Cambiar el nombre de host de Unified Manager

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/es-es/active-iq-unified-manager-918/config/task_change_unified_manager_host_name_on_vmware.html on November 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Cambiar el nombre de host de Unified Manager 1
Cambiar el nombre de host de la máquina virtual Active IQ Unified Manager 1
Generar un certificado de seguridad HTTPS en Active IQ Unified Manager 1
Reinicia la máquina virtual de Active IQ Unified Manager 4
Cambia el nombre de host de Active IQ Unified Manager en sistemas Linux 4

Cambiar el nombre de host de Unified Manager

Cambiar el nombre de host de la máquina virtual Active IQ Unified Manager

Al host de red se le asigna un nombre cuando se implementa por primera vez el appliance virtual Unified Manager. Puedes cambiar el nombre de host después de la implementación. Si cambias el nombre de host, también debes volver a generar el certificado HTTPS.

Antes de empezar

Para realizar estas tareas, debes haber iniciado sesión en Unified Manager como usuario de mantenimiento o tener asignado el rol de Application Administrator.

Puedes usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web de Unified Manager. Si configuraste una dirección IP estática para tu red durante la implementación, habrás asignado un nombre al host de la red. Si configuraste la red mediante DHCP, el nombre de host debería obtenerse 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 haya asignado el nombre de host, si lo cambias y pretendes utilizar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, deberás generar un nuevo certificado de seguridad.

Si accedes a la interfaz de usuario web utilizando la dirección IP del servidor en lugar del nombre de host, no es necesario generar un nuevo certificado si cambias el nombre de host. Sin embargo, es una práctica recomendada actualizar el certificado para que el nombre de host que figura en él coincida con el nombre de host real.

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

El nuevo certificado no entrará en vigor hasta que se reinicie la máquina virtual de Unified Manager.

Pasos

1. Generar un certificado de seguridad HTTPS

   Si deseas utilizar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debes volver a generar el certificado HTTPS para asociarlo al nuevo nombre de host.

2. Reinicia la máquina virtual de Unified Manager

   Una vez regenerado el certificado HTTPS, debes reiniciar la máquina virtual de Unified Manager.

Generar un certificado de seguridad HTTPS en Active IQ Unified Manager

Cuando instalas Active IQ Unified Manager por primera vez, el sistema instala un certificado HTTPS predeterminado. Puedes generar un nuevo certificado de seguridad HTTPS que sustituya al certificado existente.

Antes de empezar

Debes tener el rol de Application Administrator.

Puede haber varias razones para regenerar el certificado, por ejemplo, si quieres usar valores más adecuados para el nombre distintivo (DN), si quieres un tamaño de clave mayor, un período de validez más largo o si el certificado actual ha caducado.

Si no tienes acceso a la interfaz de usuario web de Unified Manager, puedes volver a generar el certificado HTTPS con los mismos valores mediante la consola de mantenimiento. Al volver a generar los certificados, puedes definir el tamaño de la clave y el período de validez de la clave. Si usas la opción `Reset Server Certificate` desde la consola de mantenimiento, se crea un nuevo certificado HTTPS válido durante 397 días. Este certificado tendrá una clave RSA de 2048 bits.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Certificado HTTPS**.
2. Haz clic en **Regenerar certificado HTTPS**.

   Aparece el cuadro de diálogo «Regenerar certificado HTTPS».

3. Selecciona una de las siguientes opciones en función de cómo quieras generar el certificado:

Si quieres…	**Haz esto…**
Vuelve a generar el certificado con los valores actuales	Haz clic en la opción **Regenerar utilizando los atributos del certificado actual**.

Si quieres…	Haz esto…
Genera el certificado utilizando diferentes valores	Haz clic en la opción **Actualizar los atributos del certificado actual**. Los campos «Common Name» y «Alternative Names» usarán los valores del certificado existente si no introduces valores nuevos. El campo «`Common Name`» debe establecerse con el FQDN del host. Los demás campos no requieren valores, pero puedes introducir valores, por ejemplo, para EMAIL, COMPANY, DEPARTMENT, City, State y Country, si quieres que esos valores se incluyan en el certificado. También puedes seleccionar entre los valores disponibles de KEY SIZE (el algoritmo de clave es «`RSA`».) y VALIDITY PERIOD. • Los valores permitidos para el tamaño de la clave son `2048`, `3072` y `4096`. • Los períodos de validez van desde un mínimo de 1 día hasta un máximo de 36500 días. Aunque se permite un período de validez de 36 500 días, se recomienda que uses un período de validez de no más de 397 días o 13 meses. Esto se debe a que, si seleccionas un período de validez de más de 397 días y tienes previsto exportar una CSR para este certificado y hacer que la firme una CA reconocida, la validez del certificado firmado que te devuelva la CA se reducirá a 397 días. • Puedes marcar la casilla «Excluir información de identificación local (p. ej., localhost)» si deseas eliminar la información de identificación local del campo «Nombres alternativos» del certificado. Cuando marcas esta casilla, en el campo «Nombres alternativos» solo se usa lo que introduzcas en el campo. Si lo dejas en blanco, el certificado resultante no tendrá ningún campo «Nombres alternativos».

4. Haz clic en **Sí** para regenerar el certificado.

5. Reinicia el servidor de Unified Manager para que el nuevo certificado entre en vigor.
6. Comprueba la información del nuevo certificado consultando el certificado HTTPS.

Reinicia la máquina virtual de Active IQ Unified Manager

Puedes reiniciar la máquina virtual desde la consola de mantenimiento de Unified Manager. Debes reiniciarla después de generar un nuevo certificado de seguridad o si se produce algún problema con la máquina virtual.

Antes de empezar

El dispositivo virtual está encendido.

Has iniciado sesión en la consola de mantenimiento como el usuario de mantenimiento.

También puedes reiniciar la máquina virtual desde vSphere utilizando la opción **Restart Guest**. Consulta la documentación de VMware para obtener más información.

Pasos

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

Cambia el nombre de host de Active IQ Unified Manager en sistemas Linux

Es posible que, en algún momento, desees cambiar el nombre de host del equipo con Red Hat Enterprise Linux en el que has instalado Unified Manager. Por ejemplo, quizá quieras cambiar el nombre del host para identificar más fácilmente tus servidores de Unified Manager por tipo, grupo de trabajo o grupo de clústeres supervisados al mostrar la lista de tus equipos Linux.

Antes de empezar

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

Puedes utilizar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web de Unified Manager. Si has configurado una dirección IP estática para tu red durante la implementación, habrás asignado un nombre al host de la red. Si has configurado la red mediante DHCP, el nombre de host debería tomarse del servidor DNS.

Independientemente de cómo se haya asignado el nombre de host, si lo cambias y piensas usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debes generar un nuevo certificado de seguridad.

Si accedes a la interfaz de usuario web utilizando la dirección IP del servidor en lugar del nombre de host, no es necesario generar un nuevo certificado si cambias el nombre de host. Sin embargo, la práctica recomendada es actualizar el certificado para que el nombre de host que figura en él coincida con el nombre de host real. El nuevo certificado no surtirá efecto hasta que se reinicie la máquina Linux.

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

Pasos

1. Inicia sesión como usuario raíz en el sistema Unified Manager que desees modificar.
2. Detén el software Unified Manager y el software MySQL asociado introduciendo el siguiente comando:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Cambia el nombre de host con el comando de Linux `hostnamectl`:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Regenera el certificado HTTPS del servidor:

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

5. Reinicia el servicio de red:

   ```
   systemctl restart NetworkManager.service
   ```

6. Después de reiniciar el servicio, comprueba si el nuevo nombre de host responde al comando «ping»:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Este comando debería devolver la misma dirección IP que se había configurado anteriormente para el nombre de host original.

7. Una vez que hayas completado y verificado el cambio del nombre de host, reinicia Unified Manager introduciendo el siguiente comando:

   ```
   systemctl start mysqld ocie ocieau
   ```

Información de copyright

Copyright © 2026 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.