



Credenciales de Azure

Set up and administration

NetApp

March 10, 2023

Tabla de Contenido

- Credenciales de Azure 1
 - Credenciales y permisos de Azure 1
 - Gestione credenciales y suscripciones de Azure para BlueXP 3

Credenciales de Azure

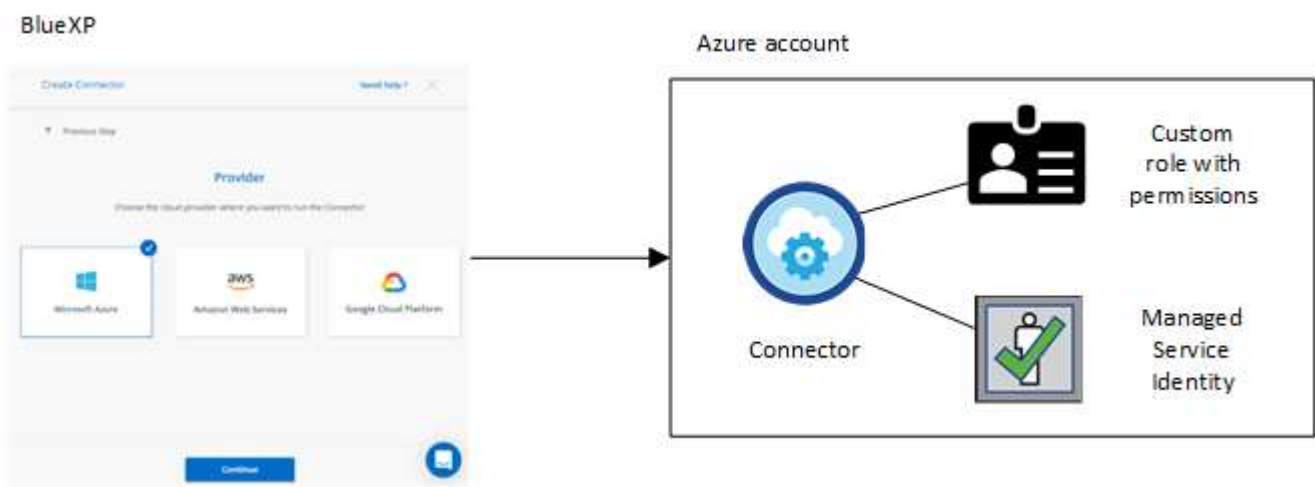
Credenciales y permisos de Azure

BlueXP le permite elegir las credenciales de Azure que desea utilizar al poner en marcha Cloud Volumes ONTAP. Puede poner en marcha todos los sistemas de Cloud Volumes ONTAP con las credenciales iniciales de Azure o bien añadir credenciales adicionales.

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 enumeran en la ["Política de implementación de conectores para Azure"](#).

Cuando BlueXP pone en marcha la máquina virtual Connector en Azure, habilita una ["identidad administrada asignada por el sistema"](#) en una máquina virtual, crea un rol personalizado y lo 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"](#).



BlueXP selecciona estas credenciales de Azure de forma predeterminada cuando crea un entorno de trabajo nuevo para Cloud Volumes ONTAP:

Details & Credentials			
Managed Service Ide...	OCCM QA1	No subscription is associated	<button>Edit Credentials</button>
Credential Name	Azure Subscription	Marketplace Subscription	

Suscripciones adicionales de Azure para una identidad gestionada

La identidad administrada 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 implementar Cloud Volumes ONTAP con diferentes credenciales de Azure, debe conceder los permisos necesarios mediante ["Crear y configurar un servicio principal en Azure Active Director"](#) 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.

Después de añadir otro conjunto de credenciales, puede cambiar a ellas al crear un nuevo entorno de trabajo:

The screenshot shows the 'Edit Account & Add Subscription' dialog box. The 'Credentials' dropdown menu is open, displaying the following options:

- cloud-manager-app | Application ID: 57c42424-88a0-480a.
- Managed Service Identity** (highlighted in blue)
- OCCM QA1 (Default)

¿Qué pasa con las puestas en marcha de Marketplace y las puestas en marcha en las instalaciones?

En las secciones anteriores se describe el método de implementación recomendado para el conector, que es de BlueXP. También puede implementar un conector en Azure desde ["Azure Marketplace"](#), y usted puede ["Instale el conector en las instalaciones"](#).

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Sólo tiene que crear y configurar manualmente la identidad administrada para el conector y, a continuación, proporcionar permisos para cualquier cuenta adicional.

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

Gestione credenciales y suscripciones de Azure para BlueXP

Al crear un sistema de Cloud Volumes ONTAP, tiene que seleccionar las credenciales de Azure para utilizarlas con ese sistema. Si utiliza licencias de pago por uso, también tendrá que elegir una suscripción a Marketplace. 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.

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.

Asociar suscripciones de Azure adicionales a una identidad administrada

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. Haga clic en **Control de acceso (IAM)**.
 - a. Haga clic en **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.
- Haga clic en **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.

Adición de 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 de *diferente* Azure, debe conceder los permisos necesarios para crear y configurar un director de servicio en Azure Active Directory para cada cuenta de Azure. A continuación, puede agregar las nuevas credenciales a BlueXP.

Concesión de permisos de Azure con un director de servicio

BlueXP necesita permisos para realizar acciones en Azure. Puede conceder los permisos necesarios a una cuenta de Azure creando y configurando un servicio principal en Azure Active Directory y obteniendo las credenciales de Azure que BlueXP necesita.

Acerca de esta tarea

La siguiente imagen muestra cómo BlueXP obtiene permisos para realizar operaciones en Azure. Un objeto principal de servicio, que está vinculado a una o más suscripciones de Azure, representa BlueXP en Azure Active Directory y se asigna a una función personalizada que permite los permisos necesarios.



Pasos

1. Cree una aplicación de Azure Active Directory.
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.

Crear una aplicación de Azure Active Directory

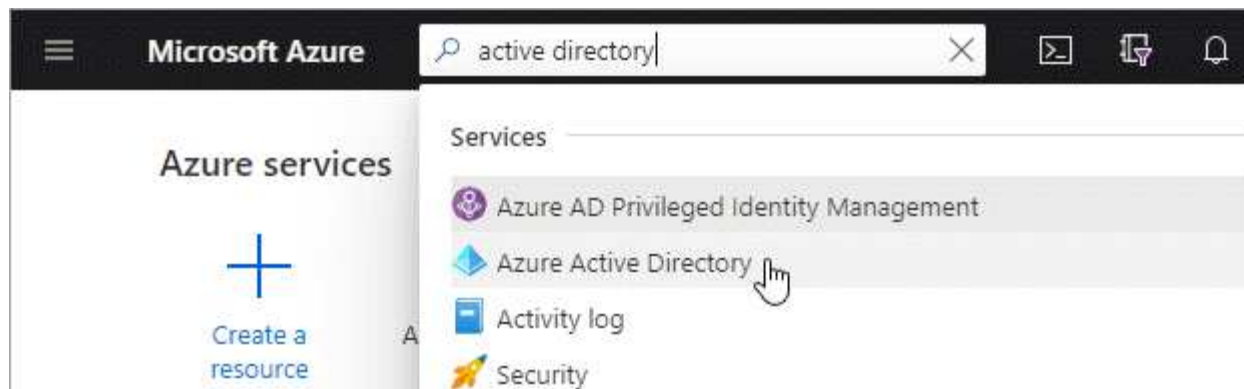
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que BlueXP pueda usar para el control de acceso basado en roles.

Antes de empezar

Debe tener los permisos adecuados en Azure para crear una aplicación de Active Directory y asignar la aplicación a un rol. Para obtener más información, consulte ["Documentación de Microsoft Azure: Permisos necesarios"](#).

Pasos

1. Desde el portal de Azure, abra el servicio **Azure Active Directory**.



2. En el menú, haga clic en **App registrs**.
3. Haga clic en **Nuevo registro**.
4. 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.
5. Haga clic en **Registrar**.

Resultado

Ha creado la aplicación AD y el director de servicio.

Asignación de 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:
 - 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.

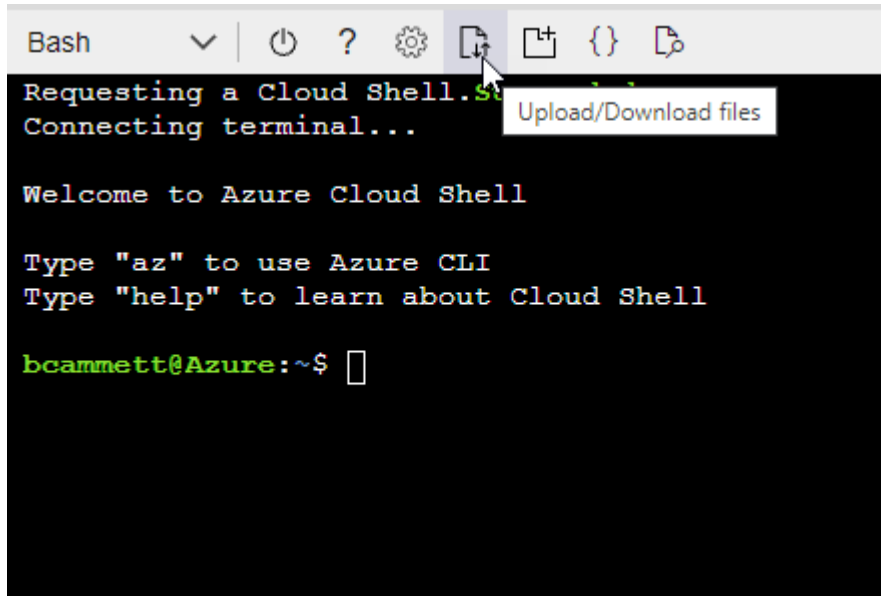
ejemplo

```
"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:

- En el portal de Azure, abra el servicio **Suscripciones**.
- Seleccione la suscripción.
- Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
- En la ficha **rol**, seleccione el rol **operador BlueXP** y haga clic en **Siguiente**.
- En la ficha **Miembros**, realice los siguientes pasos:
 - Mantener seleccionado **Usuario, grupo o principal de servicio**.
 - Haga clic en **Seleccionar miembros**.



- Busque el nombre de la aplicación.

Veamos un ejemplo:



- Seleccione la aplicación y haga clic en **Seleccionar**.
 - Haga clic en **Siguiente**.
- f. Haga clic en **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.

Agregar 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 **Azure Active Directory**, haga clic en **App registrs** y seleccione la aplicación.
2. Haga clic en **permisos de API > Agregar un permiso**.
3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.

Request API permissions













Select an API

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

Commonly used Microsoft APIs



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

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

4. Haga clic en **Access Azure Service Management como usuarios de la organización** y, a continuación, haga clic en **Agregar permisos**.

Request API permissions

[← All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

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

Obteniendo 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 **Azure Active Directory**, haga clic en **App registrs** y seleccione la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



Crear un secreto de cliente

Necesita crear un secreto de cliente y, a continuación, proporcionar BlueXP con el valor del secreto para que BlueXP pueda utilizarlo para autenticar con Azure AD.

Pasos

1. Abra el servicio **Azure Active Directory**.
2. Haga clic en **App registres** y seleccione su aplicación.
3. Haga clic en **certificados y secretos > Nuevo secreto de cliente**.

- Proporcione una descripción del secreto y una duración.
- Haga clic en **Agregar**.
- Copie el valor del secreto de cliente.

Client secrets

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

+ New client secret			
DESCRIPTION	EXPIRES	VALUE	
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	Copy to clipboard

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.

Agregar 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.

Lo que necesitará

Debe crear un conector para poder cambiar la configuración de BlueXP. ["Vea cómo"](#).

Pasos

- En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.



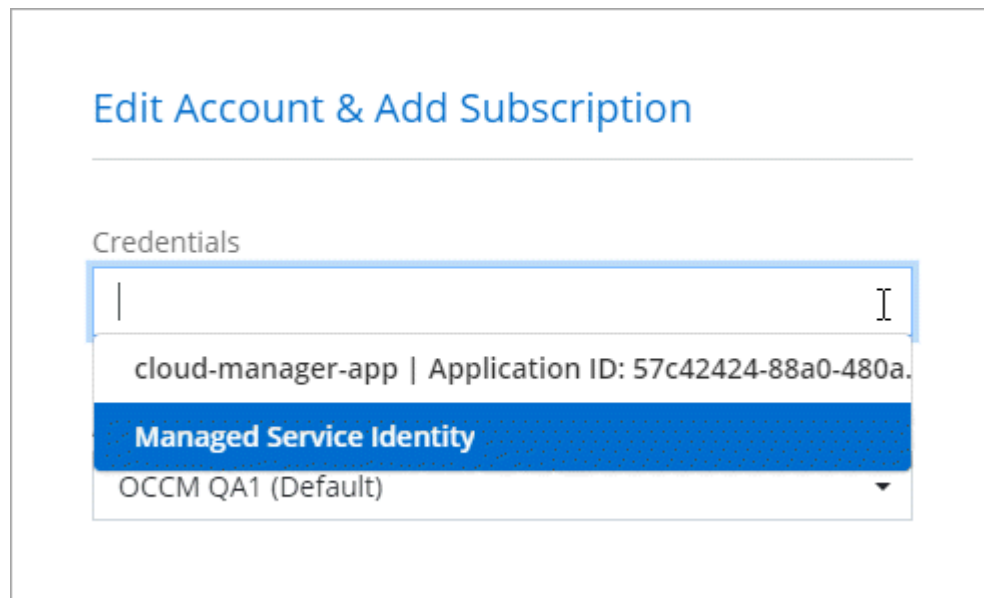
- Haga clic en **Agregar credenciales** y siga los pasos del asistente.
 - Ubicación de credenciales:** Seleccione **Microsoft Azure > conector**.
 - Definir credenciales:** Introduzca información acerca del principal de servicio de Azure Active Directory que otorga los permisos necesarios:
 - ID de aplicación (cliente): Consulte [Obteniendo el ID de aplicación y el ID de directorio](#).
 - ID de directorio (arrendatario): Consulte [Obteniendo el ID de aplicación y el ID de directorio](#).
 - Client Secret: Consulte [Crear un secreto de cliente](#).
 - Suscripción al mercado:** Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

Para pagar por Cloud Volumes ONTAP a una tarifa por hora (PAYGO), estas credenciales de Azure deben estar asociadas con una suscripción a Azure Marketplace.

d. **Revisión:** Confirme los detalles acerca de las nuevas credenciales y haga clic en **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.

Asociación de 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 le permite crear un sistema de pago por uso Cloud Volumes ONTAP y usar otros servicios cloud de NetApp.

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

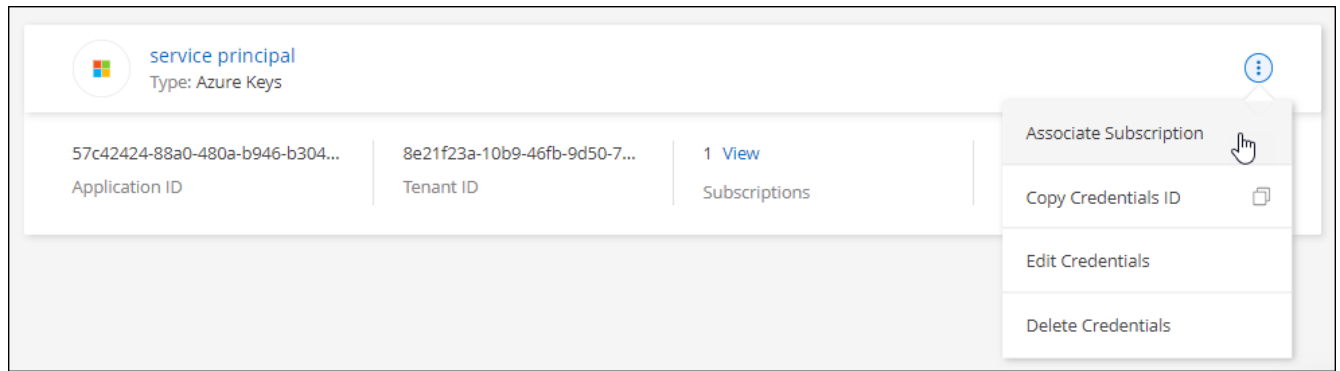
- No asoció una suscripción cuando agregó inicialmente las credenciales a BlueXP.
- Desea sustituir una suscripción existente de Azure Marketplace por una nueva suscripción.

Lo que necesitará

Debe crear un conector para poder cambiar la configuración de BlueXP. "[Vea cómo](#)".

Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Suscripción asociada**.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y haga clic en **asociado**.
4. Para asociar las credenciales con una nueva suscripción, haga clic en **Agregar suscripción > continuar** y siga los pasos de Azure Marketplace:
 - a. Si se le solicita, inicie sesión en su cuenta de Azure.
 - b. Haga clic en **Suscribirse**.
 - c. Rellene el formulario y haga clic en **Suscribirse**.
 - d. Una vez completado el proceso de suscripción, haga clic en **Configurar cuenta ahora**.

Se le redirigirá al sitio web de BlueXP.

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

- Seleccione las cuentas de NetApp a las que desea asociar esta suscripción.
- En el campo **sustituir suscripción existente**, elija si desea sustituir automáticamente la suscripción existente para una cuenta con esta nueva suscripción.

BlueXP reemplaza la suscripción existente para todas las credenciales de la 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 el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Haga clic en **Guardar**.

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

► https://docs.netapp.com/es-es/cloud-manager-setup-admin//media/video_subscribing_azure.mp4

(video)

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, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Editar credenciales**.
3. Realice los cambios necesarios y, a continuación, haga clic en **aplicar**.

Eliminación de 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, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Eliminar credenciales**.
3. Haga clic en **Eliminar** para confirmar.

Información de copyright

Copyright © 2023 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.