



Más formas de crear conectores

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

- Más formas de crear conectores 1
 - Requisitos del host del conector 1
 - Creación de un conector desde AWS Marketplace 2
 - Creación de un conector desde Azure Marketplace 5
 - Instalar el software del conector en un host Linux existente 8

Más formas de crear conectores

Requisitos del host del conector

El software del conector debe ejecutarse en un host que cumpla con requisitos específicos del sistema operativo, requisitos de RAM, requisitos de puerto, etc.

Se requiere un host dedicado

El conector no es compatible con un host compartido con otras aplicaciones. El host debe ser un host dedicado.

CPU

4 núcleos o 4 vCPU

RAM

14 GB

Tipo de instancia de AWS EC2

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos t3.xlarge y el uso de ese tipo de instancia al implementar el conector directamente desde Cloud Manager.

Tamaño de la máquina virtual de Azure

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos DS3 v2 y utilizar ese tamaño de equipo virtual al implementar el conector directamente desde Cloud Manager.

Tipo de máquina GCP

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Le recomendamos n1-standard-4 y utilizar ese tipo de máquina cuando ponga en marcha el conector directamente desde Cloud Manager.

Sistemas operativos compatibles

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

El sistema Red Hat Enterprise Linux debe estar registrado con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software necesario de terceros durante la instalación del conector.

El conector es compatible con las versiones en inglés de estos sistemas operativos.

Hipervisor

Un hipervisor de configuración básica o alojado certificado Ejecute CentOS o Red Hat Enterprise Linux <https://access.redhat.com/certified-hypervisors>["Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"^]

Espacio en disco en /opt

Debe haber 100 GB de espacio disponibles

Acceso a Internet de salida

Se requiere acceso saliente a Internet para instalar el conector y el conector para gestionar recursos y procesos dentro de su entorno de cloud público. Para ver una lista de extremos, consulte ["Requisitos de red para el conector"](#).

Creación de un conector desde AWS Marketplace

Es mejor crear un conector directamente desde Cloud Manager, pero puede iniciar un conector desde AWS Marketplace, si prefiere no especificar claves de acceso de AWS. Después de crear y configurar el conector, Cloud Manager lo utilizará automáticamente al crear nuevos entornos de trabajo.

Pasos

1. Crear una política de IAM y un rol para la instancia de EC2:
 - a. Descargue la política de IAM de Cloud Manager desde la siguiente ubicación:

["NetApp Cloud Manager: Políticas de AWS, Azure y GCP"](#)
 - b. Desde la consola de IAM, cree su propia política copiando y pegando el texto de la política IAM de Cloud Manager.
 - c. Cree un rol IAM con el tipo de rol Amazon EC2 y asocie la política que ha creado en el paso anterior al rol.
2. Ahora vaya a la ["Cloud Manager en el mercado de AWS"](#) Para poner en marcha Cloud Manager desde una AMI.

El usuario de IAM debe disponer de permisos de AWS Marketplace para suscribirse y cancelar la suscripción.

3. En la página Marketplace, haga clic en **continuar a Suscribirse** y luego haga clic en **continuar a Configuración**.

a

Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

Typical Total Price
\$0.226/hr

Total pricing per instance for services hosted on t3.xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

Product Overview

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

Highlights

- See Product Overview for instructions on how to deploy NetApp Cloud Manager.

b

Cloud Manager - Manual Installation without access keys

[Continue to Configuration](#)

< Product Detail [Subscribe](#)

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

- Cambie cualquiera de las opciones predeterminadas y haga clic en **continuar a Iniciar**.
- En **elegir acción**, seleccione **Iniciar a través de EC2** y, a continuación, haga clic en **Iniciar**.

Estos pasos describen cómo iniciar la instancia desde la consola EC2 porque la consola permite asociar un rol IAM a la instancia de Cloud Manager. Esto no es posible usando la acción **Iniciar desde el sitio web**.

- Siga las instrucciones para configurar y desplegar la instancia:
 - elegir tipo de instancia:** En función de la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.xlarge).

["Revise los requisitos de la instancia"](#).

- **Configurar instancia:** Seleccione un VPC y una subred, elija la función de IAM que creó en el paso 1, habilite la protección de terminación (recomendado) y elija cualquier otra opción de configuración que cumpla sus requisitos.

Number of instances ⓘ	<input type="text" value="1"/>	Launch into Auto Scaling Group ⓘ
Purchasing option ⓘ	<input type="checkbox"/> Request Spot instances	
Network ⓘ	<input type="text" value="vpc-a76d91c2 VPC4QA (default)"/>	Create new VPC
Subnet ⓘ	<input type="text" value="subnet-39536c13 QASubnet1 us-east-1b"/> 155 IP Addresses available	Create new subnet
Auto-assign Public IP ⓘ	<input type="text" value="Enable"/>	
Placement group ⓘ	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation ⓘ	<input type="text" value="Open"/>	Create new Capacity Reservation
IAM role ⓘ	<input type="text" value="Cloud_Manager"/>	Create new IAM role
CPU options ⓘ	<input type="checkbox"/> Specify CPU options	
Shutdown behavior ⓘ	<input type="text" value="Stop"/>	
Enable termination protection ⓘ	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring ⓘ	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	

- **almacenamiento:** Mantenga las opciones de almacenamiento predeterminadas.
- **Agregar etiquetas:** Introduzca etiquetas para la instancia, si lo desea.
- **Configurar grupo de seguridad:** Especifique los métodos de conexión necesarios para la instancia de conector: SSH, HTTP y HTTPS.
- **Revisión:** Revise sus selecciones y haga clic en **Iniciar**.

AWS inicia el software con la configuración especificada. La instancia y el software del conector deben estar funcionando en aproximadamente cinco minutos.

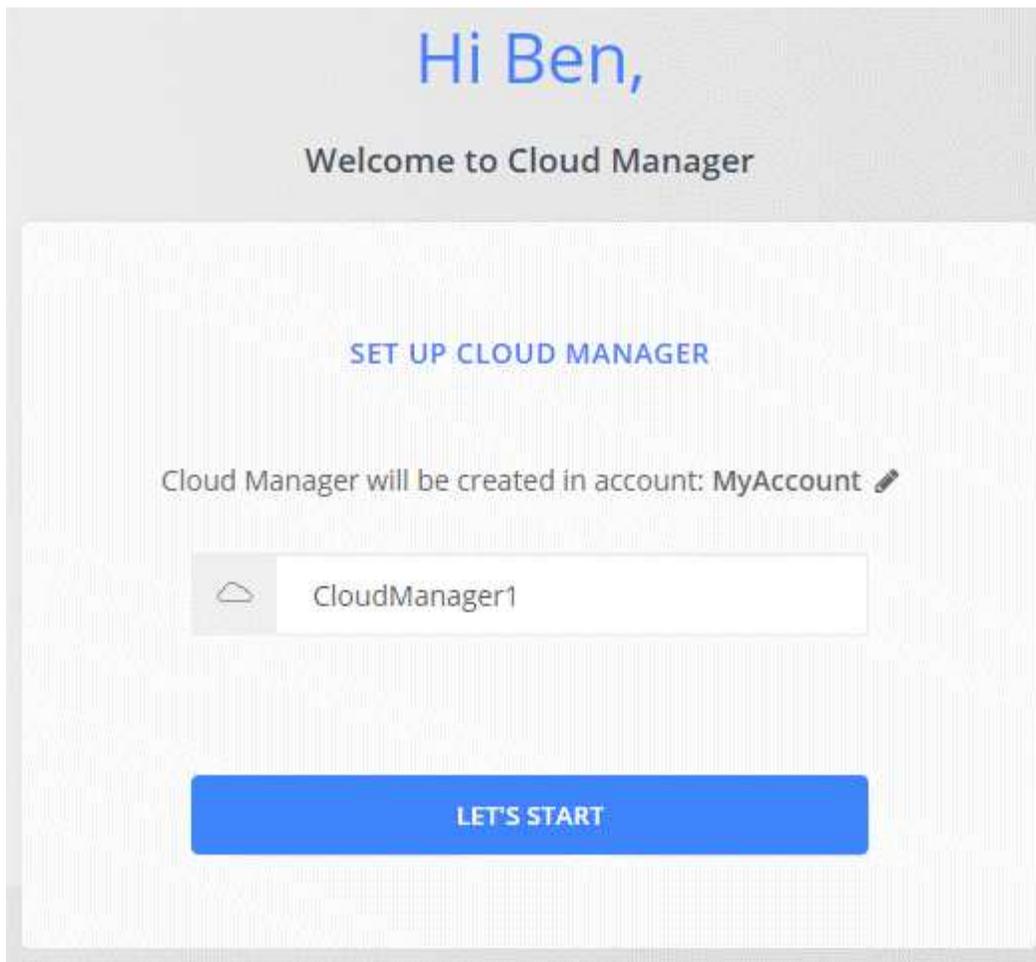
- Abra un explorador Web desde un host que tenga una conexión con la instancia de Connector e introduzca la siguiente URL:

```
<a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>
```

- Después de iniciar sesión, configure el conector:
 - Especifique la cuenta de Cloud Central que desea asociar con el conector.

["Obtenga más información acerca de las cuentas de Cloud Central"](#).

- Escriba un nombre para el sistema.



Resultado

El conector ya está instalado y configurado con su cuenta de Cloud Central. Cloud Manager utilizará automáticamente este conector cuando cree nuevos entornos de trabajo. Pero si tiene más de un conector, necesitará "[alterne entre ellos](#)".

Creación de un conector desde Azure Marketplace

Es mejor crear un conector directamente desde Cloud Manager, pero si lo prefiere, puede iniciar un conector desde Azure Marketplace. Después de crear y configurar el conector, Cloud Manager lo utilizará automáticamente al crear nuevos entornos de trabajo.

Creación de un conector en Azure

Implemente el conector en Azure con la imagen en Azure Marketplace y luego inicie sesión en el conector para especificar su cuenta de Cloud Central.

Pasos

1. "[Vaya a la página de Azure Marketplace para Cloud Manager](#)".
2. Haga clic en **Get Now** y, a continuación, haga clic en **Continue**.
3. En el portal de Azure, haga clic en **Crear** y siga los pasos para configurar la máquina virtual.

Tenga en cuenta lo siguiente al configurar la máquina virtual:

- Cloud Manager puede ofrecer un rendimiento óptimo tanto con discos HDD como SSD.
- Elija un tamaño de máquina virtual que cumpla los requisitos de CPU y RAM. Recomendamos DS3 v2.

["Revise los requisitos de las máquinas virtuales"](#).

- Para el grupo de seguridad de red, el conector requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

["Obtenga más información sobre las reglas de grupo de seguridad para el conector"](#).

- En **Gestión**, active **identidad administrada asignada por el sistema** para el conector seleccionando **On**.

Esta configuración es importante porque una identidad administrada permite que la máquina virtual Connector se identifique a sí misma en Azure Active Directory sin proporcionar credenciales. ["Obtenga más información sobre las identidades gestionadas para recursos de Azure"](#).

4. En la página **revisar + crear**, revise las selecciones y haga clic en **Crear** para iniciar la implementación.

Azure implementa la máquina virtual con los ajustes especificados. El software de la máquina virtual y el conector debe estar funcionando en aproximadamente cinco minutos.

5. Abra un explorador Web desde un host que tenga una conexión con la máquina virtual Connector e introduzca la siguiente URL:

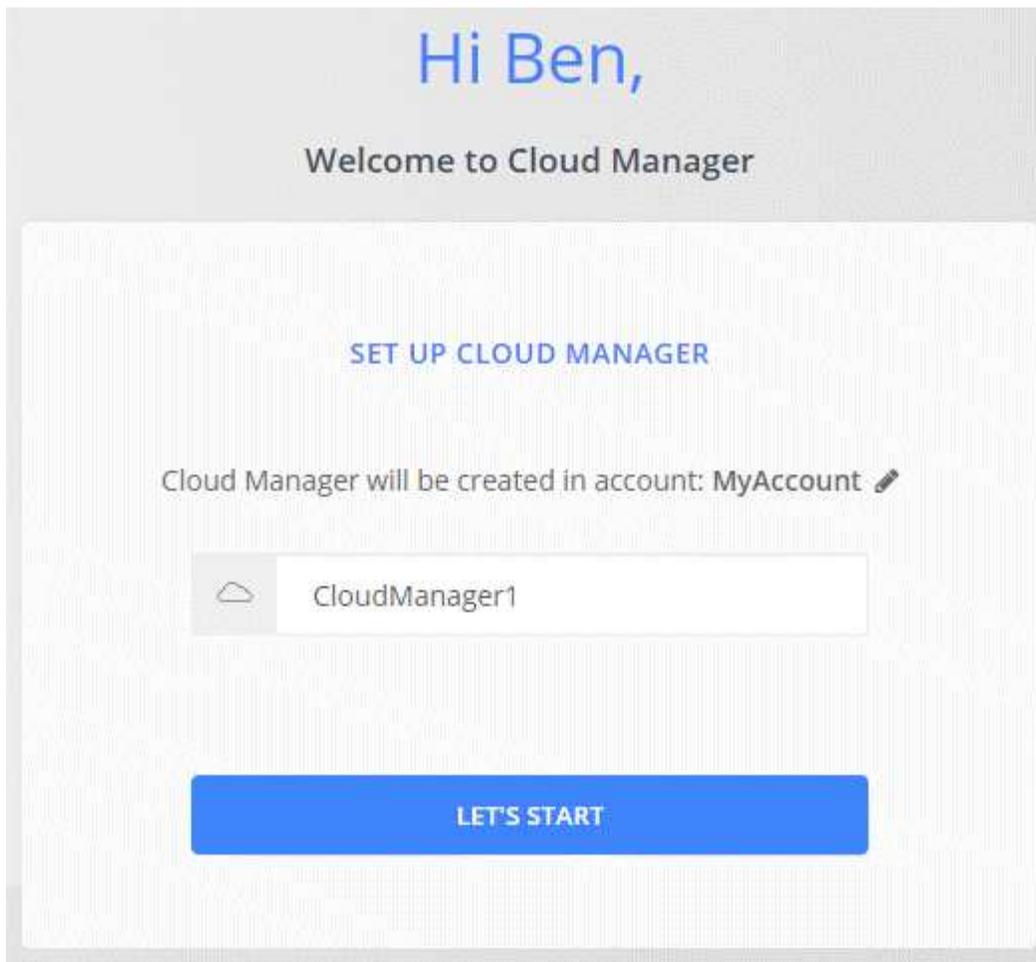
```
<a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>
```

6. Después de iniciar sesión, configure el conector:

- a. Especifique la cuenta de Cloud Central que desea asociar con el conector.

["Obtenga más información acerca de las cuentas de Cloud Central"](#).

- b. Escriba un nombre para el sistema.



Resultado

El conector ahora está instalado y configurado. Debe conceder permisos de Azure para que los usuarios puedan poner en marcha Cloud Volumes ONTAP en Azure.

Concesión de permisos de Azure

Cuando implementó Connector en Azure, debería haber habilitado un ["identidad administrada asignada por el sistema"](#). Ahora debe conceder los permisos de Azure necesarios creando una función personalizada y, a continuación, asignando la función a la máquina virtual Connector para una o más suscripciones.

Pasos

1. Cree un rol personalizado mediante la política de Cloud Manager:
 - 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-  
3bzb6b6b6b3b6bbb3bzb6b6b3b6b3bb6b3b6x-b6b6b3bb
```

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:

```
az role definition create --role-definition
C:\Policy_for_cloud_Manager_Azure_3.8.7.json
```

Ahora debe tener un rol personalizado denominado operador de Cloud Manager que puede asignar a la máquina virtual conector.

2. Asigne el rol a la máquina virtual conector para una o más suscripciones:

- a. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar sistemas Cloud Volumes ONTAP.
- b. Haga clic en **Control de acceso (IAM)**.
- c. 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**.
- d. Si desea implementar Cloud Volumes ONTAP desde suscripciones adicionales, cambie a esa suscripción y repita estos pasos.

Resultado

Connector ahora tiene los permisos que necesita para gestionar recursos y procesos en su entorno de cloud público. Cloud Manager utilizará automáticamente este conector cuando cree nuevos entornos de trabajo. Pero si tiene más de un conector, necesitará "[alterne entre ellos](#)".

Instalar el software del conector en un host Linux existente

La forma más común de crear un conector es directamente desde Cloud Manager o desde el mercado de un proveedor de cloud. Pero tiene la opción de descargar e instalar el software Connector en un host Linux existente en su red o en la nube.



Si desea crear un sistema Cloud Volumes ONTAP en Google Cloud, también debe tener un conector en Google Cloud. No puede utilizar un conector que se ejecute en otra ubicación.

Requisitos

- El host debe encontrarse "[Requisitos para el conector](#)".
- Debe registrarse un sistema Red Hat Enterprise Linux con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software necesario de terceros durante la instalación.
- El instalador del conector tiene acceso a varias direcciones URL durante el proceso de instalación. Debe

asegurarse de que se permita el acceso saliente a Internet a estos puntos finales:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

Es posible que el host intente actualizar paquetes de sistema operativo durante la instalación. El host puede ponerse en contacto con diferentes sitios de duplicación para estos paquetes de SO.

Acerca de esta tarea

- No se requieren privilegios de usuario raíz para instalar el conector.
- La instalación instala las herramientas de línea de comandos de AWS (awscli) para habilitar los procedimientos de recuperación del soporte de NetApp.

Si recibe un mensaje que ha fallado al instalar el awscli, puede ignorar el mensaje de forma segura. El conector puede funcionar correctamente sin las herramientas.

- El instalador disponible en el sitio de soporte de NetApp puede ser una versión anterior. Después de la instalación, el conector se actualiza automáticamente si hay una nueva versión disponible.

Pasos

1. Descargue el software Cloud Manager del "[Sitio de soporte de NetApp](#)"Y, a continuación, cópielo en el host Linux.

Para obtener ayuda sobre la conexión y copia del archivo en una instancia de EC2 en AWS, consulte "[Documentación de AWS: Conexión a la instancia de Linux mediante SSH](#)".

2. Asigne permisos para ejecutar el script.

ejemplo

```
chmod +x OnCommandCloudManager-V3.8.4.sh
. Ejecute el script de instalación:
```

```
./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

silent ejecuta la instalación sin solicitar información.

se requiere *proxy* si el host está detrás de un servidor proxy.

proxyport es el puerto del servidor proxy.

proxyuser es el nombre de usuario del servidor proxy, si se requiere autenticación básica.

proxypwd es la contraseña del nombre de usuario que ha especificado.

3. A menos que haya especificado el parámetro *silent*, escriba **y** para continuar la secuencia de comandos y, a continuación, introduzca los puertos HTTP y HTTPS cuando se le solicite.

Cloud Manager ya está instalado. Al finalizar la instalación, el servicio Cloud Manager (occm) se reinicia dos veces si especificó un servidor proxy.

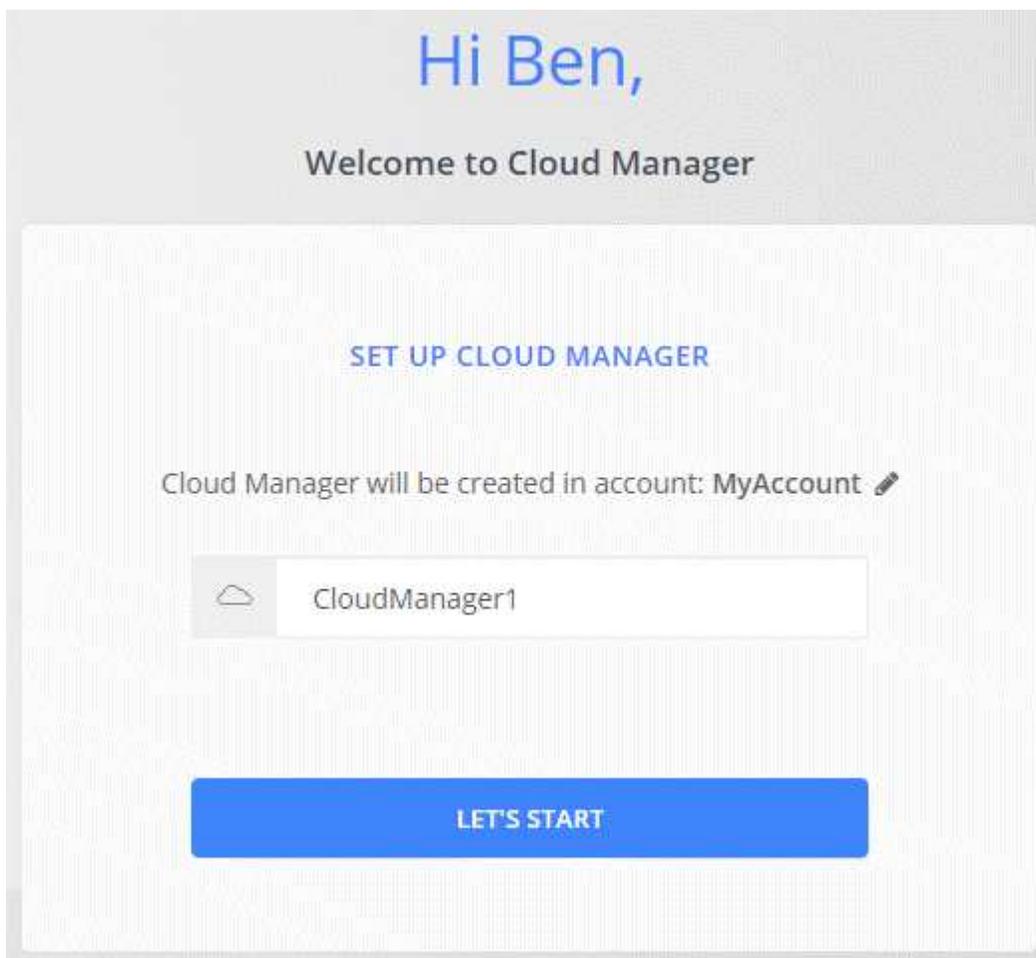
- Abra un explorador web e introduzca la siguiente URL:

```
<a href="https://<em>ipaddress</em>:<em>port</em>" class="bare">https://<em>ipaddress</em>:<em>port</em></a>
```

ipaddress puede ser localhost, una dirección IP privada o una dirección IP pública, dependiendo de la configuración del host. Por ejemplo, si el conector está en la nube pública sin una dirección IP pública, debe introducir una dirección IP privada desde un host que tenga una conexión con el host del conector.

Port es obligatorio si cambia los puertos HTTP (80) o HTTPS (443) predeterminados. Por ejemplo, si el puerto HTTPS se ha cambiado a 8443, debe introducir `https://ipaddress:8443`

- Regístrese en NetApp Cloud Central o inicie sesión.
- Después de iniciar sesión, configure Cloud Manager:
 - Especifique la cuenta de Cloud Central que desea asociar con el conector.
["Obtenga más información acerca de las cuentas de Cloud Central"](#).
 - Escriba un nombre para el sistema.



Resultado

El conector ya está instalado y configurado con su cuenta de Cloud Central. Cloud Manager utilizará automáticamente este conector cuando cree nuevos entornos de trabajo.

Después de terminar

Configure permisos para que Cloud Manager pueda gestionar recursos y procesos en su entorno de cloud público:

- AWS: ["Configure una cuenta de AWS y, a continuación, añádela Cloud Manager"](#).
- Azure: ["Configure una cuenta de Azure y añada a. Cloud Manager"](#).
- GCP: Configure una cuenta de servicio que tenga los permisos que Cloud Manager necesita para crear y gestionar sistemas Cloud Volumes ONTAP en proyectos.
 - a. ["Crear un rol en GCP"](#) esto incluye los permisos definidos en la ["Política de Cloud Manager para GCP"](#).
 - b. ["Cree una cuenta de servicio de GCP y aplique el rol personalizado que acaba de crear"](#).
 - c. ["Asocie esta cuenta de servicio a la máquina virtual del conector"](#).
 - d. Si desea poner en marcha Cloud Volumes ONTAP en otros proyectos, ["Conceda el acceso añadiendo la cuenta de servicio con la nube La función de gerente de ese proyecto"](#). Deberá repetir este paso con cada proyecto.

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.