Configurar Active IQ 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/concept_configure_unified_manager.html on November 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configurar Active IQ Unified Manager . . . 1
- Infórmate sobre cómo configurar Active IQ Unified Manager . . . 1
- Conoce la secuencia de configuración en Active IQ Unified Manager . . . 1
- Accede a la interfaz de usuario web en Active IQ Unified Manager . . . 1
- Realiza la configuración inicial de la interfaz de usuario web de Active IQ Unified Manager . . . 2
- Agrega clústeres a Active IQ Unified Manager . . . 4
- Configurar notificaciones . . . 6
  - Configura Active IQ Unified Manager para que envíe notificaciones de alerta . . . 6
  - Configura los ajustes de notificación de eventos en Active IQ Unified Manager . . . 7
  - Habilita la autenticación remota en Active IQ Unified Manager . . . 8
  - Desactivar los grupos anidados de la autenticación remota en Active IQ Unified Manager . . . 9
  - Configura los servicios de autenticación en Active IQ Unified Manager . . . 10
  - Agrega servidores de autenticación a Active IQ Unified Manager . . . 11
  - Comprueba la configuración de los servidores de autenticación en Active IQ Unified Manager . . . 13
  - Agrega alertas en Active IQ Unified Manager . . . 13
- Cambiar la contraseña de usuario local en Active IQ Unified Manager . . . 15
- Configura el tiempo de espera por inactividad de la sesión en Active IQ Unified Manager . . . 16
- Configura el tiempo de espera de la sesión usando la CLI en Active IQ Unified Manager . . . 16
- Cambiar el nombre de host de Unified Manager . . . 17
  - Cambiar el nombre de host de la máquina virtual Active IQ Unified Manager . . . 17
  - Generar un certificado de seguridad HTTPS en Active IQ Unified Manager . . . 17
  - Reinicia la máquina virtual de Active IQ Unified Manager . . . 20
  - Cambia el nombre de host de Active IQ Unified Manager en sistemas Linux . . . 20
- Activar y desactivar la gestión del almacenamiento basado en políticas en Active IQ Unified Manager . . . 21

Configurar Active IQ Unified Manager

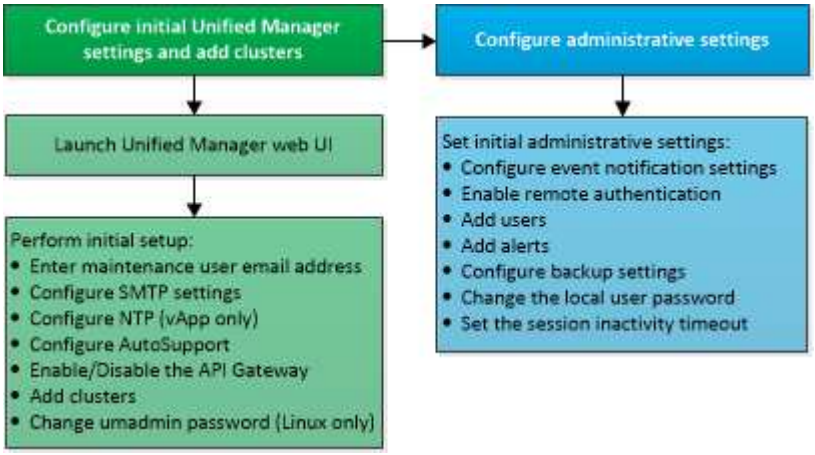
Infórmate sobre cómo configurar Active IQ Unified Manager

Tras instalar Active IQ Unified Manager (anteriormente conocido como OnCommand Unified Manager) debes completar la configuración inicial (también denominada «asistente de primera experiencia») para acceder a la interfaz de usuario web. A continuación, podrás realizar tareas de configuración adicionales, 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 tu instancia de Unified Manager. Otros procedimientos son ajustes de configuración recomendados que resulta útil aplicar en tu nueva instancia, o que conviene conocer antes de iniciar la supervisión periódica de tus sistemas ONTAP.

Conoce la secuencia de configuración en Active IQ Unified Manager

El flujo de trabajo de configuración describe las tareas que debes realizar antes de poder utilizar Unified Manager.



Accede a la interfaz de usuario web en Active IQ Unified Manager

Una vez instalado Unified Manager, puedes acceder a la interfaz de usuario web para configurarlo y así poder empezar a supervisar tus sistemas ONTAP.

Antes de empezar

- Si es la primera vez que accedes a la interfaz de usuario web, debes iniciar sesión como usuario de mantenimiento (o como usuario umadmin para instalaciones de Linux).
- Si tienes previsto permitir que los usuarios accedan a Unified Manager utilizando el nombre abreviado en lugar de usar el nombre de dominio completo (FQDN) o la dirección IP, la configuración de tu red debe resolver ese nombre abreviado en un FQDN válido.

- Si el servidor utiliza un certificado digital autofirmado, es posible que el navegador muestre una advertencia indicando que el certificado no es de confianza. Puedes aceptar el riesgo para continuar con el acceso o instalar un certificado digital firmado por una autoridad de certificación (CA) para la autenticación del servidor.

Pasos

1. Inicia la interfaz de usuario web de Unified Manager desde tu navegador utilizando la URL que aparece al final de la instalación. La URL es la dirección IP o el dominio completo (FQDN) del servidor de Unified Manager.

   El enlace tiene el siguiente formato: `https://URL`.

2. Inicia sesión en la interfaz de usuario web de Unified Manager con tus credenciales de usuario de mantenimiento.

> Si realizas tres intentos fallidos consecutivos de iniciar sesión en la interfaz de usuario web en el plazo de una hora, el sistema bloqueará tu acceso y tendrás que ponerte en contacto con el administrador del sistema. Esto solo se aplica a los usuarios locales.

Realiza la configuración inicial de la interfaz de usuario web de Active IQ Unified Manager

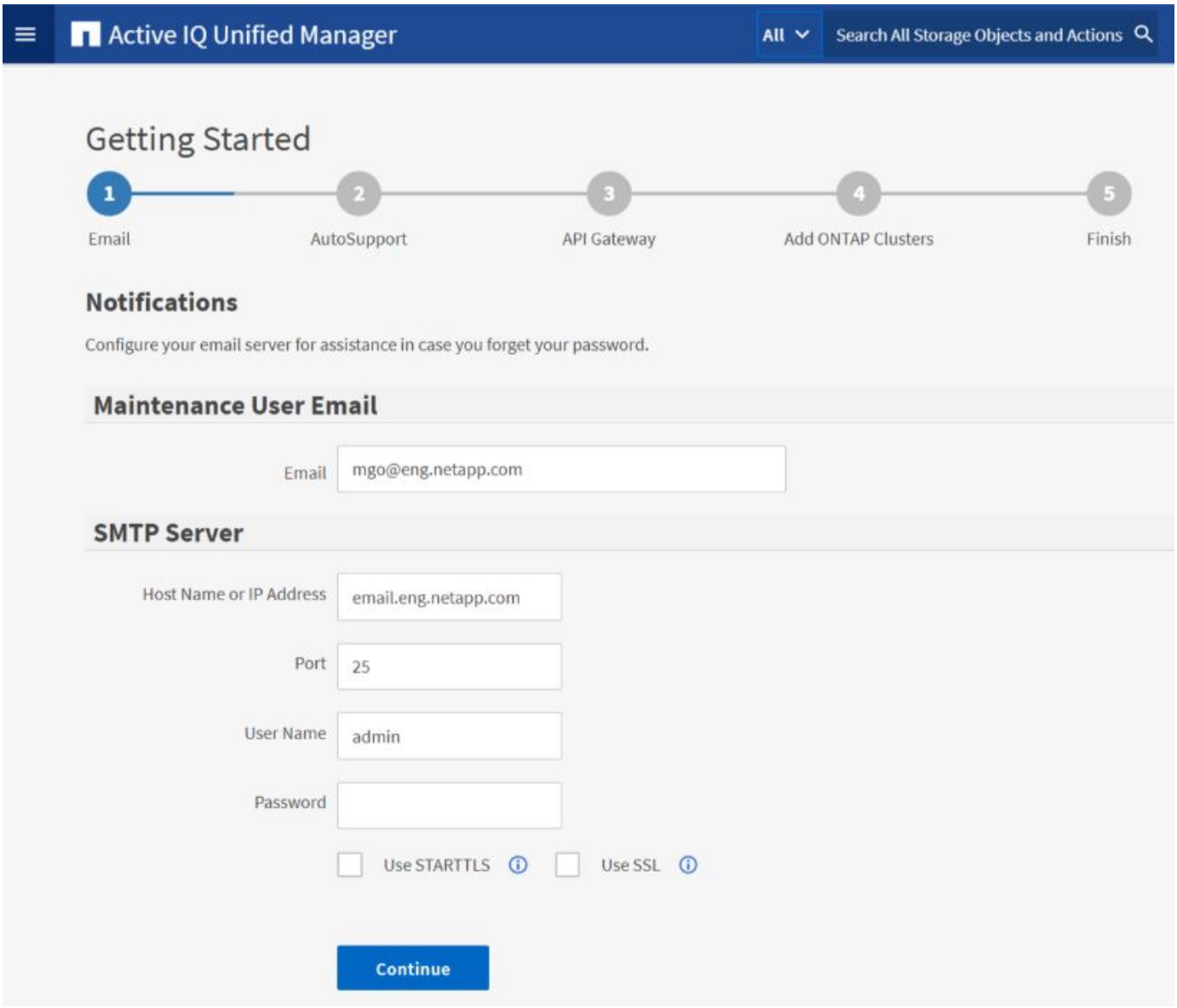
Para usar Unified Manager, primero debes configurar las opciones de configuración inicial, como el servidor NTP, la dirección de correo electrónico del usuario de mantenimiento, el nombre de host del servidor SMTP y la incorporación de clústeres ONTAP.

Antes de empezar

Debes haber realizado las siguientes operaciones:

- Abre la interfaz de usuario web de Unified Manager con la URL proporcionada después de la instalación
- Has iniciado sesión con el nombre de usuario y la contraseña de mantenimiento (usuario «umadmin» para instalaciones en Linux) creados durante la instalación

La página Active IQ Unified ManagerGetting Started solo aparece la primera vez que accedes a la interfaz de usuario web. La página de abajo corresponde a una instalación en VMware.



Si más adelante quieres cambiar alguna de estas opciones, puedes seleccionar la opción que prefieras en las opciones «General» del panel de navegación izquierdo de Unified Manager. Ten en cuenta que la configuración de NTP es solo para instalaciones de VMware y que se puede cambiar más adelante mediante la consola de mantenimiento de Unified Manager.

Pasos

1. En la página de configuración inicial de Active IQ Unified Manager, introduce la dirección de correo electrónico del usuario de mantenimiento, el nombre de host del servidor SMTP y cualquier opción SMTP adicional, así como el servidor NTP (solo en instalaciones de VMware). A continuación, haz clic en **Continue**.

   Si has seleccionado la opción **Usar STARTTLS** o **Usar SSL**, aparecerá una página con el certificado tras hacer clic en el botón **Continuar**. Comprueba los datos del certificado y acéptalo para continuar con la configuración inicial de la interfaz de usuario web.

2. En la página AutoSupport, haz clic en **Agree and Continue** para habilitar el envío de mensajes de AutoSupport desde Unified Manager a NetAppActive IQ.

   Si necesitas configurar un proxy para disponer de acceso a internet con el fin de enviar contenido de

AutoSupport, o si deseas desactivar AutoSupport, utiliza la opción **General** > **AutoSupport** de la interfaz de usuario web.

3. En los sistemas Red Hat, cambia la contraseña del usuario umadmin de la cadena predeterminada “admin” a una cadena personalizada.
4. En la página «Configurar API Gateway», selecciona si deseas utilizar la función de API Gateway que permite a Unified Manager gestionar los clústeres ONTAP que tienes previsto supervisar mediante las API REST de ONTAP. A continuación, haz clic en **Continuar**.

   Puedes activar o desactivar esta configuración más adelante en la interfaz de usuario web, en **General** > **Feature Settings** > **API Gateway**. Para obtener más información sobre las API, consulta "Primeros pasos con API de REST de Active IQ Unified Manager".

5. Añade los clústeres que quieras que gestione Unified Manager y, a continuación, haz clic en **Siguiente**. Para cada clúster que tengas previsto gestionar, debes tener el nombre de host o la dirección IP de gestión 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. Puedes añadir clústeres más adelante en la interfaz de usuario web desde **Gestión de almacenamiento** > **Configuración de clústeres**.

6. En la página «Resumen», comprueba que todos los ajustes sean correctos y haz clic en **Finalizar**.

La página «Introducción» se cierra y aparece la página «Panel de control de Unified Manager».

Agrega clústeres a Active IQ Unified Manager

Puedes añadir un clúster a Active IQ Unified Manager para poder supervisarlo. Esto incluye la posibilidad de obtener información sobre el clúster, como su estado, capacidad, rendimiento y configuración, lo que te permitirá detectar y resolver cualquier problema que pueda surgir.

Antes de empezar

- Debes tener el rol de Application Administrator o Storage Administrator.
- Debes disponer de la siguiente información:
  - Unified Manager es compatible con clústeres ONTAP locales, ONTAP Select y Cloud Volumes ONTAP.
  - Nombre de host o dirección IP de gestión del clúster

    El nombre de host es el nombre de dominio completo (FQDN) o el nombre abreviado que utiliza Unified Manager para conectarse al clúster. El nombre de host debe resolverse a la dirección IP de gestión del clúster.

    La dirección IP de gestión del clúster debe ser el LIF de gestión del clúster de la máquina virtual de almacenamiento administrativa (SVM). Si usas un LIF de gestión de nodo, la operación falla.

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

    Esta cuenta debe tener el rol *admin* con acceso a aplicación configurado en *ontapi*, *amqp*, *console* y *http*.

- El número de puerto para conectarte al clúster mediante el protocolo HTTPS (normalmente el puerto 443)
- Tienes los certificados necesarios:

  Certificado SSL (HTTPS): este certificado es propiedad de Unified Manager. Con una instalación nueva de Unified Manager, se genera un certificado SSL (HTTPS) autofirmado de forma predeterminada. NetApp recomienda actualizarlo a un certificado firmado por una CA para mayor seguridad. Si el certificado del servidor caduca, debes regenerarlo y reiniciar Unified Manager para que los servicios incorporen el nuevo certificado. Para obtener más información sobre cómo regenerar el certificado SSL, consulta "Generar un certificado de seguridad HTTPS".

  Certificado EMS: este certificado es propiedad de Unified Manager. Se utiliza durante la autenticación para las notificaciones EMS recibidas de ONTAP.

  Certificados para la comunicación TLS mutua: se utilizan durante la comunicación TLS mutua entre Unified Manager y ONTAP. La autenticación basada en certificados está habilitada para un clúster, en función de la versión de ONTAP. Si la versión de ONTAP del clúster es inferior a la 9.5, la autenticación basada en certificados no está habilitada.

  La autenticación basada en certificados no se habilita automáticamente para un clúster si actualizas una versión anterior de Unified Manager. Sin embargo, puedes habilitarla modificando y guardando los detalles del clúster. Si el certificado caduca, debes volver a generarlo para incorporar el nuevo certificado. Para obtener más información sobre cómo ver y volver a generar el certificado, consulta "Editar clústeres".

  - Puedes añadir un clúster desde la interfaz de usuario web y la autenticación basada en certificados se activa automáticamente.
  - Puedes añadir un clúster mediante Unified Manager CLI, la autenticación basada en certificados no está habilitada de forma predeterminada. Si añades un clúster mediante Unified Manager CLI, tienes que editar el clúster mediante Unified Manager UI. Puedes consultar "Comandos compatibles de la CLI de Unified Manager" para añadir un clúster mediante Unified Manager CLI.
  - Si la autenticación basada en certificados está habilitada para un clúster y haces una copia de seguridad de Unified Manager desde un servidor y la restauras en otro servidor de Unified Manager en el que ha cambiado el nombre de host o la dirección IP, la supervisión del clúster puede fallar. Para evitar este fallo, edita y guarda los detalles del clúster. Para obtener más información sobre cómo editar los detalles del clúster, consulta "Editar clústeres".

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

- Debes disponer de espacio suficiente en el servidor de Unified Manager. No podrás añadir un clúster al servidor si ya se ha ocupado más del 90 % del espacio del directorio de la base de datos.

Para una configuración de MetroCluster, debes añadir tanto el clúster local como el remoto, y ambos deben estar configurados correctamente.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **Gestión del almacenamiento** > **Configuración del clúster**.
2. En la página Configuración del clúster, haz clic en **Add**.
3. En el cuadro de diálogo «Añadir clúster», especifica los valores necesarios, como el nombre de host o la dirección IP del clúster, el nombre de usuario, la contraseña y el número de puerto.

   Puedes cambiar la dirección IP de gestión del clúster de IPv6 a IPv4 o de IPv4 a IPv6. La nueva dirección IP aparecerá en la cuadrícula del clúster y en la página de configuración del clúster una vez que haya finalizado el siguiente ciclo de supervisión.
4. Haz clic en **Enviar**.
5. En el cuadro de diálogo «Autorizar host», haz clic en **Ver certificado** para consultar la información del certificado del clúster.
6. Haz clic en **Sí**.

   Una vez guardados los datos del clúster, podrás ver el certificado para la comunicación TLS mutua de dicho clúster.

   Si la autenticación basada en certificados no está habilitada, Unified Manager comprueba el certificado únicamente cuando se añade el clúster por primera vez. Unified Manager no comprueba el certificado en cada llamada a la API de ONTAP.

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

Como la recopilación de 15 días de datos de rendimiento consume mucha CPU, se recomienda escalonar la incorporación de nuevos clústeres para que las consultas de recopilación de continuidad de datos no se ejecuten en demasiados clústeres al mismo tiempo. Además, si reinicias Unified Manager durante el periodo de recopilación de continuidad de datos, la recopilación se detendrá y verás lagunas en los gráficos de rendimiento durante el intervalo de tiempo que falta.

Si recibes un mensaje de error indicando que no puedes añadir el clúster, comprueba si los relojes de los dos sistemas están desincronizados y si la fecha de inicio del certificado HTTPS de Unified Manager es posterior a la fecha del clúster. Debes asegurarte de que los relojes estén sincronizados mediante NTP o un servicio similar.

Información relacionada

"Instalación de un certificado HTTPS firmado y devuelto por una CA"

Configurar notificaciones

Configura Active IQ Unified Manager para que envíe notificaciones de alerta

Puedes configurar Unified Manager para que envíe notificaciones que te avisen de los

eventos que se producen en tu entorno. Antes de poder enviar notificaciones, debes configurar otras opciones de Unified Manager.

Antes de empezar

Debes tener el rol de Application Administrator.

Una vez implementado Unified Manager y completada la configuración inicial, deberías plantearte configurar tu entorno para que active alertas y genere correos electrónicos de notificación o trampas SNMP en función de la recepción de eventos.

Pasos

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

   Si quieres recibir notificaciones de alerta cuando se produzcan determinados eventos en tu entorno, debes configurar un servidor SMTP e indicar una dirección de correo electrónico desde la que se enviará la notificación de alerta. Si quieres utilizar trampas SNMP, puedes seleccionar esa opción y proporcionar la información necesaria.

2. "Habilitar la autenticación remota".

   Si deseas que los usuarios remotos de LDAP o Active Directory puedan acceder a la instancia de Unified Manager y recibir notificaciones de alertas, debes habilitar la autenticación remota.

3. "Añade servidores de autenticación".

   Puedes añadir servidores de autenticación para que los usuarios remotos del servidor de autenticación puedan acceder a Unified Manager.

4. "Agregar usuarios".

   Puedes añadir varios tipos diferentes de usuarios locales o remotos y asignarles roles específicos. Cuando creas una alerta, asignas un usuario para que reciba las notificaciones de la alerta.

5. "Agregar alertas".

   Una vez que hayas añadido la dirección de correo electrónico para el envío de notificaciones, hayas añadido a los usuarios que recibirán las notificaciones, hayas configurado los ajustes de red y hayas configurado las opciones SMTP y SNMP necesarias para tu entorno, ya podrás asignar alertas.

Configura los ajustes de notificación de eventos en Active IQ Unified Manager

Puedes configurar Unified Manager para que envíe notificaciones de alerta cuando se genere un evento o cuando se asigne un evento a un usuario. Puedes configurar el servidor SMTP que se utiliza para enviar la alerta y establecer varios mecanismos de notificación; por ejemplo, las notificaciones de alerta se pueden enviar como correos electrónicos o capturas SNMP.

Antes de empezar

Debes disponer de la siguiente información:

- Dirección de correo electrónico desde la que se envía la notificación de alerta

  La dirección de correo electrónico aparece en el campo «`From`» de las notificaciones de alerta enviadas.

Si por cualquier motivo no se puede entregar el correo electrónico, esta dirección de correo electrónico también se utiliza como destinatario del correo no entregado.

- 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 la trampa que recibirá la trampa SNMP, junto con la versión de SNMP, el puerto de salida de la trampa, la comunidad y otros valores de configuración de SNMP necesarios

  Para especificar varios destinos de trap, separa cada host con una coma. En este caso, el resto de la configuración de SNMP, como la versión y el puerto de trap de salida, debe ser el mismo para todos los hosts de la lista.

Debes tener el rol de Application Administrator o Storage Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Notifications**.
2. En la página Notifications, configura los ajustes adecuados.

   Notas:

   - Si el campo "De" aparece rellenado de forma predeterminada con la dirección "ActiveIQUnifiedManager@localhost.com", debes cambiarla por una dirección de correo electrónico real y válida para asegurarte de que todas las notificaciones por correo electrónico se entreguen correctamente.
   - Si no se puede resolver el nombre de host del servidor SMTP, puedes especificar la dirección IP (IPv4 o IPv6) del servidor SMTP en lugar del nombre de host.
3. Haz clic en **Guardar**.
4. Si has seleccionado la opción **Use STARTTLS** o **Use SSL**, aparecerá una página del certificado después de hacer clic en el botón **Save**. Comprueba los datos del certificado y acéptalo para guardar la configuración de notificaciones.

   Puedes hacer clic en el botón **Ver detalles del certificado** para ver los detalles del certificado. Si el certificado existente ha caducado, desmarca la casilla **Usar STARTTLS** o **Usar SSL**, guarda la configuración de notificaciones y vuelve a marcar la casilla **Usar STARTTLS** o **Usar SSL** para ver un certificado nuevo.

Habilita la autenticación remota en Active IQ Unified Manager

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

Antes de empezar

Debes tener el rol de Application Administrator.

El servidor de Unified Manager debe conectarse directamente al servidor de autenticación. Debes desactivar cualquier cliente LDAP local, como SSSD (System Security Services Daemon) o NSLCD (Name Service LDAP Caching Daemon).

Puedes 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.

Se admite la autenticación remota a través de LDAP y LDAPS (LDAP seguro). Unified Manager utiliza el puerto 389 como puerto predeterminado para la comunicación no segura y el puerto 636 como puerto predeterminado para la comunicación segura.

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

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Remote Authentication**.
2. Marca la casilla **Habilitar autenticación remota…**.
3. En el campo Servicio de autenticación, selecciona el tipo de servicio y configura el servicio de autenticación.

Para el tipo de autenticación…	Introduce la siguiente información…
Active Directory	• Nombre del administrador del servidor de autenticación en uno de los siguientes formatos: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (utilizando la notación LDAP adecuada) • Contraseña de administrador • Nombre distintivo base (utilizando la notación LDAP adecuada)
Open LDAP	• Nombre distintivo de enlace (en la notación LDAP adecuada) • Contraseña de enlace • Nombre distintivo base

Si la autenticación de un usuario de Active Directory tarda mucho tiempo o se agota el tiempo de espera, es probable que el servidor de autenticación tarde mucho en responder. Desactivar la compatibilidad con grupos anidados en Unified Manager podría reducir el tiempo de autenticación.

Si seleccionas la opción «Usar conexión segura» para el servidor de autenticación, Unified Manager se comunicará con el servidor de autenticación mediante el protocolo Secure Sockets Layer (SSL).

4. **Opcional:** añade servidores de autenticación y comprueba que la autenticación funciona.
5. Haz clic en **Guardar**.

Desactivar los grupos anidados de la autenticación remota en Active IQ Unified Manager

Si tienes habilitada la autenticación remota, puedes desactivar la autenticación de grupos anidados para que solo los usuarios individuales, y no los miembros de grupos, puedan autenticarse de forma remota en Unified Manager. Puedes desactivar los grupos

anidados cuando desees mejorar el tiempo de respuesta de la autenticación de Active Directory.

Antes de empezar

- Debes tener el rol de Application Administrator.
- Desactivar los grupos anidados solo es aplicable cuando utilizas Active Directory.

Desactivar la compatibilidad con grupos anidados en Unified Manager podría reducir el tiempo de autenticación. Si se desactiva la compatibilidad con grupos anidados y 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 de la izquierda, haz clic en **General** > **Remote Authentication**.
2. Marca la casilla **Desactivar búsqueda de grupos anidados**.
3. Haz clic en **Guardar**.

Configura los servicios de autenticación en Active IQ Unified Manager

Los servicios de autenticación te permiten autenticar a usuarios o grupos remotos en un servidor de autenticación antes de concederles acceso a Unified Manager. Puedes autenticar a los usuarios utilizando servicios de autenticación predefinidos, como Active Directory u OpenLDAP, o configurando tu propio mecanismo de autenticación.

Antes de empezar

- Debes haber activado la autenticación remota.
- Debes tener el rol de Application Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Remote Authentication**.
2. Selecciona uno de los siguientes servicios de autenticación:

Si seleccionas…	Entonces haz lo siguiente…
Active Directory	a. Introduce el nombre y la contraseña del administrador. b. Especifica el nombre distintivo base del servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, el nombre distintivo base es **cn=ou,dc=domain,dc=com**.

Si seleccionas…	Entonces haz lo siguiente…
OpenLDAP	a. Introduce el nombre distintivo de enlace y la contraseña de enlace. b. Especifica el nombre distintivo base del servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, el nombre distintivo base es **cn=ou,dc=domain,dc=com**.
Otros	a. Introduce el nombre distintivo de enlace y la contraseña de enlace. b. Especifica el nombre distintivo base del servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, el nombre distintivo base es **cn=ou,dc=domain,dc=com**. c. Especifica la versión de protocolo LDAP que admite el servidor de autenticación. d. Introduce el nombre de usuario, la pertenencia a grupos, el grupo de usuarios y los atributos de los miembros.

Si deseas modificar el servicio de autenticación, debes eliminar todos los servidores de autenticación existentes y, a continuación, añadir nuevos servidores de autenticación.

3. Haz clic en **Guardar**.

Agrega servidores de autenticación a Active IQ Unified Manager

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

Antes de empezar

- Debes tener disponible la siguiente información:
  - Nombre de host o dirección IP del servidor de autenticación
  - Número de puerto del servidor de autenticación
- Debes haber habilitado la autenticación remota y haber configurado tu servicio de autenticación para que el servidor de gestión pueda autenticar a usuarios o grupos remotos en el servidor de autenticación.
- Debes tener el rol de Application Administrator.

Si el servidor de autenticación que estás añadiendo forma parte de un par de alta disponibilidad (HA) (que utiliza la misma base de datos), también puedes añadir el servidor de autenticación asociado. Esto permite que el servidor de gestión se comunique con el servidor asociado cuando no se puede acceder a uno de los

servidores de autenticación.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Remote Authentication**.
2. Activa o desactiva la opción **Usar conexión segura**:

Si quieres…	Entonces haz lo siguiente…
Actívalo	a. Selecciona la opción **Usar conexión segura**. b. En la sección «Servidores de autenticación», haz clic en **Add**. c. En el cuadro de diálogo Añadir servidor de autenticación, introduce el nombre de autenticación o la dirección IP (IPv4 o IPv6) del servidor. d. En el cuadro de diálogo Autorizar host, haz clic en Ver certificado. e. En el cuadro de diálogo «Ver certificado», comprueba la información del certificado y, a continuación, haz clic en **Cerrar**. f. En el cuadro de diálogo «Autorizar host», haz clic en **Sí**. 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 el puerto 636 como puerto predeterminado para la comunicación segura y el puerto 389 para la comunicación no segura.
Desactívalo	a. Desmarca la opción **Usar conexión segura**. b. En la sección «Servidores de autenticación», haz clic en **Add**. c. En el cuadro de diálogo «Añadir servidor de autenticación», especifica el nombre de host o la dirección IP (IPv4 o IPv6) del servidor, así como los detalles del puerto. d. Haz clic en **Add**.

El servidor de autenticación que has añadido aparece en el área Servidores.

3. Realiza una autenticación de prueba para comprobar que puedes autenticar a los usuarios en el servidor de autenticación que has añadido.

Comprueba la configuración de los servidores de autenticación en Active IQ Unified Manager

Puedes validar la configuración de tus servidores de autenticación para asegurarte de que el servidor de gestión pueda comunicarse con ellos. Puedes validar la configuración buscando un usuario remoto o un grupo remoto en tus servidores de autenticación y autenticándolos con la configuración establecida.

Antes de empezar

- Debes haber habilitado la autenticación remota y haber configurado tu servicio de autenticación para que el servidor de Unified Manager pueda autenticar al usuario o grupo remoto.
- Debes haber añadido tus servidores de autenticación para que el servidor de gestión pueda buscar al usuario o grupo remoto en esos servidores y autenticarlos.
- Debes tener el rol de Application Administrator.

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

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Remote Authentication**.
2. Haz clic en **Probar autenticación**.
3. En el cuadro de diálogo «Probar usuario», introduce el nombre de usuario y la contraseña del usuario remoto o el nombre de usuario del grupo remoto y, a continuación, haz clic en **Probar**.

   Si vas a autenticar un grupo remoto, no debes introducir la contraseña.

Agrega alertas en Active IQ Unified Manager

Puedes configurar alertas para que te avisen cuando se genere un evento concreto. Puedes configurar alertas para un único recurso, para un grupo de recursos o para eventos de un tipo de gravedad concreto. Puedes especificar la frecuencia con la que quieres recibir las notificaciones y asociar un script a la alerta.

Antes de empezar

- Debes haber configurado los parámetros de notificación, como la dirección de correo electrónico del usuario, el servidor SMTP y el host de trampas SNMP, para que el servidor Active IQ Unified Manager pueda utilizar estos parámetros para enviar notificaciones a los usuarios cuando se genere un evento.
- Debes conocer los recursos y los eventos para los que deseas activar la alerta, y los nombres de usuario o las direcciones de correo electrónico de los usuarios a los que quieres notificar.
- Si quieres que se ejecute un script en función del evento, debes haber añadido el script a Unified Manager usando la página Scripts.
- Debes tener el rol de Application Administrator o Storage Administrator.

Puedes crear una alerta directamente desde la página de detalles del evento después de recibir un evento, además de crear una alerta desde la página de configuración de alertas, como se describe aquí.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **Gestión del almacenamiento** > **Configuración de alertas**.
2. En la página «Configuración de alertas», haz clic en **Add**.
3. En el cuadro de diálogo «Añadir alerta», haz clic en **Nombre** e introduce un nombre y una descripción para la alerta.
4. Haz clic en **Recursos** y selecciona los recursos que quieras incluir o excluir de la alerta.

   Puedes establecer un filtro especificando una cadena de texto en el campo **Name contains** para seleccionar un grupo de recursos. En función de la cadena de texto que especifiques, la lista de recursos disponibles muestra únicamente aquellos recursos que coinciden con la regla del filtro. La cadena de texto que especifiques distingue entre mayúsculas y minúsculas.

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

5. Haz clic en **Eventos** y selecciona los eventos según el nombre del evento o el tipo de gravedad del evento para los que quieras activar una alerta.

   Para seleccionar más de un evento, pulsa la tecla Ctrl mientras haces tus selecciones.

6. Haz clic en **Acciones** y selecciona los usuarios a los que deseas notificar, elige la frecuencia de las notificaciones, indica si se enviará una trampa SNMP al receptor de trampas y asigna un script que se ejecutará cuando se genere una alerta.

   Si modificas la dirección de correo electrónico especificada para el usuario y vuelves a abrir la alerta para editarla, el campo Nombre aparece en blanco porque la dirección de correo electrónico modificada ya no está asociada al usuario que se había seleccionado anteriormente. Además, si modificaste la dirección de correo electrónico del usuario seleccionado desde la página Usuarios, la dirección de correo electrónico modificada no se actualiza para el usuario seleccionado.

   También puedes optar por notificar a los usuarios mediante trampas SNMP.

7. Haz clic en **Guardar**.

Ejemplo de cómo añadir una alerta

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

- Nombre de la alerta: HealthTest
- Recursos: incluye todos los volúmenes cuyo nombre contiene “abc” y excluye todos los volúmenes cuyo nombre contiene “xyz”
- Eventos: incluye todos los eventos críticos de salud
- Acciones: incluye "sample@domain.com", un script “Test” y tienes que notificar al usuario cada 15 minutos

Realiza los siguientes pasos en el cuadro de diálogo «Add Alert»:

Pasos

1. Haz clic en **Nombre** e introduce **HealthTest** en el campo **Nombre de la alerta**.

2. Haz clic en **Recursos** y, en la pestaña **Incluir**, selecciona **Volúmenes** en la lista desplegable.
    a. Escribe **abc** en el campo **El nombre contiene** para mostrar los volúmenes cuyo nombre contenga “abc”.
    b. Selecciona **<<All Volumes whose name contains 'abc'>>** en el área Recursos disponibles y muévelo al área Recursos seleccionados.
    c. Haz clic en **Excluir**, introduce **xyz** en el campo **El nombre contiene** y, a continuación, haz clic en **Add**.
3. Haz clic en **Eventos** y selecciona **Crítico** en el campo de gravedad del evento.
4. Selecciona **All Critical Events** en el área «Matching Events» y muévelo al área «Selected Events».
5. Haz clic en **Acciones** e introduce **sample@domain.com** en el campo «Avisar a estos usuarios».
6. Selecciona **Recordar cada 15 minutos** para notificar al usuario cada 15 minutos.

    Puedes configurar una alerta para que envíe notificaciones de forma repetida a los destinatarios durante un tiempo especificado. Debes determinar el tiempo desde el cual la notificación del evento está activa para la alerta.

7. En el menú «Seleccionar script para ejecutar», selecciona el script **Test**.
8. Haz clic en **Guardar**.

Cambiar la contraseña de usuario local en Active IQ Unified Manager

Puedes cambiar la contraseña de acceso de tu usuario local para evitar posibles riesgos de seguridad.

Antes de empezar

Debes haber iniciado sesión como usuario local.

Las contraseñas del usuario de mantenimiento y de los usuarios remotos no se pueden cambiar siguiendo estos pasos. Para cambiar la contraseña de un usuario remoto, ponte en contacto con tu administrador de contraseñas. Para cambiar la contraseña del usuario de mantenimiento, consulta "Uso de la consola de mantenimiento".

Pasos

1. Inicia sesión en Unified Manager.
2. En la barra de menús superior, haz clic en el icono de usuario y luego en **Cambiar contraseña**.

    La opción **Cambiar contraseña** no aparece si eres un usuario remoto.

3. En el cuadro de diálogo Cambiar contraseña, introduce la contraseña actual y la nueva contraseña.
4. Haz clic en **Guardar**.

Si Unified Manager está configurado en un entorno de alta disponibilidad, debes cambiar la contraseña en el segundo nodo de la configuración. Ambas instancias deben tener la misma contraseña.

Configura el tiempo de espera por inactividad de la sesión en Active IQ Unified Manager

Puedes especificar el valor del tiempo de espera por inactividad de Unified Manager para que la sesión se cierre automáticamente tras un determinado periodo de inactividad. Por defecto, el tiempo de espera está fijado en 4.320 minutos (72 horas).

Antes de empezar

Debes tener el rol de Application Administrator.

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

Esta opción no está disponible si has activado la autenticación mediante Security Assertion Markup Language (SAML).

Pasos

1. En el panel de navegación izquierdo, haz clic en **General** > **Feature Settings**.
2. En la página **Configuración de funciones**, especifica el tiempo de espera por inactividad seleccionando una de las siguientes opciones:

Si quieres…	Entonces haz lo siguiente…
No configures ningún tiempo de espera para que la sesión no se cierre automáticamente	En el panel **Inactivity Timeout**, desplaza el control deslizante hacia la izquierda (desactivado) y haz clic en **Apply**.
Establece un número concreto de minutos como valor de tiempo de espera	En el panel **Tiempo de espera por inactividad**, desplaza el control deslizante hacia la derecha (activado), especifica el valor del tiempo de espera por inactividad en minutos y haz clic en **Aplicar**.

Configura el tiempo de espera de la sesión usando la CLI en Active IQ Unified Manager

Puedes establecer un valor máximo de tiempo de espera de la sesión para Unified Manager mediante la CLI, de modo que la sesión finalice automáticamente después de un determinado periodo de tiempo. De forma predeterminada, el tiempo de espera de tu sesión está establecido en el valor máximo, que es de 4.320 minutos (72 horas). Esto significa que tu sesión finaliza automáticamente después de 72 horas, incluso si has iniciado sesión y estás usando activamente Unified Manager.

Acerca de esta tarea

Debes tener el rol de Application Administrator.

La configuración del tiempo de espera de la sesión afecta a todas las sesiones de los usuarios que hayan iniciado sesión.

Pasos

1. Inicia sesión en la CLI de Unified Manager introduciendo el `um cli login` comando. Utiliza un nombre

de usuario y una contraseña válidos para la autenticación.

2. Introduce el comando `um option set max.session.timeout.value=<in mins>` para modificar el valor del tiempo de espera de la sesión.

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
   ```

Activar y desactivar la gestión del almacenamiento basado en políticas en Active IQ Unified Manager

A partir de Unified Manager 9.7, puedes aprovisionar cargas de trabajo de almacenamiento (volúmenes y LUN) en tus clústeres 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 aplicar políticas de calidad de servicio (QoS), pero, cuando se aplica mediante Unified Manager, te permite aprovisionar y gestionar cargas de trabajo en todos los clústeres que supervisa tu instancia de Unified Manager.

Debes tener el rol de Application Administrator.

Esta opción está activada de forma predeterminada, pero puedes desactivarla si no deseas aprovisionar y gestionar cargas de trabajo mediante Unified Manager.

Cuando está activada, esta opción añade muchos elementos nuevos a la interfaz de usuario:

Nuevo contenido	Ubicación
Una página para aprovisionar nuevas cargas de trabajo	Disponible en **Tareas comunes** > **Aprovisionamiento**
Una página para crear políticas de nivel de servicio de rendimiento	Disponible en **Configuración** > **Políticas** > **Niveles de servicio de rendimiento**
Una página para crear directivas de eficiencia del almacenamiento para el rendimiento	Disponible en **Configuración** > **Políticas** > **Eficiencia de almacenamiento**
Paneles que describen el rendimiento actual y las IOPS de tus cargas de trabajo	Disponible desde el panel de control

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

Pasos

1. En el panel de navegación izquierdo, haz clic en **General** > **Feature Settings**.
2. En la página **Configuración de funciones**, desactiva o activa la gestión del almacenamiento basado en políticas seleccionando una de las siguientes opciones:

Si quieres…	Entonces haz lo siguiente…
Desactivar la gestión del almacenamiento basada en políticas	En el panel **Gestión del almacenamiento basada en políticas**, desplaza el control deslizante hacia la izquierda.
Habilita la gestión del almacenamiento basada en políticas	En el panel **gestión de almacenamiento basada en políticas**, desplaza el control deslizante hacia la derecha.

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.