# Configuración de Unified Manager para enviar notificaciones de alerta

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

# Tabla de contenidos

# Configuración de Unified Manager para enviar notificaciones de alerta

Puede configurar Unified Manager para que envíe notificaciones que le alertan de los eventos de su entorno. Antes de que las notificaciones se puedan enviar, debe configurar varias otras opciones de Unified Manager.

**Lo que necesitará**

Debe tener la función Administrador de aplicaciones.

Después de implementar Unified Manager y completar la configuración inicial, se debe considerar configurar el entorno para activar alertas y generar correos electrónicos de notificación o capturas SNMP en función de la recepción de eventos.

**Pasos**

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

   Si desea que las notificaciones de alerta se envíen cuando ciertos eventos ocurran en el entorno, debe configurar un servidor SMTP y suministrar una dirección de correo electrónico desde la que se enviará la notificación de alerta. Si desea utilizar capturas SNMP, puede seleccionar esa opción y proporcionar la información necesaria.

2. "Habilite la autenticación remota".

   Si desea que los usuarios remotos de LDAP o Active Directory accedan a la instancia de Unified Manager y reciban notificaciones de alerta, debe habilitar la autenticación remota.

3. "Agregue servidores de autenticación".

   Puede agregar servidores de autenticación para que los usuarios remotos dentro del servidor de autenticación puedan acceder a Unified Manager.

4. "Añadir usuarios".

   Puede añadir varios tipos de usuarios locales o remotos y asignar roles específicos. Cuando crea una alerta, asigna un usuario para que reciba las notificaciones de alerta.

5. "Añadir alertas".

   Después de añadir la dirección de correo electrónico para enviar notificaciones, se añadieron usuarios para recibir las notificaciones, configurar los ajustes de red y configurar las opciones SMTP y SNMP necesarias para el entorno, y después puede asignar alertas.

## Configuración de los ajustes de notificación de eventos

Es posible configurar Unified Manager para que envíe notificaciones de alerta cuando se genera un evento o cuando se asigna un evento a un usuario. Puede configurar el servidor SMTP que se usa para enviar la alerta y se pueden configurar varios mecanismos de notificación; por ejemplo, las notificaciones de alerta se pueden enviar

como correos electrónicos o capturas SNMP.

**Lo que necesitará**

Debe tener la siguiente información:

- Dirección de correo electrónico desde la cual se envía la notificación de alertas

  La dirección de correo electrónico aparece en el campo «'de'» en las notificaciones de alerta enviadas. Si el correo electrónico no se puede entregar por cualquier motivo, esta dirección de correo electrónico también se utiliza como destinatario para el correo no entregable.

- 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 captura que recibirá la captura SNMP, junto con la versión SNMP, el puerto de capturas saliente, la comunidad y otros valores de configuración SNMP requeridos

  Para especificar varios destinos de capturas, separe cada host con una coma. En este caso, todas las demás configuraciones de SNMP, como la versión y el puerto de captura saliente, deben ser las mismas para todos los hosts de la lista.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

**Pasos**

1. En el panel de navegación izquierdo, haga clic en **General** > **Notificaciones**.
2. En la página Notifications, configure los ajustes adecuados.

   **Notas:**

   - Si la dirección de origen está precargada con la dirección "ActiveIQUnifiedManager@localhost.com", debe cambiarla a una dirección de correo electrónico real y operativa para asegurarse de que todas las notificaciones de correo electrónico se entregan correctamente.
   - Si no se puede resolver el nombre de host del servidor SMTP, puede especificar la dirección IP (IPv4 o IPv6) del servidor SMTP en lugar del nombre de host.
3. Haga clic en **Guardar**.
4. Si ha seleccionado la opción **usar STARTTLS** o **usar SSL**, aparecerá una página de certificado después de hacer clic en el botón **Guardar**. Compruebe los detalles del certificado y acepte el certificado para guardar la configuración de notificación.

   Puede hacer clic en el botón **Ver detalles del certificado** para ver los detalles del certificado. Si el certificado existente ha caducado, desactive la casilla **usar STARTTLS** o **usar SSL**, guarde la configuración de notificación y vuelva a marcar la casilla **usar STARTTLS** o **usar SSL** para ver un nuevo certificado.

# Habilitación de la autenticación remota

Puede habilitar la autenticación remota para que el servidor de Unified Manager pueda comunicarse con los servidores de autenticación. Los usuarios del servidor de autenticación pueden acceder a la interfaz gráfica de Unified Manager para gestionar los

objetos de almacenamiento y los datos.

**Lo que necesitará**

Debe tener la función Administrador de aplicaciones.

> El servidor de Unified Manager debe estar conectado directamente con el servidor de autenticación. Debe deshabilitar cualquier cliente LDAP local, como SSSD (demonio de servicios de seguridad del sistema) o NSLCD (demonio de almacenamiento en caché LDAP del servicio de nombres).

Puede 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.

La autenticación remota es compatible con LDAP y LDAPS (LDAP seguro). Unified Manager utiliza 389 como puerto predeterminado para la comunicación no segura y 636 como puerto predeterminado para la comunicación segura.

> El certificado que se utiliza para autenticar usuarios debe cumplir el formato X.509.

**Pasos**

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Marque la casilla para **Activar autenticación remota…**.
3. En el campo Servicio de autenticación, seleccione el tipo de servicio y configure el servicio de autenticación.

| Para tipo de autenticación… | Introduzca la siguiente información… |
|---|---|
| Active Directory | • Nombre del administrador del servidor de autenticación en uno de los siguientes formatos:<br>◦ `domainname\username`<br>◦ `username@domainname`<br>◦ `Bind Distinguished Name` (Usando la notación LDAP adecuada)<br>• Contraseña de administrador<br>• Nombre completo base (con la notación LDAP adecuada) |
| Abra LDAP | • Enlazar nombre distintivo (en la notación LDAP correspondiente)<br>• Enlazar contraseña<br>• Nombre distintivo de base |

Si la autenticación de un usuario de Active Directory tarda mucho tiempo o agota el tiempo de espera, es probable que el servidor de autenticación tarde mucho tiempo en responder. Al deshabilitar la compatibilidad con los grupos anidados en Unified Manager, es posible que se reduzca el tiempo de autenticación.

Si selecciona la opción Use Secure Connection para el servidor de autenticación, Unified Manager se comunica con el servidor de autenticación mediante el protocolo Secure Sockets Layer (SSL).

4. **Opcional:** Agregue servidores de autenticación y pruebe la autenticación.
5. Haga clic en **Guardar**.

# Deshabilitar grupos anidados de la autenticación remota

Si tiene habilitada la autenticación remota, puede deshabilitar la autenticación de grupos anidados para que solo los usuarios individuales y no los miembros de grupos se puedan autenticar de forma remota a Unified Manager. Puede deshabilitar los grupos anidados cuando desee mejorar el tiempo de respuesta de autenticación de Active Directory.

**Lo que necesitará**

- Debe tener la función Administrador de aplicaciones.
- La desactivación de grupos anidados sólo se aplica cuando se utiliza Active Directory.

Al deshabilitar la compatibilidad con los grupos anidados en Unified Manager, es posible que se reduzca el tiempo de autenticación. Si la compatibilidad de grupos anidados está deshabilitada y, si 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 izquierdo, haga clic en **General** > **autenticación remota**.
2. Active la casilla de verificación **Desactivar búsqueda de grupo anidada**.
3. Haga clic en **Guardar**.

# Configurar servicios de autenticación

Los servicios de autenticación permiten la autenticación de usuarios remotos o grupos remotos en un servidor de autenticación antes de otorgar acceso a Unified Manager. Puede autenticar usuarios utilizando servicios de autenticación predefinidos (como Active Directory u OpenLDAP) o configurando su propio mecanismo de autenticación.

**Lo que necesitará**

- Debe haber habilitado la autenticación remota.
- Debe tener la función Administrador de aplicaciones.

**Pasos**

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Seleccione uno de los siguientes servicios de autenticación:

| Si selecciona… | Realice lo siguiente… |
| --- | --- |
| Active Directory | a. Introduzca el nombre y la contraseña del administrador.<br>b. Especifique el nombre completo base del servidor de autenticación.<br><br>Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**. |
| OpenLDAP | a. Introduzca el nombre distintivo del enlace y la contraseña de enlace.<br>b. Especifique el nombre completo base del servidor de autenticación.<br><br>Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**. |
| Otros | a. Introduzca el nombre distintivo del enlace y la contraseña de enlace.<br>b. Especifique el nombre completo base del servidor de autenticación.<br><br>Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**.<br><br>c. Especifique la versión de protocolo LDAP que admite el servidor de autenticación.<br>d. Introduzca el nombre de usuario, la pertenencia a grupos, el grupo de usuarios y los atributos miembro. |

Si desea modificar el servicio de autenticación, debe eliminar todos los servidores de autenticación existentes y, a continuación, agregar nuevos servidores de autenticación.

3. Haga clic en **Guardar**.

# Añadiendo servidores de autenticación

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

**Lo que necesitará**

- Debe estar disponible la siguiente información:
  - Nombre de host o dirección IP del servidor de autenticación
  - Número de puerto del servidor de autenticación
- Debe haber habilitado la autenticación remota y configurado el servicio de autenticación para que el servidor de administración pueda autenticar usuarios o grupos remotos en el servidor de autenticación.
- Debe tener la función Administrador de aplicaciones.

Si el servidor de autenticación que va a añadir forma parte de un par de alta disponibilidad (ha) (con la misma base de datos), también puede añadir el servidor de autenticación asociado. Esto permite que el servidor de administración se comunique con el asociado cuando no se puede acceder a uno de los servidores de autenticación.

**Pasos**

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Activar o desactivar la opción **utilizar conexión segura**:

| Si desea… | Realice lo siguiente… |
|---|---|
| Habilite | a. Seleccione la opción **utilizar conexión segura**.<br>b. En el área servidores de autenticación, haga clic en **Agregar**.<br>c. En el cuadro de diálogo Add Authentication Server, introduzca el nombre o la dirección IP de autenticación (IPv4 o IPv6) del servidor.<br>d. En el cuadro de diálogo autorizar host, haga clic en Ver certificado.<br>e. En el cuadro de diálogo Ver certificado, compruebe la información del certificado y, a continuación, haga clic en **Cerrar**.<br>f. En el cuadro de diálogo autorizar host, haga clic en **Sí**.<br>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 636 como puerto predeterminado para una comunicación segura y el número de puerto 389 para una comunicación no segura. |

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Deshabilitarla | a. Desactive la opción **utilizar conexión segura**.<br>b. En el área servidores de autenticación, haga clic en **Agregar**.<br>c. En el cuadro de diálogo Add Authentication Server, especifique el nombre de host o la dirección IP (IPv4 o IPv6) del servidor y los detalles del puerto.<br>d. Haga clic en **Agregar**. |

El servidor de autenticación que ha agregado se muestra en el área servidores.

3. Realice una autenticación de prueba para confirmar que puede autenticar usuarios en el servidor de autenticación que ha agregado.

# Prueba de la configuración de los servidores de autenticación

Puede validar la configuración de los servidores de autenticación para garantizar que el servidor de gestión pueda comunicarse con ellos. Puede validar la configuración buscando un usuario remoto o un grupo remoto desde los servidores de autenticación y autentificándolos con la configuración configurada.

**Lo que necesitará**

- Usted debe haber habilitado la autenticación remota y configurado el servicio de autenticación para que el servidor de Unified Manager pueda autenticar el usuario remoto o el grupo remoto.
- Debe haber agregado los servidores de autenticación para que el servidor de administración pueda buscar el usuario remoto o el grupo remoto desde estos servidores y autentificarlos.
- Debe tener la función Administrador de aplicaciones.

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

**Pasos**

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Haga clic en **probar autenticación**.
3. En el cuadro de diálogo probar usuario, especifique el nombre de usuario y la contraseña del usuario remoto o el nombre de usuario del grupo remoto y, a continuación, haga clic en **Prueba**.

   Si va a autenticar un grupo remoto, no debe introducir la contraseña.

# Adición de alertas

Puede configurar alertas para que le notifiquen un evento determinado. Es posible

configurar alertas para un solo recurso, para un grupo de recursos o para eventos de un tipo de gravedad determinado. Puede especificar la frecuencia con la que desea que se le notifique y asociar un script a la alerta.

**Lo que necesitará**

- Debe haber configurado los ajustes de notificación, como la dirección de correo electrónico de usuario, el servidor SMTP y el host de captura SNMP, con el fin de permitir que el servidor Active IQ Unified Manager utilice estos ajustes para enviar notificaciones a los usuarios cuando se genera un evento.
- Debe conocer los recursos y los eventos sobre los que desea activar la alerta, así como los nombres de usuario o las direcciones de correo electrónico de los usuarios a los que desea notificar.
- Si desea que un script se ejecute según el evento, debe haber añadido el script a Unified Manager mediante la página Scripts.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede crear una alerta directamente desde la página de detalles Event después de recibir un evento además de crear una alerta desde la página Alert Setup, tal y como se describe aquí.

**Pasos**

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página Configuración de alertas, haga clic en **Agregar**.
3. En el cuadro de diálogo Agregar alerta, haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.
4. Haga clic en **Recursos** y seleccione los recursos que se incluirán o excluirán de la alerta.

   Puede establecer un filtro especificando una cadena de texto en el campo **Nombre contiene** para seleccionar un grupo de recursos. Según la cadena de texto que especifique, la lista de recursos disponibles solo muestra los recursos que coinciden con la regla de filtro. La cadena de texto que especifique distingue mayúsculas y minúsculas.

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

5. Haga clic en **Eventos** y seleccione los eventos según el nombre del evento o el tipo de gravedad del evento para el que desea activar una alerta.

   Para seleccionar más de un evento, pulse la tecla Ctrl mientras realiza las selecciones.

6. Haga clic en **acciones** y seleccione los usuarios a los que desea notificar, elija la frecuencia de notificación, elija si se enviará una captura SNMP al receptor de capturas y asigne una secuencia de comandos para que se ejecute cuando se genere una alerta.

   Si modifica la dirección de correo electrónico especificada para el usuario y vuelve a abrir la alerta para su edición, el campo Nombre aparecerá en blanco porque la dirección de correo electrónico modificada ya no está asignada al usuario que se seleccionó previamente. Además, si modificó la dirección de correo electrónico del usuario seleccionado desde la página usuarios, la dirección de correo electrónico modificada no se actualizará para el usuario seleccionado.

También puede optar por notificar a los usuarios a través de las capturas SNMP.

7. Haga clic en **Guardar**.

## Ejemplo de añadir una alerta

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

- Nombre de alerta: HealthTest
- Recursos: Incluye todos los volúmenes cuyo nombre contenga «'abc'» y excluye todos los volúmenes cuyo nombre contenga «'xyz'».
- Eventos: Incluye todos los eventos críticos de salud
- Acciones: Incluye «sample@domain.com», una secuencia de comandos «'Prueba» y el usuario deberá recibir una notificación cada 15 minutos

Realice los siguientes pasos en el cuadro de diálogo Agregar alerta:

**Pasos**

1. Haga clic en **Nombre** e introduzca **HealthTest** en el campo **Nombre de alerta**.
2. Haga clic en **Recursos** y, en la ficha incluir, seleccione **volúmenes** en la lista desplegable.
   a. Introduzca **abc** en el campo **Name contains** para mostrar los volúmenes cuyo nombre contenga "'abc'".
   b. Seleccione **<<All Volumes whose name contains 'abc'>>** en el área Recursos disponibles y muévalos al área Recursos seleccionados.
   c. Haga clic en **excluir** e introduzca **xyz** en el campo **Nombre contiene** y, a continuación, haga clic en **Agregar**.
3. Haga clic en **Eventos** y seleccione **críticos** en el campo gravedad del evento.
4. Seleccione **todos los eventos críticos** en el área Eventos coincidentes y muévalos al área Eventos seleccionados.
5. Haga clic en **acciones** e introduzca **sample@domain.com** en el campo Alerta a estos usuarios.
6. Seleccione **Recordar cada 15 minutos** para notificar al usuario cada 15 minutos.

   Puede configurar una alerta para que envíe repetidamente notificaciones a los destinatarios durante un período de tiempo específico. Debe determinar la hora desde la cual está activa la notificación de eventos para la alerta.

7. En el menú Select Script to Execute, seleccione **Test** script.
8. Haga clic en **Guardar**.