Configurar notificaciones

Active IQ Unified Manager

NetApp
November 13, 2026

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

Tabla de contenidos

Configurar notificaciones . . . 1
- Configura Active IQ Unified Manager para que envíe notificaciones de alerta . . . 1
- Configura los ajustes de notificación de eventos en Active IQ Unified Manager . . . 1
- Habilita la autenticación remota en Active IQ Unified Manager . . . 3
- Desactivar los grupos anidados de la autenticación remota en Active IQ Unified Manager . . . 4
- Configura los servicios de autenticación en Active IQ Unified Manager . . . 4
- Agrega servidores de autenticación a Active IQ Unified Manager . . . 5
- Comprueba la configuración de los servidores de autenticación en Active IQ Unified Manager . . . 7
- Agrega alertas en Active IQ Unified Manager . . . 7
  - Ejemplo de cómo añadir una alerta . . . 9

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**.
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.

Si quieres…	Entonces haz lo siguiente…
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**.

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.