



Cambiar el nombre de host de Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

Tabla de contenidos

- Cambiar el nombre de host de Unified Manager 1
 - Cambiar el nombre del host del dispositivo virtual Unified Manager 1
 - Generar un certificado de seguridad HTTPS 2
 - Reinicie la máquina virtual de Unified Manager 4
- Cambiar el nombre de host de Unified Manager en sistemas Linux 4

Cambiar el nombre de host de Unified Manager

En algún momento, es posible que desee cambiar el nombre de host del sistema en el que ha instalado Unified Manager. Por ejemplo, es posible que desee cambiar el nombre del host para identificar más fácilmente sus servidores Unified Manager por tipo, grupo de trabajo o grupo de clústeres monitoreado.

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

Cambiar el nombre del host del dispositivo virtual Unified Manager

Al host de red se le asigna un nombre cuando se implementa por primera vez el dispositivo virtual Unified Manager. Puede cambiar el nombre del host después de la implementación. Si cambia el nombre del host, también deberá regenerar el certificado HTTPS.

Antes de empezar

Debe iniciar sesión en Unified Manager como usuario de mantenimiento o tener asignado el rol de Administrador de aplicaciones para realizar estas tareas.

Puede utilizar 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 su red durante la implementación, entonces deberá designar un nombre para el host de la red. Si configuró la red usando 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 automáticamente y se asocia con el certificado de seguridad.

Independientemente de cómo se asignó el nombre de host, si cambia el nombre de host y pretende utilizar 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 utilizando la dirección IP del servidor en lugar del nombre de host, no tendrá que generar un nuevo certificado si cambia el nombre de host. Sin embargo, la mejor práctica es actualizar el certificado para que el nombre de host en el certificado coincida con el nombre de host real.

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

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

Pasos

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

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

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

Después de regenerar 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. Puede generar un nuevo certificado de seguridad HTTPS que reemplace el certificado existente.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

Puede haber varias razones para regenerar el certificado, por ejemplo, si desea tener mejores valores para el nombre distinguido (DN), si desea un tamaño de clave mayor, un período de vencimiento más largo o si el certificado actual ha vencido.

Si no tiene acceso a la interfaz de usuario web de Unified Manager, puede regenerar el certificado HTTPS con los mismos valores utilizando la consola de mantenimiento. Al regenerar certificados, puede definir el tamaño de la clave y la duración de validez de la clave. Si utiliza el `Reset Server Certificate` opción desde la consola de mantenimiento, luego se crea un nuevo certificado HTTPS que es válido por 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**.

Se muestra el cuadro de diálogo Regenerar certificado HTTPS.

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

Si quieres...	Haz esto...
Regenerar el certificado con los valores actuales	Haga clic en la opción Regenerar usando los atributos del certificado actual .

Si quieres...	Haz esto...
Generar el certificado utilizando diferentes valores	Haga clic en la opción Actualizar los atributos del certificado actual. Los campos Nombre común y Nombres alternativos utilizarán los valores del certificado existente si no ingresa valores nuevos. El "Nombre común" debe establecerse en el FQDN del host. Los demás campos no requieren valores, pero puede ingresar valores, por ejemplo, para CORREO ELECTRÓNICO, EMPRESA, DEPARTAMENTO, Ciudad, Estado y País si desea que esos valores se completen en el certificado. También puede seleccionar entre el TAMAÑO DE CLAVE disponible (el algoritmo de clave es "RSA".) y el PERÍODO DE VALIDEZ.  • Los valores permitidos para el tamaño de la clave son 2048 , 3072 y 4096 . • Los períodos de validez son mínimo de 1 día y máximo de 36500 días. Aunque se permite un período de validez de 36.500 días, se recomienda utilizar un período de validez de no más de 397 días o 13 meses. Porque si selecciona un período de validez de más de 397 días y planea exportar un CSR para este certificado y hacer que lo firme una CA conocida, la validez del certificado firmado que le devuelva la CA se reducirá a 397 días. • Puede seleccionar la casilla de verificación "Excluir información de identificación local (por ejemplo, localhost)" si desea eliminar la información de identificación local del campo Nombres alternativos en el certificado. Cuando esta casilla de verificación está seleccionada, solo lo que ingrese en el campo se utilizará en el campo Nombres alternativos. Si se deja en blanco, el certificado resultante no tendrá ningún campo de 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. Verifique la información del nuevo certificado viendo el certificado HTTPS.

Reinicie la máquina virtual de Unified Manager

Puede reiniciar la máquina 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.

Antes de empezar

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 utilizando la opción **Reiniciar invitado**. Consulte la documentación de VMware para obtener más información.

Pasos

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

Cambiar el nombre de host de Unified Manager en sistemas Linux

En algún momento, es posible que desee cambiar el nombre de host de la máquina Red Hat Enterprise Linux en la que ha instalado Unified Manager. Por ejemplo, es posible que desee cambiar el nombre del host para identificar más fácilmente sus servidores Unified Manager por tipo, grupo de trabajo o grupo de clúster monitoreado cuando enumera sus máquinas Linux.

Antes de empezar

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

Puede utilizar 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 su red durante la implementación, entonces deberá designar un nombre para el host de la red. Si configuró la red usando 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 pretende utilizar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, deberá generar un nuevo certificado de seguridad.

Si accede a la interfaz de usuario web utilizando la dirección IP del servidor en lugar del nombre de host, no tendrá que generar un nuevo certificado si cambia el nombre de host. Sin embargo, la mejor práctica es actualizar el certificado para que el nombre de host en el certificado coincida con el nombre de host real. El nuevo certificado no tendrá efecto hasta que se reinicie la máquina Linux.

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

Pasos

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

```
systemctl stop ocieau ocie mysqld
```

3. Cambiar el nombre del host usando Linux `hostnamectl` dominio:

```
hostnamectl set-hostname new_FQDN
```

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

4. Regenerar el certificado HTTPS para el servidor:

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

5. Reiniciar el servicio de red:

```
systemctl restart NetworkManager.service
```

6. Después de reiniciar el servicio, verifique 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 estableció anteriormente para el nombre de host original.

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

```
systemctl start mysqld ocie ocieau
```

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.