Realizar tareas de configuración y administración

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

Realizar tareas de configuración y administración . . . 1
- 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
  - 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 . . . 15
  - 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 . . . 16
  - Activar y desactivar la gestión del almacenamiento basado en políticas en Active IQ Unified Manager . . . 21
- Configura la copia de seguridad de Active IQ Unified Manager . . . 22
- Gestiona la configuración de las funciones . . . 22
  - Infórmate sobre la configuración de las funciones en Active IQ Unified Manager . . . 22
  - Habilita la gestión del almacenamiento basada en políticas en Active IQ Unified Manager . . . 23
  - Descubre la función API Gateway de Active IQ Unified Manager . . . 23
  - Especifica el tiempo de espera por inactividad en Active IQ Unified Manager . . . 24
  - Habilita los eventos del portal de Active IQ en Active IQ Unified Manager . . . 24
  - Activar y desactivar la configuración de seguridad para el cumplimiento en Active IQ Unified Manager . . . 25
  - Activar y desactivar la carga de scripts en Active IQ Unified Manager . . . 26
  - Agrega un banner de inicio de sesión en Active IQ Unified Manager . . . 26
- Utiliza la consola de mantenimiento . . . 26
  - Infórmate sobre la consola de mantenimiento en Active IQ Unified Manager . . . 26
  - Conoce al usuario de mantenimiento en Active IQ Unified Manager . . . 27
  - Capacidades de usuario de diagnóstico en Active IQ Unified Manager . . . 27
  - Accede a la consola de mantenimiento en Active IQ Unified Manager . . . 27
  - Accede a la consola de mantenimiento usando la consola de la máquina virtual vSphere en Active IQ Unified Manager . . . 28
  - Menús de la consola de mantenimiento . . . 29
  - Cambiar la contraseña del usuario de mantenimiento en Windows en Active IQ Unified Manager . . . 34
  - Cambia la contraseña umadmin de Active IQ Unified Manager en sistemas Linux . . . 34
  - Cambiar los puertos que utiliza Active IQ Unified Manager para los protocolos HTTP y HTTPS . . . 35
  - Agrega interfaces de red a Active IQ Unified Manager . . . 36
  - Regenerar el certificado de cliente en Active IQ Unified Manager . . . 36
  - Añade espacio en disco . . . 37
- Gestionar el acceso de los usuarios . . . 40
  - Agregar usuarios . . . 40
  - Editar la configuración de usuario en Active IQ Unified Manager . . . 42
  - Ver usuarios en Active IQ Unified Manager . . . 42
  - Eliminar usuarios o grupos en Active IQ Unified Manager . . . 42
  - Infórmate sobre el control de acceso basado en roles en Active IQ Unified Manager . . . 43

Conoce los tipos de usuario en Active IQ Unified Manager . . . 43
Conoce los roles de usuario en Active IQ Unified Manager . . . 44
Infórmate sobre los roles y las funciones de los usuarios en Active IQ Unified Manager . . . 45
Gestiona la configuración de la autenticación SAML . . . 46
Habilita la autenticación SAML en Active IQ Unified Manager . . . 46
Usa un proveedor de identidad en Active IQ Unified Manager . . . 47
Habilita la autenticación SAML en Active IQ Unified Manager . . . 48
Cambiar el proveedor de identidad de autenticación SAML en Active IQ Unified Manager . . . 49
Actualiza la configuración de autenticación SAML después de un cambio en el certificado de seguridad de Active IQ Unified Manager . . . 50
Desactivar la autenticación SAML en Active IQ Unified Manager . . . 51
Desactivar la autenticación SAML desde la consola de mantenimiento de Active IQ Unified Manager . . . 52
Utiliza la página de autenticación SAML en Active IQ Unified Manager . . . 52
Gestionar la autenticación . . . 53
Editar servidores de autenticación en Active IQ Unified Manager . . . 53
Eliminar servidores de autenticación en Active IQ Unified Manager . . . 54
Autentícate con Active Directory u OpenLDAP en Active IQ Unified Manager . . . 54
Registro de auditoría . . . 55
Utiliza la página de autenticación remota en Active IQ Unified Manager . . . 57
Gestiona certificados de seguridad . . . 60
Ver el certificado de seguridad HTTPS en Active IQ Unified Manager . . . 60
Descargar una solicitud de firma de certificado HTTPS en Active IQ Unified Manager . . . 61
Instala un certificado HTTPS firmado por una autoridad de certificación (CA) en Active IQ Unified Manager . . . 61
Conoce los certificados HTTPS generados mediante herramientas externas en Active IQ Unified Manager Unified Manager . . . 62
Descripciones de las páginas para la gestión de certificados . . . 65

Realizar tareas de configuración y administración

Configurar Active IQ Unified Manager

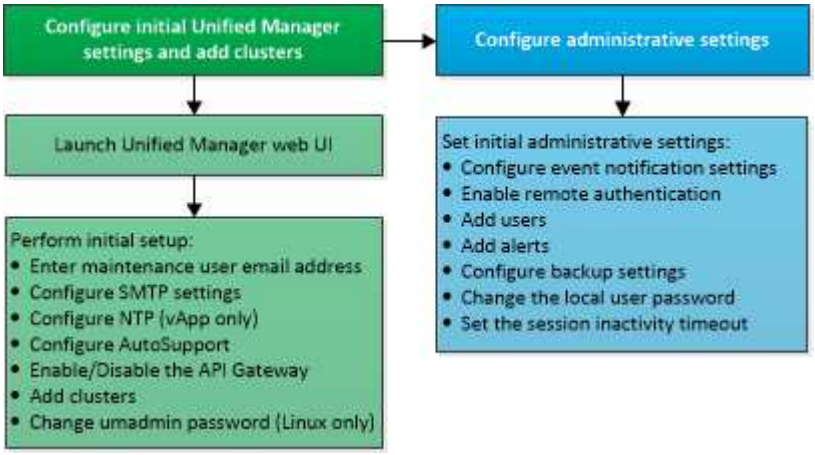
Infórmate sobre cómo configurar Active IQ Unified Manager

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

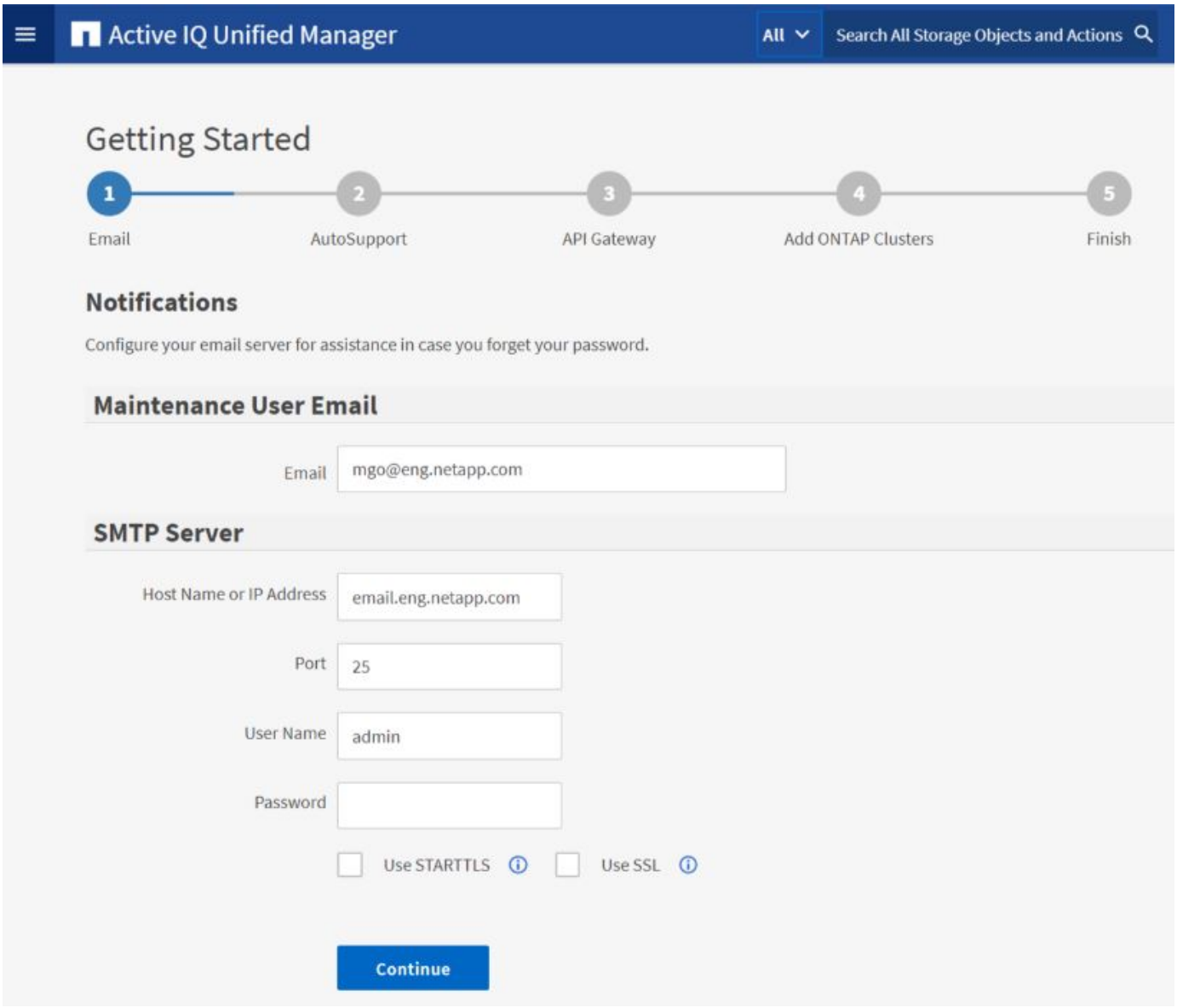
Para usar Unified Manager, primero debes configurar las opciones de configuración inicial, como el servidor NTP, la dirección de correo electrónico del usuario de mantenimiento, el nombre de host del servidor SMTP y la incorporación de clústeres ONTAP.

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**.
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**.

Si seleccionas…	Entonces haz lo siguiente…
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.

Configura la copia de seguridad de Active IQ Unified Manager

Puedes configurar la función de copia de seguridad en Unified Manager mediante una serie de pasos de configuración que debes realizar en los sistemas host y a través de la consola de mantenimiento.

Para obtener información sobre los pasos de configuración, consulta "Gestión de las operaciones de copia de seguridad y restauración".

Gestiona la configuración de las funciones

Infórmate sobre la configuración de las funciones en Active IQ Unified Manager

La página Configuración de funciones te permite activar y desactivar funciones específicas en Active IQ Unified Manager. Esto incluye crear y gestionar objetos de almacenamiento basados en políticas, activar API Gateway y Login Banner, cargar scripts para gestionar alertas, establecer un tiempo de espera para una sesión de la interfaz de usuario web en función del tiempo de inactividad y desactivar la recepción de eventos de la plataforma Active IQ.

La página «Configuración de funciones» solo está disponible para los usuarios con el rol Application Administrator.

Para obtener información sobre Scripts Upload, consulta "Activar y desactivar la carga de scripts".

Habilita la gestión del almacenamiento basada en políticas en Active IQ Unified Manager

La opción **Gestión del almacenamiento basada en políticas** permite gestionar el almacenamiento en función de los objetivos de nivel de servicio (SLO). Esta opción está activada de forma predeterminada.

Al activar esta función, podrás aprovisionar cargas de trabajo de almacenamiento en los clústeres ONTAP añadidos a tu instancia de Active IQ Unified Manager y gestionar dichas cargas de trabajo según los Performance Service Levels y las Storage Efficiency Policies asignados.

Puedes activar o desactivar esta función desde **General** > **Configuración de funciones** > **Gestión del almacenamiento basada en políticas**. Al activar esta función, las siguientes páginas estarán disponibles para su uso y supervisión:

- Aprovisionamiento (aprovisionamiento de carga de trabajo de almacenamiento)
- **Políticas** > **Niveles de servicio de rendimiento**
- **Políticas** > **Eficiencia en el almacenamiento**
- Columna «Cargas de trabajo gestionadas por nivel de servicio de rendimiento» en la página «Configuración de clústeres»
- Panel de rendimiento de la carga de trabajo en el **Dashboard**

Puedes usar las pantallas para crear Performance Service Levels y Storage Efficiency Policies, y aprovisionar cargas de trabajo de almacenamiento. También puedes supervisar las cargas de trabajo de almacenamiento que cumplen con los Performance Service Levels asignados, así como las que no los cumplen. El panel Workload Performance y Workload IOPS también te permite evaluar la capacidad total, disponible y usada, así como el rendimiento (IOPS) de los clústeres de tu centro de datos en función de las cargas de trabajo de almacenamiento aprovisionadas en ellos.

Tras activar esta función, puedes ejecutar las API de REST de Unified Manager para realizar algunas de estas funciones desde **Barra de menús** > **Botón de ayuda** > **Documentación de la API** > categoría **storage-provider**. Como alternativa, puedes introducir el nombre de host o la dirección IP y la URL para acceder a la página de la API de REST con el formato https://<hostname>/docs/api/

Para obtener más información sobre las APIs, consulta "Primeros pasos con API de REST de Active IQ Unified Manager".

Descubre la función API Gateway de Active IQ Unified Manager

La función API Gateway permite que Active IQ Unified Manager sea un único plano de control desde el que puedes gestionar varios clústeres ONTAP sin tener que iniciar sesión en cada uno por separado.

Puedes activar esta función desde las páginas de configuración que aparecen al iniciar sesión por primera vez en Unified Manager. También puedes activar o desactivar esta función desde **General** > **Configuración de**

funciones > **API Gateway**.

Las API de REST de Unified Manager son diferentes de las API de REST de ONTAP, y no todas las funcionalidades de las API de REST de ONTAP se pueden usar mediante las API de REST de Unified Manager. Sin embargo, si tienes un requisito del negocio específico para acceder a las API de ONTAP y gestionar funciones concretas que no están expuestas en Unified Manager, puedes habilitar la función API Gateway y ejecutar las API de ONTAP. La puerta de enlace actúa como un proxy para canalizar las solicitudes de API manteniendo las solicitudes de encabezado y cuerpo en el mismo formato que en las API de ONTAP. Puedes usar tus credenciales de Unified Manager y ejecutar las API específicas para acceder a los clústeres de ONTAP y gestionarlos sin pasar credenciales individuales de clúster. Unified Manager funciona como un único punto de gestión para ejecutar las API en los clústeres de ONTAP gestionados por tu instancia de Unified Manager. La respuesta que devuelven las API es la misma que la que devuelven las respectivas API de REST de ONTAP cuando se ejecutan directamente desde ONTAP.

Una vez activada esta función, puedes ejecutar las API de REST de Unified Manager desde **Barra de menús** > **Botón de ayuda** > **Documentación de la API** > categoría **gateway**. Como alternativa, puedes introducir el nombre de host o la dirección IP y la URL para acceder a la página de la API de REST con el formato `https://<hostname>/docs/api/`

Para obtener más información sobre las APIs, consulta "Primeros pasos con API de REST de Active IQ Unified Manager".

Especifica el tiempo de espera por inactividad en Active IQ Unified Manager

Puedes especificar el valor del tiempo de espera por inactividad para Active IQ Unified Manager. Después del tiempo de inactividad especificado, la aplicación cierra sesión automáticamente. Esta opción está activada de forma predeterminada.

Puedes desactivar esta función o modificar el tiempo en **General** > **Feature Settings** > **Inactivity Timeout**. Una vez que actives esta función, debes especificar el límite de tiempo de inactividad (en minutos) en el campo **LOGOUT AFTER**, tras el cual el sistema cerrará automáticamente la sesión. El valor predeterminado es 4320 minutos (72 horas).

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

Habilita los eventos del portal de Active IQ en Active IQ Unified Manager

Puedes especificar si quieres activar o desactivar los eventos del portal Active IQ. Esta configuración permite que el portal Active IQ detecte y muestre eventos adicionales sobre la configuración del sistema, el cableado, etc. Esta opción está activada de forma predeterminada.

Al habilitar esta función, Active IQ Unified Manager muestra los eventos detectados por el portal Active IQ. Estos eventos se crean aplicando un conjunto de reglas a los mensajes de AutoSupport generados por todos los sistemas de almacenamiento supervisados. Estos eventos son diferentes de los demás eventos de Unified Manager e identifican incidentes o riesgos relacionados con la configuración del sistema, el cableado, las buenas prácticas y los problemas de disponibilidad.

Puedes elegir activar o desactivar esta función desde **General** > **Feature Settings** > **Active IQ Portal Events**. En los sitios sin acceso a una red externa, debes cargar las reglas manualmente desde **Storage Management** > **Event Setup** > **Upload Rules**.

Esta función está activada de forma predeterminada. Si desactivas esta función, Active IQ deja de detectar o mostrar eventos en Unified Manager. Si está desactivada, al activar esta función, Unified Manager puede recibir los eventos de Active IQ en un clúster a la hora predefinida de 00:15 según la zona horaria de ese clúster.

Activar y desactivar la configuración de seguridad para el cumplimiento en Active IQ Unified Manager

Con el botón **Customize** del panel **Security Dashboard** de la página **Features Settings**, puedes activar o desactivar los parámetros de seguridad para la supervisión del cumplimiento en Unified Manager.

Los ajustes que se activan o desactivan desde esta página determinan el estado general de cumplimiento de los clústeres y las máquinas virtuales de almacenamiento en Unified Manager. En función de las selecciones realizadas, las columnas correspondientes se muestran en la vista **Seguridad: todos los clústeres** de la página de inventario de clústeres y en la vista **Seguridad: todas las máquinas virtuales de almacenamiento** de la página de inventario de máquinas virtuales de almacenamiento.

Solo los usuarios con el rol de administrador pueden modificar estas configuraciones.

Los criterios de seguridad de tus clústeres de ONTAP, máquinas virtuales de almacenamiento y volúmenes se evalúan según las recomendaciones definidas en "Guía de refuerzo de la seguridad para NetApp ONTAP 9". El panel Seguridad del panel de control y la página Seguridad muestran el estado predeterminado de cumplimiento de seguridad de tus clústeres, máquinas virtuales de almacenamiento y volúmenes. También se generan eventos de seguridad y se habilitan acciones de administración para los clústeres y las máquinas virtuales de almacenamiento que tienen infracciones de seguridad.

Personaliza la configuración de seguridad

Para personalizar la configuración de la supervisión del cumplimiento según corresponda a tu entorno ONTAP, sigue estos pasos:

Pasos

1. Haz clic en **General > Configuración de funciones > Panel de seguridad > Personalizar**. Aparece la ventana emergente **Personalizar la configuración del panel de seguridad**.

   Los parámetros de cumplimiento de seguridad que actives o desactives pueden afectar directamente a las vistas de seguridad predeterminadas, los informes y los informes programados de las pantallas Clusters y Storage VMs. Si habías cargado un informe de excel desde estas pantallas antes de modificar los parámetros de seguridad, es posible que los informes de excel descargados tengan errores.

2. Para activar o desactivar la configuración personalizada de tus clústeres ONTAP, selecciona la configuración general requerida en **Cluster**. Para obtener información sobre las opciones para personalizar el cumplimiento de los clústeres, consulta "Categorías de cumplimiento de los clústeres".
3. Para activar o desactivar la configuración personalizada de tus VM de almacenamiento, selecciona la configuración general requerida en **Storage VM**. Para obtener información sobre las opciones para personalizar el cumplimiento de las VM de almacenamiento, consulta "Categorías de cumplimiento de las máquinas virtuales de almacenamiento".

Personalizar la configuración de AutoSupport y de autenticación

En la sección **Configuración de AutoSupport**, puedes especificar si se debe usar HTTPS para enviar mensajes de AutoSupport desde ONTAP.

Desde la sección **Configuración de autenticación**, puedes habilitar que se generen alertas de Unified Manager para el usuario administrador predeterminado de ONTAP.

Activar y desactivar la carga de scripts en Active IQ Unified Manager

La posibilidad de cargar scripts en Unified Manager y ejecutarlos está habilitada de forma predeterminada. Si tu organización no quiere permitir esta actividad por motivos de seguridad, puedes desactivar esta funcionalidad.

Antes de empezar

Debes tener el rol de Application Administrator.

Pasos

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

Si quieres…	Entonces haz lo siguiente…
Desactiva los scripts	En el panel **Carga de scripts**, desplaza el control deslizante hacia la izquierda.
Habilitar scripts	En el panel **Script Upload**, desplaza el control deslizante hacia la derecha.

Agrega un banner de inicio de sesión en Active IQ Unified Manager

Agregar un banner de inicio de sesión permite a tu organización mostrar cualquier información, como quién tiene permiso para acceder al sistema y los términos y condiciones de uso durante el inicio y cierre de sesión.

Cualquier usuario, como los operadores de almacenamiento o los administradores, puede ver esta ventana emergente del banner de inicio de sesión al iniciar sesión, al cerrar sesión y cuando se agota el tiempo de espera de la sesión.

Utiliza la consola de mantenimiento

Infórmate sobre la consola de mantenimiento en Active IQ Unified Manager

La consola de mantenimiento de Unified Manager te permite mantener la configuración de tu sistema Unified Manager y realizar los cambios necesarios para evitar que se produzcan problemas.

En función del sistema operativo en el que hayas instalado Unified Manager, la consola de mantenimiento

ofrece las siguientes funciones:

- Soluciona cualquier problema que surja con tu dispositivo virtual, especialmente si la interfaz web de Unified Manager no está disponible
- Actualizar a versiones más recientes de Unified Manager
- Generar paquetes de soporte para enviarlos al soporte técnico
- Configura los ajustes de red
- Cambiar la contraseña del usuario de mantenimiento
- Conéctate a un proveedor de datos externo para enviar estadísticas de rendimiento
- Modificar la recopilación interna de datos de rendimiento
- Restaura la base de datos y los parámetros de configuración de Unified Manager a partir de una copia de seguridad anterior.

Conoce al usuario de mantenimiento en Active IQ Unified Manager

El usuario de mantenimiento se crea durante la instalación de Unified Manager en un sistema Red Hat Enterprise Linux. El nombre del usuario de mantenimiento es el usuario “umadmin”. El usuario de mantenimiento tiene el rol Application Administrator en la interfaz de usuario web, y ese usuario puede crear usuarios posteriores y asignarles roles.

El usuario de mantenimiento, o usuario «umadmin», también puede acceder a la consola de mantenimiento de Unified Manager.

Capacidades de usuario de diagnóstico en Active IQ Unified Manager

El objetivo del acceso de diagnóstico es permitir que el soporte técnico te ayude a solucionar problemas, y solo debes usarlo cuando te lo indique el soporte técnico.

El usuario encargado del diagnóstico puede ejecutar comandos a nivel del sistema operativo cuando así se lo indique el soporte técnico, con el fin de solucionar problemas.

Accede a la consola de mantenimiento en Active IQ Unified Manager

Si la interfaz de usuario de Unified Manager no está operativa, o si necesitas realizar funciones que no están disponibles en la interfaz de usuario, puedes acceder a la consola de mantenimiento para gestionar tu sistema Unified Manager.

Antes de empezar

Debes haber instalado y configurado Unified Manager.

Tras 15 minutos de inactividad, la consola de mantenimiento cierra tu sesión.

Cuando se instala en VMware, si ya has iniciado sesión como usuario de mantenimiento a través de la consola de VMware, no puedes iniciar sesión simultáneamente mediante Secure Shell.

Paso

1. Sigue estos pasos para acceder a la consola de mantenimiento:

En este sistema operativo…	Sigue estos pasos…
VMware	a. Con Secure Shell, conéctate a la dirección IP o al nombre de dominio completo del dispositivo virtual Unified Manager. b. Inicia sesión en la consola de mantenimiento con tu nombre de usuario de mantenimiento y tu contraseña.
Linux	a. Con Secure Shell, conéctate a la dirección IP o al dominio completo del sistema Unified Manager. b. Inicia sesión en el sistema con el nombre de usuario de mantenimiento (umadmin) y la contraseña. c. Escribe el comando `maintenance_console` y pulsa Intro.
Windows	a. Inicia sesión en el sistema Unified Manager con credenciales de administrador. b. Abre PowerShell como administrador de Windows. c. Escribe el comando `maintenance_console` y pulsa Intro.

Se muestra el menú de la consola de mantenimiento de Unified Manager.

Accede a la consola de mantenimiento usando la consola de la máquina virtual vSphere en Active IQ Unified Manager

Si la interfaz de usuario de Unified Manager no está operativa o si necesitas realizar funciones que no están disponibles en la interfaz de usuario, puedes acceder a la consola de mantenimiento para reconfigurar tu dispositivo virtual.

Antes de empezar

- Debes ser el usuario de mantenimiento.
- El appliance virtual debe estar encendido para poder acceder a la consola de mantenimiento.

Pasos

1. En vSphere Client, localiza el dispositivo virtual de Unified Manager.
2. Haz clic en la pestaña **NetApp Console**.
3. Haz clic dentro de la ventana de la consola para iniciar sesión.
4. Inicia sesión en la consola de mantenimiento con tu nombre de usuario y contraseña.

   Tras 15 minutos de inactividad, la consola de mantenimiento cierra tu sesión.

Menús de la consola de mantenimiento

Infórmate sobre los menús de la consola de mantenimiento en Active IQ Unified Manager

La consola de mantenimiento consta de diferentes menús que te permiten mantener y gestionar funciones especiales y ajustes de configuración del servidor Unified Manager.

Dependiendo del sistema operativo en el que hayas instalado Unified Manager, la consola de mantenimiento consta de los siguientes menús:

- Actualizar Unified Manager (solo VMware)
- Configuración de red (solo VMware)
- Configuración del sistema (solo VMware)
  a. Soporte/Diagnóstico
  b. Restablecer el certificado del servidor
  c. Regenerar el certificado de cliente
  d. Copia de seguridad y restauración
  e. Proveedor externo de datos
  f. Configuración del intervalo de sondeo de rendimiento
  g. Desactivar la autenticación SAML
  h. Ver/Modificar los puertos de la aplicación
  i. Configuración del registro de depuración
  j. Controla el acceso al puerto 3306 de MySQL
  k. Salir

Selecciona el número de la lista para acceder a la opción de menú específica. Por ejemplo, para copia de seguridad y restauración, selecciona *4*.

Menú de configuración de red en Active IQ Unified Manager

El menú «Configuración de red» te permite gestionar los ajustes de red. Debes utilizar este menú cuando la interfaz de usuario de Unified Manager no esté disponible.

> Este menú no está disponible si Unified Manager está instalado en Red Hat Enterprise Linux o en Microsoft Windows.

Las siguientes opciones de menú están disponibles.

- **Mostrar la configuración de la dirección IP**

  Muestra la configuración de red actual del dispositivo virtual, incluida la dirección IP, la red, la dirección de difusión, la máscara de red, la puerta de enlace y los servidores DNS.

- **Cambiar la configuración de la dirección IP**

  Te permite modificar cualquier configuración de red del dispositivo virtual, incluida la dirección IP, la máscara de red, la puerta de enlace o los servidores DNS. Si cambias la configuración de red de DHCP a

una configuración estática mediante la consola de mantenimiento, no podrás editar el nombre de host. Debes seleccionar **Commit Changes** para que estos surtan efecto.

- **Mostrar la configuración de búsqueda de nombres de dominio**

  Muestra la lista de búsqueda de nombres de dominio que se usa para resolver nombres de host.

- **Cambiar la configuración de búsqueda de nombres de dominio**

  Te permite modificar los nombres de dominio en los que quieres buscar al resolver nombres de host. Debes seleccionar **Commit Changes** para que los cambios surtan efecto.

- **Mostrar rutas estáticas**

  Muestra las rutas de red estáticas actuales.

- **Modificar rutas estáticas**

  Te permite añadir o eliminar rutas de red estáticas. Debes seleccionar **Commit Changes** para que los cambios surtan efecto.

  - **Agregar ruta**

    Te permite añadir una ruta estática.

  - **Eliminar ruta**

    Te permite eliminar una ruta estática.

  - **Atrás**

    Te lleva de vuelta al **Menú principal**.

  - **Salir**

    Sale de la consola de mantenimiento.

- **Desactivar interfaz de red**

  Desactiva todas las interfaces de red disponibles. Si solo hay una interfaz de red disponible, no puedes desactivarla. Debes seleccionar **Commit Changes** para que los cambios surtan efecto.

- **Habilitar interfaz de red**

  Activa las interfaces de red disponibles. Debes seleccionar **Commit Changes** para que los cambios surtan efecto.

- **Guardar cambios**

  Aplica los cambios realizados en la configuración de red del dispositivo virtual. Debes seleccionar esta opción para aplicar los cambios realizados o no se aplicarán.

- **Hacer ping a un host**

  Realiza una prueba de ping a un host de destino para confirmar cambios en la dirección IP o en la configuración de DNS.

- **Restablecer la configuración predeterminada**

  Restablece todos los ajustes a los valores predeterminados de fábrica. Debes seleccionar **Commit Changes** para que estos surtan efecto.

- **Atrás**

  Te lleva de vuelta al **Menú principal**.

- **Salir**

  Sale de la consola de mantenimiento.

Utiliza el menú Configuración del sistema en Active IQ Unified Manager

El menú «Configuración del sistema» te permite gestionar tu dispositivo virtual, ya que ofrece diversas opciones, como consultar el estado del servidor, así como reiniciar y apagar la máquina virtual.

Cuando Unified Manager está instalado en un sistema Linux o Microsoft Windows, en este menú solo está disponible la opción “Restore from a Unified Manager Backup”.

Las siguientes opciones de menú están disponibles:

- **Mostrar el estado del servidor**

  Muestra el estado actual del servidor. Las opciones de estado incluyen En ejecución y No en ejecución.

  Si el servidor no está en funcionamiento, es posible que tengas que ponerte en contacto con el soporte técnico.

- **Reiniciar la máquina virtual**

  Reinicia la máquina virtual y detiene todos los servicios. Después de reiniciarse, la máquina virtual y los servicios se vuelven a iniciar.

- **Apagar la máquina virtual**

  Apaga la máquina virtual y detiene todos los servicios.

  Solo puedes seleccionar esta opción desde la consola de la máquina virtual.

- **Cambiar <logged in user> contraseña de usuario**

  Cambia la contraseña del usuario que tiene la sesión iniciada en ese momento, que solo puede ser el usuario de mantenimiento.

- **Aumentar el tamaño del disco de datos**

  Aumenta el tamaño del disco de datos (disco 3) de la máquina virtual.

- **Aumentar el tamaño del disco de intercambio**

  Aumenta el tamaño del disco de intercambio (disco 2) en la máquina virtual.

- **Cambiar zona horaria**

  Cambia la zona horaria según tu ubicación.

- **Cambiar el servidor NTP**

  Modifica la configuración del servidor NTP, como la dirección IP o el dominio completo (FQDN).

- **Cambiar el servicio NTP**

  Permite alternar entre los `ntp` y `systemd-timesyncd` servicios.

- **Restaurar desde una copia de seguridad de Unified Manager**

  Restaura la base de datos y los parámetros de configuración de Unified Manager a partir de una copia de seguridad anterior.

- **Restablecer el certificado del servidor**

  Restablece el certificado de seguridad del servidor.

- **Cambiar el nombre de host**

  Cambia el nombre de host en el que está instalado el dispositivo virtual.

- **Atrás**

  Sale del menú de configuración del sistema y vuelve al menú principal.

- **Salir**

  Sale del menú de la consola de mantenimiento.

Utiliza el menú Soporte y diagnóstico en Active IQ Unified Manager

El menú Soporte y diagnóstico te permite generar un paquete de soporte que puedes enviar al soporte técnico para obtener ayuda con la solución de problemas.

Las siguientes opciones de menú están disponibles:

- **Generar paquete de soporte ligero**

  Te permite generar un paquete de soporte ligero que contiene solo 30 días de registros y registros de la base de datos de configuración; excluye los datos de rendimiento, los archivos de registro de adquisición y el volcado de memoria del servidor.

- **Generar paquete de soporte**

  Te permite crear un paquete de soporte completo (archivo 7-Zip) con información de diagnóstico en el directorio inicial del usuario de diagnóstico. Si tu sistema está conectado a internet, también puedes cargar el paquete de soporte en NetApp.

  El archivo incluye información generada por un mensaje de AutoSupport, el contenido de la base de datos de Unified Manager, datos detallados sobre el funcionamiento interno del servidor de Unified Manager y registros de nivel detallado que normalmente no se incluyen en los mensajes de AutoSupport ni en el

paquete de soporte ligero.

Descubre más opciones del menú de la consola de mantenimiento en Active IQ Unified Manager

Las siguientes opciones de menú te permiten realizar diversas tareas administrativas en el servidor de Unified Manager.

Las siguientes opciones de menú están disponibles:

- **Restablecer el certificado del servidor**

  Regenera el certificado del servidor HTTPS.

  Puedes regenerar el certificado del servidor en la GUI de Unified Manager haciendo clic en **General** > **HTTPS Certificates** > **Regenerate HTTPS Certificate**.

- **Desactivar la autenticación SAML**

  Desactiva la autenticación SAML, de modo que el proveedor de identidades (IdP) ya no proporcione autenticación de inicio de sesión a los usuarios que acceden a la interfaz gráfica de usuario (GUI) de Unified Manager. Esta opción de la consola se suele utilizar cuando un problema con el servidor IdP o con la configuración de SAML impide a los usuarios acceder a la interfaz gráfica de usuario (GUI) de Unified Manager.

- **Proveedor externo de datos**

  Ofrece opciones para conectar Unified Manager a un proveedor de datos externo. Después de establecer la conexión, los datos de rendimiento se envían a un servidor externo para que los expertos en rendimiento del almacenamiento puedan representar gráficamente las métricas de rendimiento con software de terceros. Se muestran las siguientes opciones:

  - **Configuración del servidor de visualización**--muestra la configuración actual y los ajustes de conexión de un proveedor de datos externo.
  - **Agregar / modificar la conexión del servidor**--te permite introducir nuevos ajustes de conexión para un proveedor de datos externo o cambiar los ajustes existentes.
  - **Modificar la configuración del servidor**--te permite introducir nuevos ajustes de configuración para un proveedor de datos externo o cambiar los ajustes existentes.
  - **Eliminar conexión del servidor**--elimina la conexión con un proveedor de datos externo.

    Una vez eliminada la conexión, Unified Manager pierde la conexión con el servidor externo.

- **Copia de seguridad y restauración**

  Para obtener más información, consulta los temas disponibles en "Gestión de las operaciones de copia de seguridad y restauración".

- **Configuración del intervalo de sondeo de rendimiento**

  Ofrece una opción para configurar la frecuencia con la que Unified Manager recopila datos estadísticos de rendimiento de los clústeres. El intervalo de recopilación predeterminado es de 5 minutos.

  Puedes cambiar este intervalo a 10 o 15 minutos si observas que las recopilaciones de los clústeres grandes no se completan a tiempo.

- **Ver/modificar los puertos de las aplicaciones**

  Ofrece la opción de cambiar los puertos predeterminados que utiliza Unified Manager para los protocolos HTTP y HTTPS, si es necesario por seguridad. Los puertos predeterminados son 80 para HTTP y 443 para HTTPS.

- **Controla el acceso al puerto 3306 de MySQL**

  Controla el acceso del host al puerto predeterminado de MySQL 3306. Por motivos de seguridad, el acceso a través de este puerto está restringido solo a localhost durante una instalación nueva de Unified Manager en sistemas Linux, Windows y VMware vSphere. Esta opción te permite alternar la visibilidad de este puerto entre localhost y hosts remotos, es decir, si en tu entorno está habilitado solo para localhost, también puedes hacer que este puerto esté disponible para hosts remotos. Como alternativa, cuando está habilitado para todos los hosts, puedes restringir el acceso a este puerto solo a localhost. Si el acceso se habilitó anteriormente en hosts remotos, la configuración se conserva en un escenario de actualización. Debes comprobar la configuración del firewall en sistemas Windows después de cambiar la visibilidad del puerto y desactivar la configuración del firewall si está configurada para restringir el acceso al puerto MySQL 3306.

- **Salir**

  Sale del menú de la consola de mantenimiento.

Cambiar la contraseña del usuario de mantenimiento en Windows en Active IQ Unified Manager

Puedes cambiar la contraseña del usuario de mantenimiento de Unified Manager cuando sea necesario.

Pasos

1. En la página de inicio de sesión de la interfaz de usuario web de Unified Manager, haz clic en **Olvidé la contraseña**.

   Aparece una página en la que se solicita el nombre del usuario cuya contraseña deseas restablecer.

2. Introduce el nombre de usuario y haz clic en **Enviar**.

   Se envía un correo electrónico con un enlace para restablecer la contraseña a la dirección de correo electrónico asociada a ese nombre de usuario.

3. Haz clic en el **enlace para restablecer la contraseña** del correo electrónico y establece la nueva contraseña.
4. Vuelve a la interfaz de usuario web e inicia sesión en Unified Manager con la nueva contraseña.

Cambia la contraseña umadmin de Active IQ Unified Manager en sistemas Linux

Por motivos de seguridad, debes cambiar la contraseña predeterminada del usuario umadmin de Unified Manager inmediatamente después de completar el proceso de instalación. Si es necesario, puedes volver a cambiar la contraseña en cualquier momento.

Antes de empezar

- Unified Manager debe instalarse en un sistema Red Hat Enterprise Linux Linux.
- Debes disponer de las credenciales de usuario raíz del sistema Linux en el que está instalado Unified Manager.

Pasos

1. Inicia sesión como usuario raíz en el sistema Linux en el que se está ejecutando Unified Manager.
2. Cambia la contraseña de umadmin:

   ```
   passwd umadmin
   ```

   El sistema te pide que introduzcas una nueva contraseña para el usuario umadmin.

Cambiar los puertos que utiliza Active IQ Unified Manager para los protocolos HTTP y HTTPS

Los puertos predeterminados que utiliza Unified Manager para los protocolos HTTP y HTTPS se pueden modificar tras la instalación si así lo requiere la seguridad. Los puertos predeterminados son el 80 para HTTP y el 443 para HTTPS.

Antes de empezar

Debes tener un ID de usuario y una contraseña autorizados para iniciar sesión en la consola de mantenimiento del servidor Unified Manager.

> Hay algunos puertos que se consideran inseguros cuando utilizas los navegadores Mozilla Firefox o Google Chrome. Compruébalo en tu navegador antes de asignar un nuevo número de puerto para el tráfico HTTP y HTTPS. Si seleccionas un puerto inseguro, es posible que no puedas acceder al sistema, por lo que tendrías que ponerte en contacto con el soporte al cliente para resolver el problema.

La instancia de Unified Manager se reinicia automáticamente tras cambiar el puerto, así que asegúrate de que sea un buen momento para dejar el sistema fuera de servicio durante un breve periodo de tiempo.

1. Inicia sesión mediante SSH como usuario de mantenimiento en el host de Unified Manager.

   Aparecen las indicaciones de la consola de mantenimiento de Unified Manager.

2. Escribe el número de la opción del menú denominada **Ver/Modificar puertos de la aplicación** y, a continuación, pulsa Intro.
3. Si se te solicita, introduce de nuevo la contraseña del usuario de mantenimiento.
4. Escribe los nuevos números de puerto para los puertos HTTP y HTTPS y, a continuación, pulsa Intro.

   Si dejas en blanco un número de puerto, se asigna el puerto predeterminado para el protocolo.

   Se te pregunta si quieres cambiar los puertos y reiniciar Unified Manager ahora.

5. Escribe **y** para cambiar los puertos y reiniciar Unified Manager.
6. Sal de la consola de mantenimiento.

Tras este cambio, los usuarios deben incluir el nuevo número de puerto en la URL para acceder a la interfaz de usuario web de Unified Manager, por ejemplo: https://host.company.com:1234, https://12.13.14.15:1122 o https://[2001:db8:0:1]:2123.

Agrega interfaces de red a Active IQ Unified Manager

Puedes añadir nuevas interfaces de red si necesitas separar el tráfico de red.

Antes de empezar

Debes haber añadido la interfaz de red al dispositivo virtual mediante vSphere.

El dispositivo virtual debe estar encendido.

> No es posible realizar esta operación si Unified Manager está instalado en Red Hat Enterprise Linux o en Microsoft Windows.

Pasos

1. En el menú principal de la consola de vSphere, selecciona **Configuración del sistema** > **Reiniciar el sistema operativo**.

   Tras reiniciar el sistema, la consola de mantenimiento puede detectar la interfaz de red recién añadida.

2. Accede a la consola de mantenimiento.
3. Selecciona **Configuración de red** > **Habilitar interfaz de red**.
4. Selecciona la nueva interfaz de red y pulsa **Enter**.

   Selecciona **eth1** y pulsa **Enter**.

5. Escribe **y** para activar la interfaz de red.
6. Introduce la configuración de red.

   Se te pedirá que introduzcas la configuración de red si utilizas una interfaz estática o si no se detecta DHCP.

   Después de introducir la configuración de red, volverás automáticamente al menú **Configuración de red**.

7. Selecciona **Commit Changes**.

   Debes confirmar los cambios para añadir la interfaz de red.

Regenerar el certificado de cliente en Active IQ Unified Manager

Puedes usar la consola de mantenimiento para volver a generar tu certificado de cliente de Unified Manager. Tu certificado tiene un periodo de validez ampliado de cinco años.

Pasos

1. Inicia sesión como usuario de mantenimiento.
2. Selecciona **Regenerate Client Certificate** y pulsa **Enter**.
3. Si el sistema te solicita que te autentifiques, introduce las credenciales necesarias.
4. Selecciona **Confirm Regeneration** y pulsa **Enter**.
5. Una vez regenerado el certificado, reinicia el servicio Unified Manager para aplicar los cambios.
6. Para comprobar el certificado actualizado, inicia sesión en ONTAP. Consulta el estado del certificado de cliente y su validez.

Información relacionada "Gestiona los certificados de ONTAP con System Manager"

Añade espacio en disco

Agrega espacio en disco al directorio de la base de datos de Active IQ Unified Manager

El directorio de la base de datos de Unified Manager contiene todos los datos de estado y rendimiento recopilados de los sistemas ONTAP. En determinadas circunstancias, puede que necesites aumentar el tamaño del directorio de la base de datos.

Por ejemplo, el directorio de la base de datos puede llenarse si Unified Manager está recopilando datos de un gran número de clústeres en los que cada uno cuenta con muchos nodos. Recibirás un evento de advertencia cuando el directorio de la base de datos esté lleno al 90 %, y un evento crítico cuando esté lleno al 95 %.

No se recopilan más datos de los clústeres cuando el directorio alcanza el 95 % de su capacidad.

Los pasos necesarios para ampliar la capacidad del directorio de datos varían en función de si Unified Manager se ejecuta en un servidor VMware ESXi, en un servidor Red Hat o en un servidor Microsoft Windows.

Aumenta el espacio del directorio de datos en un host Linux en Active IQ Unified Manager

Si al configurar inicialmente el host Linux no asignaste suficiente espacio en disco al directorio `/opt/netapp/data` para admitir Unified Manager y posteriormente instalaste Unified Manager, puedes añadir espacio en disco tras la instalación aumentando el espacio disponible en el directorio `/opt/netapp/data`.

Antes de empezar

Debes tener acceso de usuario raíz al equipo con Red Hat Enterprise Linux en el que está instalado Unified Manager.

Te recomendamos que realices una copia de seguridad de la base de datos de Unified Manager antes de aumentar el tamaño del directorio de datos.

Pasos

1. Inicia sesión como usuario raíz en el equipo Linux al que quieras añadir espacio en disco.
2. Detén el servicio de Unified Manager y el software MySQL asociado en el orden indicado:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Crea una carpeta de copia de seguridad temporal (por ejemplo, `/backup-data`) con espacio en disco suficiente para albergar los datos del actual `/opt/netapp/data` directorio.
4. Copia el contenido y la configuración de privilegios del directorio existente `/opt/netapp/data` al directorio de datos de copia de seguridad:

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. Si SE Linux está activado:

   a. Obtén el tipo de SE Linux de las carpetas de la carpeta existente `/opt/netapp/data`:

```
se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
head -1
```

El sistema muestra un mensaje de confirmación similar al siguiente:

```
echo $se_type
mysqld_db_t
```

a. Ejecuta el comando chcon para configurar el tipo de SE Linux del directorio de copia de seguridad:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Elimina el contenido del directorio `/opt/netapp/data`:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Aumenta el tamaño del directorio `/opt/netapp/data` hasta un mínimo de 150 GB mediante comandos LVM o añadiendo discos adicionales.

> Si has creado `/opt/netapp/data` a partir de un disco, no debes intentar montar `/opt/netapp/data` como un recurso compartido de NFS o CIFS. Esto se debe a que, en este caso, si intentas ampliar el espacio en disco, es posible que algunos comandos de LVM, como `resize` y `extend`, no funcionen como se espera.

8. Comprueba que el propietario `/opt/netapp/data` del directorio (mysql) y el grupo (root) no hayan cambiado:

```
ls -ltr /opt/netapp/ | grep data
```

El sistema muestra un mensaje de confirmación similar al siguiente:

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. Si SE Linux está activado, comprueba que el contexto del `/opt/netapp/data` directorio siga configurado como mysqld_db_t:
   a. `touch /opt/netapp/data/abc`
   b. `ls -Z /opt/netapp/data/abc`

El sistema muestra un mensaje de confirmación similar al siguiente:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Elimina el archivo abc para que este archivo superfluo no provoque un error en la base de datos en el futuro.

11. Copia el contenido de backup-data de nuevo en el directorio `/opt/netapp/data` ampliado:

    ```
    cp -arp /backup-data/* /opt/netapp/data/
    ```

12. Si SE Linux está activado, ejecuta el siguiente comando:

    ```
    chcon -R --type=mysqld_db_t /opt/netapp/data
    ```

13. Inicia el servicio MySQL:

    ```
    systemctl start mysqld
    ```

14. Una vez iniciado el servicio MySQL, inicia los servicios ocie y ocieau en el orden indicado:

    ```
    systemctl start ocie ocieau
    ```

15. Una vez iniciados todos los servicios, elimina la carpeta de copia de seguridad `/backup-data`:

    ```
    rm -rf /backup-data
    ```

Agrega espacio al disco de datos en una máquina virtual de VMware en Active IQ Unified Manager

Si necesitas aumentar la cantidad de espacio en el disco de datos para la base de datos de Unified Manager, puedes agregar capacidad después de la instalación aumentando el espacio en disco mediante la consola de mantenimiento de Unified Manager.

Antes de empezar

- Debes tener acceso a vSphere Client.
- La máquina virtual no debe tener ninguna instantánea almacenada localmente.
- Debes disponer de las credenciales de usuario de mantenimiento.

Te recomendamos que hagas una copia de seguridad de tu máquina virtual antes de aumentar el tamaño de los discos virtuales.

Pasos

1. En el cliente de vSphere, selecciona la máquina virtual de Unified Manager y, a continuación, añade más capacidad de disco al disco de datos `disk 3`. Consulta la documentación de VMware para obtener más detalles.

   En algunos casos raros, la implementación de Unified Manager utiliza “Hard Disk 2” para el disco de datos en lugar de “Hard Disk 3”. Si esto ha ocurrido en tu implementación, aumenta el espacio del disco que sea más grande. El disco de datos siempre tendrá más espacio que el otro disco.

2. En el cliente de vSphere, selecciona la máquina virtual de Unified Manager y, a continuación, selecciona la pestaña **NetApp Console**.
3. Haz clic en la ventana de la consola y, a continuación, inicia sesión en la consola de mantenimiento con tu nombre de usuario y contraseña.
4. En el menú principal, introduce el número correspondiente a la opción **Configuración del sistema**.
5. En el menú de configuración del sistema, introduce el número correspondiente a la opción **Aumentar el tamaño del disco de datos**.

Agrega espacio a la unidad lógica en un servidor Windows en Active IQ Unified Manager

Si necesitas aumentar el espacio en disco de la base de datos de Unified Manager, puedes ampliar la capacidad de la unidad lógica en la que está instalado Unified Manager.

Antes de empezar

Debes tener privilegios de administrador de Windows.

Te recomendamos que hagas una copia de seguridad de la base de datos de Unified Manager antes de ampliar el espacio en disco.

Pasos

1. Inicia sesión como administrador en el servidor Windows al que quieras añadir espacio en disco.
2. Sigue el paso que corresponda al método que quieras utilizar para añadir más espacio:

Opción	Descripción
En un servidor físico, añade capacidad a la unidad lógica en la que está instalado el servidor de Unified Manager.	Sigue los pasos del tema de Microsoft: "Ampliar un volumen básico"
En un servidor físico, añade un disco duro.	Sigue los pasos del tema de Microsoft: "Añadir unidades de disco duro"
En una máquina virtual, aumenta el tamaño de una partición de disco.	Sigue los pasos que se indican en el tema de VMware: "Aumentar el tamaño de una partición de disco"

Gestionar el acceso de los usuarios

Agregar usuarios

Agregar usuarios en Active IQ Unified Manager

Puedes añadir usuarios locales o usuarios de bases de datos a través de la página «Usuarios». También puedes añadir usuarios remotos o grupos que pertenezcan a un servidor de autenticación. Puedes asignar roles a estos usuarios y, en función de los privilegios de dichos roles, los usuarios podrán gestionar los objetos de almacenamiento y los datos con Unified Manager, o bien consultar los datos en una base de datos.

Antes de empezar

- Debes tener el rol de Application Administrator.
- Para añadir un usuario o grupo remoto, debes haber habilitado la autenticación remota y haber configurado tu servidor de autenticación.
- Si tienes previsto configurar la autenticación SAML para que un proveedor de identidad (IdP) autentique a los usuarios que acceden a la interfaz gráfica, asegúrate de que esos usuarios estén definidos como usuarios “remote”.

Los usuarios de tipo “local” o “maintenance” no pueden acceder a la UI cuando la autenticación SAML está habilitada.

Si añades un grupo desde Windows Active Directory, todos los miembros directos y los subgrupos anidados pueden autenticarse en Unified Manager, a menos que se desactiven los subgrupos anidados. Si añades un grupo desde OpenLDAP u otros servicios de autenticación, solo los miembros directos de ese grupo pueden autenticarse en Unified Manager.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Users**.
2. En la página «Usuarios», haz clic en **Add**.
3. En el cuadro de diálogo Add User, selecciona el tipo de usuario que quieres añadir e introduce la información necesaria.

   Al introducir la información de usuario necesaria, debes indicar una dirección de correo electrónico que sea exclusiva de ese usuario. Debes evitar indicar direcciones de correo electrónico que usen varios usuarios.

4. Haz clic en **Add**.

Crear un usuario de base de datos en Active IQ Unified Manager

Para permitir una conexión entre Workflow Automation y Unified Manager, o para acceder a las vistas de la base de datos, primero debes crear un usuario de base de datos con el rol Integration Schema o Report Schema en la interfaz de usuario web de Unified Manager.

Antes de empezar

Debes tener el rol de Application Administrator.

Los usuarios de la base de datos proporcionan integración con Workflow Automation y acceso a vistas de base de datos específicas para informes. Los usuarios de la base de datos no tienen acceso a la interfaz de usuario web de Unified Manager ni a la consola de mantenimiento, y no pueden ejecutar llamadas API.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Users**.
2. En la página «Users», haz clic en **Add**.
3. En el cuadro de diálogo Add User, selecciona **Database User** en la lista desplegable **Type**.
4. Escribe un nombre y una contraseña para el usuario de la base de datos.
5. En la lista desplegable **Función**, selecciona la función adecuada.

Si eres…	Elige este rol
Conexión de Unified Manager con Workflow Automation	Esquema de integración
Acceso a informes y otras vistas de la base de datos	Esquema del informe

6. Haz clic en **Add**.

Editar la configuración de usuario en Active IQ Unified Manager

Puedes modificar la configuración de usuario --como la dirección de correo electrónico y el rol-- que se especifica para cada usuario. Por ejemplo, puede que quieras cambiar el rol de un usuario que sea operador de almacenamiento y asignarle privilegios de administrador de almacenamiento.

Antes de empezar

Debes tener el rol de Application Administrator.

Cuando modificas el rol asignado a un usuario, los cambios se aplican cuando ocurre cualquiera de las siguientes acciones:

- Cierras sesión y vuelves a iniciar sesión en Unified Manager.
- Se alcanzó el tiempo de espera de la sesión de 24 horas.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Users**.
2. En la página «Usuarios», selecciona el usuario cuya configuración quieras editar y haz clic en **Editar**.
3. En el cuadro de diálogo «Editar usuario», modifica la configuración adecuada especificada para el usuario.
4. Haz clic en **Guardar**.

Ver usuarios en Active IQ Unified Manager

Puedes usar la página «Usuarios» para ver la lista de usuarios que gestionan objetos de almacenamiento y datos con Unified Manager. Puedes ver detalles sobre los usuarios, como el nombre de usuario, el tipo de usuario, la dirección de correo electrónico y el rol que se les ha asignado.

Antes de empezar

Debes tener el rol de Application Administrator.

Paso

1. En el panel de navegación de la izquierda, haz clic en **General** > **Users**.

Eliminar usuarios o grupos en Active IQ Unified Manager

Puedes eliminar uno o varios usuarios de la base de datos del servidor de gestión para impedir que determinados usuarios accedan a Unified Manager. También puedes eliminar grupos para que ninguno de los usuarios que los componen pueda volver a acceder al servidor de gestión.

Antes de empezar

- Al eliminar grupos remotos, debes haber reasignado los eventos que están asignados a los usuarios de dichos grupos.

  Si eliminas usuarios locales o remotos, los eventos asignados a dichos usuarios se desasignan automáticamente.

- Debes tener el rol de Application Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Users**.
2. En la página «Usuarios», selecciona los usuarios o grupos que quieras eliminar y, a continuación, haz clic en **Eliminar**.
3. Haz clic en **Sí** para confirmar la eliminación.

Infórmate sobre el control de acceso basado en roles en Active IQ Unified Manager

El RBAC (control de acceso basado en roles) permite controlar quién tiene acceso a las distintas funciones y recursos del servidor Active IQ Unified Manager. El RBAC permite a los administradores gestionar grupos de usuarios mediante la definición de roles. Si necesitas restringir el acceso a determinadas funciones a administradores concretos, debes configurar cuentas de administrador para ellos. Si quieres restringir la información que los administradores pueden ver y las operaciones que pueden realizar, debes asignar roles a las cuentas de administrador que crees.

El servidor de gestión utiliza RBAC para el inicio de sesión de usuarios y los permisos de roles. Si no has modificado la configuración predeterminada del servidor de gestión para el acceso de los usuarios administrativos, no es necesario que inicies sesión para verlos.

Cuando inicias una operación que requiere privilegios específicos, el servidor de gestión te solicita que inicies sesión. Por ejemplo, para crear cuentas de administrador, debes iniciar sesión con acceso a la cuenta Application Administrator.

Conoce los tipos de usuario en Active IQ Unified Manager

Un tipo de usuario especifica el tipo de cuenta que tiene el usuario e incluye usuarios remotos, grupos remotos, usuarios locales, usuarios de bases de datos y usuarios de mantenimiento. Cada uno de estos tipos tiene su propio rol, que asigna un usuario con el rol de Administrator.

Los tipos de usuario de Unified Manager son los siguientes:

- **Usuario de mantenimiento**

  Se crea durante la configuración inicial de Unified Manager. A continuación, el usuario de mantenimiento crea usuarios adicionales y les asigna roles. El usuario de mantenimiento también es el único usuario con acceso a la consola de mantenimiento. Cuando Unified Manager se instala en un sistema Red Hat Enterprise Linux, al usuario de mantenimiento se le asigna el nombre de usuario «`umadmin.`».

- **Usuario local**

  Accedes a la interfaz de usuario de Unified Manager y realizas funciones en función del rol que te haya asignado el usuario de mantenimiento o un usuario con el rol de Application Administrator.

- **Grupo remoto**

  Un grupo de usuarios que acceden a la UI de Unified Manager mediante las credenciales almacenadas en el servidor de autenticación. El nombre de esta cuenta debe coincidir con el nombre de un grupo

almacenado en el servidor de autenticación. Todos los usuarios del grupo remoto tienen acceso a la UI de Unified Manager mediante sus credenciales de usuario individuales. Los grupos remotos pueden realizar funciones según los roles asignados.

- **Usuario remoto**

  Accede a la interfaz de usuario de Unified Manager con las credenciales almacenadas en el servidor de autenticación. Un usuario remoto realiza funciones según el rol que le haya asignado el usuario de mantenimiento o un usuario con el rol de Application Administrator.

- **Usuario de la base de datos**

  Tiene acceso de solo lectura a los datos de la base de datos de Unified Manager, no tiene acceso a la interfaz web de Unified Manager ni a la consola de mantenimiento, y no puede ejecutar llamadas a la API.

Conoce los roles de usuario en Active IQ Unified Manager

El usuario de mantenimiento o Application Administrator asigna un rol a cada usuario. Cada rol contiene determinados privilegios. El alcance de las actividades que puedes realizar en Unified Manager depende del rol que se te haya asignado y de los privilegios que este contenga.

Unified Manager incluye los siguientes roles de usuario predefinidos:

- **Operador**

  Muestra información del sistema de almacenamiento y otros datos recopilados por Unified Manager, incluidos historiales y tendencias de capacidad. Este rol permite al operador de almacenamiento ver, asignar, reconocer, resolver y añadir notas a los eventos.

- **Administrador de almacenamiento**

  Configura las operaciones de gestión del almacenamiento en Unified Manager. Esta función permite al administrador de almacenamiento configurar umbrales, crear alertas y establecer otras opciones y políticas específicas de la gestión del almacenamiento.

- **Administrador de aplicaciones**

  Configura los parámetros no relacionados con la gestión del almacenamiento. Este rol permite gestionar usuarios, certificados de seguridad, el acceso a bases de datos y opciones administrativas, entre las que se incluyen la autenticación, el SMTP, las redes y AutoSupport.

  > Al instalar Unified Manager en sistemas Linux, el usuario inicial con el rol Application Administrator se llama automáticamente “umadmin”.

- **Esquema de integración**

  Esta función permite el acceso de solo lectura a las vistas de la base de datos de Unified Manager para integrar Unified Manager con OnCommand Workflow Automation (WFA).

- **Esquema del informe**

  Este rol permite el acceso de solo lectura a los informes y a otras vistas de la base de datos directamente desde la base de datos de Unified Manager. Las bases de datos que se pueden ver incluyen:

- netapp_model_view
- netapp_performance
- ocum
- ocum_report
- ocum_report_birt
- opm
- scalemonitor

Infórmate sobre los roles y las funciones de los usuarios en Active IQ Unified Manager

En función del rol de usuario que se te haya asignado, podrás determinar qué operaciones puedes realizar en Unified Manager.

La siguiente tabla muestra las funciones que puede realizar cada rol de usuario:

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema del informe
Ver información del sistema de almacenamiento	•	•	•	•	•
Ver otros datos, como historiales y tendencias de capacidad	•	•	•	•	•
Ver, asignar y resolver eventos	•	•	•		
Ver objetos del servicio de almacenamiento, como asociaciones SVM y pools de recursos	•	•	•		
Ver las políticas de umbral	•	•	•		
Gestiona objetos del servicio de almacenamiento, como asociaciones de SVM y grupos de recursos		•	•		
Definir alertas		•	•		

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema del informe
Gestiona las opciones de gestión del almacenamiento		•	•		
Gestionar las políticas de gestión del almacenamiento		•	•		
Gestiona usuarios			•		
Gestionar opciones administrativas			•		
Definir políticas de umbral			•		
Gestiona el acceso a la base de datos			•		
Gestionar la integración con WFA y facilitar el acceso a las vistas de la base de datos				•	
Programar y guardar informes		•	•		
Ejecuta operaciones “Fix It” desde "Management Actions"		•	•		
Conceder acceso de solo lectura a las vistas de la base de datos					•

Gestiona la configuración de la autenticación SAML

Habilita la autenticación SAML en Active IQ Unified Manager

Después de configurar los ajustes de autenticación remota, puedes habilitar la autenticación mediante el Lenguaje de Marcado para Confirmaciones de Seguridad

(SAML) para que un proveedor de identidades (IdP) seguro autentique a los usuarios remotos antes de que puedan acceder a la interfaz de usuario web de Unified Manager.

Ten en cuenta que, una vez habilitada la autenticación SAML, solo los usuarios remotos tendrán acceso a la interfaz de usuario gráfica de Unified Manager. Los usuarios locales y los usuarios de mantenimiento no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento.

Usa un proveedor de identidad en Active IQ Unified Manager

Al configurar Unified Manager para que utilice un proveedor de identidad (IdP) con el fin de realizar la autenticación SAML para todos los usuarios remotos, es necesario tener en cuenta algunos ajustes de configuración obligatorios para que la conexión con Unified Manager funcione correctamente.

Debes introducir el URI y los metadatos de Unified Manager en el servidor IdP. Puedes copiar esta información de la página Unified ManagerSAML Authentication. Unified Manager se considera el proveedor de servicios (SP) en el estándar Security Assertion Markup Language (SAML).

Estándares de cifrado compatibles

- Estándar de cifrado avanzado (AES): AES-128 y AES-256
- Algoritmo de hash seguro (SHA): SHA-1 y SHA-256

Proveedores de identidad validados

- Shibboleth
- Servicios de federación de Active Directory (ADFS)

Requisitos de configuración de ADFS

- Debes definir tres reglas de notificación en el siguiente orden, que son necesarias para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de usuario autenticado.

Regla de reclamación	Valor
SAM-account-name	ID de nombre
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Grupos de tokens — nombre no calificado	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Debes establecer el método de autenticación en “Forms Authentication” o los usuarios podrían recibir un error al cerrar sesión en Unified Manager. Sigue estos pasos:
  a. Abre la consola de administración de ADFS.
  b. Haz clic en la carpeta «Políticas de autenticación» en la vista de árbol de la izquierda.
  c. En Acciones, a la derecha, haz clic en Edit Global Primary Authentication Policy.
  d. Configura el método de autenticación de la intranet como «`Forms Authentication`» en lugar de la opción predeterminada «`Windows Authentication`».
- En algunos casos, el inicio de sesión a través del IdP se rechaza cuando el certificado de seguridad de

Unified Manager está firmado por una autoridad de certificación (CA). Existen dos soluciones provisionales para resolver este problema:

- Sigue las instrucciones que figuran en el enlace para desactivar la comprobación de revocación en el servidor ADFS para la parte de confianza asociada al certificado de CA encadenado:

  "Desactivar la comprobación de revocación por Relying Party Trust"

- Aloja el servidor CA en el servidor ADFS para firmar la solicitud de certificado del servidor Unified Manager.

Otros requisitos de configuración

- La desviación horaria de Unified Manager está configurada en 5 minutos, por lo que la diferencia horaria entre el servidor IdP y el servidor Unified Manager no puede ser superior a 5 minutos; de lo contrario, la autenticación fallará.

Habilita la autenticación SAML en Active IQ Unified Manager

Puedes habilitar la autenticación mediante Security Assertion Markup Language (SAML) para que un proveedor de identidad (IdP) seguro autentique a los usuarios remotos antes de que puedan acceder a la interfaz de usuario web de Unified Manager.

Antes de empezar

- Debes haber configurado la autenticación remota y haber comprobado que funciona correctamente.
- Debes haber creado al menos un Usuario remoto o un Grupo remoto con el rol de administrador de aplicaciones.
- El proveedor de identidad (IdP) debe ser compatible con Unified Manager y debe estar configurado.
- Debes disponer de la URL del IdP y de los metadatos.
- Debes tener acceso al servidor IdP.

Después de habilitar la autenticación SAML desde Unified Manager, los usuarios no podrán acceder a la interfaz de usuario gráfica hasta que configures el IdP con la información del host del servidor de Unified Manager. Por lo tanto, debes tener todo listo para completar ambas partes de la conexión antes de iniciar el proceso de configuración. Puedes configurar el IdP antes o después de configurar Unified Manager.

Solo los usuarios remotos tendrán acceso a la interfaz gráfica de usuario de Unified Manager una vez que se haya habilitado la autenticación SAML. Los usuarios locales y los usuarios de Maintenance no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento, a los comandos de Unified Manager ni a las ZAPIs.



Unified Manager se reinicia automáticamente después de que completes la configuración de SAML en esta página.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **SAML Authentication**.
2. Marca la casilla **Enable SAML authentication**.

   Se muestran los campos necesarios para configurar la conexión con el IdP.

3. Introduce la URI del IdP y los metadatos del IdP necesarios para conectar el servidor de Unified Manager

al servidor del IdP.

Si puedes acceder al servidor IdP directamente desde el servidor Unified Manager, puedes hacer clic en el botón **Obtener metadatos del IdP** después de introducir la URI del IdP para que el campo «Metadatos del IdP» se complete automáticamente.

4. Copia el URI de los metadatos del host de Unified Manager o guarda los metadatos del host en un archivo de texto XML.

   Ya puedes configurar el servidor IdP con esta información.

5. Haz clic en **Guardar**.

   Aparece un cuadro de diálogo para confirmar que deseas completar la configuración y reiniciar Unified Manager.

6. Haz clic en **Confirm and Logout** y Unified Manager se reinicia.

La próxima vez que los usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager introducirán sus credenciales en la página de inicio de sesión del IdP en lugar de en la página de inicio de sesión de Unified Manager.

Si aún no lo has hecho, accede a tu IdP e introduce el URI del servidor de Unified Manager y los metadatos para completar la configuración.

> Cuando usas ADFS como proveedor de identidad, la GUI de Unified Manager no respeta el tiempo de espera de ADFS y seguirá funcionando hasta que se alcance el tiempo de espera de la sesión de Unified Manager. Puedes cambiar el tiempo de espera de la sesión de la GUI haciendo clic en **General** > **Feature Settings** > **Inactivity Timeout**.

Cambiar el proveedor de identidad de autenticación SAML en Active IQ Unified Manager

Puedes cambiar el proveedor de identidad (IdP) que utiliza Unified Manager para autenticar a los usuarios remotos.

Antes de empezar

- Debes disponer de la URL del IdP y de los metadatos.
- Debes tener acceso al IdP.

Puedes configurar el nuevo IdP antes o después de configurar Unified Manager.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **SAML Authentication**.
2. Introduce la nueva URI de IdP y los metadatos de IdP necesarios para conectar el servidor de Unified Manager al IdP.

   Si se puede acceder al IdP directamente desde el servidor de Unified Manager, puedes hacer clic en el botón **Obtener metadatos del IdP** después de introducir la URL del IdP para que el campo «Metadatos del IdP» se rellene automáticamente.

3. Copia el URI de metadatos de Unified Manager o guarda los metadatos en un archivo de texto XML.

4. Haz clic en **Guardar configuración**.

   Aparece un cuadro de diálogo para confirmar que deseas cambiar la configuración.

5. Haz clic en **OK**.

Accede al nuevo IdP e introduce la URI del servidor de Unified Manager y los metadatos para completar la configuración.

La próxima vez que los usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager, introducirán sus credenciales en la nueva página de inicio de sesión del IdP en lugar de en la antigua página de inicio de sesión del IdP.

Actualiza la configuración de autenticación SAML después de un cambio en el certificado de seguridad de Active IQ Unified Manager

Cualquier cambio en el certificado de seguridad HTTPS instalado en el servidor de Unified Manager requiere que actualices la configuración de autenticación SAML. El certificado se actualiza si cambias el nombre del sistema host, asignas una nueva dirección IP al sistema host o modificas manualmente el certificado de seguridad del sistema.

Una vez cambiado el certificado de seguridad y reiniciado el servidor de Unified Manager, la autenticación SAML dejará de funcionar y los usuarios no podrán acceder a la interfaz gráfica de Unified Manager. Debes actualizar la configuración de autenticación SAML tanto en el servidor IdP como en el servidor de Unified Manager para volver a habilitar el acceso a la interfaz de usuario.

Pasos

1. Inicia sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduce el número correspondiente a la opción **Desactivar la autenticación SAML**.

   Aparece un mensaje para confirmar que deseas desactivar la autenticación SAML y reiniciar Unified Manager.

3. Inicia la interfaz de usuario de Unified Manager con el FQDN o la dirección IP actualizados, acepta el certificado del servidor actualizado en tu navegador e inicia sesión con las credenciales del usuario de mantenimiento.
4. En la página **Configuración/Autenticación**, selecciona la pestaña **Autenticación SAML** y configura la conexión con el IdP.
5. Copia el URI de los metadatos del host de Unified Manager o guarda los metadatos del host en un archivo de texto XML.
6. Haz clic en **Guardar**.

   Aparece un cuadro de diálogo para confirmar que deseas completar la configuración y reiniciar Unified Manager.

7. Haz clic en **Confirm and Logout** y Unified Manager se reinicia.
8. Accede a tu servidor IdP e introduce el URI y los metadatos del servidor de Unified Manager para completar la configuración.

Proveedor de identidad	Pasos de configuración
ADFS	a. Elimina la entrada de confianza de usuario autenticado existente en la GUI de administración de ADFS. b. Añade una nueva entrada de confianza de parte dependiente utilizando el `saml_sp_metadata.xml` del servidor Unified Manager actualizado. c. Define las tres reglas de reclamaciones necesarias para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de la parte dependiente. d. Reinicia el servicio ADFS de Windows.
Shibboleth	a. Actualiza el nuevo FQDN del servidor Unified Manager en los archivos `attribute-filter.xml` y `relying-party.xml`. b. Reinicia el servidor web Apache Tomcat y espera a que el puerto 8005 esté en línea.

9. Inicia sesión en Unified Manager y comprueba que la autenticación SAML funciona correctamente a través de tu proveedor de identidad (IdP).

Desactivar la autenticación SAML en Active IQ Unified Manager

Puedes desactivar la autenticación SAML cuando desees dejar de autenticar a los usuarios remotos a través de un proveedor de identidad (IdP) seguro antes de que puedan iniciar sesión en la interfaz de usuario web de Unified Manager. Cuando la autenticación SAML está desactivada, los proveedores de servicios de directorio configurados, como Active Directory o LDAP, realizan la autenticación de inicio de sesión.

Una vez que desactives la autenticación SAML, los usuarios locales y los usuarios de mantenimiento podrán acceder a la interfaz gráfica de usuario, además de los usuarios remotos configurados.

También puedes desactivar la autenticación SAML mediante la consola de mantenimiento de Unified Manager si no tienes acceso a la interfaz gráfica de usuario.

Unified Manager se reinicia automáticamente tras desactivar la autenticación SAML.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **SAML Authentication**.
2. Desmarca la casilla **Habilitar autenticación SAML**.
3. Haz clic en **Guardar**.

   Aparece un cuadro de diálogo para confirmar que deseas completar la configuración y reiniciar Unified Manager.

4. Haz clic en **Confirm and Logout** y Unified Manager se reinicia.

La próxima vez que los usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, introducirán sus credenciales en la página de inicio de sesión de Unified Manager en lugar de en la página de inicio de sesión del IdP.

Accede a tu IdP y elimina el URI y los metadatos del servidor de Unified Manager.

Desactivar la autenticación SAML desde la consola de mantenimiento de Active IQ Unified Manager

Es posible que tengas que desactivar la autenticación SAML desde la consola de mantenimiento cuando no haya acceso a la GUI de Unified Manager. Esto podría ocurrir en casos de configuración incorrecta o si no se puede acceder al IdP.

Antes de empezar

Debes tener acceso a la consola de mantenimiento como el usuario de mantenimiento.

Cuando la autenticación SAML está desactivada, los proveedores de servicios de directorio configurados, como Active Directory o LDAP, realizan la autenticación de inicio de sesión. Los usuarios locales y los usuarios de mantenimiento podrán acceder a la interfaz gráfica de usuario, además de los usuarios remotos configurados.

También puedes desactivar la autenticación SAML desde la página Setup/Authentication de la interfaz de usuario.

Unified Manager se reinicia automáticamente tras desactivar la autenticación SAML.

Pasos

1. Inicia sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduce el número correspondiente a la opción **Desactivar la autenticación SAML**.

   Aparece un mensaje para confirmar que deseas desactivar la autenticación SAML y reiniciar Unified Manager.

3. Escribe **y** y, a continuación, pulsa Enter y Unified Manager se reinicia.

La próxima vez que los usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, introducirán sus credenciales en la página de inicio de sesión de Unified Manager en lugar de en la página de inicio de sesión del IdP.

Si es necesario, accede a tu IdP y elimina la URL del servidor de Unified Manager y los metadatos.

Utiliza la página de autenticación SAML en Active IQ Unified Manager

Puedes usar la página «Autenticación SAML» para configurar Unified Manager para que autentique a los usuarios remotos mediante SAML a través de un proveedor de identidad (IdP) seguro antes de que puedan iniciar sesión en la interfaz web de Unified Manager.

- Debes tener el rol Application Administrator para crear o modificar la configuración de SAML.
- Debes haber configurado la autenticación remota.

- Debes haber configurado al menos un usuario remoto o un grupo remoto.

Después de configurar la autenticación remota y los usuarios remotos, puedes marcar la casilla «Enable SAML authentication» para habilitar la autenticación mediante un proveedor de identidad seguro.

- **URI del IdP**

  El URI para acceder al IdP desde el servidor de Unified Manager. A continuación se enumeran algunos ejemplos de URI.

  URI de ejemplo de ADFS:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  URI de ejemplo de Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Metadatos del IdP**

  Los metadatos del IdP en formato XML.

  Si se puede acceder a la URL del IdP desde el servidor de Unified Manager, puedes hacer clic en el botón **Obtener metadatos del IdP** para rellenar este campo.

- **Sistema host (FQDN)**

  El nombre de dominio completo (FQDN) del sistema host de Unified Manager, tal y como se definió durante la instalación. Puede modificar este valor si es necesario.

- **URI del host**

  El URI para acceder al sistema host de Unified Manager desde el IdP.

- **Metadatos del host**

  Los metadatos del sistema host en formato XML.

Gestionar la autenticación

Editar servidores de autenticación en Active IQ Unified Manager

Puedes cambiar el puerto que utiliza el servidor de Unified Manager para comunicarse con tu servidor de autenticación.

Antes de empezar

Debes tener el rol de Application Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Remote Authentication**.
2. Marca la casilla **Disable Nested Group Lookup**.

3. En la sección **Servidores de autenticación**, selecciona el servidor de autenticación que quieras editar y, a continuación, haz clic en **Editar**.
4. En el cuadro de diálogo **Editar servidor de autenticación**, modifica los detalles del puerto.
5. Haz clic en **Guardar**.

Eliminar servidores de autenticación en Active IQ Unified Manager

Puedes eliminar un servidor de autenticación si deseas impedir que el servidor Unified Manager se comunique con dicho servidor. Por ejemplo, si deseas cambiar el servidor de autenticación con el que se comunica el servidor de gestión, puedes eliminar el servidor de autenticación y añadir uno nuevo.

Antes de empezar

Debes tener el rol de Application Administrator.

Al eliminar un servidor de autenticación, los usuarios remotos o los grupos del servidor de autenticación ya no podrán acceder a Unified Manager.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Remote Authentication**.
2. Selecciona uno o varios servidores de autenticación que quieras eliminar y, a continuación, haz clic en **Eliminar**.
3. Haz clic en **Sí** para confirmar la solicitud de eliminación.

   Si la opción **Usar conexión segura** está activada, los certificados asociados al servidor de autenticación se eliminan junto con el propio servidor de autenticación.

Autentícate con Active Directory u OpenLDAP en Active IQ Unified Manager

Puedes habilitar la autenticación remota en el servidor de gestión y configurarlo para que se comunique con tus servidores de autenticación, de modo que los usuarios de los servidores de autenticación puedan acceder a Unified Manager.

Puedes utilizar uno de los siguientes servicios de autenticación predefinidos o especificar tu propio servicio de autenticación:

- Microsoft Active Directory

  No puedes utilizar Microsoft Lightweight Directory Services.

- OpenLDAP

Puedes seleccionar el servicio de autenticación necesario y añadir los servidores de autenticación adecuados para permitir que los usuarios remotos del servidor de autenticación accedan a Unified Manager. El servidor de autenticación mantiene las credenciales de los usuarios o grupos remotos. El servidor de gestión utiliza el Protocolo Ligero de Acceso a Directorios (LDAP) para autenticar a los usuarios remotos en el servidor de autenticación configurado.

En el caso de los usuarios locales creados en Unified Manager, el servidor de gestión mantiene su propia base de datos de nombres de usuario y contraseñas. El servidor de gestión se encarga de la autenticación y

no utiliza Active Directory ni OpenLDAP para ello.

Registro de auditoría

Conoce los registros de auditoría en Active IQ Unified Manager

Puedes detectar si los registros de auditoría se han visto comprometidos con Audit Logs. Audit Logs supervisa y registra todas las actividades que realiza un usuario. Las auditorías se realizan para todas las funcionalidades de la interfaz de usuario y de las API expuestas públicamente de Active IQ Unified Manager.

Puedes usar **Audit Log: File View** para ver y acceder a todos los archivos de registro de auditoría disponibles en tu Active IQ Unified Manager. Los archivos de Audit Log: File View se muestran según su fecha de creación. Esta vista muestra información de todos los registros de auditoría capturados en el sistema desde la instalación o actualización hasta el presente. Cada vez que realizas una acción en Unified Manager, la información se actualiza y está disponible en los registros. El estado de cada archivo de registro se captura mediante el atributo “File Integrity Status”, que se supervisa activamente para detectar manipulaciones o la eliminación del archivo de registro. Los registros de auditoría pueden tener uno de los siguientes estados cuando están disponibles en el sistema:

Estado	Descripción
ACTIVO	Archivo en el que se registran actualmente los registros.
NORMAL	Archivo que está inactivo, comprimido y almacenado en el sistema.
MANIPULADO	Archivo que ha sido comprometido por un usuario que ha editado manualmente el archivo.
MANUAL_DELETE	Archivo que eliminó un usuario autorizado.
ROLLOVER_DELETE	Archivo que se eliminó debido a la rotación según la política de configuración de rotación.
UNEXPECTED_DELETE	Archivo que se borró por razones desconocidas.

La página «Registro de auditoría» incluye los siguientes botones de comando:

- Configura
- Borrar
- Descargar

El botón **DELETE** te permite eliminar cualquiera de los registros de auditoría que aparecen en la vista Audit Logs. Puedes eliminar un registro de auditoría y, si lo deseas, indicar un motivo para eliminar el archivo, lo que te ayudará en el futuro a determinar si la eliminación fue válida. La columna REASON muestra el motivo junto con el nombre del usuario que realizó la operación de eliminación.

Eliminar un archivo de registro hará que se elimine del sistema, pero la entrada correspondiente en la tabla de la base de datos no se eliminará.

Puedes descargar los registros de auditoría desde Active IQ Unified Manager con el botón **DOWNLOAD** en la sección Audit Logs y exportar los archivos de registro de auditoría. Los archivos marcados como «`NORMAL`» o «`TAMPERED`» se descargan en un formato comprimido `.gzip`.

Los archivos de registro de auditoría se archivan periódicamente y se guardan en la base de datos para su consulta. Antes del archivado, los registros de auditoría se firman digitalmente para garantizar su seguridad e integridad.

Cuando se genera un paquete completo de AutoSupport, el paquete de soporte incluye tanto los archivos de registro de auditoría archivados como los activos. Pero cuando se genera un paquete de soporte ligero, solo incluye los registros de auditoría activos. No se incluyen los registros de auditoría archivados.

Configura los registros de auditoría de Active IQ Unified Manager

Puedes usar el botón **Configure** en la sección Audit Logs para configurar la política de rotación de los archivos de registro de auditoría y también habilitar el registro remoto para los Audit Logs.

Puedes configurar los valores de **MAX FILE SIZE** y **AUDIT LOG RETENTION DAYS** según la cantidad y la frecuencia de los datos que quieras almacenar en el sistema. El valor del campo **TOTAL AUDIT LOG SIZE** es el tamaño total de los datos del registro de auditoría presentes en el sistema. La política de rotación está determinada por los valores de los campos **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** y **TOTAL AUDIT LOG SIZE**. Cuando el tamaño de la copia de seguridad del registro de auditoría alcanza el valor configurado en **TOTAL AUDIT LOG SIZE**, se elimina el archivo que se archivó primero. Esto significa que se elimina el archivo más antiguo. Pero la entrada del archivo sigue disponible en la base de datos y se marca como “Rollover Delete”. El valor de **AUDIT LOG RETENTION DAYS** corresponde al número de días durante los que se conservan los archivos del registro de auditoría. Cualquier archivo más antiguo que el valor establecido en este campo se rota.

Pasos

1. Haz clic en **Registros de auditoría** > > **Configurar**.
2. Introduce valores en **TAMAÑO MÁXIMO DEL ARCHIVO**, **TAMAÑO TOTAL DEL REGISTRO DE AUDITORÍA** y **DÍAS DE RETENCIÓN DEL REGISTRO DE AUDITORÍA**.

   Para activar el registro remoto, selecciona **Activar registro remoto**.

Habilita el registro remoto de los registros de auditoría en Active IQ Unified Manager

Puedes marcar la casilla **Enable Remote Logging** en el cuadro de diálogo «Configurar registros de auditoría» para habilitar el registro remoto de auditoría. Puedes usar esta función para transferir los registros de auditoría a un servidor remoto de Syslog. Esto te permitirá gestionar tus registros de auditoría cuando haya limitaciones de espacio.

El registro remoto de los registros de auditoría proporciona una copia de seguridad a prueba de manipulaciones en caso de que se manipulen los archivos de registros de auditoría del servidor Active IQ Unified Manager.

Pasos

1. En el cuadro de diálogo **Configurar registros de auditoría**, marca la casilla **Habilitar registro remoto**.

   Se muestran campos adicionales para configurar el registro remoto.

2. Introduce el **HOSTNAME** y el **PORT** del servidor remoto al que quieres conectarte.
3. En el campo **CERTIFICADO DE LA CA DEL SERVIDOR**, haz clic en **EXPLORAR** para seleccionar un certificado público del servidor de destino.

El certificado debe cargarse en formato `.pem`. Este certificado debe obtenerse del servidor Syslog de destino y no debe haber caducado. El certificado debe contener el “hostname” seleccionado como parte del atributo `SubjectAltName`(SAN).

4. Introduce los valores en los siguientes campos: **CHARSET**, **tiempo de espera de conexión**, **retraso de reconexión**.

   Los valores de estos campos deben expresarse en milisegundos.

5. Selecciona el formato Syslog y la versión de protocolo TLS que necesites en los campos **FORMATO** y **PROTOCOLO**.
6. Marca la casilla **Habilitar autenticación de clientes** si el servidor Syslog de destino requiere autenticación basada en certificados.

   Deberás descargar el certificado de autenticación de clientes y cargarlo en el servidor Syslog antes de guardar la configuración del registro de auditoría, de lo contrario, la conexión fallará. Dependiendo del tipo de servidor Syslog, es posible que tengas que crear un hash del certificado de autenticación de clientes.

   Ejemplo: syslog-ng requiere que se cree un <hash> del certificado mediante el comando `openssl x509 -noout -hash -in cert.pem`, y luego debes crear un enlace simbólico del certificado de autenticación de clientes a un archivo con el nombre <hash>.0.

7. Haz clic en **Guardar** para configurar la conexión con tu servidor y activar el registro remoto.

   Se te redirigirá a la página Audit Logs.

> El valor de **Tiempo de espera de conexión** puede afectar a la configuración. Si la configuración tarda más tiempo en responder que el valor definido, puede producirse un error de configuración debido a un error de conexión. Para establecer una conexión correcta, aumenta el valor de **Tiempo de espera de conexión** e intenta realizar la configuración de nuevo.

Utiliza la página de autenticación remota en Active IQ Unified Manager

Puedes usar la página «Autenticación remota» para configurar Unified Manager para que se comunique con tu servidor de autenticación y autentique a los usuarios remotos que intenten iniciar sesión en la interfaz de usuario web de Unified Manager.

Debes tener el rol de Application Administrator o Storage Administrator.

Una vez marcada la casilla «Habilitar autenticación remota», podrás habilitar la autenticación remota mediante un servidor de autenticación.

- **Servicio de autenticación**

  Te permite configurar el servidor de gestión para autenticar a los usuarios en proveedores de servicios de directorio, como Active Directory u OpenLDAP, o bien especificar tu propio mecanismo de autenticación. Solo puedes especificar un servicio de autenticación si has habilitado la autenticación remota.

  - **Active Directory**
    - Nombre del administrador

      Especifica el nombre del administrador del servidor de autenticación.

- Password

  Especifica la contraseña para acceder al servidor de autenticación.

- Nombre distintivo base

  Especifica la ubicación de los usuarios remotos en el 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**.

- Desactivar la búsqueda de grupos anidados

  Especifica si quieres habilitar o deshabilitar la opción de búsqueda de grupos anidados. De forma predeterminada, esta opción está deshabilitada. Si utilizas Active Directory, puedes acelerar la autenticación deshabilitando la compatibilidad con grupos anidados.

- Utiliza una conexión segura

  Especifica el servicio de autenticación que se usa para comunicarse con los servidores de autenticación.

◦ **OpenLDAP**

- Nombre distintivo de enlace

  Especifica el nombre distintivo de enlace que se usa junto con el nombre distintivo base para encontrar usuarios remotos en el servidor de autenticación.

- Contraseña de enlace

  Especifica la contraseña para acceder al servidor de autenticación.

- Nombre distintivo base

  Especifica la ubicación de los usuarios remotos en el 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**.

- Utiliza una conexión segura

  Especifica que se usa Secure LDAP para comunicarse con los servidores de autenticación LDAP.

◦ **Otros**

- Nombre distintivo de enlace

  Especifica el nombre distintivo de enlace que se usa junto con el nombre distintivo base para buscar usuarios remotos en el servidor de autenticación que has configurado.

- Contraseña de enlace

  Especifica la contraseña para acceder al servidor de autenticación.

- Nombre distintivo base

  Especifica la ubicación de los usuarios remotos en el 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**.

- Versión de protocolo

  Especifica la versión de protocolo del Protocolo ligero de acceso a directorios (LDAP) que admite tu servidor de autenticación. Puedes especificar si la versión de protocolo debe detectarse automáticamente o establecerla en 2 o 3.

- Atributo de nombre de usuario

  Especifica el nombre del atributo del servidor de autenticación que contiene los nombres de inicio de sesión de usuario que debe autenticar el servidor de gestión.

- Atributo de pertenencia a grupos

  Especifica un valor que asigna la pertenencia al grupo del servidor de gestión a los usuarios remotos en función de un atributo y un valor especificados en el servidor de autenticación del usuario.

- UGID

  Si los usuarios remotos figuran como miembros de un objeto GroupOfUniqueNames en el servidor de autenticación, esta opción te permite asignar la pertenencia al grupo del servidor de gestión a los usuarios remotos en función de un atributo especificado en ese objeto GroupOfUniqueNames.

- Desactivar la búsqueda de grupos anidados

  Especifica si quieres habilitar o deshabilitar la opción de búsqueda de grupos anidados. De forma predeterminada, esta opción está deshabilitada. Si utilizas Active Directory, puedes acelerar la autenticación deshabilitando la compatibilidad con grupos anidados.

- Miembro

  Especifica el nombre del atributo que utiliza tu servidor de autenticación para almacenar información sobre cada uno de los miembros de un grupo.

- Clase de objeto de usuario

  Especifica la clase de objeto de un usuario en el servidor de autenticación remota.

- Clase de objeto de grupo

  Especifica la clase de objeto de todos los grupos del servidor de autenticación remoto.

  Los valores que introduzcas para los atributos *Member*, *User Object Class* y *Group Object Class* deben coincidir con los añadidos en tus configuraciones de Active Directory, OpenLDAP y LDAP. De lo contrario, la autenticación podría fallar.

- Utiliza una conexión segura

  Especifica el servicio de autenticación que se usa para comunicarse con los servidores de autenticación.

  Si quieres modificar el servicio de autenticación, asegúrate de eliminar cualquier servidor de autenticación existente y de añadir nuevos servidores de autenticación.

Área de servidores de autenticación

El área «Servidores de autenticación» muestra los servidores de autenticación con los que se comunica el servidor de gestión para localizar y autenticar a los usuarios remotos. Las credenciales de los usuarios o grupos remotos las gestiona el servidor de autenticación.

- **Botones de comando**

  Te permite añadir, editar o eliminar servidores de autenticación.

  - Agregar

    Te permite añadir un servidor de autenticación.

  Si el servidor de autenticación que estás añadiendo forma parte de un par de alta disponibilidad (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 uno de los servidores de autenticación no esté accesible.

  - Editar

    Te permite editar la configuración del servidor de autenticación seleccionado.

  - Borrar

    Elimina los servidores de autenticación seleccionados.

- **Nombre o dirección IP**

  Muestra el nombre de host o la dirección IP del servidor de autenticación que se usa para autenticar al usuario en el servidor de gestión.

- **Puerto**

  Muestra el número de puerto del servidor de autenticación.

- **Probar autenticación**

  Este botón valida la configuración de tu servidor de autenticación al autenticar a un usuario o grupo remoto.

  Durante las pruebas, si solo especificas el nombre de usuario, el servidor de gestión busca al usuario remoto en el servidor de autenticación, pero no lo autentica. Si especificas tanto el nombre de usuario como la contraseña, el servidor de gestión busca y autentica al usuario remoto.

  No puedes comprobar la autenticación si la autenticación remota está desactivada.

Gestiona certificados de seguridad

Ver el certificado de seguridad HTTPS en Active IQ Unified Manager

Puedes comparar los datos del certificado HTTPS con el certificado recuperado en tu navegador para asegurarte de que la conexión cifrada de tu navegador con Unified Manager no está siendo interceptada.

Antes de empezar

Debes tener el rol de Operator, Application Administrator o Storage Administrator.

Ver el certificado te permite comprobar el contenido de un certificado regenerado o ver los nombres alternativos del sujeto (SAN) desde los que puedes acceder a Unified Manager.

Paso

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

   El certificado HTTPS aparece en la parte superior de la página

Si necesitas consultar información más detallada sobre el certificado de seguridad, además de la que se muestra en la página «HTTPS Certificate», puedes consultar el certificado de conexión en tu navegador.

Descargar una solicitud de firma de certificado HTTPS en Active IQ Unified Manager

Puedes descargar una solicitud de firma de certificado para el certificado de seguridad HTTPS actual, de modo que puedas proporcionar el archivo a una autoridad de certificación para que lo firme. Un certificado firmado por una autoridad de certificación ayuda a prevenir ataques de intermediario y ofrece una mejor protección de seguridad que un certificado autofirmado.

Antes de empezar

Debes tener el rol de Application Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Certificado HTTPS**.
2. Haz clic en **Descargar solicitud de firma de certificado HTTPS**.
3. Guarda el archivo `<hostname>.csr`.

Puedes enviar el archivo a una autoridad de certificación para que lo firme y, a continuación, instalar el certificado firmado.

Instala un certificado HTTPS firmado por una autoridad de certificación (CA) en Active IQ Unified Manager

Puedes cargar e instalar un certificado de seguridad una vez que una autoridad de certificación lo haya firmado y devuelto. El archivo que cargues e instales debe ser una versión firmada del certificado autofirmado existente. Un certificado firmado por una autoridad de certificación ayuda a prevenir los ataques man-in-the-middle y ofrece una mayor protección de seguridad que un certificado autofirmado.

*Qué. Antes de empezar

Debes haber realizado las siguientes acciones:

- Descargué el archivo de solicitud de firma de certificado e hice que una autoridad de certificación lo firmara

- Se guardó la cadena de certificados en formato PEM
- Se incluyeron todos los certificados de la cadena, desde el certificado del servidor de Unified Manager hasta el certificado de firma raíz, incluidos los certificados intermedios presentes

Debes tener el rol de Application Administrator.

Si la validez del certificado para el que se ha creado una CSR es superior a 397 días, la CA reducirá dicha validez a 397 días antes de firmar y devolver el certificado

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Certificado HTTPS**.
2. Haz clic en **Install HTTPS Certificate**.
3. En el cuadro de diálogo que aparece, haz clic en **Seleccionar archivo…** para localizar el archivo que quieres cargar.
4. Selecciona el archivo y luego haz clic en **Instalar** para instalarlo.

   Para más información, consulta "Instalación de un certificado HTTPS generado con herramientas externas".

Ejemplo de cadena de certificados

El siguiente ejemplo muestra cómo podría verse el archivo de la cadena de certificados:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Conoce los certificados HTTPS generados mediante herramientas externas en Active IQ Unified Manager Unified Manager

Puedes instalar certificados autofirmados o firmados por una autoridad de certificación (CA), generados con una herramienta externa como OpenSSL, BoringSSL, LetsEncrypt.

Debes cargar la clave privada junto con la cadena de certificados, ya que estos certificados son un par de claves pública y privada generado externamente. Los algoritmos permitidos para los pares de claves son “RSA” y “EC”. La opción **Install HTTPS Certificate** está disponible en la página HTTPS Certificates en la sección General. El archivo que subas debe tener el siguiente formato de entrada.

1. Clave privada del servidor que pertenece al host de Active IQ Unified Manager
2. Certificado del servidor que coincide con la clave privada
3. Certificado de las CA en orden inverso hasta la raíz, que se usan para firmar el certificado anterior

Formato para cargar un certificado con un par de claves EC

Las curvas permitidas son “prime256v1” y “secp384r1”. Ejemplo de certificado con un par EC generado externamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Formato para cargar un certificado con un par de claves RSA

Los tamaños de clave permitidos para el par de claves RSA correspondiente al certificado del host son 2048, 3072 y 4096. certificado con un **par de claves RSA** generado externamente:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
```

```
<Root signing certificate>
-----END CERTIFICATE-----
```

Una vez subido el certificado, debes reiniciar la instancia de Active IQ Unified Manager para que los cambios surtan efecto.

Comprobaciones durante la carga de certificados generados externamente

El sistema realiza comprobaciones durante la carga de un certificado generado con herramientas externas. Si alguna de las comprobaciones falla, el certificado se rechaza. También se incluyen comprobaciones de validación para los certificados generados a partir de la CSR dentro del producto y para los certificados generados con herramientas externas.

- La clave privada de la entrada se valida con el certificado de host de la entrada.
- El nombre común (CN) del certificado del host se compara con el nombre de dominio completo (FQDN) del host.
- El nombre común (CN) del certificado del host no debe estar vacío ni en blanco y no debe establecerse como localhost.
- La fecha de inicio de validez no debe estar en el futuro y la fecha de caducidad del certificado no debe estar en el pasado.
- Si existe una CA intermedia o una CA, la fecha de inicio de validez del certificado no debe estar en el futuro y la fecha de vencimiento de la validez no debe estar en el pasado.

La clave privada en la entrada no debe estar cifrada. Si hay claves privadas cifradas, el sistema las rechazará.

Ejemplo 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Ejemplo 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Ejemplo 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
```

```
-----END EC PRIVATE KEY-----
```

Si falla la instalación del certificado, consulta el artículo de la base de conocimientos (KB): "ActiveIQ Unified Manager no consigue instalar un certificado generado externamente"

Descripciones de las páginas para la gestión de certificados

Conoce la página de certificados HTTPS en Active IQ Unified Manager

La página «Certificado HTTPS» te permite consultar el certificado de seguridad actual, descargar una solicitud de firma de certificado, generar un nuevo certificado HTTPS autofirmado o instalar un nuevo certificado HTTPS.

Si no has generado un nuevo certificado HTTPS autofirmado, el certificado que aparece en esta página es el que se generó durante la instalación.

Botones de comando

Los botones de comando te permiten realizar las siguientes operaciones:

- **Descargar solicitud de firma de certificado HTTPS**

  Descarga una solicitud de certificación para el certificado HTTPS actualmente instalado. Tu navegador te pedirá que guardes el archivo <hostname>.csr para que puedas enviarlo a una autoridad de certificación para que lo firme.

- **Instalar un certificado HTTPS**

  Te permite cargar e instalar un certificado de seguridad una vez que una autoridad de certificación lo haya firmado y devuelto. El nuevo certificado entra en vigor después de reiniciar el servidor de gestión.

- **Regenerar certificado HTTPS**

  Te permite generar un nuevo certificado HTTPS autofirmado, que sustituye al certificado de seguridad actual. El nuevo certificado entrará en vigor tras reiniciar Unified Manager.

Cuadro de diálogo Regenerar un certificado HTTPS en Active IQ Unified Manager

El cuadro de diálogo «Regenerar certificado HTTPS» te permite personalizar la información de seguridad y a continuación generar un nuevo certificado HTTPS con dicha información.

En esta página aparece la información actual del certificado.

Las opciones “Regenerate Using Current Certificate Attributes” y “Update the Current Certificate Attributes” te permiten regenerar el certificado con la información actual o generar un certificado con información nueva.

- **Nombre común**

  Obligatorio. El nombre de dominio completo (FQDN) que deseas proteger.

  En las configuraciones de alta disponibilidad de Unified Manager, utiliza la dirección IP virtual.

- **Correo electrónico**

  Opcional. Una dirección de correo electrónico para contactar con tu organización; normalmente la dirección de correo electrónico del administrador de certificados o del departamento de TI.

- **Empresa**

  Opcional. Normalmente el nombre legal de tu empresa.

- **Departamento**

  Opcional. El nombre del departamento de tu empresa.

- **Ciudad**

  Opcional. La ciudad en la que se encuentra tu empresa.

- **Estado**

  Opcional. El estado o la provincia donde se encuentra tu empresa, sin abreviaturas.

- **País**

  Opcional. El país donde se encuentra tu empresa. Suele ser un código ISO de dos letras del país.

- **Nombres alternativos**

  Obligatorio. Nombres de dominio adicionales, distintos del principal, que puedes usar para acceder a este servidor además de localhost u otras direcciones de red existentes. Separa cada nombre alternativo con una coma.

  Marca la casilla «`Excluir información de identificación local (p. ej., localhost)`» si quieres eliminar la información de identificación local del campo Nombres alternativos del certificado. Cuando esta casilla está marcada, en el campo Nombres alternativos solo se usa lo que introduzcas en el campo. Si se deja en blanco, el certificado resultante no tendrá ningún campo Nombres alternativos.

- **TAMAÑO DE LA CLAVE (algoritmo de la clave: RSA)**

  El algoritmo de clave está configurado en RSA. Puedes seleccionar uno de estos tamaños de clave: 2048, 3072 o 4096 bits. El tamaño de clave predeterminado está configurado en 2048 bits.

- **PERÍODO DE VALIDEZ**

  El periodo de validez predeterminado es de 397 días. Si has actualizado desde una versión anterior, es posible que veas que la validez del certificado anterior no ha cambiado.

Para obtener más información, consulta "Generar certificados HTTPS".

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.