Gestión de la autenticación

Active IQ Unified Manager 9.9

NetApp
April 05, 2024

Tabla de contenidos

Gestión de la autenticación . . . 1
- Habilitación de la autenticación remota . . . 1
- Deshabilitar grupos anidados de la autenticación remota . . . 2
- Configurar servicios de autenticación . . . 3
- Añadiendo servidores de autenticación . . . 4
- Prueba de la configuración de los servidores de autenticación . . . 5
- Editar servidores de autenticación . . . 6
- Eliminar servidores de autenticación . . . 7
- Autenticación con Active Directory u OpenLDAP . . . 7
- Habilitación de la autenticación SAML . . . 8
- Requisitos del proveedor de identidades . . . 9
- Cambiar el proveedor de identidades utilizado para la autenticación SAML . . . 10
- Deshabilitación de la autenticación SAML . . . 11
- Registro de auditoría . . . 12
- Descripción de las ventanas de autenticación y cuadros de diálogo . . . 15

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.

Además, puede habilitar la autenticación SAML para que los usuarios remotos se autentiquen a través de un proveedor de identidad segura (IDP) antes de poder iniciar sesión en la interfaz de usuario web de Unified Manager.

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.

Antes de empezar

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).

Acerca de esta tarea

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: ◦ `domainname \ username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Usando la notación LDAP adecuada) • Contraseña de administrador • Nombre completo base (con la notación LDAP adecuada)
Abra LDAP	• Enlazar nombre distintivo (en la notación LDAP correspondiente) • Enlazar contraseña • 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).

1. Añada servidores de autenticación y pruebe la autenticación.
2. 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.

Antes de empezar

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

Acerca de esta tarea

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.

Antes de empezar

- 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	1. Introduzca el nombre y la contraseña del administrador. 2. Especifique el nombre completo 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	1. Introduzca el nombre distintivo del enlace y la contraseña de enlace. 2. Especifique el nombre completo 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 selecciona…	Realice lo siguiente…
Otros	1. Introduzca el nombre distintivo del enlace y la contraseña de enlace. 2. Especifique el nombre completo 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`. 3. Especifique la versión de protocolo LDAP que admite el servidor de autenticación. 4. 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.

1. 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.

Antes de empezar

- 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.

Acerca de esta tarea

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	1. Seleccione la opción **utilizar conexión segura**. 2. En el área servidores de autenticación, haga clic en **Agregar**. 3. En el cuadro de diálogo Add Authentication Server, introduzca el nombre o la dirección IP de autenticación (IPv4 o IPv6) del servidor. 4. En el cuadro de diálogo autorizar host, haga clic en Ver certificado. 5. En el cuadro de diálogo Ver certificado, compruebe la información del certificado y, a continuación, haga clic en **Cerrar**. 6. En el cuadro de diálogo autorizar host, haga 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 636 como puerto predeterminado para una comunicación segura y el número de puerto 389 para una comunicación no segura.
Deshabilitarla	1. Desactive la opción **utilizar conexión segura**. 2. En el área servidores de autenticación, haga clic en **Agregar**. 3. 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. 4. Haga clic en **Agregar**.

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

1. 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.

Antes de empezar

- 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.

Acerca de esta tarea

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 **Usuario de prueba**, 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.

Editar servidores de autenticación

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

Antes de empezar

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.

Antes de empezar

Debe tener la función Administrador de aplicaciones.

Acerca de esta tarea

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.

Habilitación de la autenticación SAML

Puede habilitar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para que los usuarios remotos se autentiquen mediante un proveedor de identidad seguro (IDP) antes de poder acceder a la interfaz de usuario web de Unified Manager.

Antes de empezar

- Debe haber configurado la autenticación remota y verificado que la autenticación se ha realizado correctamente.
- Debe haber creado al menos un usuario remoto, o un grupo remoto, con la función Administrador de aplicaciones.
- El proveedor de identidades (IDP) debe ser compatible con Unified Manager y debe configurarse.
- Debe tener la URL y los metadatos de IDP.
- Debe tener acceso al servidor IDP.

Acerca de esta tarea

Después de habilitar la autenticación SAML de Unified Manager, los usuarios no pueden acceder a la interfaz gráfica de usuario hasta que el IDP se haya configurado con la información de host del servidor de Unified Manager. Por lo tanto, debe estar preparado para completar ambas partes de la conexión antes de iniciar el proceso de configuración. El IDP se puede configurar antes o después de configurar Unified Manager.

Solo los usuarios remotos tendrán acceso a la interfaz gráfica de usuario de Unified Manager después de habilitar la autenticación SAML. 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, los comandos de Unified Manager o las ZAPI.

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación SAML**.
2. Seleccione la casilla de verificación **Habilitar autenticación SAML**.

   Se mostrarán los campos necesarios para configurar la conexión IDP.

3. Introduzca el URI de IDP y los metadatos de IDP necesarios para conectar el servidor de Unified Manager al servidor de IDP.

   Si se puede acceder al servidor IDP directamente desde el servidor de Unified Manager, puede hacer clic en el botón **Fetch IDP Metadata** después de introducir el URI IDP para rellenar el campo IDP Metadata automáticamente.

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

   Ahora es posible configurar el servidor IDP con esta información.

5. Haga clic en **Guardar**.

   Aparece un cuadro de mensaje para confirmar que desea completar la configuración y reiniciar Unified Manager.

6. Haga clic en **Confirmar y cerrar sesión** y se reiniciará Unified Manager.

Resultados

La próxima vez que los usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager, deberán introducir sus credenciales en la página de inicio de sesión de IDP en lugar de en la página de inicio de sesión de Unified Manager.

Después de terminar

Si no se ha completado todavía, acceda a IDP e introduzca el URI del servidor de Unified Manager y los metadatos para completar la configuración.

Cuando se utiliza ADFS como proveedor de identidades, la interfaz gráfica de usuario de Unified Manager no cumple el tiempo de espera de ADFS y continúa funcionando hasta que se alcanza el tiempo de espera de la sesión de Unified Manager. Puede cambiar el tiempo de espera de la sesión de la GUI haciendo clic en **General** > **Configuración de características** > **tiempo de espera de inactividad**.

Requisitos del proveedor de identidades

Al configurar Unified Manager para que utilice un proveedor de identidades (IDP) para realizar la autenticación SAML de todos los usuarios remotos, debe tener en cuenta algunos ajustes de configuración necesarios para que la conexión a Unified Manager se haya realizado correctamente.

Debe introducir el URI y los metadatos de Unified Manager en el servidor IDP. Puede copiar esta información desde la página autenticación de Unified Manager SAML. Unified Manager se considera el proveedor de servicios (SP) en el estándar de lenguaje de marcado de aserción de seguridad (SAML).

Estándares de cifrado compatibles

- Estándar de cifrado avanzado (AES): AES-128 y AES-256
- Secure Hash Algorithm (SHA): SHA-1 y SHA-256

Proveedores de identidades validados

- Shibboleth
- Servicios de Federación de Active Directory (ADFS).

Requisitos de configuración de ADFS

- Debe definir tres reglas de reclamación en el siguiente orden que se requieren para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de parte confiable.

Regla de reclamación	Valor
SAM-account-name	ID del nombre
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Grupos de token — Nombre no cualificado	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Debe establecer el método de autenticación en "'autenticación de formularios'" o los usuarios pueden recibir un error al cerrar sesión en Unified Manager . Siga estos pasos:
  a. Abra la Consola de administración de ADFS.
  b. Haga clic en la carpeta Directivas de autenticación de la vista de árbol izquierda.
  c. En acciones a la derecha, haga clic en Editar directiva de autenticación primaria global.
  d. Establezca el método de autenticación de la intranet en "'autenticación de formularios'" en lugar del valor predeterminado "'autenticación de Windows'".
- En algunos casos, se rechaza iniciar sesión mediante el IDP cuando el certificado de seguridad de Unified Manager está firmado por CA. Existen dos soluciones alternativas para resolver este problema:
  - Siga las instrucciones identificadas en el vínculo para deshabilitar la comprobación de revocación en el servidor ADFS para la parte de confianza asociada al certificado de CA encadenada:

    "Desactive el control de revocación por confianza de parte de confianza"

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

Otros requisitos de configuración

- La desviación del reloj de Unified Manager se establece en 5 minutos, por lo que la diferencia de hora entre el servidor IDP y el servidor Unified Manager no puede ser superior a 5 minutos o se producirá un error en la autenticación.

Cambiar el proveedor de identidades utilizado para la autenticación SAML

Es posible cambiar el proveedor de identidades (IDP) que Unified Manager utiliza para autenticar usuarios remotos.

Antes de empezar

- Debe tener la URL y los metadatos de IDP.
- Debe tener acceso al IDP.

Acerca de esta tarea

El nuevo IDP se puede configurar antes o después de configurar Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación SAML**.
2. Introduzca el URI nuevo 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, puede hacer clic en el botón **Fetch IDP Metadata** después de introducir la URL del IDP para rellenar el campo IDP Metadata automáticamente.

3. Copie el URI de metadatos de Unified Manager o guarde los metadatos en un archivo de texto XML.
4. Haga clic en **Guardar configuración**.

   Aparece un cuadro de mensaje para confirmar que desea cambiar la configuración.

5. Haga clic en **Aceptar**.

Después de terminar

Acceda al nuevo IDP e introduzca el 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, deberán introducir sus credenciales en la nueva página de inicio de sesión de IDP en lugar de en la página de inicio de sesión de IDP anterior.

Deshabilitación de la autenticación SAML

Es posible deshabilitar la autenticación SAML cuando se desea dejar de autenticar usuarios remotos a través de un proveedor de identidad segura (IDP) para poder iniciar sesión en la interfaz de usuario web de Unified Manager. Cuando se deshabilita la autenticación SAML, los proveedores de servicios de directorio configurados, como Active Directory o LDAP, realizan la autenticación de inicio de sesión.

Acerca de esta tarea

Después de deshabilitar 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 puede deshabilitar la autenticación SAML con la consola de mantenimiento de Unified Manager si no tiene acceso a la interfaz gráfica de usuario.

Unified Manager se reinicia automáticamente después de deshabilitar la autenticación de SAML.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación SAML**.
2. Desactive la casilla de verificación **Activar autenticación SAML**.
3. Haga clic en **Guardar**.

   Aparece un cuadro de mensaje para confirmar que desea completar la configuración y reiniciar Unified Manager.

4. Haga clic en **Confirmar y cerrar sesión** y se reiniciará Unified Manager.

Resultados

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

Después de terminar

Acceda a IDP y elimine el URI del servidor de Unified Manager y los metadatos.

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.
NORMAL	Archivo inactivo, comprimido y almacenado en el sistema.
MANIPULADO	Archivo que ha sido comprometido por un usuario que ha editado el archivo manualmente.

Estado	Descripción
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.

Acerca de esta tarea

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.

Acerca de esta tarea

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.

Descripción de las ventanas de autenticación y cuadros de diálogo

Puede habilitar la autenticación LDAP desde la página Configuración/autenticación.

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, el nombre distintivo 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, el nombre distintivo 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, el nombre distintivo 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.

Página autenticación SAML

Es posible usar la página autenticación de SAML para configurar Unified Manager para autenticar usuarios remotos mediante SAML a través de un proveedor de identidad seguro (IDP) para que puedan iniciar sesión en la interfaz de usuario web de Unified Manager.

- Debe tener el rol de administrador de aplicaciones para crear o modificar la configuración de SAML.
- Debe haber configurado la autenticación remota.
- Debe haber configurado al menos un usuario remoto o un grupo remoto.

Después de configurar la autenticación remota y los usuarios remotos, puede seleccionar la casilla de comprobación Habilitar autenticación SAML para habilitar la autenticación mediante un proveedor de identidades seguro.

- **URI de IDP**

  El URI para acceder al IDP desde el servidor de Unified Manager. A continuación se enumeran los URI de ejemplo.

  URI de ejemplo de ADFS:

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

  Ejemplo de URI de Shibboleth:

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

- **Metadatos IDP**

  Los metadatos de IDP tienen formato XML.

  Si se puede acceder a la URL de IDP desde el servidor de Unified Manager, puede hacer clic en el botón **Fetch IDP Metadata** para rellenar este campo.

- **Sistema host (FQDN)**

  El nombre de dominio completo del sistema host de Unified Manager, tal como se define durante la instalación. Puede cambiar este valor si es necesario.

- **URI de 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.