



Azure

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

- Azure 1
 - Credenciales y permisos de Azure 1
 - Administrar credenciales y suscripciones de Azure para Cloud Manager 3

Azure

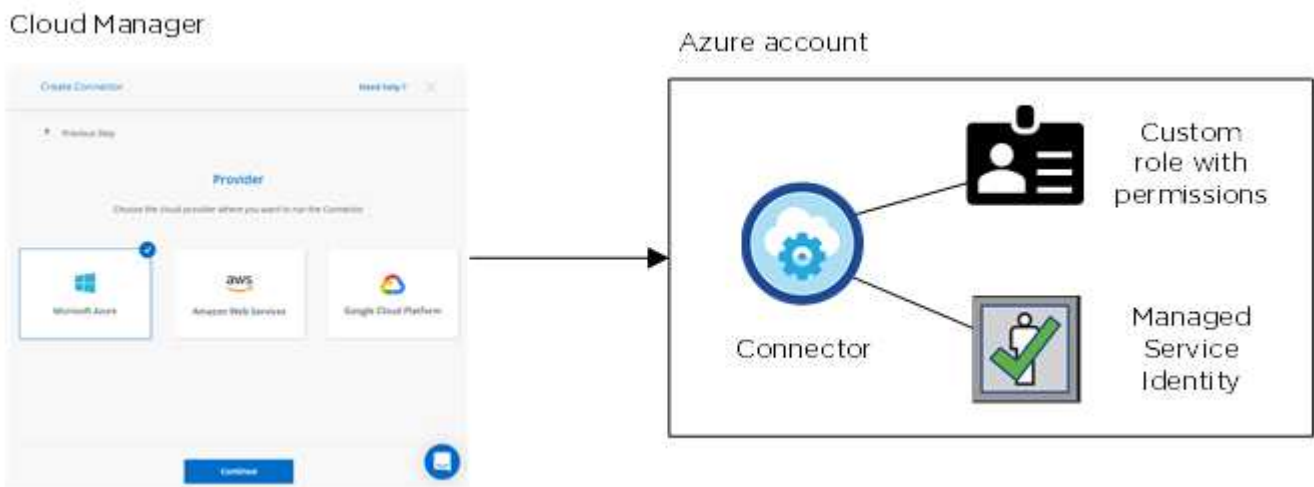
Credenciales y permisos de Azure

Cloud Manager permite elegir las credenciales de Azure que se utilizarán al implementar 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 Cloud Manager, necesita utilizar una cuenta de Azure que tenga permisos para implementar la máquina virtual Connector. Los permisos necesarios se enumeran en la ["Política de implementación de conectores para Azure"](#).

Cuando Cloud Manager implementa 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. El rol proporciona permisos a Cloud Manager para gestionar recursos y procesos dentro de esa suscripción de Azure. ["Revise cómo Cloud Manager utiliza los permisos"](#).



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

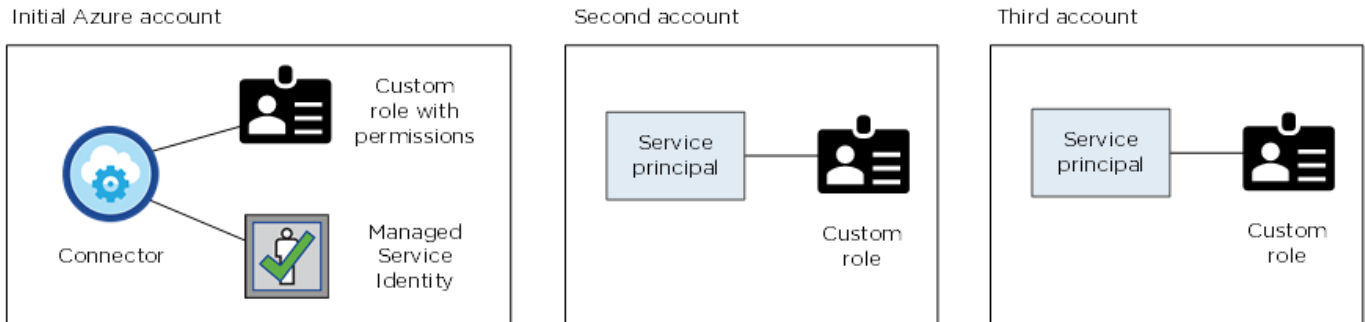
Details & Credentials			
Managed Service Ide...	OCCM QA1	ⓘ No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

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"](#).

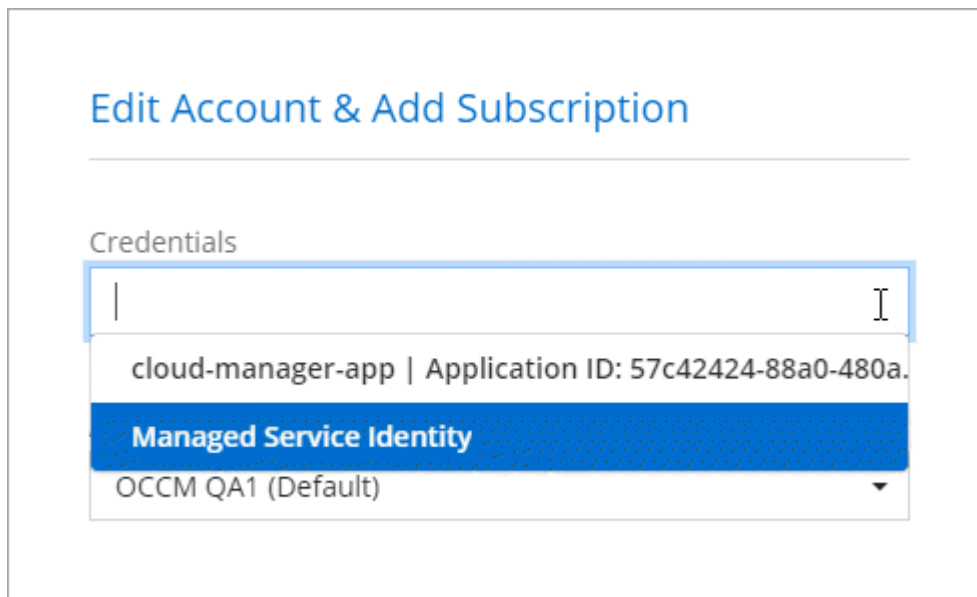
Credenciales adicionales de Azure

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 Directorio"](#) 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 ["Añada las credenciales de la cuenta a Cloud Manager"](#) 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:



¿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 puesta en marcha recomendado para el conector, que es de NetApp Cloud Central. 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.

Administrar credenciales y suscripciones de Azure para Cloud Manager

Al crear un sistema Cloud Volumes ONTAP, necesita seleccionar las credenciales de Azure y la suscripción a Marketplace para utilizar con ese sistema. Si gestiona varias suscripciones a Azure Marketplace, puede asignar cada una de ellas a diferentes credenciales de Azure desde la página Credentials.

Existen dos formas de gestionar las credenciales de Azure en Cloud Manager. En primer lugar, si desea implementar Cloud Volumes ONTAP en diferentes cuentas de Azure, tendrá que proporcionar los permisos necesarios y añadir las credenciales a Cloud Manager. La segunda es asociar suscripciones adicionales a la identidad administrada de Azure.



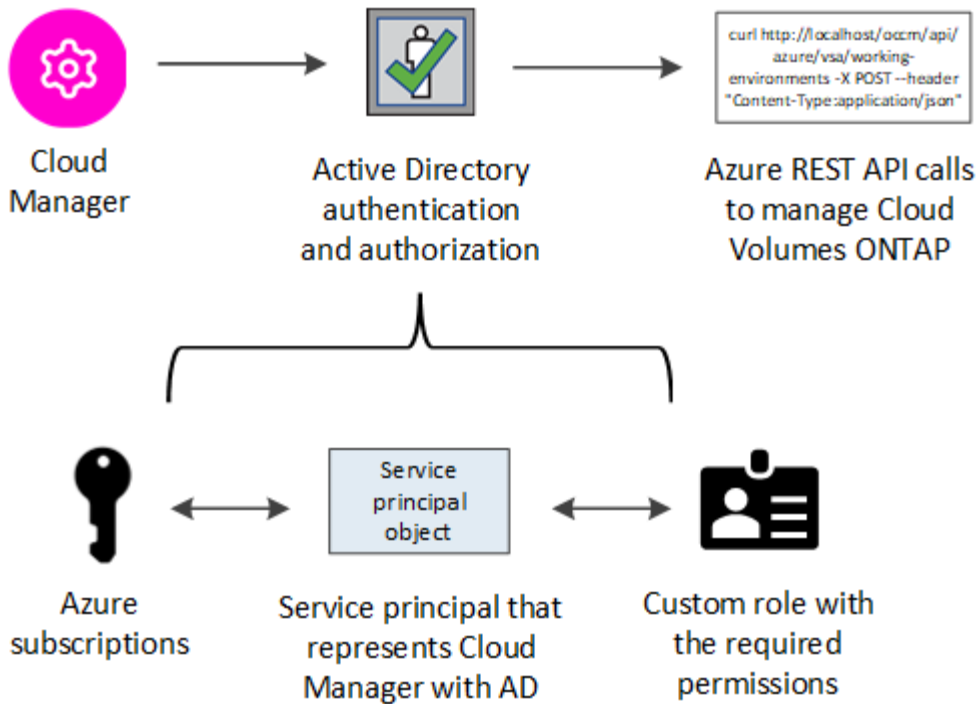
Cuando implementa un conector desde Cloud Manager, Cloud Manager agrega automáticamente la cuenta de Azure en la que implementó Connector. No se agrega una cuenta inicial si instaló manualmente el software Connector en un sistema existente. "[Obtenga más información acerca de las cuentas y los permisos de Azure](#)".

Concesión de permisos de Azure con un director de servicio

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

Acerca de esta tarea

La siguiente imagen muestra cómo Cloud Manager obtiene permisos para realizar operaciones en Azure. Un objeto principal de servicio, que está vinculado a una o varias suscripciones de Azure, representa Cloud Manager 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

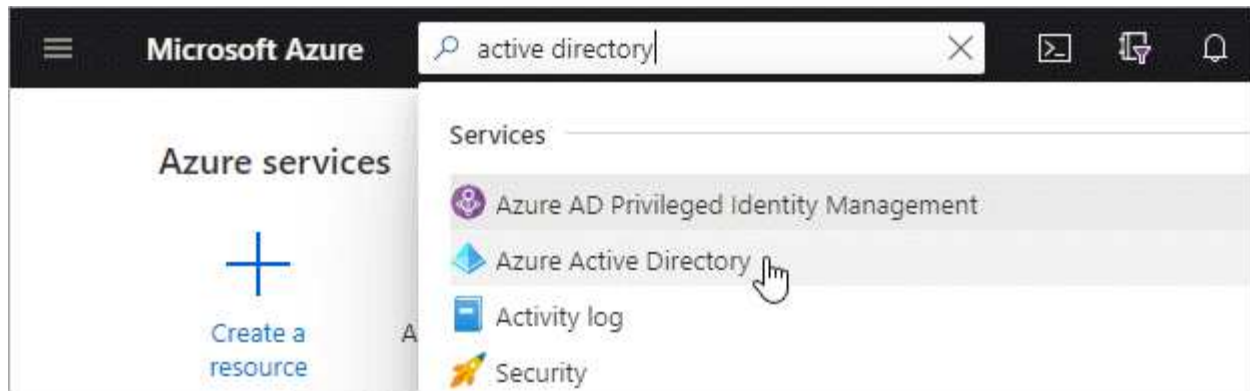
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que Cloud Manager pueda usar para el control de acceso basado en roles.

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 Cloud Manager).
 - **Redirigir URI:** Seleccione **Web** y, a continuación, escriba cualquier dirección URL; por ejemplo, https://url
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 personalizado de operador de "OnCommand Cloud Manager" para que Cloud Manager tenga permisos en Azure.

Pasos

1. Crear un rol personalizado:
 - a. Descargue el "[Política de Azure de Cloud Manager](#)".
 - 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.


El ejemplo siguiente muestra cómo crear una función personalizada con la CLI de Azure 2.0:

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

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](#)

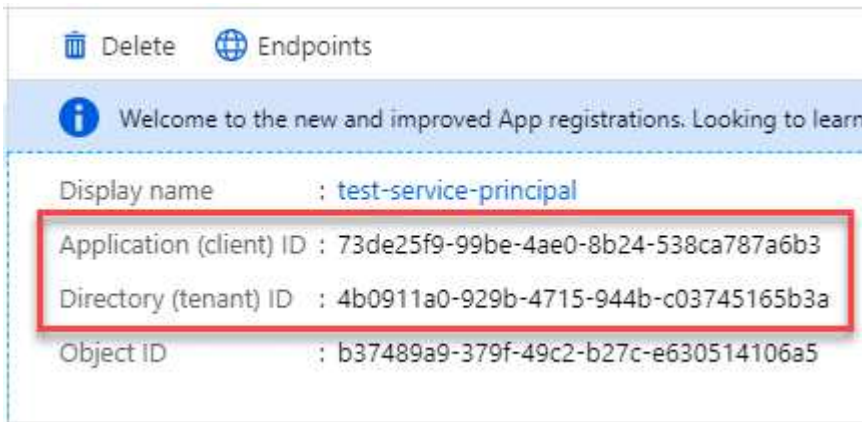
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) 	-

Obteniendo el ID de aplicación y el ID de directorio

Cuando agrega la cuenta de Azure a Cloud Manager, necesita proporcionar el ID de la aplicación (cliente) y el ID de directorio (inquilino) para la aplicación. Cloud Manager utiliza los ID 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)**.



Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

Crear un secreto de cliente

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



Al agregar la cuenta a Cloud Manager, Cloud Manager hace referencia al secreto de cliente como la clave de aplicación.

Pasos

1. Abra el servicio **Azure Active Directory**.
2. Haga clic en **App registros** y seleccione su aplicación.
3. Haga clic en **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Haga clic en **Agregar**.
6. 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.

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 Cloud Manager al añadir una cuenta de Azure.

Añadir credenciales de Azure a Cloud Manager

Después de proporcionar una cuenta de Azure con los permisos requeridos, puede añadir las credenciales para esa cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "[Vea cómo](#)".

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.



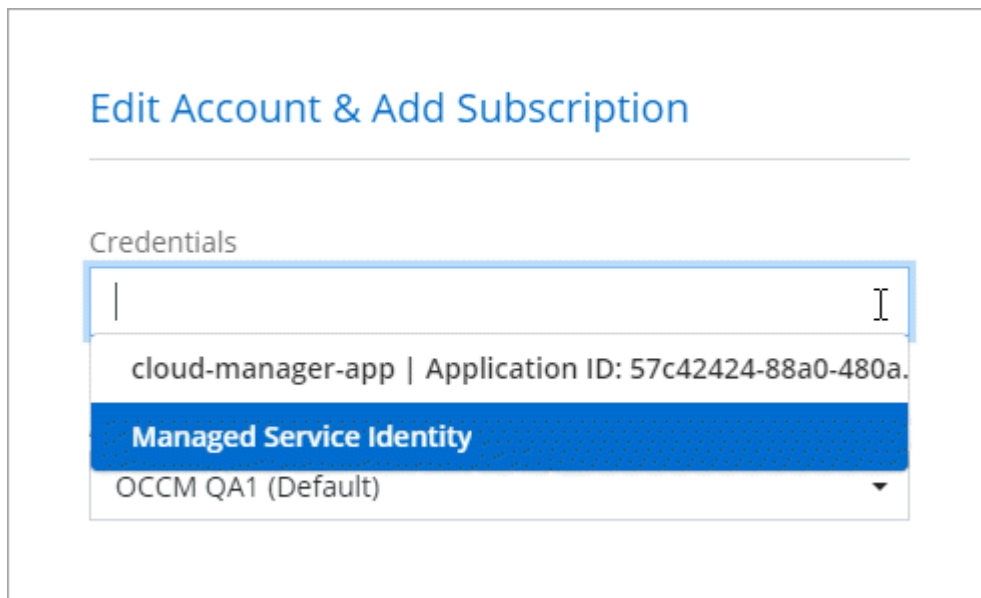
2. Haga clic en **Agregar credenciales** y seleccione **Microsoft Azure**.
3. Introduzca la información acerca del director del servicio de Azure Active Directory que otorga los permisos necesarios:
 - ID de aplicación (cliente): Consulte [Obteniendo el ID de aplicación y el ID de directorio](#).
 - ID de directorio (arrendatario): Consulte [Obteniendo el ID de aplicación y el ID de directorio](#).
 - Client Secret: Consulte [Crear un secreto de cliente](#).
4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **continuar**.
5. Elija la suscripción de pago por uso que desee asociar con las credenciales o haga clic en **Agregar suscripción** si aún no tiene una.

Para crear un sistema de Cloud Volumes ONTAP de pago por uso, las credenciales de Azure deben estar asociadas con una suscripción a Cloud Volumes ONTAP desde Azure Marketplace.

6. 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"](#):



Asociación de una suscripción de Azure Marketplace a credenciales

Después de añadir sus credenciales de Azure a Cloud Manager, 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 escenarios en los que puede asociar una suscripción a Azure Marketplace después de haber añadido las credenciales a Cloud Manager:

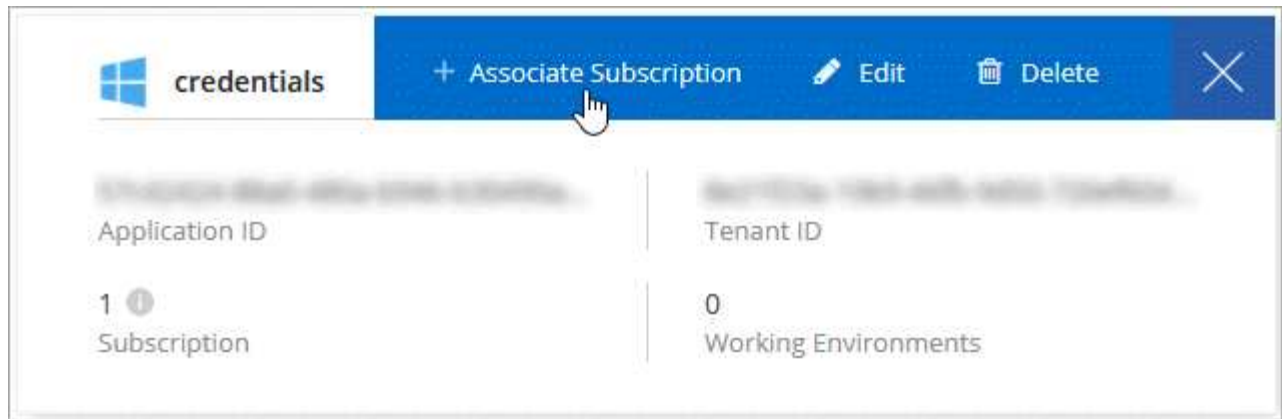
- No asoció una suscripción al agregar inicialmente las credenciales a Cloud Manager.
- Desea sustituir una suscripción existente de Azure Marketplace por una nueva suscripción.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. ["Vea cómo"](#).

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Pase el ratón sobre un conjunto de credenciales y haga clic en el menú de acciones.
3. En el menú, haga clic en **Suscripción asociada**.



4. Seleccione una suscripción de la lista desplegable o haga clic en **Agregar suscripción** y siga los pasos para crear una nueva suscripción.

El siguiente vídeo se inicia desde el contexto del asistente de entorno de trabajo, pero muestra el mismo flujo de trabajo después de hacer clic en **Agregar suscripción**:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure.mp4 (video)

Asociar suscripciones de Azure adicionales a una identidad administrada

Cloud Manager le permite elegir las credenciales de Azure y la suscripción a Azure en la que desea 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 implementar un conector desde Cloud Manager. Cuando implementó el conector, Cloud Manager creó el rol de operador de Cloud Manager y lo 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 Cloud Manager**.

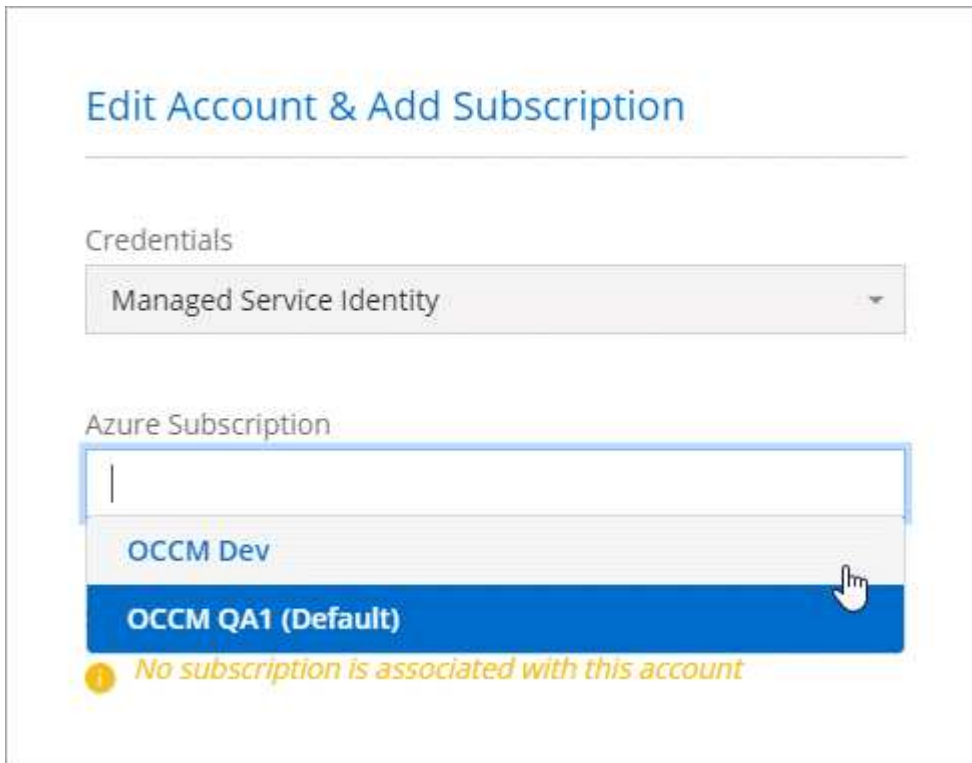


Es el nombre predeterminado que se proporciona en la "Política de Cloud Manager". Si seleccionó otro nombre para el rol, seleccione ese nombre.

- 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.



Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.