



Configurando Active IQ Unified Manager

Active IQ Unified Manager 9.14

NetApp

November 12, 2024

Tabla de contenidos

- Configurando Active IQ Unified Manager 1
 - Descripción general de la secuencia de configuración 1
 - Acceder a la interfaz de usuario web de Unified Manager 1
 - Realizando la configuración inicial de la interfaz de usuario web de Unified Manager 2
 - Añadir clústeres 4
 - Configuración de Unified Manager para enviar notificaciones de alerta 6
 - Cambiando la contraseña de usuario local 15
 - Configurar el tiempo de espera de inactividad de la sesión 16
 - Cambie el nombre de host de Unified Manager 16
 - Habilitar y deshabilitar la gestión del almacenamiento basada en políticas 21

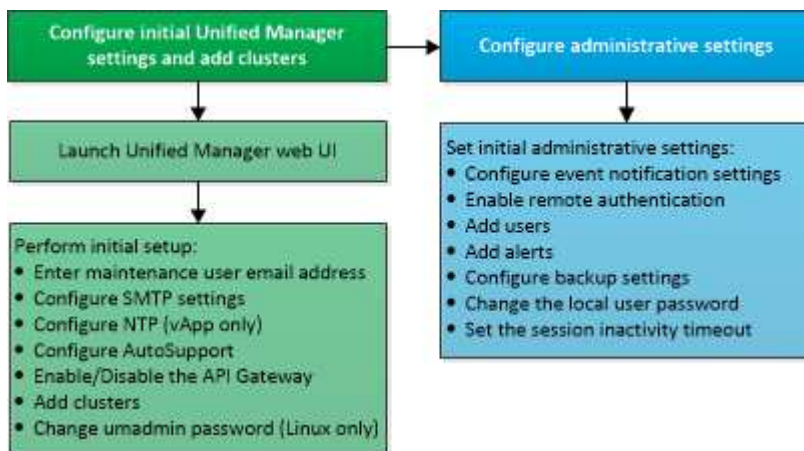
Configurando Active IQ Unified Manager

Después de instalar Active IQ Unified Manager (anteriormente Unified Manager de OnCommand), debe completar la configuración inicial (también llamada el primer asistente de experiencia) para acceder a la interfaz de usuario web de. Después, puede realizar otras tareas de configuración, como añadir clústeres, configurar la autenticación remota, añadir usuarios y añadir alertas.

Algunos de los procedimientos descritos en este manual son necesarios para completar la configuración inicial de su instancia de Unified Manager. Otros procedimientos son los ajustes de configuración recomendados que son útiles para configurar en la nueva instancia, o que son buenos saber acerca de antes de iniciar la supervisión regular de los sistemas ONTAP.

Descripción general de la secuencia de configuración

En el flujo de trabajo de configuración, se describen las tareas que deben realizarse para poder usar Unified Manager.



Acceder a la interfaz de usuario web de Unified Manager

Después de instalar Unified Manager, puede acceder a la interfaz de usuario web de para configurar Unified Manager de modo que pueda comenzar a supervisar los sistemas de ONTAP.

Lo que necesitará

- Si es la primera vez que accede a la interfaz de usuario web, debe iniciar sesión como el usuario de mantenimiento (o usuario umadmin para instalaciones de Linux).
- Si piensa permitir a los usuarios acceder a Unified Manager mediante el nombre corto en lugar de usar el nombre de dominio completo (FQDN) o la dirección IP, la configuración de red debe resolver este nombre corto con un FQDN válido.
- Si el servidor utiliza un certificado digital autofirmado, es posible que el explorador muestre una advertencia que indica que el certificado no es de confianza. Puede reconocer el riesgo de continuar con el acceso o instalar un certificado digital firmado por una entidad de certificación (CA) para la autenticación del servidor.

Pasos

1. Inicie la interfaz de usuario web de Unified Manager desde el explorador mediante la URL que se muestra al final de la instalación. La URL es la dirección IP o el nombre de dominio completo (FQDN) del servidor de Unified Manager.

El enlace está en el siguiente formato `https://URL:`.

2. Inicie sesión en la interfaz de usuario web de Unified Manager con sus credenciales de usuario de mantenimiento.



Si se realizan tres intentos consecutivos para iniciar sesión en la interfaz de usuario web en una hora, se bloqueará fuera del sistema y deberá ponerse en contacto con el administrador del sistema. Esto es aplicable únicamente para usuarios locales.

Realizando la configuración inicial de la interfaz de usuario web de Unified Manager

Para utilizar Unified Manager, primero es necesario configurar las opciones de configuración iniciales, incluido el servidor NTP, la dirección de correo electrónico del usuario de mantenimiento, el host del servidor SMTP y añadir clústeres de ONTAP.

Lo que necesitará

Debe haber realizado las siguientes operaciones:

- Inició la interfaz de usuario web de Unified Manager mediante la URL proporcionada después de la instalación
- Inició sesión con el nombre de usuario y la contraseña de mantenimiento (usuario umadmin para instalaciones Linux) creados durante la instalación

La página Active IQ Unified Manager Getting Started aparece solo cuando se accede por primera vez a la interfaz de usuario web. La siguiente página procede de una instalación en VMware.

Getting Started



Notifications

Configure your email server for assistance in case you forget your password.

Maintenance User Email

Email

SMTP Server

Host Name or IP Address

Port

User Name

Password

Use STARTTLS i Use SSL i

Continue

Si desea cambiar alguna de estas opciones más adelante, puede seleccionar su opción en las opciones General del panel de navegación izquierdo de Unified Manager. Tenga en cuenta que la configuración de NTP es solo para instalaciones de VMware y se puede cambiar más adelante con la consola de mantenimiento de Unified Manager.

Pasos

1. En la página Active IQ Unified Manager Initial Setup, introduzca la dirección de correo electrónico de usuario de mantenimiento, el nombre de host del servidor SMTP y todas las opciones adicionales SMTP, y el servidor NTP (solo instalaciones VMware). A continuación, haga clic en **continuar**.



Si ha seleccionado la opción **usar STARTTLS** o **usar SSL**, aparecerá una página de certificado después de hacer clic en el botón **continuar**. Compruebe los detalles del certificado y acepte el certificado para continuar con la configuración inicial de la interfaz de usuario web.

2. En la página AutoSupport, haga clic en **Acepto y continúe** para activar el envío de mensajes de AutoSupport desde Unified Manager a Active IQ de NetApp.

Si necesita designar un proxy para proporcionar acceso a Internet con el fin de enviar contenido

AutoSupport, o si desea desactivar AutoSupport, utilice la opción **General > AutoSupport** de la interfaz de usuario web.

3. En los sistemas Red Hat y CentOS, cambie la contraseña de usuario umadmin de la cadena "admin" predeterminada a una cadena personalizada.
4. En la página Set up API Gateway, seleccione si desea utilizar la función API Gateway que permite a Unified Manager gestionar los clústeres de ONTAP que planea supervisar mediante API de REST de ONTAP. A continuación, haga clic en **continuar**.

Puede activar o desactivar esta configuración más adelante en la interfaz de usuario web desde **General > Configuración de la función > puerta de enlace API**. Para obtener más información sobre las API, consulte "[Primeros pasos con API de REST de Active IQ Unified Manager](#)".

5. Añada los clústeres que desea que Unified Manager administre y haga clic en **Siguiente**. Para cada clúster que vaya a administrar, debe tener el nombre de host o la dirección IP de administración del clúster (IPv4 o IPv6) junto con las credenciales de nombre de usuario y contraseña; el usuario debe tener el rol «'admin'».

Este paso es opcional. Puede agregar clústeres más adelante en la interfaz de usuario web desde **Storage Management > Cluster Setup**.

6. En la página Summary (Resumen), compruebe que todos los ajustes son correctos y haga clic en **Finish** (Finalizar).

Se cierra la página Getting Started y se muestra la página Unified Manager Dashboard.

Añadir clústeres

Puede añadir un clúster a la Active IQ Unified Manager para poder supervisar el clúster. Esto incluye la capacidad de obtener información del clúster, como el estado, la capacidad, el rendimiento y la configuración del clúster, para poder encontrar y resolver cualquier problema que pueda ocurrir.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe tener la siguiente información:
 - Unified Manager admite clústeres de ONTAP en las instalaciones, ONTAP Select, Cloud Volumes ONTAP.
 - El nombre de host o la dirección IP de administración del clúster

El nombre de host es el nombre FQDN o el nombre corto que Unified Manager utiliza para conectarse con el clúster. El nombre de host debe resolver a la dirección IP de administración del clúster.

La dirección IP de administración del clúster debe ser el LIF de gestión del clúster de la máquina virtual de almacenamiento (SVM) administrativa. Si utiliza un LIF de gestión de nodos, la operación da error.

- El clúster debe ejecutar el software ONTAP versión 9.1 o posterior.
- Nombre de usuario y contraseña del administrador de ONTAP

Esta cuenta debe tener el rol *admin* con acceso a aplicaciones establecido en *ontapi*, *Console* y *http*.

- El número de puerto para conectarse al clúster mediante el protocolo HTTPS (por lo general, puerto 443)
- Tiene los certificados necesarios:

Certificado SSL (HTTPS): Este certificado es propiedad de Unified Manager. Se genera un certificado SSL (HTTPS) autofirmado predeterminado con una instalación nueva de Unified Manager. NetApp recomienda actualizarlo a certificado firmado por CA para mejorar la seguridad. Si el certificado de servidor caduca, debe volver a regenerarlo y reiniciar Unified Manager para que los servicios incorporen el nuevo certificado. Para obtener más información sobre la regeneración de certificados SSL, consulte "[Generar un certificado de seguridad HTTPS](#)".

Certificado EMS: Este certificado es propiedad de Unified Manager. Se usa durante la autenticación de notificaciones EMS que se reciben de ONTAP.

Certificados para la comunicación mutua con TLS: Se utiliza durante la comunicación mutua con TLS entre Unified Manager y ONTAP. La autenticación basada en certificados está habilitada para un clúster de acuerdo con la versión de ONTAP. Si el clúster que ejecuta la versión de ONTAP es inferior a la versión 9.5, la autenticación basada en certificados no está habilitada.

La autenticación basada en certificado no se habilita automáticamente para un clúster, si va a actualizar una versión anterior de Unified Manager. Sin embargo, puede habilitarla mediante la modificación y el guardado de los detalles del clúster. Si el certificado caduca, debe regenerarlo para incorporar el nuevo certificado. Para obtener más información sobre la visualización y regeneración del certificado, consulte "[Editar clústeres](#)".



- Puede añadir un clúster desde la interfaz de usuario web y la autenticación basada en certificado se habilita automáticamente.
- Puede añadir un clúster mediante la CLI de Unified Manager, la autenticación basada en certificado no está habilitada de forma predeterminada. Si se añade un clúster mediante la CLI de Unified Manager, se deberá editar el clúster mediante la interfaz de usuario de Unified Manager. Puede "[Comandos de CLI de Unified Manager compatibles](#)" ver para añadir un clúster mediante la CLI de Unified Manager.
- Si la autenticación basada en certificados está habilitada para un clúster, y realiza el backup de Unified Manager desde un servidor y la restauración a otro servidor de Unified Manager donde se cambia el nombre de host o la dirección IP, la supervisión del clúster puede fallar. Para evitar el error, edite y guarde los detalles del clúster. Para obtener más información sobre la edición de detalles del clúster, consulte "[Editar clústeres](#)".

+ **Certificados de clúster:** Este certificado es propiedad de ONTAP. No es posible añadir un clúster a Unified Manager con un certificado caducado y si el certificado ya ha caducado, debe volver a generarlo antes de añadir el clúster. Para obtener información sobre la generación de certificados, consulte el artículo de la base de conocimientos (KB) "[Cómo renovar un certificado autofirmado de ONTAP en la interfaz de usuario de System Manager](#)".

- Debe tener espacio suficiente en el servidor de Unified Manager. Se le impide agregar un clúster al servidor cuando ya se consume más del 90% del espacio en el directorio de la base de datos.

Para una configuración de MetroCluster, debe añadir los clústeres local y remoto, y los clústeres deben configurarse correctamente.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management > Cluster Setup**.
2. En la página Cluster Setup, haga clic en **Add**.
3. En el cuadro de diálogo Add Cluster, especifique los valores requeridos, como el nombre de host o la dirección IP del clúster, el nombre de usuario, la contraseña y el número de puerto.

Es posible cambiar la dirección IP de gestión del clúster de IPv6 a IPv4 o de IPv4 a IPv6. La nueva dirección IP se refleja en la cuadrícula del clúster y en la página de configuración del clúster una vez completado el siguiente ciclo de supervisión.

4. Haga clic en **Enviar**.
5. En el cuadro de diálogo autorizar host, haga clic en **Ver certificado** para ver la información del certificado sobre el clúster.
6. Haga clic en **Sí**.

Después de guardar los detalles del clúster, puede ver el certificado para la comunicación TLS mutua para un clúster.

Si la autenticación basada en certificados no está habilitada, Unified Manager comprueba el certificado solo cuando se añade el clúster inicialmente. Unified Manager no comprueba el certificado para cada llamada API a ONTAP.

Después de detectar todos los objetos de un clúster nuevo, Unified Manager comienza a recopilar datos históricos de rendimiento de los 15 días anteriores. Estas estadísticas se recopilan mediante la funcionalidad de recogida de continuidad de datos. Esta función le proporciona más de dos semanas de información sobre el rendimiento de un clúster inmediatamente después de añadir. Una vez completado el ciclo de recogida de continuidad de datos, se recogen datos de rendimiento del clúster en tiempo real, de forma predeterminada, cada cinco minutos.



Dado que la recogida de 15 días de datos de rendimiento requiere un uso intensivo de la CPU, se sugiere escalonar la adición de nuevos clústeres de manera que las encuestas de recogida de continuidad de datos no se ejecuten en demasiados clústeres al mismo tiempo. Además, si reinicia Unified Manager durante el período de recogida de continuidad de datos, la recogida se detiene y verá vacíos en los gráficos de rendimiento correspondientes al periodo que falta.



Si recibe un mensaje de error que no puede añadir el clúster, compruebe si los relojes de los dos sistemas no están sincronizados y la fecha de inicio del certificado HTTPS de Unified Manager es posterior a la fecha del clúster. Debe asegurarse de que los relojes se sincronicen con NTP o un servicio similar.

Información relacionada

["Instalar una CA firmada y devolvió un certificado HTTPS"](#)

Configuración de Unified Manager para enviar notificaciones de alerta

Puede configurar Unified Manager para que envíe notificaciones que le alertan de los eventos de su entorno. Antes de que las notificaciones se puedan enviar, debe configurar

varias otras opciones de Unified Manager.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Después de implementar Unified Manager y completar la configuración inicial, se debe considerar configurar el entorno para activar alertas y generar correos electrónicos de notificación o capturas SNMP en función de la recepción de eventos.

Pasos

1. "Configure los ajustes de notificación de eventos".

Si desea que las notificaciones de alerta se envíen cuando ciertos eventos ocurran en el entorno, debe configurar un servidor SMTP y suministrar una dirección de correo electrónico desde la que se enviará la notificación de alerta. Si desea utilizar capturas SNMP, puede seleccionar esa opción y proporcionar la información necesaria.

2. "Habilite la autenticación remota".

Si desea que los usuarios remotos de LDAP o Active Directory accedan a la instancia de Unified Manager y reciban notificaciones de alerta, debe habilitar la autenticación remota.

3. "Agregue servidores de autenticación".

Puede agregar servidores de autenticación para que los usuarios remotos dentro del servidor de autenticación puedan acceder a Unified Manager.

4. "Añadir usuarios".

Puede añadir varios tipos de usuarios locales o remotos y asignar roles específicos. Cuando crea una alerta, asigna un usuario para que reciba las notificaciones de alerta.

5. "Añadir alertas".

Después de añadir la dirección de correo electrónico para enviar notificaciones, se añadieron usuarios para recibir las notificaciones, configurar los ajustes de red y configurar las opciones SMTP y SNMP necesarias para el entorno, y después puede asignar alertas.

Configuración de los ajustes de notificación de eventos

Es posible configurar Unified Manager para que envíe notificaciones de alerta cuando se genera un evento o cuando se asigna un evento a un usuario. Puede configurar el servidor SMTP que se usa para enviar la alerta y se pueden configurar varios mecanismos de notificación; por ejemplo, las notificaciones de alerta se pueden enviar como correos electrónicos o capturas SNMP.

Lo que necesitará

Debe tener la siguiente información:

- Dirección de correo electrónico desde la cual se envía la notificación de alertas

La dirección de correo electrónico aparece en el campo «de» en las notificaciones de alerta enviadas. Si el correo electrónico no se puede entregar por cualquier motivo, esta dirección de correo electrónico también se utiliza como destinatario para el correo no entregable.

- El nombre de host del servidor SMTP, así como el nombre de usuario y la contraseña para acceder al servidor
- Nombre de host o dirección IP del host de destino de captura que recibirá la captura SNMP, junto con la versión SNMP, el puerto de capturas saliente, la comunidad y otros valores de configuración SNMP requeridos

Para especificar varios destinos de capturas, separe cada host con una coma. En este caso, todas las demás configuraciones de SNMP, como la versión y el puerto de captura saliente, deben ser las mismas para todos los hosts de la lista.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > Notificaciones**.
2. En la página Notifications, configure los ajustes adecuados.

Notas:

- Si la dirección de origen se rellena previamente con la dirección «ActiveIQUnifiedManager@localhost.com», debe cambiarla a una dirección de correo electrónico real y funcional para asegurarse de que todas las notificaciones de correo electrónico se envíen correctamente.
 - Si no se puede resolver el nombre de host del servidor SMTP, puede especificar la dirección IP (IPv4 o IPv6) del servidor SMTP en lugar del nombre de host.
3. Haga clic en **Guardar**.
 4. Si ha seleccionado la opción **usar STARTTLS** o **usar SSL**, aparecerá una página de certificado después de hacer clic en el botón **Guardar**. Compruebe los detalles del certificado y acepte el certificado para guardar la configuración de notificación.

Puede hacer clic en el botón **Ver detalles del certificado** para ver los detalles del certificado. Si el certificado existente ha caducado, desactive la casilla **usar STARTTLS** o **usar SSL**, guarde la configuración de notificación y vuelva a marcar la casilla **usar STARTTLS** o **usar SSL** para ver un nuevo certificado.

Habilitación de la autenticación remota

Puede habilitar la autenticación remota para que el servidor de Unified Manager pueda comunicarse con los servidores de autenticación. Los usuarios del servidor de autenticación pueden acceder a la interfaz gráfica de Unified Manager para gestionar los objetos de almacenamiento y los datos.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.



El servidor de Unified Manager debe estar conectado directamente con el servidor de autenticación. Debe deshabilitar cualquier cliente LDAP local, como SSSD (demonio de servicios de seguridad del sistema) o NSLCD (demonio de almacenamiento en caché LDAP del servicio de nombres).

Puede habilitar la autenticación remota mediante Open LDAP o Active Directory. Si la autenticación remota está deshabilitada, los usuarios remotos no pueden acceder a Unified Manager.

La autenticación remota es compatible con LDAP y LDAPS (LDAP seguro). Unified Manager utiliza 389 como puerto predeterminado para la comunicación no segura y 636 como puerto predeterminado para la comunicación segura.



El certificado que se utiliza para autenticar usuarios debe cumplir el formato X.509.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > autenticación remota**.
2. Marque la casilla para **Activar autenticación remota....**
3. En el campo Servicio de autenticación, seleccione el tipo de servicio y configure el servicio de autenticación.

Para tipo de autenticación...	Introduzca la siguiente información...
Active Directory	<ul style="list-style-type: none"> • Nombre del administrador del servidor de autenticación en uno de los siguientes formatos: <ul style="list-style-type: none"> ◦ domainname\username ◦ username@domainname ◦ Bind Distinguished Name (Usando la notación LDAP apropiada) • Contraseña de administrador • Nombre completo base (con la notación LDAP adecuada)
Abra LDAP	<ul style="list-style-type: none"> • Enlazar nombre distintivo (en la notación LDAP correspondiente) • Enlazar contraseña • Nombre distintivo de base

Si la autenticación de un usuario de Active Directory tarda mucho tiempo o agota el tiempo de espera, es probable que el servidor de autenticación tarde mucho tiempo en responder. Al deshabilitar la compatibilidad con los grupos anidados en Unified Manager, es posible que se reduzca el tiempo de autenticación.

Si selecciona la opción Use Secure Connection para el servidor de autenticación, Unified Manager se comunica con el servidor de autenticación mediante el protocolo Secure Sockets Layer (SSL).

4. **Opcional:** Agregue servidores de autenticación y pruebe la autenticación.
5. Haga clic en **Guardar**.

Deshabilitar grupos anidados de la autenticación remota

Si tiene habilitada la autenticación remota, puede deshabilitar la autenticación de grupos anidados para que solo los usuarios individuales y no los miembros de grupos se puedan autenticar de forma remota a Unified Manager. Puede deshabilitar los grupos anidados cuando desee mejorar el tiempo de respuesta de autenticación de Active Directory.

Lo que necesitará

- Debe tener la función Administrador de aplicaciones.
- La desactivación de grupos anidados sólo se aplica cuando se utiliza Active Directory.

Al deshabilitar la compatibilidad con los grupos anidados en Unified Manager, es posible que se reduzca el tiempo de autenticación. Si la compatibilidad de grupos anidados está deshabilitada y, si se añade un grupo remoto a Unified Manager, los usuarios individuales deben ser miembros del grupo remoto para autenticarse en Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > autenticación remota**.
2. Active la casilla de verificación **Desactivar búsqueda de grupo anidada**.
3. Haga clic en **Guardar**.

Configurar servicios de autenticación

Los servicios de autenticación permiten la autenticación de usuarios remotos o grupos remotos en un servidor de autenticación antes de otorgar acceso a Unified Manager. Puede autenticar usuarios utilizando servicios de autenticación predefinidos (como Active Directory u OpenLDAP) o configurando su propio mecanismo de autenticación.

Lo que necesitará

- Debe haber habilitado la autenticación remota.
- Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > autenticación remota**.
2. Seleccione uno de los siguientes servicios de autenticación:

Si selecciona...	Realice lo siguiente...
Active Directory	<p>a. Introduzca el nombre y la contraseña del administrador.</p> <p>b. Especifique el nombre completo base del servidor de autenticación.</p> <p>Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es cn=ou,dc=domain,dc=com.</p>
OpenLDAP	<p>a. Introduzca el nombre distintivo del enlace y la contraseña de enlace.</p> <p>b. Especifique el nombre completo base del servidor de autenticación.</p> <p>Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es cn=ou,dc=domain,dc=com.</p>
Otros	<p>a. Introduzca el nombre distintivo del enlace y la contraseña de enlace.</p> <p>b. Especifique el nombre completo base del servidor de autenticación.</p> <p>Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es cn=ou,dc=domain,dc=com.</p> <p>c. Especifique la versión de protocolo LDAP que admite el servidor de autenticación.</p> <p>d. Introduzca el nombre de usuario, la pertenencia a grupos, el grupo de usuarios y los atributos miembro.</p>



Si desea modificar el servicio de autenticación, debe eliminar todos los servidores de autenticación existentes y, a continuación, agregar nuevos servidores de autenticación.

3. Haga clic en **Guardar**.

Añadiendo servidores de autenticación

Puede añadir servidores de autenticación y habilitar la autenticación remota en el servidor de gestión para que los usuarios remotos dentro del servidor de autenticación puedan acceder a Unified Manager.


Lo que necesitará

- Debe estar disponible la siguiente información:
 - Nombre de host o dirección IP del servidor de autenticación
 - Número de puerto del servidor de autenticación
- Debe haber habilitado la autenticación remota y configurado el servicio de autenticación para que el servidor de administración pueda autenticar usuarios o grupos remotos en el servidor de autenticación.
- Debe tener la función Administrador de aplicaciones.

Si el servidor de autenticación que va a añadir forma parte de un par de alta disponibilidad (ha) (con la misma base de datos), también puede añadir el servidor de autenticación asociado. Esto permite que el servidor de administración se comuniquen con el asociado cuando no se puede acceder a uno de los servidores de autenticación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > autenticación remota**.
2. Activar o desactivar la opción **utilizar conexión segura**:

Si desea...	Realice lo siguiente...
Habilite	<ol style="list-style-type: none">a. Seleccione la opción utilizar conexión segura.b. En el área servidores de autenticación, haga clic en Agregar.c. En el cuadro de diálogo Add Authentication Server, introduzca el nombre o la dirección IP de autenticación (IPv4 o IPv6) del servidor.d. En el cuadro de diálogo autorizar host, haga clic en Ver certificado.e. En el cuadro de diálogo Ver certificado, compruebe la información del certificado y, a continuación, haga clic en Cerrar.f. En el cuadro de diálogo autorizar host, haga clic en Sí. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"><p>Al activar la opción usar autenticación de conexión segura, Unified Manager se comunica con el servidor de autenticación y muestra el certificado. Unified Manager utiliza 636 como puerto predeterminado para una comunicación segura y el número de puerto 389 para una comunicación no segura.</p></div>

Si desea...	Realice lo siguiente...
Deshabilitarla	<ol style="list-style-type: none"> Desactive la opción utilizar conexión segura. En el área servidores de autenticación, haga clic en Agregar. En el cuadro de diálogo Add Authentication Server, especifique el nombre de host o la dirección IP (IPv4 o IPv6) del servidor y los detalles del puerto. Haga clic en Agregar.

El servidor de autenticación que ha agregado se muestra en el área servidores.

- Realice una autenticación de prueba para confirmar que puede autenticar usuarios en el servidor de autenticación que ha agregado.

Prueba de la configuración de los servidores de autenticación

Puede validar la configuración de los servidores de autenticación para garantizar que el servidor de gestión pueda comunicarse con ellos. Puede validar la configuración buscando un usuario remoto o un grupo remoto desde los servidores de autenticación y autenticándolos con la configuración configurada.

Lo que necesitará

- Usted debe haber habilitado la autenticación remota y configurado el servicio de autenticación para que el servidor de Unified Manager pueda autenticar el usuario remoto o el grupo remoto.
- Debe haber agregado los servidores de autenticación para que el servidor de administración pueda buscar el usuario remoto o el grupo remoto desde estos servidores y autenticarlos.
- Debe tener la función Administrador de aplicaciones.

Si el servicio de autenticación está establecido en Active Directory y si está validando la autenticación de usuarios remotos que pertenecen al grupo principal del servidor de autenticación, la información sobre el grupo principal no se muestra en los resultados de la autenticación.

Pasos

- En el panel de navegación izquierdo, haga clic en **General > autenticación remota**.
- Haga clic en **probar autenticación**.
- En el cuadro de diálogo probar usuario, especifique el nombre de usuario y la contraseña del usuario remoto o el nombre de usuario del grupo remoto y, a continuación, haga clic en **Prueba**.

Si va a autenticar un grupo remoto, no debe introducir la contraseña.

Adición de alertas

Puede configurar alertas para que le notifiquen un evento determinado. Es posible configurar alertas para un solo recurso, para un grupo de recursos o para eventos de un tipo de gravedad determinado. Puede especificar la frecuencia con la que desea que se

le notifique y asociar un script a la alerta.

Lo que necesitará

- Debe haber configurado los ajustes de notificación, como la dirección de correo electrónico de usuario, el servidor SMTP y el host de captura SNMP, con el fin de permitir que el servidor Active IQ Unified Manager utilice estos ajustes para enviar notificaciones a los usuarios cuando se genera un evento.
- Debe conocer los recursos y los eventos sobre los que desea activar la alerta, así como los nombres de usuario o las direcciones de correo electrónico de los usuarios a los que desea notificar.
- Si desea que un script se ejecute según el evento, debe haber añadido el script a Unified Manager mediante la página Scripts.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede crear una alerta directamente desde la página de detalles Event después de recibir un evento además de crear una alerta desde la página Alert Setup, tal y como se describe aquí.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento > Configuración de alertas**.
2. En la página Configuración de alertas, haga clic en **Agregar**.
3. En el cuadro de diálogo Agregar alerta, haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.
4. Haga clic en **Recursos** y seleccione los recursos que se incluirán o excluirán de la alerta.

Puede establecer un filtro especificando una cadena de texto en el campo **Nombre contiene** para seleccionar un grupo de recursos. Según la cadena de texto que especifique, la lista de recursos disponibles solo muestra los recursos que coinciden con la regla de filtro. La cadena de texto que especifique distingue mayúsculas y minúsculas.

Si un recurso cumple las reglas de inclusión y exclusión especificadas, la regla de exclusión tiene prioridad sobre la regla de inclusión y no se genera la alerta para los eventos relacionados con el recurso excluido.

5. Haga clic en **Eventos** y seleccione los eventos según el nombre del evento o el tipo de gravedad del evento para el que desea activar una alerta.



Para seleccionar más de un evento, pulse la tecla Ctrl mientras realiza las selecciones.

6. Haga clic en **acciones** y seleccione los usuarios a los que desea notificar, elija la frecuencia de notificación, elija si se enviará una captura SNMP al receptor de capturas y asigne una secuencia de comandos para que se ejecute cuando se genere una alerta.



Si modifica la dirección de correo electrónico especificada para el usuario y vuelve a abrir la alerta para su edición, el campo Nombre aparecerá en blanco porque la dirección de correo electrónico modificada ya no está asignada al usuario que se seleccionó previamente. Además, si modificó la dirección de correo electrónico del usuario seleccionado desde la página usuarios, la dirección de correo electrónico modificada no se actualizará para el usuario seleccionado.

También puede optar por notificar a los usuarios a través de las capturas SNMP.

7. Haga clic en **Guardar**.

Ejemplo de añadir una alerta

Este ejemplo muestra cómo crear una alerta que cumpla con los siguientes requisitos:

- Nombre de alerta: HealthTest
- Recursos: Incluye todos los volúmenes cuyo nombre contenga «'abc'» y excluye todos los volúmenes cuyo nombre contenga «'xyz'».
- Eventos: Incluye todos los eventos críticos de salud
- Acciones: Incluye «sample@domain.com», una secuencia de comandos «'Prueba'» y el usuario deberá recibir una notificación cada 15 minutos

Realice los siguientes pasos en el cuadro de diálogo Agregar alerta:

Pasos

1. Haga clic en **Nombre** e introduzca **HealthTest** en el campo **Nombre de alerta**.
2. Haga clic en **Recursos** y, en la ficha incluir, seleccione **volúmenes** en la lista desplegable.
 - a. Introduzca **abc** en el campo **Name contains** para mostrar los volúmenes cuyo nombre contenga "abc".
 - b. Seleccione **<<All Volumes whose name contains 'abc'>>** en el área Recursos disponibles y muévelo al área Recursos seleccionados.
 - c. Haga clic en **excluir** e introduzca **xyz** en el campo **Nombre contiene** y, a continuación, haga clic en **Agregar**.
3. Haga clic en **Eventos** y seleccione **críticos** en el campo gravedad del evento.
4. Seleccione **todos los eventos críticos** en el área Eventos coincidentes y muévalos al área Eventos seleccionados.
5. Haga clic en **acciones** e introduzca **sample@domain.com** en el campo Alerta a estos usuarios.
6. Seleccione **Recordar cada 15 minutos** para notificar al usuario cada 15 minutos.

Puede configurar una alerta para que envíe repetidamente notificaciones a los destinatarios durante un período de tiempo específico. Debe determinar la hora desde la cual está activa la notificación de eventos para la alerta.

7. En el menú Select Script to Execute, seleccione **Test** script.
8. Haga clic en **Guardar**.

Cambiando la contraseña de usuario local

Es posible cambiar la contraseña de inicio de sesión de usuario local para evitar riesgos potenciales para la seguridad.

Lo que necesitará

Debe iniciar sesión como usuario local.

Las contraseñas del usuario de mantenimiento y de los usuarios remotos no se pueden cambiar mediante estos pasos. Para cambiar una contraseña de usuario remoto, póngase en contacto con el administrador de contraseñas. Para cambiar la contraseña de usuario de mantenimiento, consulte ["Mediante la consola de mantenimiento"](#).

Pasos

1. Inicie sesión en Unified Manager.
2. En la barra de menús superior, haga clic en el icono de usuario y, a continuación, haga clic en **Cambiar contraseña**.

La opción **Cambiar contraseña** no se muestra si es un usuario remoto.

3. En el cuadro de diálogo Change Password, introduzca la contraseña actual y la contraseña nueva.
4. Haga clic en **Guardar**.

Si Unified Manager se configura en una configuración de alta disponibilidad, debe cambiar la contraseña en el segundo nodo de la configuración. Ambas instancias deben tener la misma contraseña.

Configurar el tiempo de espera de inactividad de la sesión

Es posible especificar el valor de tiempo de espera de inactividad para Unified Manager a fin de que la sesión se finalice automáticamente después de un cierto periodo de tiempo. De manera predeterminada, el tiempo de espera está configurado en 4,320 minutos (72 horas).

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Esta configuración afecta a todas las sesiones de usuario que han iniciado sesión.



Esta opción no está disponible si tiene habilitada la autenticación del lenguaje de marcado de aserción de seguridad (SAML).

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > Configuración de funciones**.
2. En la página **Configuración de característica**, especifique el tiempo de espera de inactividad seleccionando una de las siguientes opciones:

Si desea...	Realice lo siguiente...
No tener tiempo de espera configurado para que la sesión nunca se cierre automáticamente	En el panel tiempo de espera de inactividad , mueva el botón deslizante hacia la izquierda (OFF) y haga clic en aplicar .
Establezca un número específico de minutos como valor de tiempo de espera	En el panel tiempo de espera de inactividad , mueva el botón deslizante hacia la derecha (Activado), especifique el valor de tiempo de espera de inactividad en minutos y haga clic en aplicar .

Cambie el nombre de host de Unified Manager

En algún momento, es posible que desee cambiar el nombre de host del sistema en el

que instaló Unified Manager. Por ejemplo, quizás desee cambiar el nombre del host para identificar más fácilmente los servidores de Unified Manager por tipo, grupo de trabajo o grupo de clústeres supervisado.

Los pasos necesarios para cambiar el nombre de host varían en función de si Unified Manager se ejecuta en un servidor VMware ESXi, en un servidor Red Hat o CentOS Linux o en un servidor Microsoft Windows.

Cambiar el nombre de host de la aplicación virtual de Unified Manager

El host de red se asigna un nombre cuando se pone en marcha el dispositivo virtual de Unified Manager por primera vez. Es posible cambiar el nombre de host después de la implementación. Si cambia el nombre de host, también debe volver a generar el certificado HTTPS.

Lo que necesitará

Debe iniciar sesión en Unified Manager como usuario de mantenimiento o tener asignado la función de administrador de aplicaciones para realizar estas tareas.

Puede usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web de Unified Manager. Si configuró una dirección IP estática para la red durante la implementación, debería haber designado un nombre para el host de red. Si configuró la red mediante DHCP, el nombre de host debe tomarse del DNS. Si DHCP o DNS no están configurados correctamente, el nombre de host "Unified Manager" se asigna y se asocia automáticamente con el certificado de seguridad.

Independientemente de cómo se asignó el nombre de host, si cambia el nombre de host y piensa usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debe generar un nuevo certificado de seguridad.

Si accede a la interfaz de usuario web mediante la dirección IP del servidor en lugar del nombre de host, no es necesario generar un nuevo certificado si cambia el nombre de host. Sin embargo, se recomienda actualizar el certificado de forma que el nombre de host del certificado coincida con el nombre de host real.

Si cambia el nombre de host en Unified Manager, debe actualizar manualmente el nombre de host en OnCommand Workflow Automation (WFA). El nombre de host no se actualiza automáticamente en WFA.

El nuevo certificado no se aplicará hasta que se reinicie la máquina virtual de Unified Manager.

Pasos

1. [Genere un certificado de seguridad HTTPS](#)

Si desea usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debe volver a generar el certificado HTTPS para asociarlo con el nuevo nombre de host.

2. [Reinicie la máquina virtual de Unified Manager](#)

Después de volver a generar el certificado HTTPS, debe reiniciar la máquina virtual de Unified Manager.

Generar un certificado de seguridad HTTPS

Cuando se instala Active IQ Unified Manager por primera vez, se instala un certificado HTTPS predeterminado. Es posible generar un nuevo certificado de seguridad HTTPS

que reemplace el certificado existente.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Puede haber varios motivos para regenerar el certificado, como si desea tener mejores valores para el nombre distintivo (DN) o si desea un tamaño de clave mayor, o un período de caducidad más largo o si el certificado actual ha caducado.

Si no tiene acceso a la interfaz de usuario web de Unified Manager, puede volver a generar el certificado HTTPS con los mismos valores mediante la consola de mantenimiento. Al regenerar los certificados, puede definir el tamaño de la clave y la duración de validez de la clave. Si usa `Reset Server Certificate` la opción de la consola de mantenimiento, se creará un nuevo certificado HTTPS que es válido durante 397 días. Este certificado tendrá una clave RSA de tamaño 2048 bits.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > Certificado HTTPS**.
2. Haga clic en **regenerar certificado HTTPS**.

Aparece el cuadro de diálogo Regenerate HTTPS Certificate.

3. Seleccione una de las siguientes opciones en función de cómo desee generar el certificado:

Si desea...	Realice lo siguiente...
Regenere el certificado con los valores actuales	Haga clic en la opción Regenerate usando atributos de certificado actuales .

Si desea...	Realice lo siguiente...
<p>Genere el certificado con diferentes valores</p>	<p>Haga clic en la opción Actualizar atributos de certificado actuales.</p> <p>Los campos Nombre común y nombres alternativos utilizarán los valores del certificado existente si no introduce nuevos valores. El "Nombre común" debe ajustarse al FQDN del host. Los demás campos no requieren valores, pero puede introducir valores, por ejemplo, PARA EL CORREO ELECTRÓNICO, LA EMPRESA, EL DEPARTAMENTO, Ciudad, provincia y país si desea que esos valores se rellenen en el certificado. También puede seleccionar EL TAMAÑO de CLAVE disponible (el algoritmo de clave es "RSA"). Y PERÍODO DE VALIDEZ.</p> <ul style="list-style-type: none"> • Los valores permitidos para el tamaño de clave son 2048, 3072 y 4096. • Los períodos de validez son como mínimo de 1 día a un máximo de 36500 días. <p>Aunque se permita un período de validez de 36500 días, se recomienda que utilice un período de validez de no más de 397 días o 13 meses. Como si selecciona un periodo de validez de más de 397 días y piensa exportar una CSR para este certificado y conseguir que la firme una CA bien conocida, la validez del certificado firmado que la CA le devolvió se reducirá a 397 días.</p> <ul style="list-style-type: none"> • Puede seleccionar la casilla de verificación "excluir información de identificación local (p. ej., localhost)" si desea quitar la información de identificación local del campo nombres alternativos del certificado. Cuando se selecciona esta casilla de verificación, sólo se utiliza lo que se introduce en el campo nombres alternativos. Cuando se deja en blanco, el certificado resultante no tendrá ningún campo nombres alternativos.

4. Haga clic en **Sí** para regenerar el certificado.
5. Reinicie el servidor de Unified Manager para que el nuevo certificado surta efecto.
6. Compruebe la información del nuevo certificado; para ello, consulte el certificado HTTPS.

Reiniciar la máquina virtual de Unified Manager

Puede reiniciar el equipo virtual desde la consola de mantenimiento de Unified Manager. Debe reiniciar después de generar un nuevo certificado de seguridad o si hay un problema con la máquina virtual.

Lo que necesitará

El dispositivo virtual está encendido.

Ha iniciado sesión en la consola de mantenimiento como usuario de mantenimiento.

También puede reiniciar la máquina virtual desde vSphere mediante la opción **Restart Guest**. Para obtener más información, consulte la documentación de VMware.

Pasos

1. Acceda a la consola de mantenimiento.
2. Seleccione **Configuración del sistema > Reiniciar Virtual Machine**.

Cambiar el nombre de host de Unified Manager en sistemas Linux

En algún momento, puede que desee cambiar el nombre de host del equipo Red Hat Enterprise Linux o CentOS en el que ha instalado Unified Manager. Por ejemplo, quizás desee cambiar el nombre del host para identificar más fácilmente los servidores de Unified Manager por tipo, grupo de trabajo o grupo de clústeres supervisado cuando enumere las máquinas Linux.

Lo que necesitará

Debe tener acceso de usuario raíz al sistema Linux en el que está instalado Unified Manager.

Puede usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web de Unified Manager. Si configuró una dirección IP estática para la red durante la implementación, debería haber designado un nombre para el host de red. Si configuró la red mediante DHCP, el nombre de host debe tomarse del servidor DNS.

Independientemente de cómo se asignó el nombre de host, si cambia el nombre de host y piensa usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debe generar un nuevo certificado de seguridad.

Si accede a la interfaz de usuario web mediante la dirección IP del servidor en lugar del nombre de host, no es necesario generar un nuevo certificado si cambia el nombre de host. Sin embargo, se recomienda actualizar el certificado de forma que el nombre de host del certificado coincida con el nombre de host real. El nuevo certificado no se aplicará hasta que se reinicie el equipo Linux.

Si cambia el nombre de host en Unified Manager, debe actualizar manualmente el nombre de host en OnCommand Workflow Automation (WFA). El nombre de host no se actualiza automáticamente en WFA.

Pasos

1. Inicie sesión como usuario raíz en el sistema Unified Manager que desee modificar.
2. Detenga el software Unified Manager y el software MySQL asociado introduciendo el comando siguiente:

```
systemctl stop ocieau ocie mysqld
```

3. Cambie el nombre de host mediante el comando Linux `hostnamectl`:

```
hostnamectl set-hostname new_FQDN
```

```
hostnamectl set-hostname nuhost.corp.widget.com
```

4. Regenera el certificado HTTPS para el servidor:

```
/opt/netapp/essentials/bin/cert.sh create
```

5. Reinicie el servicio de red:

```
systemctl restart NetworkManager.service
```

6. Después de reiniciar el servicio, compruebe si el nuevo nombre de host puede hacer ping a sí mismo:

```
ping new_hostname
```

```
ping nuhost
```

Este comando debe devolver la misma dirección IP que se configuró con anterioridad para el nombre de host original.

7. Después de completar y verificar el cambio de nombre de host, reinicie Unified Manager introduciendo el comando siguiente:

```
systemctl start mysqld ocie ocieau
```

Habilitar y deshabilitar la gestión del almacenamiento basada en políticas

A partir de Unified Manager 9.7, puede aprovisionar cargas de trabajo de almacenamiento (volúmenes y LUN) en los clústeres de ONTAP y gestionar esas cargas de trabajo en función de los niveles de servicio de rendimiento asignados. Esta funcionalidad es similar a crear cargas de trabajo en ONTAP System Manager y asociar políticas de calidad de servicio, pero cuando se aplica mediante Unified Manager, puede aprovisionar y gestionar cargas de trabajo en todos los clústeres que supervisa la instancia de Unified Manager.

Debe tener la función Administrador de aplicaciones.

Esta opción está habilitada de forma predeterminada, pero puede deshabilitarla si no se desean aprovisionar y gestionar cargas de trabajo mediante Unified Manager.

Cuando está activada, esta opción proporciona muchos elementos nuevos en la interfaz de usuario:

Nuevo contenido	Ubicación
Una página para aprovisionar nuevas cargas de trabajo	Disponible en tareas comunes > aprovisionamiento
Página para crear políticas de nivel de servicio de rendimiento	Disponible en Ajustes > políticas > niveles de servicio de rendimiento
Página para crear políticas de eficiencia del almacenamiento de rendimiento	Disponible en Ajustes > políticas > eficiencia del almacenamiento
Paneles que describen el rendimiento de su carga de trabajo actual y las IOPS de su carga de trabajo	Disponible en la consola

Consulte la ayuda en línea del producto para obtener más información sobre estas páginas y sobre esta función.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General > Configuración de funciones**.
2. En la página **Configuración de función**, desactive o habilite la administración del almacenamiento basada en políticas eligiendo una de las siguientes opciones:

Si desea...	Realice lo siguiente...
Desactive la administración del almacenamiento basada en políticas	En el panel Administración de almacenamiento basada en directivas , mueva el botón deslizable hacia la izquierda.
Gestión del almacenamiento basada en normativas	En el panel Administración de almacenamiento basada en directivas , mueva el botón deslizable hacia la derecha.

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.