Gestión de la autenticación

Active IQ Unified Manager 9.11

NetApp
December 18, 2023

Tabla de contenidos

Gestión de la autenticación

Puede habilitar la autenticación mediante LDAP o Active Directory en el servidor de Unified Manager y configurarla para que funcione con los servidores con el fin de autenticar usuarios remotos.

Para habilitar la autenticación remota, configurar los servicios de autenticación y agregar servidores de autenticación, consulte la sección anterior en **Configuración de Unified Manager para enviar notificaciones de alerta**.

Editar servidores de autenticación

Es posible cambiar el puerto que utiliza Unified Manager Server para comunicarse con el servidor de autenticación.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Active la casilla **Desactivar búsqueda de grupo anidada**.
3. En el área **servidores de autenticación**, seleccione el servidor de autenticación que desea editar y, a continuación, haga clic en **Editar**.
4. En el cuadro de diálogo **Editar servidor de autenticación**, edite los detalles del puerto.
5. Haga clic en **Guardar**.

Eliminar servidores de autenticación

Puede eliminar un servidor de autenticación si desea impedir que Unified Manager Server se comunique con el servidor de autenticación. Por ejemplo, si desea cambiar un servidor de autenticación con el que el servidor de administración está comunicando, puede eliminar el servidor de autenticación y agregar un nuevo servidor de autenticación.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Cuando se elimina un servidor de autenticación, los usuarios remotos o grupos del servidor de autenticación ya no pueden acceder a Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Seleccione uno o varios servidores de autenticación que desee eliminar y, a continuación, haga clic en **Eliminar**.
3. Haga clic en **Sí** para confirmar la solicitud de eliminación.

   Si la opción **usar conexión segura** está activada, los certificados asociados con el servidor de

autenticación se eliminarán junto con el servidor de autenticación.

Autenticación con Active Directory u OpenLDAP

Es posible habilitar la autenticación remota en el servidor de gestión y configurar el servidor de gestión para que se comunique con los servidores de autenticación, de modo que los usuarios dentro de los servidores de autenticación puedan acceder a Unified Manager.

Puede utilizar uno de los siguientes servicios de autenticación predefinidos o especificar su propio servicio de autenticación:

- Active Directory de Microsoft

  No puede usar los servicios de directorio ligero de Microsoft.

- OpenLDAP

Puede seleccionar el servicio de autenticación requerido y añadir los servidores de autenticación adecuados para habilitar los usuarios remotos en el servidor de autenticación para acceder a Unified Manager. El servidor de autenticación mantiene las credenciales de los usuarios o grupos remotos. El servidor de gestión usa el protocolo ligero de acceso a directorios (LDAP) para autenticar a los usuarios remotos dentro del servidor de autenticación configurado.

Para los usuarios locales que se crean en Unified Manager, el servidor de gestión mantiene su propia base de datos de nombres de usuario y contraseñas. El servidor de gestión realiza la autenticación y no utiliza Active Directory ni OpenLDAP para la autenticación.

Registro de auditoría

Es posible detectar si los registros de auditoría se ven comprometidos con el uso de registros de auditoría. Todas las actividades realizadas por un usuario se supervisan y registran en los registros de auditoría. Las auditorías se realizan para todas las interfaces de usuario y las funcionalidades de Active IQ Unified Manager de las API expuestas al público.

Es posible usar el registro de auditoría: Vista de archivo para ver y acceder a todos los archivos de registro de auditoría disponibles en Active IQ Unified Manager. Los archivos del Registro de auditoría: Vista de archivo se muestran en función de su fecha de creación. Esta vista muestra información de todo el registro de auditoría capturado desde la instalación o actualización al presente en el sistema. Siempre que se realiza 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 "'Estado de integridad de archivo'", que se supervisa activamente para detectar la manipulación o eliminación del archivo de registro. Los registros de auditoría pueden tener uno de los siguientes estados cuando los registros de auditoría están disponibles en el sistema:

Estado	Descripción
ACTIVO	Archivo en el que se registran actualmente los registros.

Estado	Descripción
NORMAL	Archivo inactivo, comprimido y almacenado en el sistema.
MANIPULADO	Archivo que ha sido comprometido por un usuario que ha editado el archivo manualmente.
ELIMINAR_MANUAL	Archivo eliminado por un usuario autorizado.
ROLLOVER_DELETE	Archivo que se eliminó debido a la rodadura basada en la directiva de configuración gradual.
INESPERADO_DELETE	Archivo eliminado por motivos desconocidos.

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

- Configurar
- Eliminar
- Descargue

El botón **DELETE** permite eliminar cualquiera de los registros de auditoría enumerados en la vista registros de auditoría. Puede eliminar un registro de auditoría y, opcionalmente, proporcionar un motivo para eliminar el archivo que ayuda en el futuro a determinar una eliminación válida. La columna MOTIVO enumera el motivo junto con el nombre del usuario que realizó la operación de eliminación.

> La eliminación de un archivo de registro provocará la eliminación del archivo del sistema, pero la entrada de la tabla DB no se eliminará.

Puede descargar los registros de auditoría de Active IQ Unified Manager con el botón **DOWNLOAD** de la sección registros de auditoría y exportar los archivos de registro de auditoría. Los archivos marcados con «'NORMAL'» o «'MANIPULADO'» se descargan en una compresión `.gzip` formato.

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

Configuración de registros de auditoría

Puede utilizar el botón **Configurar** de la sección registros de auditoría para configurar la directiva de implementación para archivos de registro de auditoría y también para habilitar el registro remoto para los registros de auditoría.

Puede establecer los valores en **MAX FILE SIZE** y **AUDIT LOG RETENTION PERID** según la cantidad y frecuencia de datos que desee almacenar en el sistema. El valor del campo **TAMAÑO TOTAL del REGISTRO de AUDITORÍA** es el tamaño de los datos totales del registro de auditoría presentes en el sistema. La directiva de recuperación viene determinada por los valores del campo **DÍAS de RETENCIÓN de REGISTRO DE AUDITORÍA**, **TAMAÑO de ARCHIVO MAX** y **TAMAÑO DE REGISTRO DE AUDITORÍA TOTAL**. Cuando el tamaño de la copia de seguridad del registro de auditoría alcanza el valor configurado en **TAMAÑO TOTAL del REGISTRO de AUDITORÍA**, el archivo que se archivó primero se elimina. Esto significa que se ha

eliminado el archivo más antiguo. Pero la entrada del fichero sigue estando disponible en la base de datos y está marcada como "'Rollover Delete'". El valor **DÍAS de RETENCIÓN del REGISTRO DE AUDITORÍA** es para el número de días que se conservan los archivos de registro de auditoría. Cualquier archivo anterior al valor establecido en este campo se repasa.

Pasos

1. Haga clic en **registros de auditoría** > > **Configurar**.
2. Introduzca los valores en **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE** y **DÍAS DE RETENCIÓN DEL REGISTRO de AUDITORÍA**.

   Si desea activar el registro remoto, debe seleccionar **Activar registro remoto**.

Habilitación de registro remoto de registros de auditoría

Puede seleccionar la casilla de verificación **Activar registro remoto** en el cuadro de diálogo Configurar registros de auditoría para habilitar el registro de auditoría remoto. Es posible usar esta función para transferir registros de auditoría a un servidor de syslog remoto. Esto le permitirá gestionar los registros de auditoría cuando haya restricciones de espacio.

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

Pasos

1. En el cuadro de diálogo **Configurar registros de auditoría**, seleccione la casilla de verificación **Activar registro remoto**.

   Se mostrarán campos adicionales para configurar el registro remoto.

2. Introduzca el **NOMBRE de HOST** y el **PUERTO** del servidor remoto al que desea conectarse.
3. En el campo **CERTIFICADO de CA de SERVIDOR**, haga clic en **EXAMINAR** para seleccionar un certificado público del servidor de destino.

   El certificado debe cargarse en `.pem` formato. Este certificado debe obtenerse del servidor de syslog de destino y no debe haber caducado. El certificado deberá contener el «'nombre de host'» seleccionado como parte de la `SubjectAltName` (SAN).

4. Introduzca los valores para los siguientes campos: **CHARSET**, **TIEMPO DE ESPERA de CONEXIÓN**, **RETARDO DE RECONEXIÓN**.

   Los valores deben estar en milisegundos para estos campos.

5. Seleccione el formato Syslog requerido y la versión del protocolo TLS en los campos **FORMAT** y **PROTOCOL**.
6. Seleccione la casilla de verificación **Activar autenticación de cliente** si el servidor Syslog de destino requiere autenticación basada en certificados.

   Deberá descargar el certificado de autenticación de cliente y cargarlo en el servidor de syslog antes de guardar la configuración del registro de auditoría; de lo contrario, se producirá un error en la conexión. Según el tipo de servidor de syslog, puede que deba crear un hash del certificado de autenticación de cliente.

Ejemplo: Syslog-ng requiere que se cree una <hash> del certificado con el comando `openssl x509 -noout -hash -in cert.pem`y, a continuación, debe vincular simbólicamente el certificado de autenticación de cliente a un archivo denominado después de <hash> .0.

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

   Se le redirigirá a la página registros de auditoría.

Autenticación remota

Puede utilizar la página autenticación remota para configurar Unified Manager para comunicarse con el servidor de autenticación con el fin de autenticar a los usuarios remotos que intentan iniciar sesión en la interfaz de usuario web de Unified Manager.

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

Después de seleccionar la casilla de verificación Habilitar autenticación remota, puede habilitar la autenticación remota mediante un servidor de autenticación.

- **Servicio de autenticación**

  Permite configurar el servidor de administración para autenticar usuarios en proveedores de servicios de directorio, como Active Directory, OpenLDAP o especificar su propio mecanismo de autenticación. Sólo puede especificar un servicio de autenticación si ha habilitado la autenticación remota.

  - **Active Directory**
    - Nombre del administrador

      Especifica el nombre de administrador del servidor de autenticación.

    - Contraseña

      Especifica la contraseña para acceder al servidor de autenticación.

    - Nombre completo 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, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**.

    - Deshabilite la búsqueda de grupo anidada

      Especifica si se habilita o deshabilita la opción de búsqueda de grupos anidados. De forma predeterminada, esta opción está deshabilitada. Si utiliza Active Directory, puede acelerar la autenticación desactivando la compatibilidad con grupos anidados.

    - Utilice Conexión segura

      Especifica el servicio de autenticación utilizado para comunicarse con los servidores de autenticación.

  - **OpenLDAP**
    - Nombre distintivo del enlace

Especifica el nombre distintivo del enlace que se utiliza junto con el nombre completo de la base para buscar usuarios remotos en el servidor de autenticación.

- Enlazar contraseña

  Especifica la contraseña para acceder al servidor de autenticación.

- Nombre completo 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, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**.

- Utilice Conexión segura

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

◦ **Otros**

- Nombre distintivo del enlace

  Especifica el nombre distintivo del enlace que se utiliza junto con el nombre completo de la base para buscar usuarios remotos en el servidor de autenticación configurado.

- Enlazar contraseña

  Especifica la contraseña para acceder al servidor de autenticación.

- Nombre completo 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, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**.

- Versión de protocolo

  Especifica la versión LDAP (Lightweight Directory Access Protocol) que admite el servidor de autenticación. Puede especificar si la versión del protocolo se debe detectar automáticamente o si se debe establecer la versión en 2 o 3.

- Atributo Nombre de usuario

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

- Atributo de pertenencia a grupos

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

- UGID

  Si los usuarios remotos se incluyen como miembros de un objeto GroupOfUniqueNames en el servidor de autenticación, esta opción permite asignar la pertenencia al grupo del servidor de administración a los usuarios remotos basándose en un atributo especificado en ese objeto

GroupOfUniqueNames.

- Deshabilite la búsqueda de grupo anidada

  Especifica si se habilita o deshabilita la opción de búsqueda de grupos anidados. De forma predeterminada, esta opción está deshabilitada. Si utiliza Active Directory, puede acelerar la autenticación desactivando la compatibilidad con grupos anidados.

- Miembro

  Especifica el nombre de atributo que el servidor de autenticación utiliza para almacenar información acerca de los miembros individuales 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 remota.

- Utilice Conexión segura

  Especifica el servicio de autenticación utilizado para comunicarse con los servidores de autenticación.

> Si desea modificar el servicio de autenticación, asegúrese de eliminar los servidores de autenticación existentes y agregar nuevos servidores de autenticación.

Área servidores de autenticación

El área servidores de autenticación muestra los servidores de autenticación con los que se comunica el servidor de administración para buscar y autenticar usuarios remotos. El servidor de autenticación mantiene las credenciales de los usuarios o grupos remotos.

- **Botones de comando**

  Permite añadir, editar o eliminar servidores de autenticación.

  - Agregar

    Permite añadir un servidor de autenticación.

  Si el servidor de autenticación que va a agregar forma parte de un par de alta disponibilidad (con la misma base de datos), también puede agregar 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.

  - Editar

    Permite editar la configuración de un servidor de autenticación seleccionado.

  - Eliminar

    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 administración.

- **Puerto**

  Muestra el número de puerto del servidor de autenticación.

- **Probar autenticación**

  Este botón valida la configuración del servidor de autenticación autenticando un usuario o grupo remoto.

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

  No se puede probar la autenticación si la autenticación remota está deshabilitada.