



Primeros pasos

Converged Systems Advisor

NetApp
October 04, 2023

Tabla de contenidos

- Primeros pasos 1
 - Puesta en marcha rápida para Converged Systems Advisor..... 1
 - Prepare su entorno 2
 - Crear cuentas para dispositivos FlexPod..... 2
 - Configurar e implementar el agente 7
 - Añada infraestructura al portal 10
 - Compartir una infraestructura con otros usuarios 11
 - Configurar notificaciones 12
 - Establezca una dirección IP estática en el agente..... 12

Primeros pasos

Puesta en marcha rápida para Converged Systems Advisor

Los primeros pasos con el agente de Converged Systems Advisor y el portal para FlexPod incluyen algunos pasos.

1 Prepare su entorno

Verifique la compatibilidad con la configuración. "[Prepare su entorno](#)".

2 Crear cuentas en dispositivos FlexPod

Configure cuentas en Cisco UCS Manager, en los switches Cisco Nexus, para sus sistemas ONTAP, para VMware y en la APIC. El agente utiliza estas cuentas para recopilar datos de configuración. "[Crear cuentas en dispositivos FlexPod](#)".

3 Conceda privilegios de usuario de CSA mediante un servidor TACACS+

Para aquellos que utilizan un servidor TACACS+, debe otorgar privilegios de usuario de CSA para los conmutadores, crear un grupo de privilegios de usuario y conceder acceso de grupo a los comandos de configuración específicos que necesita CSA. "[Conceda privilegios de usuario de CSA mediante un servidor TACACS+](#)".

4 Configurar e implementar el agente

Ponga en marcha el agente de Converged Systems Advisor en un servidor VMware ESXi. El agente recopila datos de configuración sobre cada dispositivo en la infraestructura convergente de FlexPod y los envía al portal del Asesor de sistemas convergentes. "[Despliegue el agente](#)".

5 Añada/comparta infraestructura en el portal

Añada cada dispositivo FlexPod al portal Converged Systems Advisor para crear una infraestructura completa que pueda supervisar. También puede compartir una infraestructura convergente para permitir a otra persona iniciar sesión en el portal de manera que pueda ver y supervisar la configuración. "[Añada y comparta infraestructura en el portal](#)".

6 Configurar notificaciones

Con una licencia Premium, puede configurar notificaciones que avisen de los cambios en la infraestructura de FlexPod mediante notificaciones por correo electrónico. "[Configurar notificaciones](#)".

7

Configure una dirección IP estática

Si su entorno no tiene un servidor DHCP, puede establecer una dirección IP estática en el agente Converged Systems Advisor. ["Establezca una dirección IP estática en el agente"](#)

Prepare su entorno

Para empezar a usar Converged Systems Advisor, debe preparar su entorno. Preparar el entorno incluye verificar la compatibilidad de la configuración y registrar una cuenta del sitio de soporte de NetApp.

Tal vez le interese ["Descubra cómo funciona Converged Systems Advisor"](#) antes de empezar.

Pasos

1. Verifique la compatibilidad en la ["Herramienta de matriz de interoperabilidad de NetApp"](#):
 - a. Compruebe que el asesor de sistemas convergentes admite su infraestructura convergente de FlexPod.
 - b. Compruebe que dispone de un servidor VMware ESXi compatible para el agente Converged Systems Advisor.

Para minimizar el uso del ancho de banda, NetApp recomienda la instalación del agente en el mismo centro de datos que la infraestructura convergente de FlexPod.

2. Asegúrese de que la red en la que instala el agente permite la conectividad entre los componentes:
 - El agente debe tener conectividad con cada componente FlexPod para poder recopilar datos de configuración.
 - El agente también requiere una conexión saliente a Internet para comunicarse con los siguientes puntos finales:
 - csa.netapp.com
 - docker.com
 - docker.io

3. Vaya a la ["Sitio de soporte de NetApp"](#) y regístrese para una cuenta, si no dispone de una.

Se necesita una cuenta en la página de soporte de NetApp para configurar el agente y acceder al portal.

Crear cuentas para dispositivos FlexPod

Para comenzar, configure cuentas para dispositivos FlexPod:

- [Cree una cuenta de solo lectura para Cisco UCS Manager](#)
- [Cree una cuenta de solo lectura para los switches Nexus](#)
- [Cree una cuenta de administrador para ONTAP](#)
- [Cree una cuenta de solo lectura para VMware](#)
- [Cree una cuenta de solo lectura en la APIC](#)

- [Conceda privilegios de usuario de CSA mediante un servidor TACACS+](#)

El agente utiliza estas cuentas para recopilar información de configuración de cada dispositivo.

Cree una cuenta de solo lectura para Cisco UCS Manager

Pasos

1. Inicie sesión en Cisco UCS Manager.
2. Cree un usuario autenticado localmente denominado *csa-readonly*.



De forma predeterminada, todos los usuarios nuevos son de sólo lectura.

Cree una cuenta de solo lectura para los switches Nexus

Pasos

1. Inicie sesión en cada switch Nexus mediante SSH o Telnet.
2. Entre al modo de configuración global:

```
configure terminal
.. Create a new user:
```

```
username [name] password [password] role network-operator
.. Save the configuration:
```

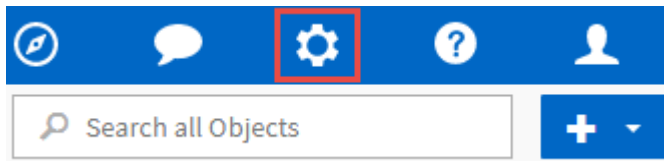
```
copy running configuration startup configuration
```

Si está utilizando un servidor TACACS+ y necesita otorgar privilegios de usuario de CSA, vaya a ["Concesión de privilegios de usuario de CSA mediante un servidor TACACS+"](#).

Cree una cuenta de administrador para ONTAP

Pasos

1. Inicie sesión en OnCommand System Manager y haga clic en el icono de configuración:



2. En la página usuarios, haga clic en **Agregar**.
3. Introduzca un nombre de usuario y una contraseña y añada **ssh**, **ontapi** y **Console** como métodos de inicio de sesión de usuario con acceso de administrador.

Add User

Username: CSA

Password:

Confirm Password:

User Login Methods

Application	Authentication	Role
console	Password	admin
ssh	Password	admin
ontapi	Password	admin

Tell me more about roles

Add Cancel

Cree una cuenta de solo lectura para VMware

Pasos

1. Inicie sesión en vCenter.
2. En el menú vCenter, seleccione **Administration**.
3. En roles, seleccione **sólo lectura**.
4. Haga clic en el icono **Clone Role action** y cambie el nombre a **CSA**.
5. Seleccione el rol **CSA** recién creado.
6. Haga clic en el icono **Editar función**.
7. En **Editar rol**, elija **Global** y, a continuación, seleccione **licencias**.
8. En la barra lateral, seleccione **Inicio de sesión único**→**usuarios y grupos**→**Crear un nuevo usuario**.
9. Nombre al nuevo usuario **CSARO** bajo EL DOMINIO vpsphere.local.
10. En la barra lateral, seleccione **permisos globales** en **Control de acceso**.
11. Elija el usuario **CSARO** y asigne EL ROL **CSA**.
12. Inicie sesión en Web Client.

Utilice el ID de usuario: **CSARO@vsphere.locloc I** y la contraseña creada previamente.

Cree una cuenta de solo lectura en la APIC

Pasos

1. Haga clic en **Admin**.
2. Haga clic en **Crear nuevos usuarios locales**.
3. En **identidad de usuario**, introduzca la información del usuario.
4. En **Seguridad**, seleccione todas las opciones de dominio de seguridad.
5. Haga clic en **+** para agregar certificados de usuario y claves SSH si es necesario.
6. Haga clic en **Siguiente**.
7. Haga clic en **+** para agregar funciones para su dominio.
8. Seleccione **Nombre de rol** en el menú desplegable.
9. Seleccione **Leer** para el **Tipo de privilegio de rol**.
10. Haga clic en **Finalizar**.

Conceda privilegios de usuario de CSA mediante un servidor TACACS+

Si está utilizando un servidor TACACS+ y necesita otorgar privilegios de usuario de CSA para los conmutadores, debe crear un grupo de privilegios de usuario y conceder acceso de grupo a los comandos de configuración específicos necesarios para CSA.

Los siguientes comandos se deben escribir en el archivo de configuración del servidor TACACS+.

Pasos

1. Introduzca lo siguiente para crear un grupo de privilegios de usuario con acceso de solo lectura:

```
group=group_name {
  default service=deny
  service=exec{
    priv-lvl=0
  }
}
```

1. Introduzca lo siguiente para otorgar acceso a los comandos que necesita CSA:

```
cmd=show {
  permit "environment"
  permit "version"
  permit "feature"
  permit "feature-set"
  permit hardware.*
  permit "interface"
  permit "interface"
  permit "interface transceiver"
  permit "inventory"
  permit "license"
  permit "module"
  permit "port-channel database"
  permit "ntp peers"
  permit "license usage"
  permit "port-channel summary"
  permit "running-config"
  permit "startup-config"
  permit "running-config diff"
  permit "switchname"
  permit "int mgmt0"
  permit "cdp neighbors detail"
  permit "vlan"
  permit "vpc"
  permit "vpc peer-keepalive"
  permit "mac address-table"
  permit "lACP port-channel"
  permit "policy-map"
  permit "policy-map system type qos"
  permit "policy-map system type queuing"
  permit "policy-map system type network-qos"
  permit "zoneset active"
  permit "san-port-channel summary"
  permit "flogi database"
  permit "fcns database detail"
  permit "fcns database detail"
  permit "zoneset active"
  permit "vsan"
  permit "vsan usage"
  permit "vsan membership"
}
```

1. Introduzca lo siguiente para agregar la cuenta de usuario de CSA al grupo recién creado:


```
user=user_account{
  member=group_name
  login=file/etc/passwd
}
```

Configurar e implementar el agente

Debe implementar el agente de Converged Systems Advisor en un servidor VMware ESXi. El agente recopila datos de configuración sobre cada dispositivo en la infraestructura convergente de FlexPod y los envía al portal del Asesor de sistemas convergentes.

Pasos

1. [Descargue e instale el agente](#)
2. [Configurar la red para el agente](#)
3. [Instale un certificado SSL en el agente](#)
4. [Configure el agente para descubrir su infraestructura de FlexPod](#)

Descargue e instale el agente

Debe implementar el agente de Converged Systems Advisor en un servidor VMware ESXi.

Acerca de esta tarea

Para minimizar el uso de ancho de banda, debe instalar el agente en un servidor VMware ESXi que se encuentre en el mismo centro de datos que la configuración de FlexPod. El agente debe tener conectividad con cada componente de FlexPod y a Internet para poder enviar datos de configuración al portal de Converged Systems Advisor mediante el puerto HTTPS 443.

El agente se implementa como máquina virtual VMware vSphere a partir de una plantilla de formato de virtualización abierta (OVF). La plantilla está basada en Debian con 1 vCPU y 2 GB de RAM (puede que se necesite más para sistemas FlexPod múltiples o más grandes).

Pasos

1. Descargue el agente:
 - a. Inicie sesión en la ["Portal del asesor de sistemas convergentes"](#).
 - b. Haga clic en **Descargar agente**.
2. Instale el agente implementando la plantilla OVF en el servidor ESXi de VMware.

En algunas versiones de VMware, es posible que reciba una advertencia al implementar la plantilla OVF. La máquina virtual se desarrolló en la versión más reciente de vCenter con compatibilidad de hardware para versiones anteriores, lo que podría generar una advertencia. Debe revisar las opciones de configuración antes de reconocer la advertencia y continuar con la instalación.

Configurar la red para el agente

Debe asegurarse de que las redes estén configuradas correctamente en la máquina virtual del agente para

habilitar la comunicación entre el agente y los dispositivos FlexPod, así como entre el agente y varios puntos finales de Internet. Tenga en cuenta que la pila de red está deshabilitada en la máquina virtual hasta que el sistema se inicialice.

Pasos

1. Asegúrese de que una conexión a Internet saliente permite el acceso a los siguientes puntos finales:
 - `csa.netapp.com`
 - `docker.com`
 - `docker.io`
2. Inicie sesión en la consola de máquina virtual del agente mediante el cliente de VMware vSphere.

El nombre de usuario predeterminado es `csa` y la contraseña predeterminada es `netapp`.



POR motivos de seguridad, SSHD está desactivado de forma predeterminada.

3. Cuando se le solicite, cambie la contraseña predeterminada y anote la contraseña porque no puede recuperarse.

Después de cambiar la contraseña, el sistema se reinicia e inicia el software del agente.

4. Si DHCP no está disponible en la subred, configure una dirección IP estática y una configuración DNS utilizando las herramientas estándar de Debian y reinicie el agente.

["Haga clic aquí para obtener instrucciones detalladas"](#).

La configuración de red de la máquina virtual Debian toma como valor predeterminado DHCP. NetworkManager está instalado y proporciona una interfaz de usuario de texto que puede iniciar desde el comando `nmtui` (consulte la ["página de manual"](#) para obtener más detalles).

Para obtener ayuda adicional sobre las redes, consulte ["La página de configuración de red en el wiki de Debian"](#).

5. Si las políticas de seguridad determinan que el agente debe estar en una red para comunicarse con los dispositivos FlexPod y otra red para comunicarse con Internet, añada una segunda interfaz de red en vCenter y configure las VLAN y las direcciones IP correctas.
6. Si se necesita un servidor proxy para el acceso a Internet, ejecute el siguiente comando:

```
sudo csa_set_proxy
```

El comando genera dos peticiones de datos y muestra el formato necesario para la entrada del proxy. El primer aviso le permite especificar un proxy HTTP, mientras que el segundo le permite especificar un proxy HTTPS.

Introduzca el siguiente proxy HTTP con el formato:

```
http://user:password@proxy-server:proxy-port
```

Déjelo en blanco si no se requiere un proxy HTTP para el acceso a Internet.

7. Una vez que la red esté activa, espere aproximadamente 5 minutos para que el sistema se actualice y se inicie.

Aparece un mensaje de difusión en la consola cuando el agente está operativo.

8. Verifique la conectividad ejecutando el siguiente comando CLI desde el agente:

```
curl -k https://www.netapp.com/us/index.aspx
```

Si el comando falla, compruebe la configuración de DNS. La máquina virtual del agente debe tener una configuración DNS válida y la capacidad de llegar a csa.netapp.com.

Instale un certificado SSL en el agente

Opcional: Si es necesario, instale un certificado SSL en el agente.

El agente crea un certificado autofirmado cuando se arranca la máquina virtual por primera vez. Si es necesario, puede eliminar ese certificado y utilizar su propio certificado SSL.

Acerca de esta tarea

Converged Systems Advisor es compatible con lo siguiente: * Cualquier cifrado compatible con OpenSSL versión 1.0.1 o superior * TLS 1.1 y TLS 1.2

Pasos

1. Inicie sesión en la consola de máquina virtual del agente.
2. Vaya a. `/opt/csa/certs`
3. Elimine el certificado autofirmado que creó el agente.
4. Pegue su certificado SSL.
5. Reiniciar la máquina virtual.

Configure el agente para descubrir su infraestructura de FlexPod

Debe configurar el agente para recopilar datos de configuración de cada dispositivo de la infraestructura convergente de FlexPod. El agente requiere credenciales para recopilar datos de configuración. Debe proporcionar las credenciales cuando configure el agente.

Pasos

1. Abra un explorador web e introduzca la dirección IP de la máquina virtual del agente.
2. Inicie sesión en el agente con el nombre de usuario y la contraseña de la cuenta del sitio de soporte de NetApp del cliente.



Para cualquier partner que ponga en marcha una versión con licencia de CSA en nombre de sus clientes, es importante que la cuenta del cliente se utilice en este paso (para la gestión de registros y soporte de NetApp).

3. Agregue los dispositivos FlexPod que desea que detecte el agente.

Dispone de dos opciones:

- a. Haga clic en **Agregar un dispositivo** para introducir detalles sobre los dispositivos FlexPod, uno por uno.
- b. Haga clic en **Importar dispositivos** para rellenar y cargar una plantilla CSV que incluya detalles sobre todos los dispositivos.

Nota: * El nombre de usuario y la contraseña deben corresponder a la cuenta que creó anteriormente para el dispositivo. * Si su entorno UCS tiene configurada la administración de usuarios LDAP, debe agregar el dominio del usuario antes que el nombre de usuario. Por ejemplo: Local\csa-readonly

Resultado

Cada dispositivo de la infraestructura de FlexPod debe aparecer en la tabla con una Marca de verificación.

Your devices list

Minimum required FlexPod configuration - 1 NetApp ONTAP, 2 Cisco Nexus and 1 Cisco UCS.

Device Type	Host Name	IP Address	Last Updated	Status
VMWare vCenter	10.61.184.230	10.61.184.230	7/12/18, 1:39 PM	✓
UCS	10.61.186.134	10.61.186.134	7/12/18, 1:36 PM	✓
NetApp ONTAP	10.61.186.82	10.61.186.82	7/12/18, 1:35 PM	✓
Cisco Nexus	10.61.186.81	10.61.186.81	7/12/18, 1:35 PM	✓
Cisco Nexus	10.61.186.80	10.61.186.80	7/12/18, 1:34 PM	✓

Añada infraestructura al portal

Después de configurar el agente, éste envía información acerca de cada dispositivo FlexPod al portal de Converged Systems Advisor. Ahora debe seleccionar cada uno de esos componentes en el portal para crear toda una infraestructura que pueda supervisar.

Pasos

1. En la "Portal del asesor de sistemas convergentes", Haga clic en **Agregar infraestructura**.
2. Complete los pasos para añadir la infraestructura:
 - a. Introduzca detalles básicos sobre la infraestructura.

Si va a agregar una infraestructura ACI de Cisco, introduzca **sí** cuando se le pregunte si FlexPod utiliza Cisco UCS Manager; e introduzca **switch Nexus en modo ACI** cuando se le pregunte el tipo de configuración de red que contiene FlexPod.

- b. Seleccione cada dispositivo que forme parte de la configuración de FlexPod.



Al seleccionar un dispositivo, la columna Elegibilidad muestra **elegible** o **no elegible**. Un dispositivo no es elegible si fue descubierto por otro agente.

3. Una vez que haya seleccionado todos los componentes necesarios, debería aparecer una Marca de verificación verde junto a cada tipo de dispositivo.

Device Name	Device IP	Device Type	Serial No.	CI Name	Eligibility	Agent Status	FlexPod Validation Criteria
<input checked="" type="checkbox"/> ACI Fabric1	10.61.186.190	ACI APIC	WZP23140FFB	Pikes_ACI	✓ Eligible	Online	<ul style="list-style-type: none"> ✓ 1 Cisco UCS Manager ✓ 1 Cisco ACI APIC ✓ 1 NetApp ONTAP Cluster ✓ 0 or 1 VMware vCenter
<input checked="" type="checkbox"/> stack4-fas	10.61.183.249	Ontap	701510000664-701510000665	Pikes_ACI	✓ Eligible	Online	
<input checked="" type="checkbox"/> stack4	10.61.186.244	UCS	FOX2010G275-FOX2013G9ZS	Pikes_ACI	✓ Eligible	Online	

- a. Agregue el "[Número de serie del asesor de sistemas convergentes](#)" para desbloquear la funcionalidad clave.
- b. Revise el resumen, acepte los términos del acuerdo de licencia y haga clic en **Agregar infraestructura**.



Si usted es socio o distribuidor, puede omitir los pasos sobre la adición de una licencia o número de serie y simplemente hacer clic en **Agregar infraestructura**.

Resultado

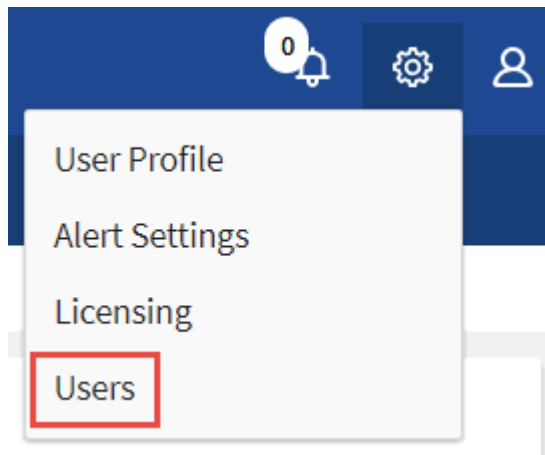
Converged Systems Advisor añade la infraestructura al portal y comienza a recopilar datos de configuración sobre cada dispositivo. Espere unos minutos para que el agente recopile información de los dispositivos.

Compartir una infraestructura con otros usuarios

Al compartir una infraestructura convergente, otra persona puede iniciar sesión en el portal de Converged Systems Advisor para poder ver y supervisar la configuración. La persona con la que comparte la infraestructura debe tener un "[Sitio de soporte de NetApp](#)" cuenta.

Pasos

1. En el portal Converged Systems Advisor, haga clic en el icono **Configuración** y, a continuación, en **usuarios**.



2. Seleccione la configuración en la tabla Usuario.
3. Haga clic en la .
4. Introduzca una o más direcciones de correo electrónico junto al rol de usuario que desea proporcionar.

["Ver las diferencias entre cada rol"](#).



Puede introducir varias direcciones de correo electrónico en un solo campo pulsando **Intro** después de la primera dirección de correo electrónico.

5. Haga clic en **Enviar**.

Resultado

El usuario debe recibir un correo electrónico que contenga instrucciones para acceder a Converged Systems Advisor.

Configurar notificaciones

Si tiene una licencia Premium, Converged Systems Advisor puede alertarle sobre los cambios realizados en su infraestructura FlexPod mediante notificaciones por correo electrónico.

Pasos

1. En el portal Converged Systems Advisor, haga clic en el icono **Configuración** y, a continuación, haga clic en **Configuración de alerta**.
2. Compruebe la notificación que desea recibir para cada infraestructura convergente que tiene una licencia Premium.

Cada notificación incluye la siguiente información:

Errores de recopilación

Le avisa cuando Converged Systems Advisor no puede recopilar datos de una infraestructura convergente.

Agente sin conexión

Le avisa cuando un agente de Converged Systems Advisor no está en línea.

Resumen de alertas diarias

Le avisa sobre las reglas fallidas que se produjeron el día anterior.

3. Haga clic en **Guardar**.

Resultado

Converged Systems Advisor ahora enviará notificaciones por correo electrónico a los usuarios asociados con la infraestructura convergente.

Establezca una dirección IP estática en el agente

Si su entorno no tiene un servidor DHCP, puede establecer una dirección IP estática en el agente Converged Systems Advisor.

Pasos

1. Inicie sesión en la consola de máquina virtual del agente mediante el cliente de VMware vSphere.

El nombre de usuario predeterminado es **csa** y la contraseña predeterminada es **netapp**. Cambie la contraseña, si se le solicita.

2. Introduzca `sudo su -` en el símbolo `csa` para convertirse en root.
3. Introduzca `# systemctl stop csa.service` Para detener el servicio CSA.
4. Introduzca lo siguiente para determinar el nombre de archivo de interfaz correcto.

En este ejemplo, el nombre del archivo de interfaz es `eth0`.

```
# ls /etc/network/interfaces.d/
```

5. Introduzca `# /sbin/ifdown eth0` para detener la interfaz activa.
6. Edite el archivo `/etc/network/interfaces.d/eth0` con el editor de su elección.

```
# nano /etc/network/interfaces.d/eth0`o.  
`# vi /etc/network/interfaces.d/eth0
```

El archivo contiene lo siguiente:

```
allow-hotplug eth0  
iface eth0 inet dhcp
```

7. Quitar `iface eth0 inet dhcp` y añada lo siguiente. NOTA: Debe sustituir los valores correctos para todas las entradas que siguen los nombres de campo en el ejemplo siguiente. Por ejemplo, `192.168.11.1` es el valor de la puerta de enlace del ejemplo. Sin embargo, en lugar de `192.168.11.1`, debe introducir la dirección correcta para la puerta de enlace.

```
iface eth0 inet static  
address 192.168.11.100  
netmask 255.255.255.0  
gateway 192.168.11.1  
dns-domain example.com  
dns-nameservers 192.168.11.1
```

8. Guarde el archivo.

En nano, introduzca **ctrl + o** seguido de **ctrl + x** para guardar.

9. Introduzca `vi/etc/resolv.conf` para abrir el archivo de configuración.
10. Agregar `nameserver <ip_address>` en la parte superior del archivo.
11. Introduzca `# ifup eth0` para iniciar la interfaz de red.
12. Introduzca `systemctl start csa.service` Para reiniciar Converged Systems Advisor.

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 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.