Cambie el nombre de host de Unified Manager

Active IQ Unified Manager 9.10

NetApp
December 18, 2023

This PDF was generated from https://docs.netapp.com/es-es/active-iq-unified-manager-910/config/task_generate_an_https_security_certificate_ocf.html on December 18, 2023. Always check docs.netapp.com for the latest.

Tabla de contenidos

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 utiliza la `Reset Server Certificate` Opción de la consola de mantenimiento, se crea 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…
Genere el certificado con diferentes valores	Haga clic en la opción **Actualizar atributos de certificado actuales**. 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. ⓘ • 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. 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. • 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.

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 con Linux `hostnamectl` comando:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Regenere el certificado HTTPS para el servidor:

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

5. Reinicie el servicio de red:

   ```
   service network restart
   ```

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
   ```

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 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.