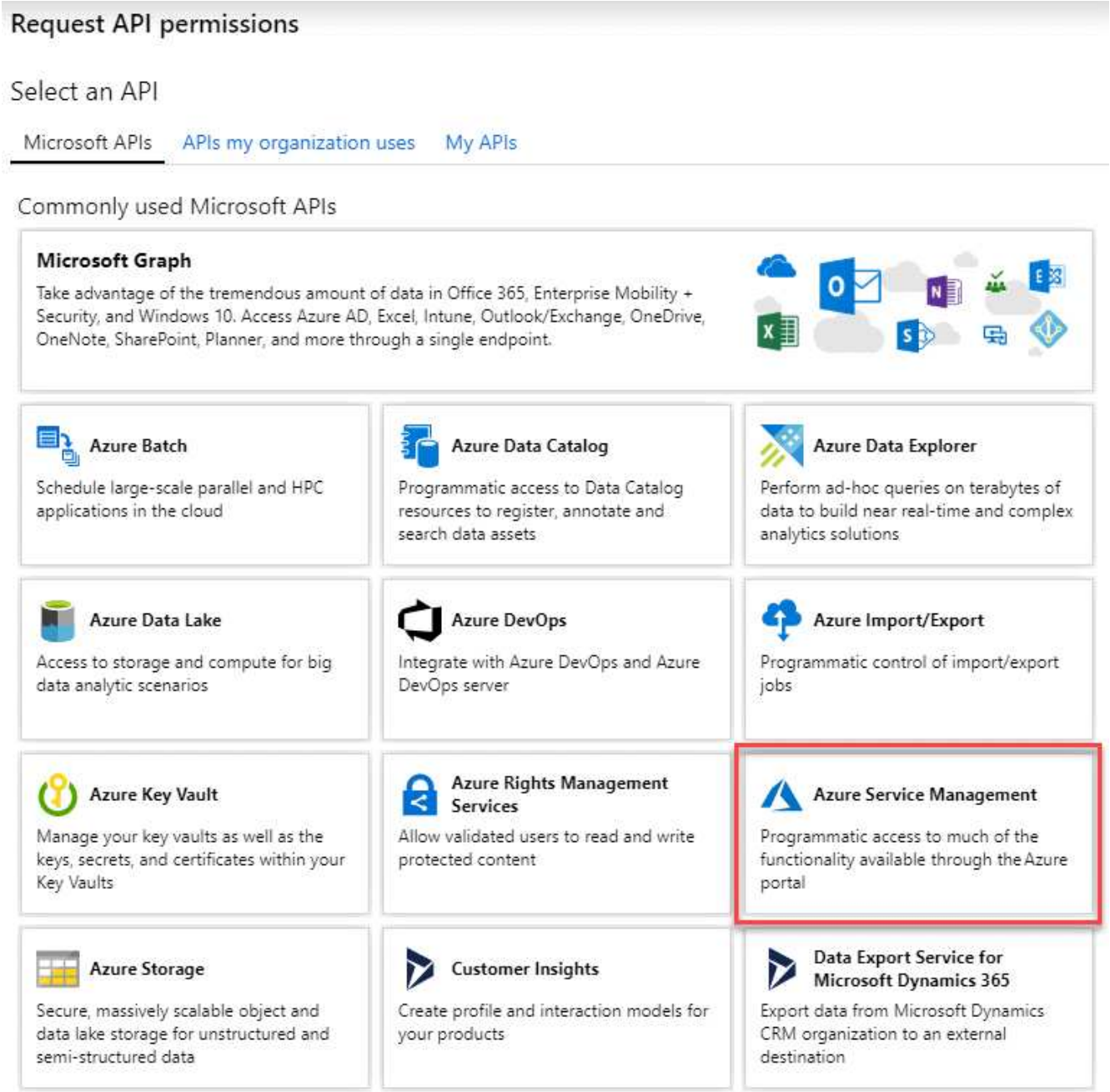
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. BlueXP le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

Añada permisos de API de administración de servicios de Windows Azure

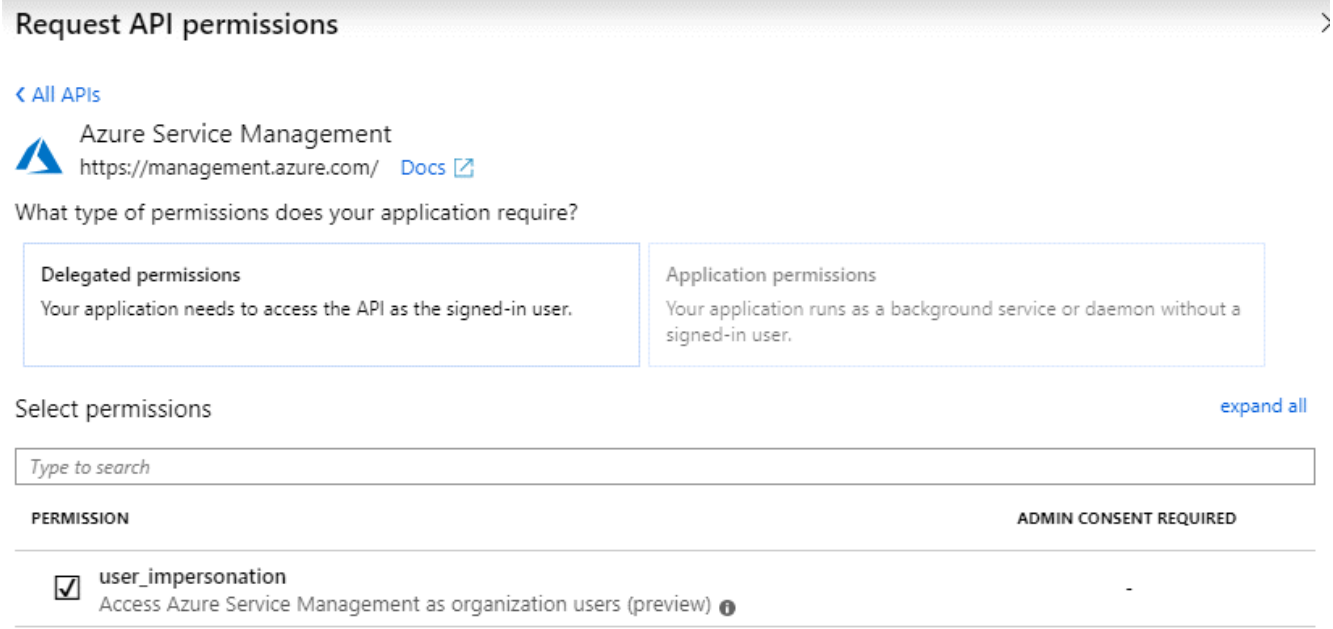
El principal de servicio debe tener permisos de "API de administración de servicios de Windows Azure".

Pasos

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Seleccione **permisos de API > Agregar un permiso**.
3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.



4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.

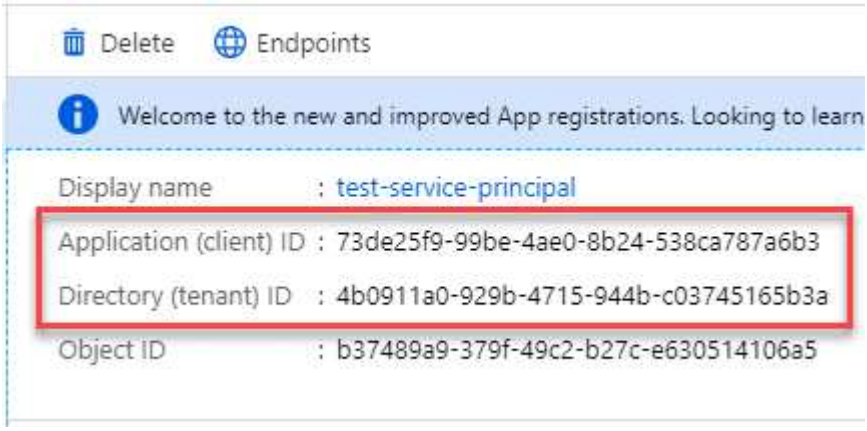


Obtener el ID de aplicación y el ID de directorio

Al agregar la cuenta de Azure a BlueXP, debe proporcionar el ID de la aplicación (cliente) y el ID de directorio (inquilino) para la aplicación. BlueXP utiliza los identificadores para iniciar sesión mediante programación.

Pasos

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



Al agregar la cuenta de Azure a BlueXP, debe proporcionar el ID de la aplicación (cliente) y el ID de directorio (inquilino) para la aplicación. BlueXP utiliza los identificadores para iniciar sesión mediante programación.

Cree un secreto de cliente

Debes crear un secreto de cliente y proporcionar a BlueXP el valor del secreto para que BlueXP pueda usarlo para autenticarse con Microsoft Entra ID.

Pasos

1. Abra el servicio **Microsoft Entra ID**.
2. Seleccione **App registres** y seleccione su aplicación.
3. Seleccione **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Seleccione **Agregar**.
6. Copie el valor del secreto de cliente.

Ahora tienes un secreto de cliente que BlueXP puede usarlo para autenticar con Microsoft Entra ID.

Resultado

Su principal de servicio ahora está configurado y debe haber copiado el ID de aplicación (cliente), el ID de directorio (arrendatario) y el valor del secreto de cliente. Necesita introducir esta información en BlueXP cuando agrega una cuenta de Azure.

Agregue las credenciales a BlueXP

Después de proporcionar una cuenta de Azure con los permisos necesarios, puede añadir las credenciales para esa cuenta a BlueXP. Completar este paso le permite iniciar Cloud Volumes ONTAP con diferentes credenciales de Azure.

Antes de empezar

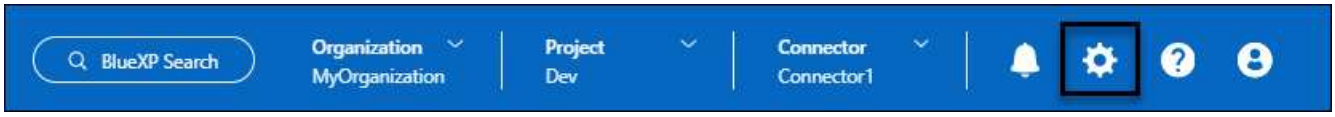
Si acaba de crear estas credenciales en su proveedor de cloud, es posible que transcurran unos minutos hasta que estén disponibles para su uso. Espere unos minutos antes de agregar las credenciales a BlueXP.

Antes de empezar

Debe crear un conector para poder cambiar la configuración de BlueXP. "Aprenda a crear un conector".

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.



2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.
   b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:

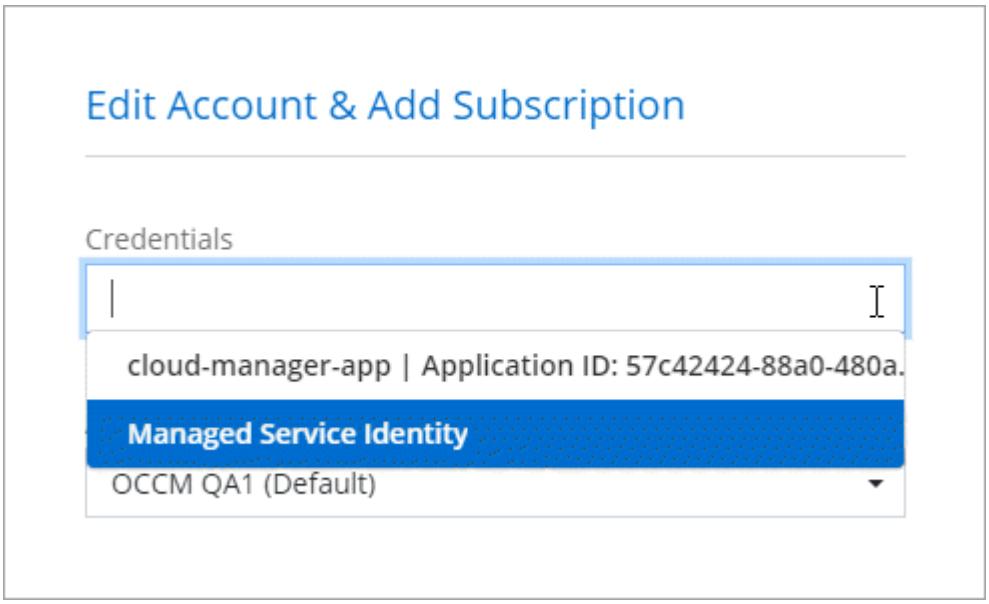
    - ID de aplicación (cliente)
    - ID de directorio (inquilino)
    - Secreto de cliente

c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

Ahora puede cambiar a un conjunto diferente de credenciales La página Details y Credentials "al crear un nuevo entorno de trabajo"



Gestionar las credenciales existentes

Gestione las credenciales de Azure que ya ha agregado a BlueXP asociando una suscripción de Marketplace, editando credenciales y suprimiéndolas.

Asocie una suscripción de Azure Marketplace a credenciales

Después de añadir sus credenciales de Azure a BlueXP, puede asociar una suscripción de Azure Marketplace a esas credenciales. La suscripción permite crear un sistema Cloud Volumes ONTAP de pago por uso y utilizar otros servicios BlueXP.

Hay dos situaciones en las que puede asociar una suscripción a Azure Marketplace después de haber añadido las credenciales a BlueXP:

- No asoció una suscripción cuando agregó inicialmente las credenciales a BlueXP.
- Desea cambiar la suscripción de Azure Marketplace asociada con las credenciales de Azure.

  La sustitución de la suscripción actual del mercado por una nueva suscripción cambia la suscripción del mercado para cualquier entorno de trabajo existente de Cloud Volumes ONTAP y todos los nuevos entornos de trabajo.

Antes de empezar

Debe crear un conector antes de poder cambiar la configuración de BlueXP. "Aprenda a crear un conector" .

Pasos

1. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Configurar suscripción**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.

3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción de la lista desplegable y seleccione **Configurar**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos de Azure Marketplace:

   a. Si se le solicita, inicie sesión en su cuenta de Azure.

   b. Seleccione **Suscribirse**.

   c. Rellene el formulario y seleccione **Suscribirse**.

   d. Una vez completado el proceso de suscripción, seleccione **Configurar cuenta ahora**.

      Serás redirigido a BlueXP.

   e. Desde la página **asignación de suscripción**:

      - Seleccione las organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
      - En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

        BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

      Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

      - Seleccione **Guardar**.

        En el siguiente vídeo se muestran los pasos para suscribirse desde Azure Marketplace:

   Suscríbase a NetApp Intelligent Services desde Azure Marketplace

Editar credenciales

Edite sus credenciales de Azure en BlueXP modificando los detalles acerca de sus credenciales de servicio de Azure. Por ejemplo, es posible que necesite actualizar el secreto de cliente si se creó un nuevo secreto para la aplicación principal de servicios.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. En la página **Credenciales de la organización** o **Credenciales de la cuenta**, selecciona el menú de

acción para un conjunto de credenciales y luego selecciona **Editar Credenciales**.

3. Realice los cambios necesarios y, a continuación, seleccione **aplicar**.

Eliminar credenciales

Si ya no necesita un conjunto de credenciales, puede eliminarlas de BlueXP. Sólo puede eliminar credenciales que no estén asociadas a un entorno de trabajo.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. En la página **Credenciales de la organización** o **Credenciales de la cuenta**, selecciona el menú de acción para un conjunto de credenciales y luego selecciona **Eliminar Credenciales**.
3. Seleccione **Eliminar** para confirmar.

Google Cloud

Obtén más información sobre los proyectos y permisos de Google Cloud

Descubre cómo BlueXP utiliza las credenciales de Google Cloud para realizar acciones en tu nombre y cómo esas credenciales están asociadas a las suscripciones del mercado. Comprender estos detalles puede resultar útil al administrar las credenciales de uno o más proyectos de Google Cloud. Por ejemplo, es posible que desee obtener información sobre la cuenta de servicio asociada a la VM de Connector.

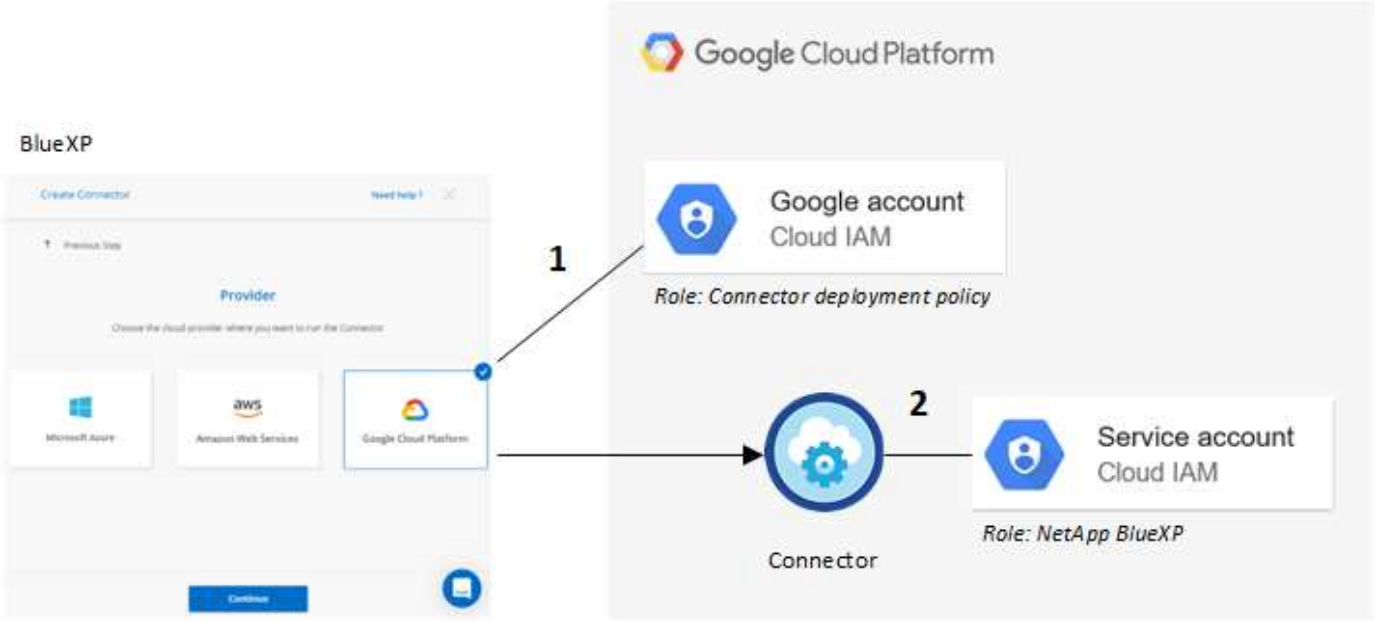
Proyecto y permisos para BlueXP

Antes de poder usar BlueXP para administrar recursos en su proyecto de Google Cloud, primero debe implementar un conector. El conector no puede ejecutarse en sus instalaciones ni en un proveedor de cloud diferente.

Deben existir dos conjuntos de permisos antes de desplegar un conector directamente desde BlueXP:

1. Debe implementar un conector utilizando una cuenta de Google que tenga permisos para iniciar la instancia de Connector VM desde BlueXP.
2. Al desplegar el conector, se le pedirá que seleccione un "cuenta de servicio" Para la instancia de máquina virtual. BlueXP obtiene permisos de la cuenta de servicio para crear y gestionar sistemas de Cloud Volumes ONTAP, para gestionar backups mediante el backup y la recuperación de BlueXP, y mucho más. Los permisos se proporcionan asociando una función personalizada a la cuenta de servicio.

La siguiente imagen muestra los requisitos de permisos descritos en los números 1 y 2 anteriores:



Para aprender a configurar los permisos, consulte las siguientes páginas:

- "Configure los permisos de Google Cloud para el modo estándar"
- "Configure los permisos para el modo restringido"
- "Configurar permisos para el modo privado"

Credenciales y suscripciones de Marketplace

Cuando implementas un Connector en Google Cloud, BlueXP crea un conjunto de credenciales predeterminado para la cuenta de servicio de Google Cloud en el proyecto en el que reside Connector. Estas credenciales deben estar asociadas a una suscripción a Google Cloud Marketplace para poder pagar por Cloud Volumes ONTAP con una tarifa por hora (PAYGO) y utilizar otros servicios de BlueXP.

"Descubre cómo asociar una suscripción a Google Cloud Marketplace".

Tenga en cuenta lo siguiente acerca de las credenciales de Google Cloud y las suscripciones al mercado:

- Solo se puede asociar un conjunto de credenciales de Google Cloud a un conector
- Solo puedes asociar una suscripción a Google Cloud Marketplace a las credenciales
- Puede reemplazar una suscripción existente de Marketplace por una nueva

Proyecto para Cloud Volumes ONTAP

Cloud Volumes ONTAP puede residir en el mismo proyecto que el conector o en un proyecto diferente. Para implementar Cloud Volumes ONTAP en un proyecto diferente, primero debe agregar la cuenta de servicio del conector y la función a ese proyecto.

- "Aprenda a configurar la cuenta de servicio"
- "Descubra cómo implementar Cloud Volumes ONTAP en Google Cloud y seleccione un proyecto"

Administrar las credenciales y suscripciones de Google Cloud para BlueXP

Puede administrar las credenciales de Google Cloud asociadas a la instancia de VM

Connector asociando una suscripción a Marketplace y solucionando el proceso de suscripción. Ambas tareas garantizan que puedas usar tu suscripción al mercado para pagar los servicios de datos.

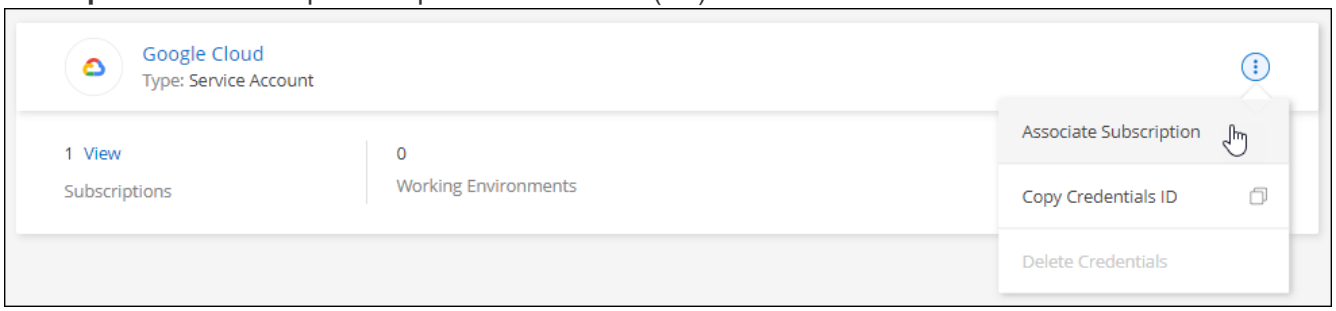
Asocie una suscripción a Marketplace con credenciales de Google Cloud

Al implementar un conector en Google Cloud, BlueXP crea un conjunto predeterminado de credenciales asociadas a la instancia de Connector VM. En cualquier momento, puedes cambiar la suscripción de Google Cloud Marketplace asociada a estas credenciales. La suscripción le permite crear un sistema Cloud Volumes ONTAP de pago por uso y utilizar otros servicios de datos.

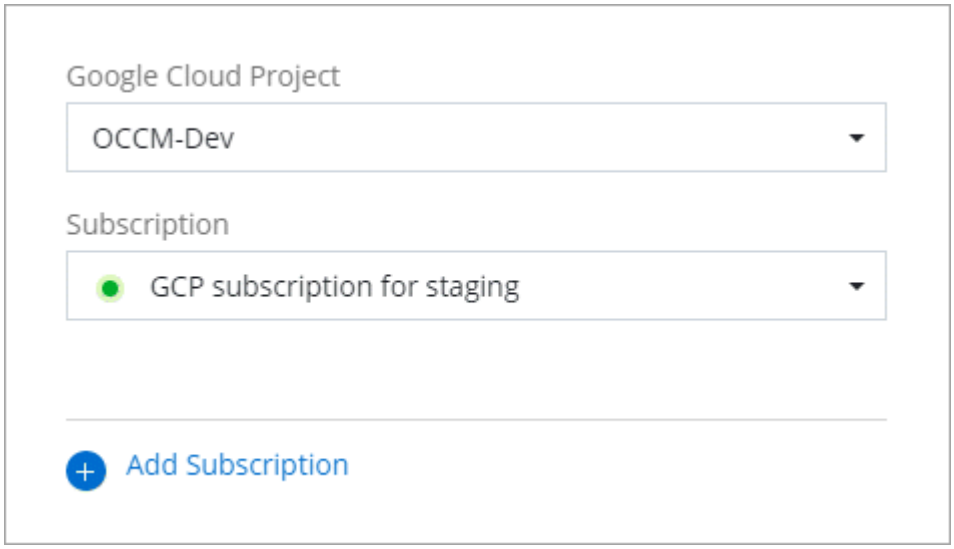
La sustitución de la suscripción actual del mercado por una nueva suscripción cambia la suscripción del mercado para cualquier entorno de trabajo existente de Cloud Volumes ONTAP y todos los nuevos entornos de trabajo.

Pasos

1. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Configurar suscripción**. +nueva captura de pantalla necesaria (TS)



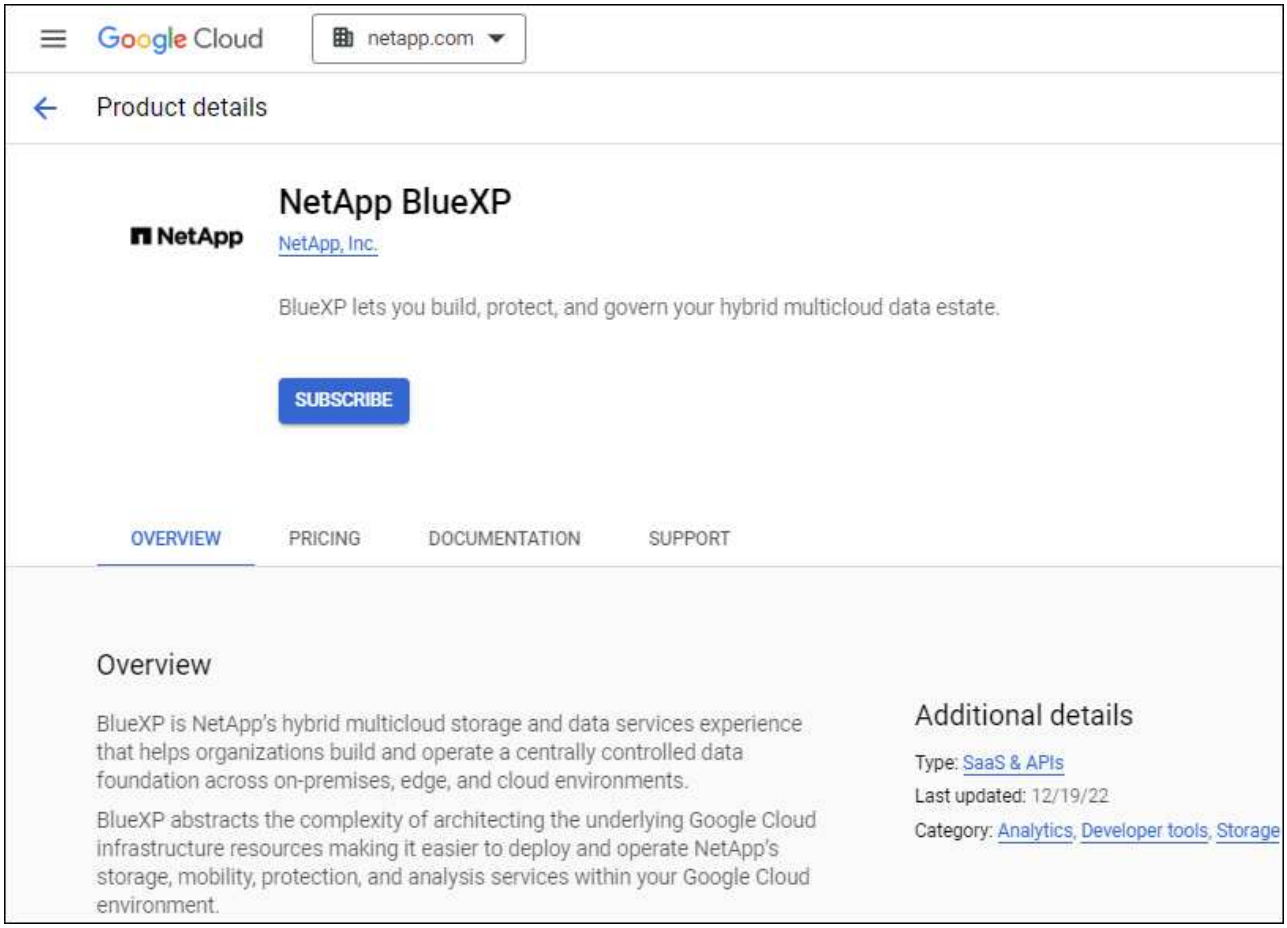
3. Para configurar una suscripción existente con las credenciales seleccionadas, seleccione un proyecto y una suscripción de Google Cloud en la lista desplegable y, a continuación, seleccione **Configurar**.



4. Si aún no tiene una suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos de Google Cloud Marketplace.

Antes de completar los siguientes pasos, asegúrese de que tiene privilegios de administrador de facturación en su cuenta de Google Cloud así como un inicio de sesión de BlueXP.

a. Después de ser redirigido a la "Página de Servicios inteligentes de NetApp en Google Cloud Marketplace" , asegúrese de que el proyecto correcto esté seleccionado en el menú de navegación superior.



b. Seleccione **Suscribirse**.

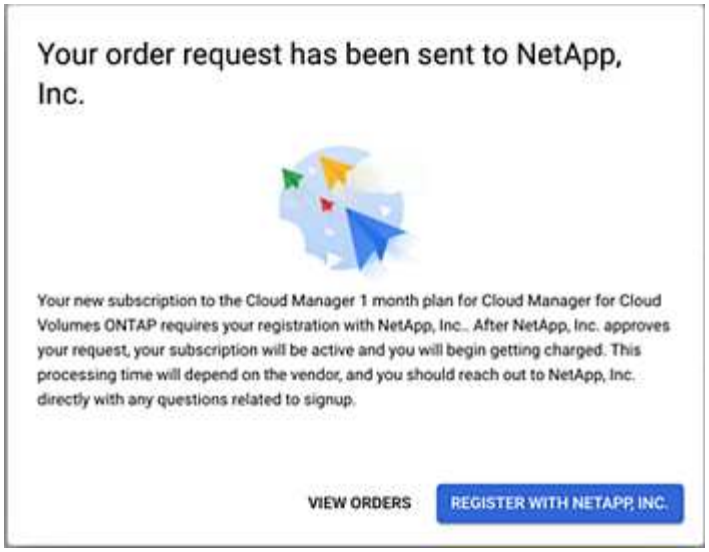
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.

d. Seleccione **Suscribirse**.

   Este paso envía la solicitud de transferencia a NetApp.

e. En el cuadro de diálogo emergente, seleccione **Registro con NetApp, Inc.**

   Este paso debe completarse para vincular la suscripción a Google Cloud con tu organización o cuenta de BlueXP . El proceso de vinculación de una suscripción no está completo hasta que se le redirigirá de esta página y, a continuación, inicie sesión en BlueXP.



f. Siga los pasos de la página **asignación de suscripción**:

> Si alguien de su organización ya se ha suscrito a la suscripción de NetApp BlueXP desde su cuenta de facturación, se le redirigirá a "La página Cloud Volumes ONTAP en el sitio Web de BlueXP" en su lugar. Si esto no se realiza de forma inesperada, póngase en contacto con el equipo de ventas de NetApp. Google sólo activa una suscripción por cuenta de facturación de Google.

- Seleccione las organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
- En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

  BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

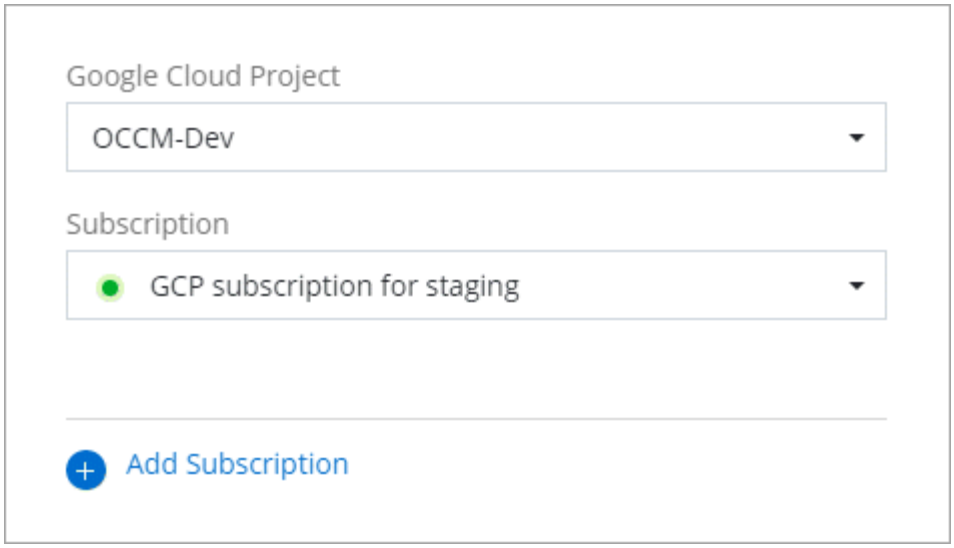
Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

  En el siguiente vídeo se muestran los pasos para suscribirse desde Google Cloud Marketplace:

Suscríbete a BlueXP desde Google Cloud Marketplace

a. Una vez completado este proceso, vuelva a la página credenciales de BlueXP y seleccione esta nueva suscripción.

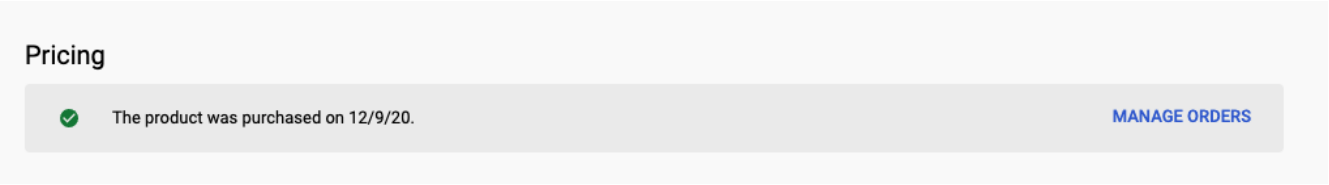


Solucione los problemas del proceso de suscripción a Marketplace

A veces, la suscripción a NetApp Intelligent Services a través de Google Cloud Marketplace puede fragmentarse debido a permisos incorrectos o por no seguir accidentalmente la redirección al sitio web de BlueXP. Si esto sucede, siga estos pasos para completar el proceso de suscripción.

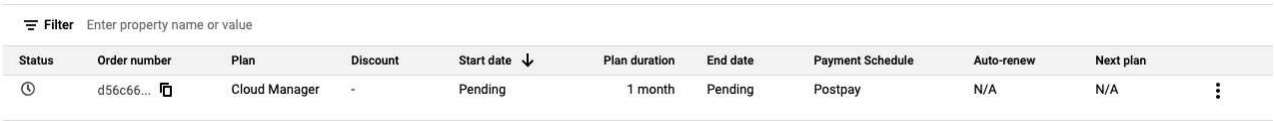
Pasos

1. Desplácese hasta la "Página de BlueXP de NetApp en Google Cloud Marketplace" para comprobar el estado del pedido. Si la página indica **Administrar en Proveedor**, desplácese hacia abajo y seleccione **gestionar pedidos**.



   - Si el pedido muestra una Marca de verificación verde y esto es inesperado, puede que ya se suscriban otras personas de la organización que utilicen la misma cuenta de facturación. Si esto no se realiza lo esperado o necesita los detalles de esta suscripción, póngase en contacto con su equipo de ventas de NetApp.

   - Si el pedido muestra un reloj y el estado **pendiente**, vuelva a la página de mercado y seleccione **Administrar en proveedor** para completar el proceso como se ha documentado anteriormente.



Permite gestionar las credenciales de NSS asociadas con BlueXP

Asocie una cuenta del sitio de soporte de NetApp a su organización de BlueXP para habilitar flujos de trabajo clave para Cloud Volumes ONTAP. Estas credenciales de NSS se asocian con toda la organización de BlueXP .

BlueXP también admite la asociación de una cuenta NSS por cuenta de usuario de BlueXP . "Aprenda a gestionar las credenciales en el nivel de usuario".

- "Obtenga más información sobre los modos de implementación de BlueXP"
- "Obtenga más información sobre la gestión de identidades y accesos de BlueXP "

Descripción general

Es necesario asociar las credenciales del sitio de soporte de NetApp con su número de serie de cuenta de BlueXP específico para habilitar las siguientes tareas en BlueXP :

- Puesta en marcha de Cloud Volumes ONTAP cuando usted traiga su propia licencia (BYOL)

  Es necesario proporcionar su cuenta NSS para que BlueXP pueda cargar su clave de licencia y activar la suscripción para el plazo que adquirió. Esto incluye actualizaciones automáticas para renovaciones de términos.

- Registro de sistemas Cloud Volumes ONTAP de pago por uso

  Se requiere que proporcione su cuenta de NSS para activar el soporte de su sistema y obtener acceso a los recursos de soporte técnico de NetApp.

- Actualizar el software Cloud Volumes ONTAP a la versión más reciente

Estas credenciales están asociadas con el número de serie de su cuenta de BlueXP específico. Los usuarios que pertenecen a la organización o cuenta de BlueXP pueden acceder a estas credenciales desde **Soporte > Administración de NSS**.

Añada una cuenta de NSS

Puede agregar y gestionar sus cuentas del sitio de soporte de NetApp para su uso con BlueXP desde la consola de soporte de BlueXP .

Cuando haya agregado su cuenta NSS, BlueXP puede utilizar esta información para aspectos como descargas de licencias, verificación de actualizaciones de software y futuros registros de soporte.

Puede asociar varias cuentas de NSS a su organización de BlueXP ; sin embargo, no puede tener cuentas de cliente ni cuentas de partner dentro de la misma organización.

> NetApp utiliza Microsoft Entra ID como proveedor de identidad para los servicios de autenticación específicos de soporte y licencias.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.
2. Seleccione **Administración de NSS > Agregar cuenta de NSS**.
3. Selecciona **Continuar** para ser redirigido a una página de inicio de sesión de Microsoft.

4. En la página de inicio de sesión, proporcione la dirección de correo electrónico y contraseña registradas en el sitio de soporte de NetApp.

   Después de iniciar sesión correctamente, NetApp almacenará el nombre de usuario de NSS.

   Se trata de un ID generado por el sistema que se asigna a su correo electrónico. En la página **NSS Management**, puede mostrar su correo electrónico desde ••• de windows

   - Si alguna vez necesita actualizar sus tokens de credenciales de inicio de sesión, también hay una opción **Actualizar credenciales** en la ••• de windows

     Con esta opción se le solicita que vuelva a iniciar sesión. Tenga en cuenta que el token de estas cuentas caduca después de 90 días. Se enviará una notificación para avisarle de ello.

El futuro

Ahora los usuarios pueden seleccionar la cuenta al crear sistemas de Cloud Volumes ONTAP nuevos y cuando registran sistemas Cloud Volumes ONTAP existentes.

- "Inicio de Cloud Volumes ONTAP en AWS"
- "Inicio de Cloud Volumes ONTAP en Azure"
- "Lanzamiento de Cloud Volumes ONTAP en Google Cloud"
- "Registro de sistemas de pago por uso"

Actualice las credenciales de NSS

Por motivos de seguridad, debe actualizar sus credenciales de NSS cada 90 días. Recibirá una notificación en el centro de notificaciones de BlueXP si su credencial de NSS ha vencido. "Obtenga información sobre el Centro de notificaciones".

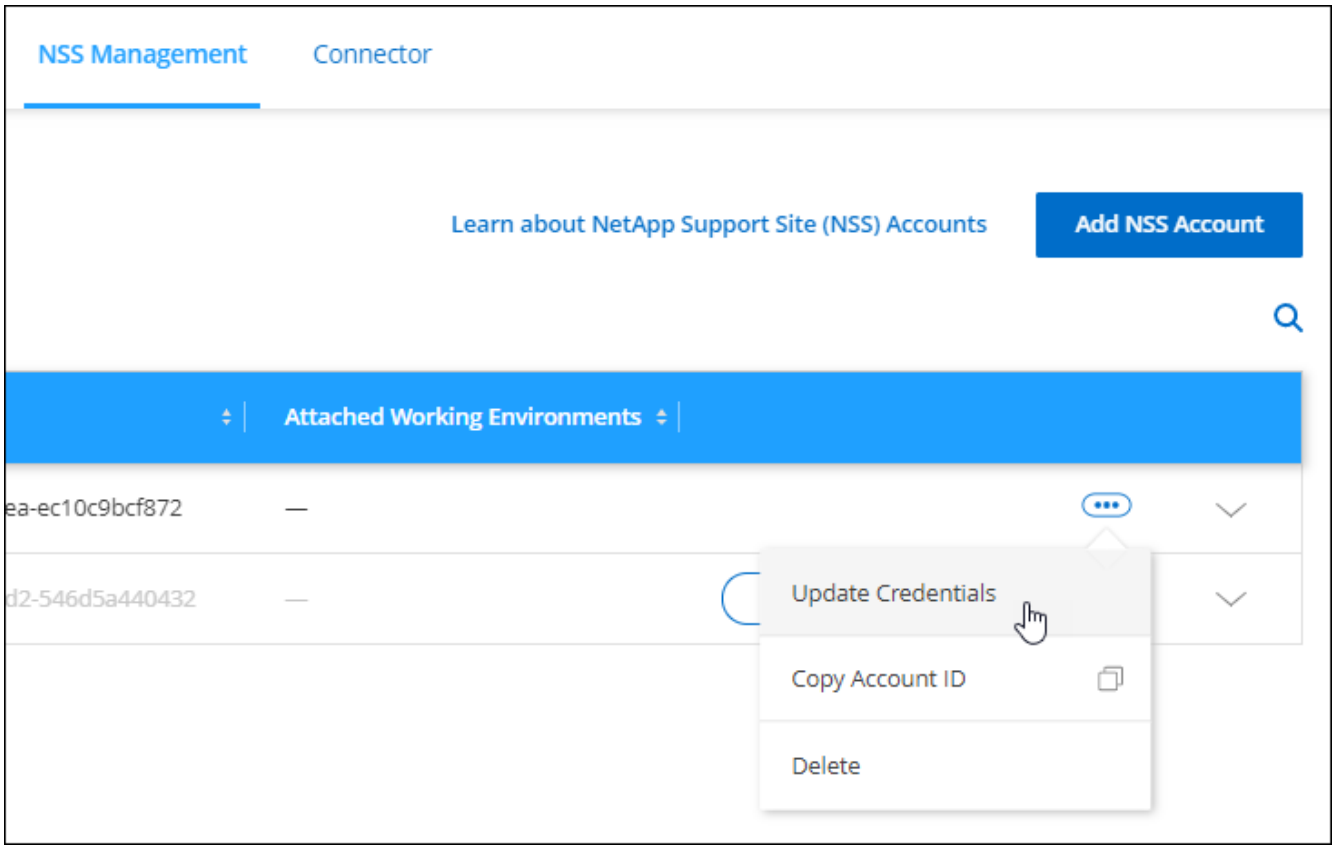
Las credenciales vencidas pueden interrumpir lo siguiente, pero no se limitan a:

- Actualizaciones de licencias en la cartera digital, lo que significa que no podrá aprovechar la capacidad recién adquirida.
- Capacidad para enviar y realizar un seguimiento de casos de soporte.

Además, puede actualizar las credenciales de NSS asociadas a su organización si desea cambiar la cuenta de NSS asociada a su organización de BlueXP . Por ejemplo, si la persona asociada a su cuenta de NSS ha abandonado la empresa.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.
2. Seleccione **NSS Management**.
3. Para la cuenta de NSS que desea actualizar, seleccione ••• Y, a continuación, seleccione **Actualizar credenciales**.



4. Cuando se le solicite, seleccione **continuar** para que se le redirija a una página de inicio de sesión de Microsoft.

   NetApp utiliza Microsoft Entra ID como proveedor de identidad para los servicios de autenticación relacionados con el soporte y la licencia.

5. En la página de inicio de sesión, proporcione la dirección de correo electrónico y contraseña registradas en el sitio de soporte de NetApp.

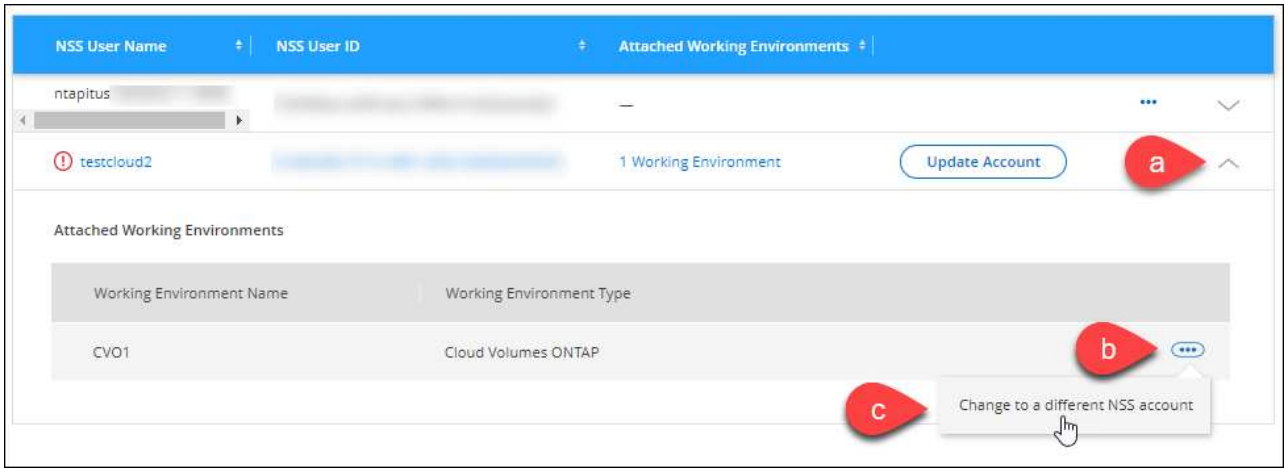
Adjunte un entorno de trabajo a una cuenta de NSS diferente

Si su organización tiene varias cuentas del sitio de soporte de NetApp, puede cambiar qué cuenta está asociada a un sistema Cloud Volumes ONTAP.

Primero debe haber asociado la cuenta con BlueXP .

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.
2. Seleccione **NSS Management**.
3. Complete los siguientes pasos para cambiar la cuenta de NSS:
   a. Expanda la fila de la cuenta del sitio de soporte de NetApp con la que está asociado actualmente el entorno de trabajo.
   b. Para el entorno de trabajo para el que desea cambiar la asociación, seleccione ⋯
   c. Seleccione **Cambiar a una cuenta de NSS diferente**.



d. Seleccione la cuenta y, a continuación, seleccione **Guardar**.

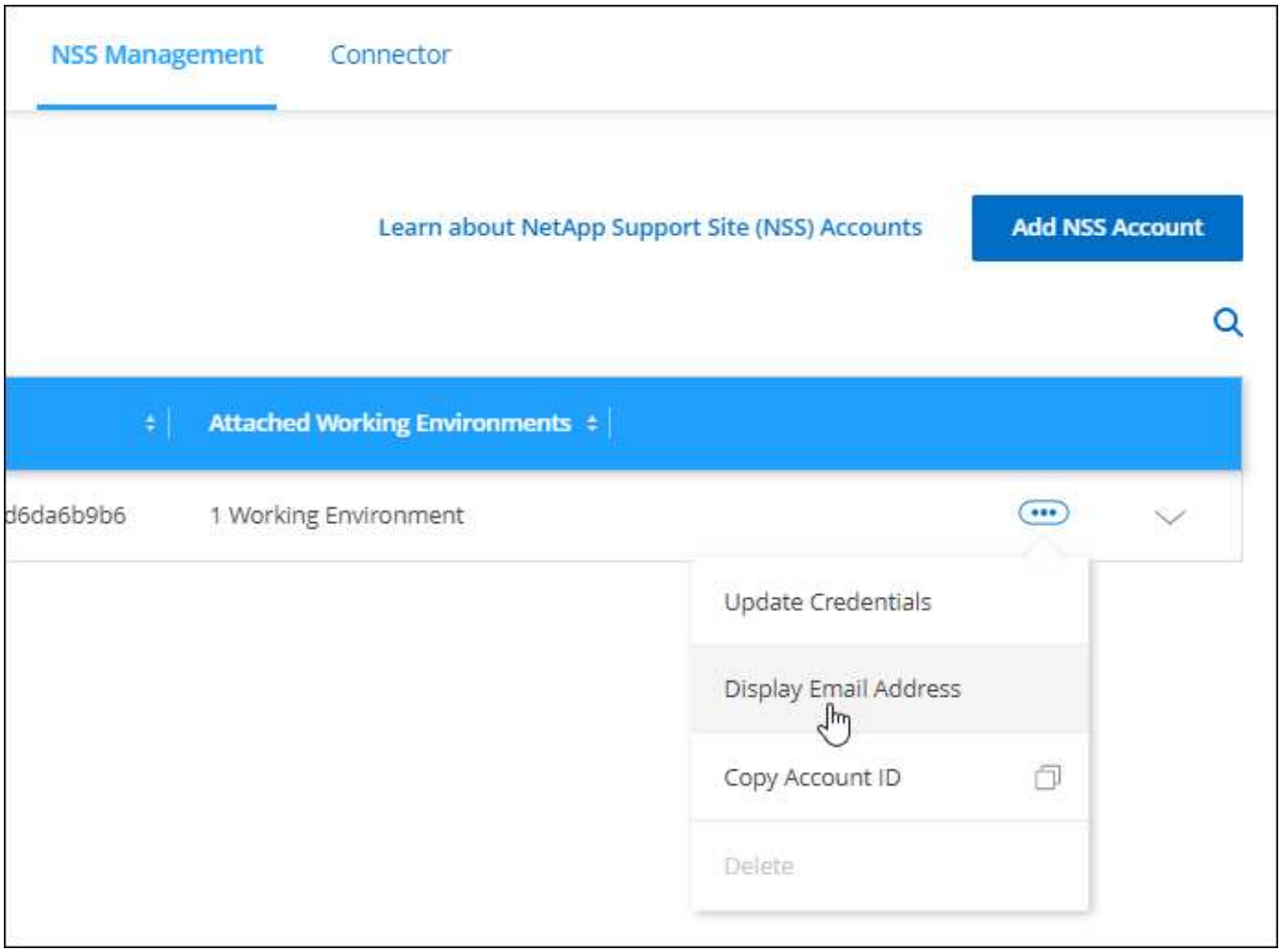
Muestra la dirección de correo electrónico de una cuenta de NSS

Por seguridad, la dirección de correo electrónico asociada a una cuenta NSS no se muestra de forma predeterminada. Puede ver la dirección de correo electrónico y el nombre de usuario asociado de una cuenta NSS.

> Cuando vaya a la página NSS Management, BlueXP genera un token para cada cuenta de la tabla. Ese token incluye información acerca de la dirección de correo electrónico asociada. El token se elimina al salir de la página. La información nunca se almacena en la caché, lo que ayuda a proteger su privacidad.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.
2. Seleccione **NSS Management**.
3. Para la cuenta NSS que desea actualizar, ••• seleccione y luego seleccione **Mostrar dirección de correo electrónico**. Puede utilizar el botón de copia para copiar la dirección de correo electrónico.



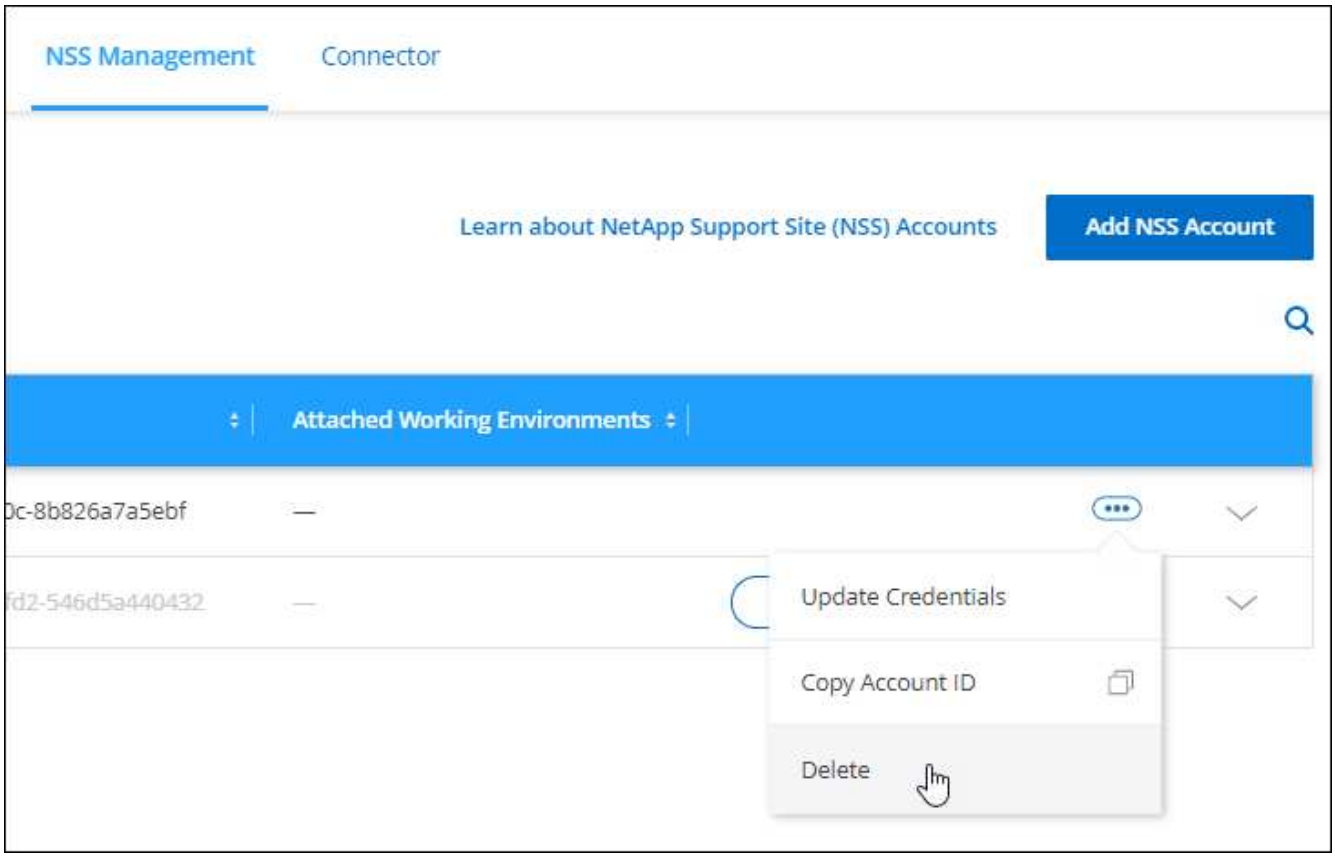
Quite una cuenta de NSS

Elimine cualquiera de las cuentas de NSS que ya no desee utilizar con BlueXP.

No se puede eliminar una cuenta asociada actualmente a un entorno de trabajo de Cloud Volumes ONTAP. Lo primero que necesitaAdjunte esos entornos de trabajo a una cuenta de NSS diferente.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.
2. Seleccione **NSS Management**.
3. Para la cuenta de NSS que desea eliminar, seleccione ••• Y, a continuación, seleccione **Eliminar**.



4. Seleccione **Eliminar** para confirmar.

Administre las credenciales asociadas con su inicio de sesión de BlueXP

En función de las acciones que haya adoptado en BlueXP, quizás tenga credenciales de ONTAP asociadas y credenciales del sitio de soporte de NetApp (NSS) con su inicio de sesión de usuario de BlueXP. Puede ver y administrar esas credenciales en BlueXP después de haberlas asociado. Por ejemplo, si cambia la contraseña para estas credenciales, deberá actualizar la contraseña en BlueXP.

Credenciales de ONTAP

Los usuarios necesitan credenciales de administrador de ONTAP para descubrir clústeres de ONTAP en BlueXP. Sin embargo, el acceso al administrador del sistema de ONTAP depende de si utiliza o no un conector.

Sin conector

Los usuarios deben introducir sus credenciales de ONTAP para acceder a ONTAP System Manager del clúster. Los usuarios pueden elegir guardar estas credenciales en BlueXP , lo que significa que no se les pedirá que las introduzcan cada vez. Las credenciales de usuario sólo son visibles para el usuario respectivo y se pueden gestionar desde la página de credenciales de usuario.

Con un conector

De forma predeterminada, no se solicita a los usuarios que introduzcan sus credenciales de ONTAP para acceder a ONTAP System Manager. Sin embargo, un administrador de BlueXP (con el rol de administrador de la organización) puede configurar BlueXP para solicitar a los usuarios que introduzcan sus credenciales de ONTAP. Cuando esta configuración está habilitada, los usuarios deben introducir sus credenciales de ONTAP

cada vez.

"Leer más."

Credenciales de NSS

Las credenciales de NSS asociadas con tu inicio de sesión de BlueXP permiten el registro de soporte, la gestión de casos y el acceso al asesor digital.

- Cuando accedes a **Soporte > Recursos** y te registras para recibir soporte, se te pedirá que asocies las credenciales de NSS con tu inicio de sesión de BlueXP.

  Esto registra su organización o cuenta para recibir soporte y activa el derecho a soporte. Solo un usuario en su organización o cuenta de BlueXP debe asociar una cuenta en el sitio de soporte de NetApp con su inicio de sesión de BlueXP para registrarse para obtener soporte y activar derechos de soporte. Una vez completado, la página **Recursos** muestra que su cuenta está registrada para soporte.

  "Aprenda a registrarse para obtener soporte"

- Al acceder a **Soporte > Administración de casos**, se le pedirá que introduzca sus credenciales de NSS, si aún no lo ha hecho. Esta página permite crear y gestionar los casos de soporte asociados con su cuenta de NSS y su empresa.
- Al acceder a Digital Advisor en BlueXP, se le pedirá que inicie sesión en Digital Advisor introduciendo sus credenciales de NSS.

Tenga en cuenta lo siguiente sobre la cuenta de NSS asociada con su inicio de sesión de BlueXP:

- La cuenta se gestiona en el nivel de usuario, lo que significa que otros usuarios que inician sesión no la pueden ver.
- Solo puede haber una cuenta de NSS asociada con Digital Advisor y la gestión de casos de soporte, por usuario.
- Si intenta asociar una cuenta del sitio de soporte de NetApp a un entorno de trabajo de Cloud Volumes ONTAP, solo puede elegir entre las cuentas de NSS que se hayan agregado a la organización o cuenta de BlueXP de la que sea miembro.

  Las credenciales en el nivel de cuenta de NSS son diferentes de la cuenta de NSS asociada con tu inicio de sesión en BlueXP. Las credenciales de nivel de cuenta de NSS le permiten implementar Cloud Volumes ONTAP con BYOL, registrar sistemas PAYGO y actualizar su software.

  "Obtenga más información sobre el uso de las credenciales de NSS con su organización o cuenta de BlueXP ".

Gestione las credenciales de usuario

Para gestionar las credenciales de usuario, actualice el nombre de usuario y la contraseña o elimine las credenciales.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione **Credenciales de usuario**.
3. Si aún no tiene ninguna cuenta de usuario, puede seleccionar **Añadir credenciales de NSS** para añadir

su cuenta del sitio de soporte de NetApp.

4. Administre las credenciales existentes eligiendo las siguientes opciones en el menú Acciones:
    - **Actualizar credenciales**: Actualizar el nombre de usuario y la contraseña de la cuenta.
    - **Eliminar credenciales**: Elimina la cuenta asociada a tu cuenta de usuario de BlueXP.

Resultado

BlueXP actualiza sus credenciales y usted ve los cambios cuando accede al clúster ONTAP, al asesor digital o a la página de Administración de casos.

Supervise las operaciones de BlueXP

Puede supervisar el estado de las operaciones que está realizando BlueXP para ver si hay algún problema que necesite solucionar. Puede ver el estado en la línea de tiempo, el Centro de notificaciones o enviar notificaciones a su correo electrónico.

La tabla compara la Línea de tiempo y el Centro de notificaciones para resaltar sus características.

Centro de notificaciones	Línea de tiempo
Muestra el estado de alto nivel de eventos y acciones	Proporciona detalles sobre cada evento o acción para una investigación posterior
Muestra el estado de la sesión de inicio de sesión actual (la información no aparece en el Centro de notificaciones después de cerrar la sesión)	Conserva el estado del último mes
Muestra solo las acciones iniciadas en la interfaz de usuario	Muestra todas las acciones de la interfaz de usuario o las API
Muestra acciones iniciadas por el usuario	Muestra todas las acciones, ya sean iniciadas por el usuario o iniciadas por el sistema
Filtrar resultados por importancia	Filtrar por servicio, acción, usuario, estado, etc.
Proporciona la capacidad de enviar notificaciones por correo electrónico a los usuarios y a otros	No dispone de funciones de correo electrónico

Audite la actividad del usuario desde la línea de tiempo de BlueXP

La línea de tiempo muestra las acciones que los usuarios completaron para administrar su organización o cuenta. Esto incluye acciones de gestión, como asociar usuarios, crear entornos de trabajo, crear conectores, etc.

La línea de tiempo ayuda a identificar quién realizó una acción o su estado.

Pasos

1. En la parte superior derecha de la consola BlueXP , selecciona ⚙> **Línea de tiempo**.
2. Utilice los filtros situados encima de la tabla para cambiar las acciones que se muestran en la tabla.

    Por ejemplo, puedes usar el filtro **Servicio** para mostrar acciones relacionadas con un servicio de BlueXP específico, o puedes usar el filtro **Usuario** para mostrar acciones relacionadas con una cuenta de usuario específica.

Descargar registros de auditoría desde la línea de tiempo

Puede descargar los registros de auditoría de la Cronología a un archivo CSV. Esto le permite mantener un registro de las acciones realizadas por los usuarios en su organización. El archivo CSV descargado contiene todas las columnas disponibles de la Cronología, independientemente de las que esté filtrando o mostrando.

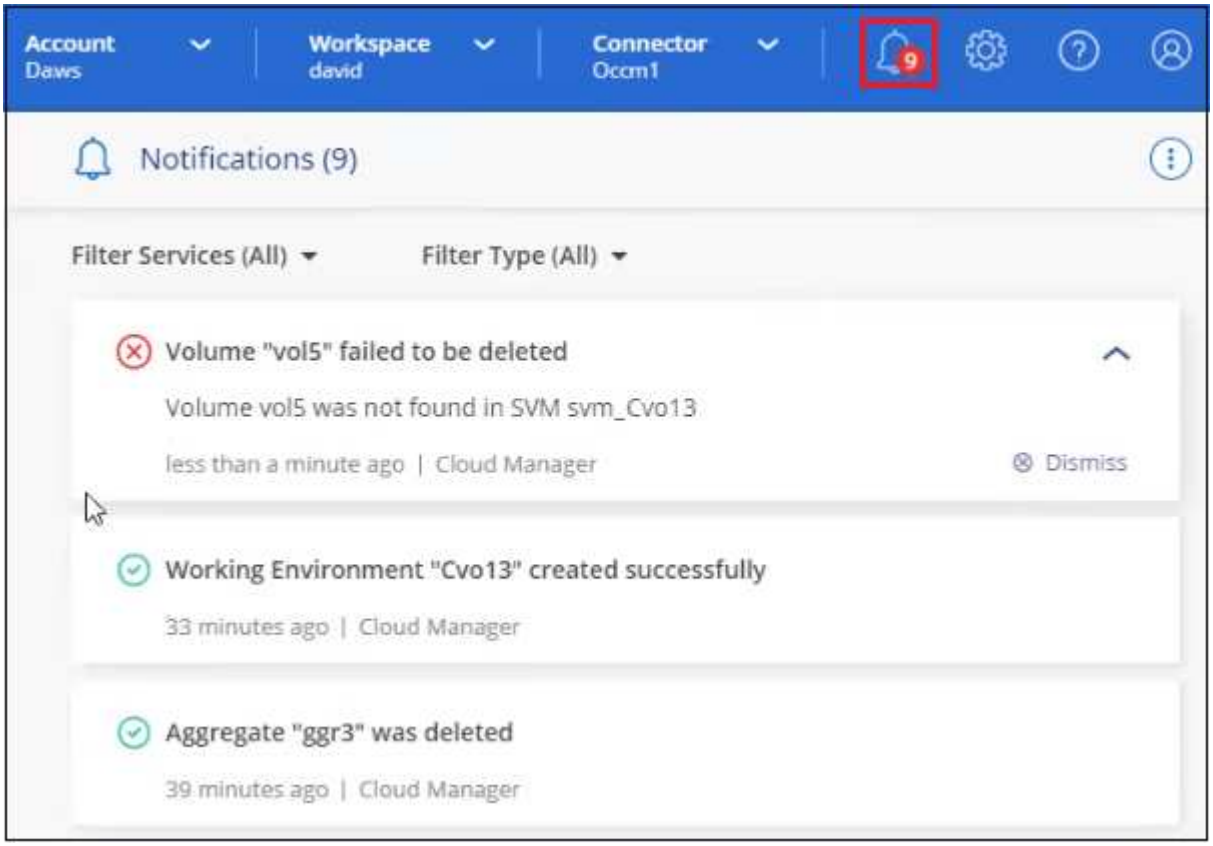
Pasos

1. En la línea de tiempo, seleccione el ícono de descarga en la esquina superior derecha de la tabla.

Supervise las actividades mediante el Centro de notificaciones

Las notificaciones rastrean el progreso de sus operaciones de BlueXP para verificar el éxito. Le permiten ver el estado de muchas acciones de BlueXP que inició durante su sesión de inicio de sesión actual. No todos los servicios de BlueXP informan información en el Centro de notificaciones en este momento.

Puede visualizar las notificaciones seleccionando la campana de notificación ( ) en la barra de menús. El color de la pequeña burbuja en la campana indica la notificación de gravedad de nivel más alto que está activa. Así que si ves una burbuja roja, significa que hay una notificación importante que debes mirar.



También puede configurar BlueXP para que envíe ciertos tipos de notificaciones por correo electrónico de modo que se le informe de la actividad importante del sistema incluso cuando no haya iniciado sesión en el sistema. Los correos electrónicos se pueden enviar a cualquier usuario que forme parte de su organización o cuenta de BlueXP , o a cualquier otro destinatario que necesite conocer ciertos tipos de actividad del sistema. Vea cómo defina los ajustes de notificación por correo electrónico.

Comparación del Centro de Notificaciones con las alertas de BlueXP

El centro de notificaciones le permite ver el estado de las operaciones que ha iniciado desde BlueXP y

configurar notificaciones de alerta para ciertos tipos de actividades del sistema. Mientras tanto, BlueXP le permite ver problemas o riesgos potenciales del entorno de almacenamiento de ONTAP relacionados con la capacidad, la disponibilidad, el rendimiento, la protección y la seguridad.

"Más información sobre las alertas de BlueXP "

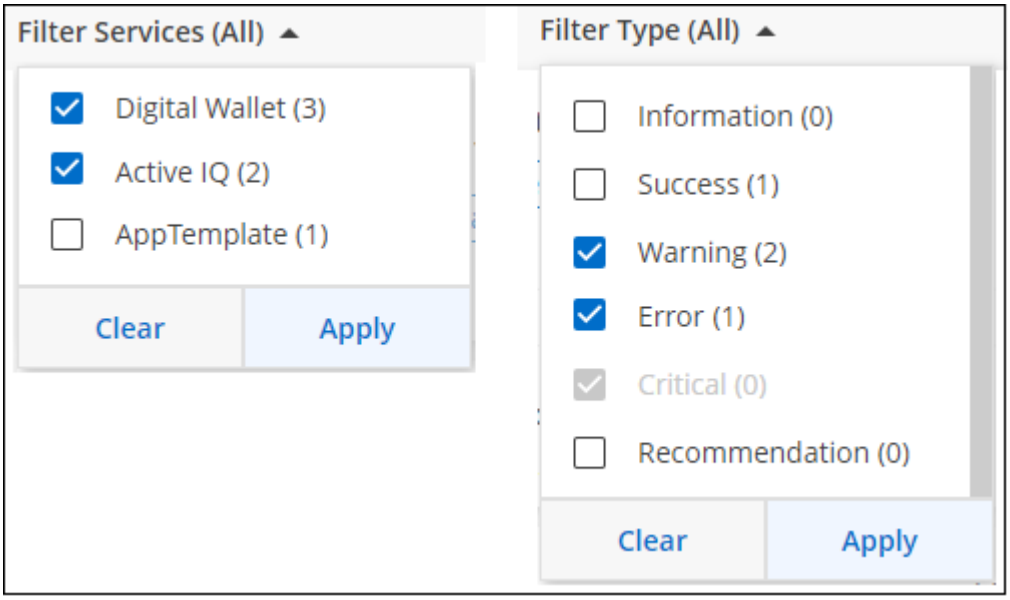
Tipos de notificación

BlueXP clasifica las notificaciones en las siguientes categorías:

Tipo de notificación	Descripción
Crítico	Se produjo un problema que podría provocar una interrupción del servicio si no se toman acciones correctivas de inmediato.
Error	Una acción o proceso terminado con un fallo, o podría dar lugar a un fallo si no se toma una acción correctiva.
Advertencia	Un problema que debe tener en cuenta para asegurarse de que no alcanza la gravedad crucial. Las notificaciones de esta gravedad no provocan interrupciones en el servicio y es posible que no sea necesario realizar ninguna acción correctiva al instante.
Recomendación	Una recomendación del sistema para que usted tome una acción para mejorar el sistema o un servicio determinado; por ejemplo: Ahorro de costos, sugerencia para nuevos servicios, configuración de seguridad recomendada, etc.
Información	Mensaje que proporciona información adicional sobre una acción o proceso.
Correcto	Una acción o proceso completado correctamente.

Filtrar notificaciones

De forma predeterminada, verá todas las notificaciones activas en el Centro de notificaciones. Puede filtrar las notificaciones que ve para mostrar solo las notificaciones que son importantes para usted. Puede filtrar por "Servicio" de BlueXP y por "Tipo" de notificación.



Por ejemplo, si desea ver sólo las notificaciones "error" y "Advertencia" para las operaciones de BlueXP,

seleccione esas entradas y sólo verá esos tipos de notificaciones.

Descartar notificaciones

Puede eliminar notificaciones de la página si ya no necesita verlos. Puede descartar notificaciones individualmente o todas a la vez.

Para descartar todas las notificaciones, en el Centro de notificaciones, seleccione ⋮ Y selecciona **descartar todo**.

Para descartar notificaciones individuales, coloque el cursor sobre la notificación y seleccione **descartar**.

Establecer los ajustes de notificación por correo electrónico

Puede enviar tipos específicos de notificaciones por correo electrónico para que se le informe de la actividad importante del sistema incluso cuando no haya iniciado sesión en BlueXP. Los correos electrónicos se pueden enviar a cualquier usuario que forme parte de su organización o cuenta de BlueXP , o a cualquier otro destinatario que necesite conocer ciertos tipos de actividad del sistema.

- BlueXP envía notificaciones por correo electrónico para el conector, la billetera digital, la copia y sincronización, y la copia de seguridad y recuperación.
- No se admite el envío de notificaciones por correo electrónico cuando el conector está instalado en un sitio sin acceso a Internet.

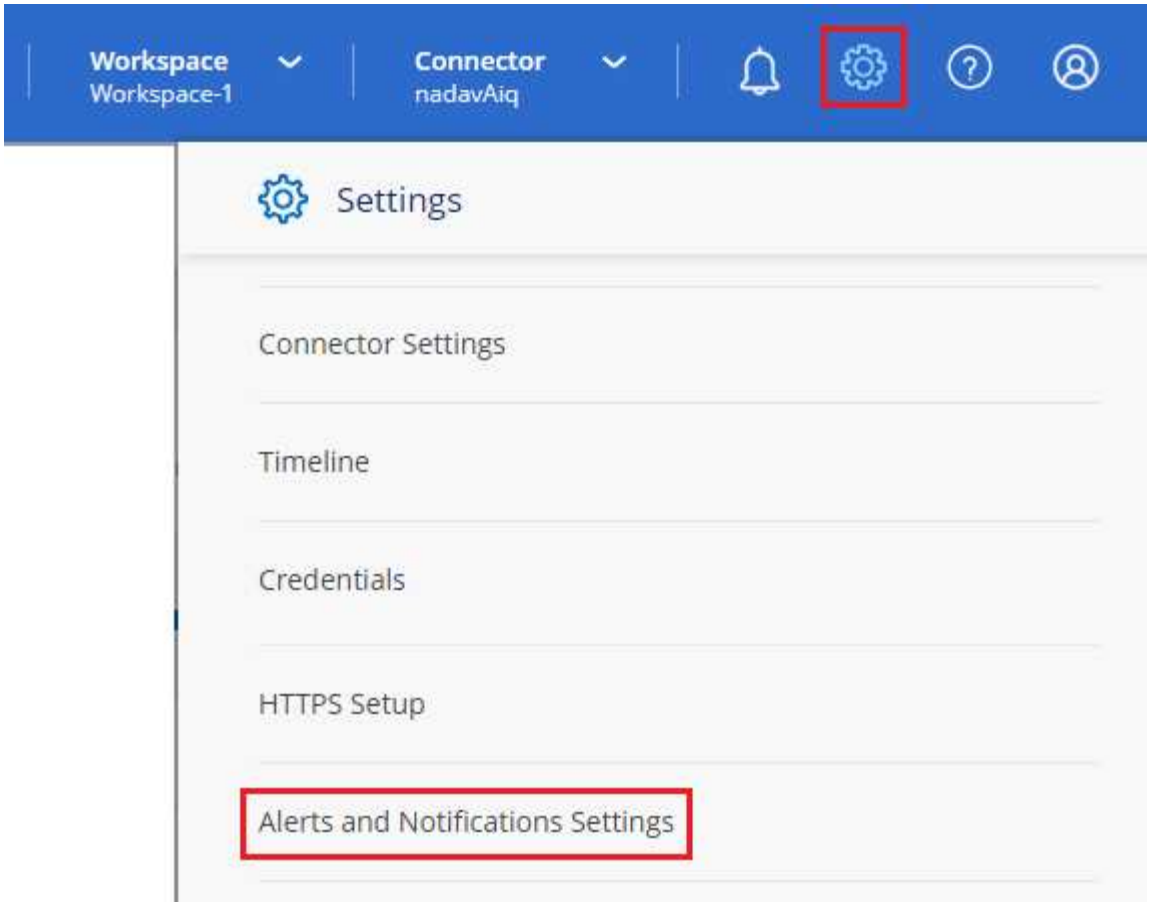
Los filtros que establezca en el Centro de notificaciones no determinan los tipos de notificaciones que recibirá por correo electrónico. De forma predeterminada, cualquier administrador de BlueXP recibirá correos electrónicos para todas las notificaciones «críticas» y «recomendaciones». Estas notificaciones se realizan en todos los servicios; no puedes elegir recibir notificaciones solo para determinados servicios, como Connectors o la copia de seguridad y recuperación de BlueXP.

Todos los demás usuarios y destinatarios están configurados para no recibir ningún correo electrónico de notificación, por lo que tendrá que configurar la configuración de notificaciones para cualquier usuario adicional.

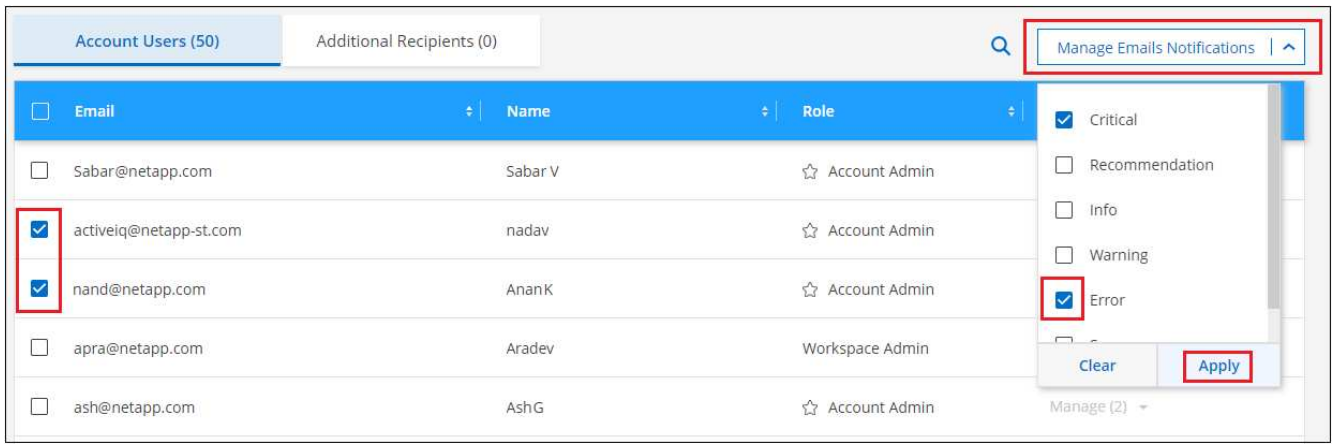
Debe tener el rol de administrador de la organización para personalizar la configuración de notificaciones.

Pasos

1. En la barra de menús de BlueXP, seleccione **Configuración > Alertas y Configuración de notificaciones**.



2. Seleccione un usuario, o varios usuarios, en la pestaña *Users* o en la pestaña *Additional Recipients* y elija el tipo de notificaciones que se van a enviar:
    - Para realizar cambios para un único usuario, seleccione el menú en la columna Notificaciones de ese usuario, compruebe los tipos de notificaciones que se van a enviar y seleccione **aplicar**.
    - Para realizar cambios en varios usuarios, marque la casilla de cada usuario, seleccione **Administrar notificaciones por correo electrónico**, seleccione los tipos de notificaciones que desea enviar y seleccione **aplicar**.



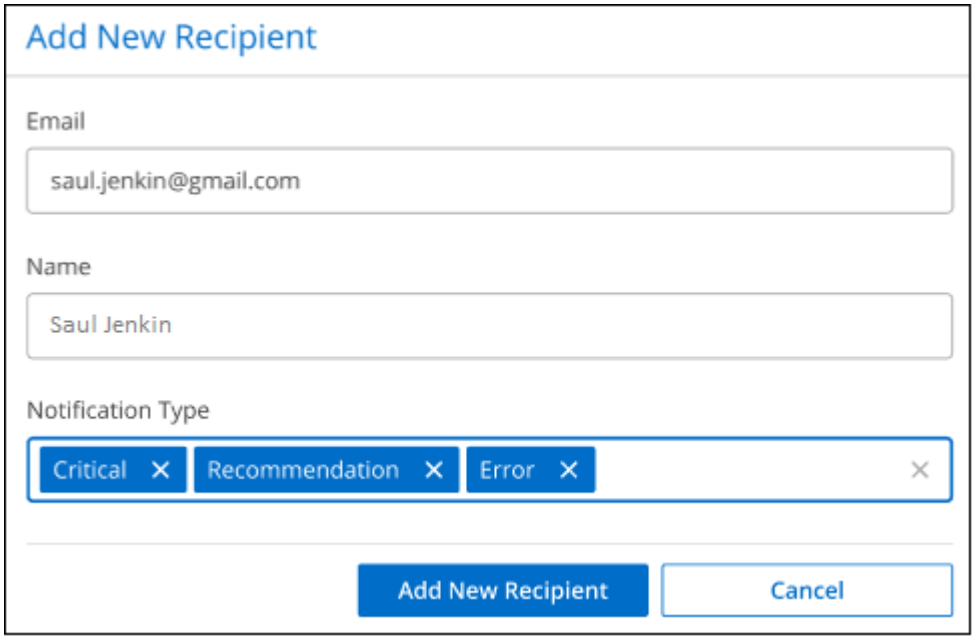
Añada otros destinatarios de correo electrónico

Los usuarios que aparecen en la pestaña *Usuarios* se completan automáticamente a partir de los usuarios de su organización o cuenta. Puede agregar direcciones de correo electrónico en la ficha *Additional Recipients*

para otras personas o grupos que no tienen acceso a BlueXP, pero que necesitan recibir notificaciones sobre ciertos tipos de alertas y notificaciones.

Pasos

1. En la página Configuración de alertas y notificaciones, seleccione **Agregar nuevos destinatarios**.



2. Introduzca el nombre, la dirección de correo electrónico y seleccione los tipos de notificaciones que recibirá el destinatario y seleccione **Agregar nuevo destinatario**.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.