Realizar tareas administrativas y de configuración

Active IQ Unified Manager 9.14

NetApp
November 12, 2024

Tabla de contenidos

Realizar tareas administrativas y de configuración

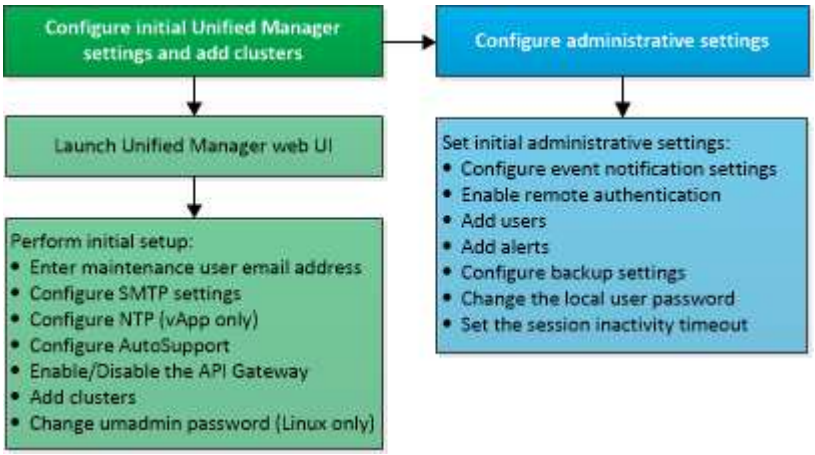
Configurando Active IQ Unified Manager

Después de instalar Active IQ Unified Manager (anteriormente Unified Manager de OnCommand), debe completar la configuración inicial (también llamada el primer asistente de experiencia) para acceder a la interfaz de usuario web de. Después, puede realizar otras tareas de configuración, como añadir clústeres, configurar la autenticación remota, añadir usuarios y añadir alertas.

Algunos de los procedimientos descritos en este manual son necesarios para completar la configuración inicial de su instancia de Unified Manager. Otros procedimientos son los ajustes de configuración recomendados que son útiles para configurar en la nueva instancia, o que son buenos saber acerca de antes de iniciar la supervisión regular de los sistemas ONTAP.

Descripción general de la secuencia de configuración

En el flujo de trabajo de configuración, se describen las tareas que deben realizarse para poder usar Unified Manager.



Acceder a la interfaz de usuario web de Unified Manager

Después de instalar Unified Manager, puede acceder a la interfaz de usuario web de para configurar Unified Manager de modo que pueda comenzar a supervisar los sistemas de ONTAP.

Lo que necesitará

- Si es la primera vez que accede a la interfaz de usuario web, debe iniciar sesión como el usuario de mantenimiento (o usuario umadmin para instalaciones de Linux).
- Si piensa permitir a los usuarios acceder a Unified Manager mediante el nombre corto en lugar de usar el nombre de dominio completo (FQDN) o la dirección IP, la configuración de red debe resolver este nombre corto con un FQDN válido.

- Si el servidor utiliza un certificado digital autofirmado, es posible que el explorador muestre una advertencia que indica que el certificado no es de confianza. Puede reconocer el riesgo de continuar con el acceso o instalar un certificado digital firmado por una entidad de certificación (CA) para la autenticación del servidor.

Pasos

1. Inicie la interfaz de usuario web de Unified Manager desde el explorador mediante la URL que se muestra al final de la instalación. La URL es la dirección IP o el nombre de dominio completo (FQDN) del servidor de Unified Manager.

   El enlace está en el siguiente formato `https://URL:`.

2. Inicie sesión en la interfaz de usuario web de Unified Manager con sus credenciales de usuario de mantenimiento.

> Si se realizan tres intentos consecutivos para iniciar sesión en la interfaz de usuario web en una hora, se bloqueará fuera del sistema y deberá ponerse en contacto con el administrador del sistema. Esto es aplicable únicamente para usuarios locales.

Realizando la configuración inicial de la interfaz de usuario web de Unified Manager

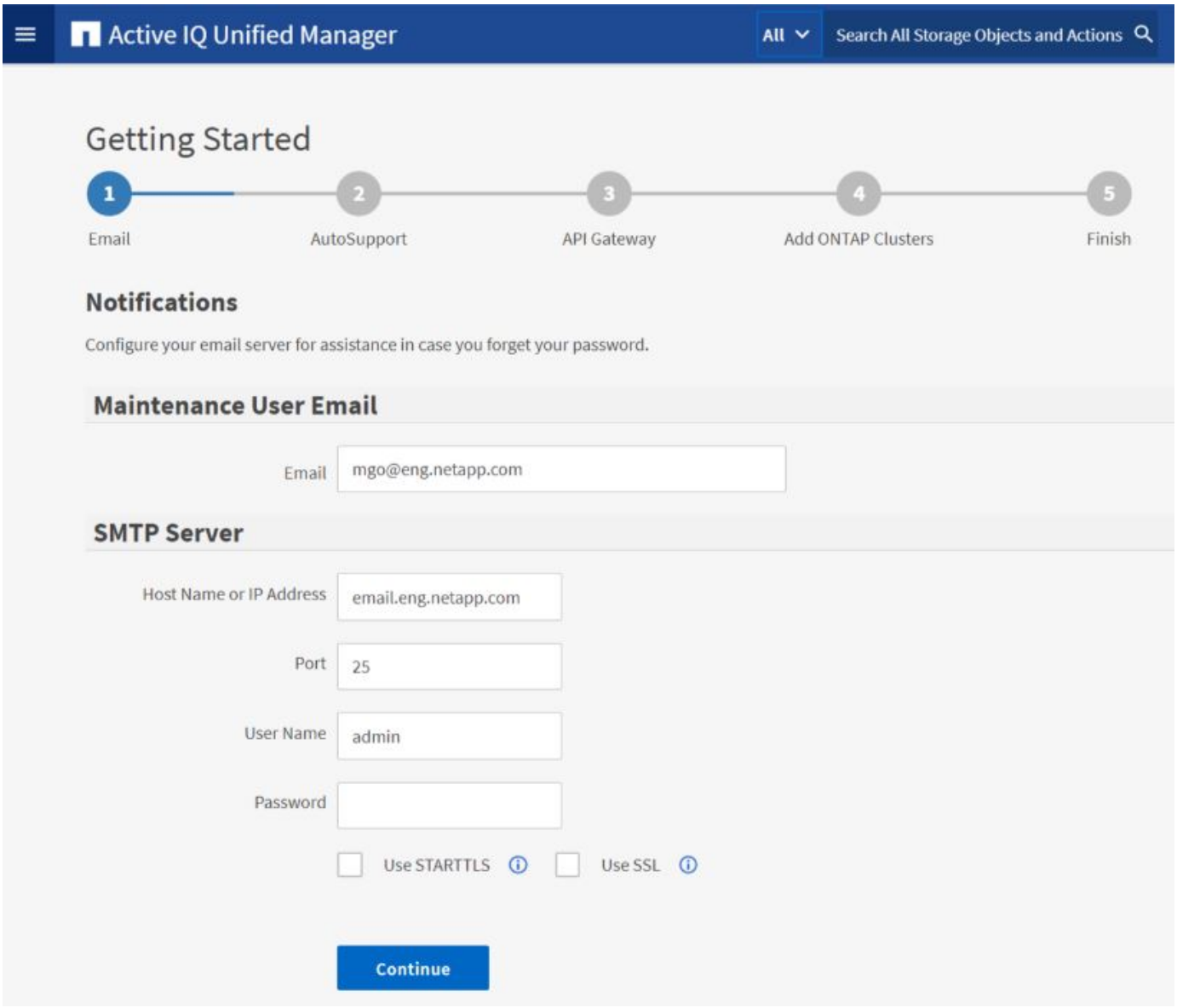
Para utilizar Unified Manager, primero es necesario configurar las opciones de configuración iniciales, incluido el servidor NTP, la dirección de correo electrónico del usuario de mantenimiento, el host del servidor SMTP y añadir clústeres de ONTAP.

Lo que necesitará

Debe haber realizado las siguientes operaciones:

- Inició la interfaz de usuario web de Unified Manager mediante la URL proporcionada después de la instalación
- Inició sesión con el nombre de usuario y la contraseña de mantenimiento (usuario umadmin para instalaciones Linux) creados durante la instalación

La página Active IQ Unified Manager Getting Started aparece solo cuando se accede por primera vez a la interfaz de usuario web. La siguiente página procede de una instalación en VMware.



Si desea cambiar alguna de estas opciones más adelante, puede seleccionar su opción en las opciones General del panel de navegación izquierdo de Unified Manager. Tenga en cuenta que la configuración de NTP es solo para instalaciones de VMware y se puede cambiar más adelante con la consola de mantenimiento de Unified Manager.

Pasos

1. En la página Active IQ Unified Manager Initial Setup, introduzca la dirección de correo electrónico de usuario de mantenimiento, el nombre de host del servidor SMTP y todas las opciones adicionales SMTP, y el servidor NTP (solo instalaciones VMware). A continuación, haga clic en **continuar**.

   Si ha seleccionado la opción **usar STARTTLS** o **usar SSL**, aparecerá una página de certificado después de hacer clic en el botón **continuar**. Compruebe los detalles del certificado y acepte el certificado para continuar con la configuración inicial de la interfaz de usuario web.

2. En la página AutoSupport, haga clic en **Acepto y continúe** para activar el envío de mensajes de AutoSupport desde Unified Manager a Active IQ de NetApp.

   Si necesita designar un proxy para proporcionar acceso a Internet con el fin de enviar contenido

AutoSupport, o si desea desactivar AutoSupport, utilice la opción **General** > **AutoSupport** de la interfaz de usuario web.

3. En los sistemas Red Hat y CentOS, cambie la contraseña de usuario umadmin de la cadena "'admin'" predeterminada a una cadena personalizada.
4. En la página Set up API Gateway, seleccione si desea utilizar la función API Gateway que permite a Unified Manager gestionar los clústeres de ONTAP que planea supervisar mediante API de REST de ONTAP. A continuación, haga clic en **continuar**.

   Puede activar o desactivar esta configuración más adelante en la interfaz de usuario web desde **General** > **Configuración de la función** > **puerta de enlace API**. Para obtener más información sobre las API, consulte "Primeros pasos con API de REST de Active IQ Unified Manager".

5. Añada los clústeres que desea que Unified Manager administre y haga clic en **Siguiente**. Para cada clúster que vaya a administrar, debe tener el nombre de host o la dirección IP de administración del clúster (IPv4 o IPv6) junto con las credenciales de nombre de usuario y contraseña; el usuario debe tener el rol «'admin'».

   Este paso es opcional. Puede agregar clústeres más adelante en la interfaz de usuario web desde **Storage Management** > **Cluster Setup**.

6. En la página Summary (Resumen), compruebe que todos los ajustes son correctos y haga clic en **Finish** (Finalizar).

Se cierra la página Getting Started y se muestra la página Unified Manager Dashboard.

Añadir clústeres

Puede añadir un clúster a la Active IQ Unified Manager para poder supervisar el clúster. Esto incluye la capacidad de obtener información del clúster, como el estado, la capacidad, el rendimiento y la configuración del clúster, para poder encontrar y resolver cualquier problema que pueda ocurrir.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe tener la siguiente información:
  - Unified Manager admite clústeres de ONTAP en las instalaciones, ONTAP Select, Cloud Volumes ONTAP.
  - El nombre de host o la dirección IP de administración del clúster

    El nombre de host es el nombre FQDN o el nombre corto que Unified Manager utiliza para conectarse con el clúster. El nombre de host debe resolver a la dirección IP de administración del clúster.

    La dirección IP de administración del clúster debe ser el LIF de gestión del clúster de la máquina virtual de almacenamiento (SVM) administrativa. Si utiliza un LIF de gestión de nodos, la operación da error.

  - El clúster de debe ejecutar el software ONTAP versión 9.1 o posterior.
  - Nombre de usuario y contraseña del administrador de ONTAP

Esta cuenta debe tener el rol *admin* con acceso a aplicaciones establecido en *ontapi*, *Console* y *http*.

- El número de puerto para conectarse al clúster mediante el protocolo HTTPS (por lo general, puerto 443)
- Tiene los certificados necesarios:

  Certificado SSL (HTTPS): Este certificado es propiedad de Unified Manager. Se genera un certificado SSL (HTTPS) autofirmado predeterminado con una instalación nueva de Unified Manager. NetApp recomienda actualizarlo a certificado firmado por CA para mejorar la seguridad. Si el certificado de servidor caduca, debe volver a regenerarlo y reiniciar Unified Manager para que los servicios incorporen el nuevo certificado. Para obtener más información sobre la regeneración de certificados SSL, consulte "Generar un certificado de seguridad HTTPS".

  Certificado EMS: Este certificado es propiedad de Unified Manager. Se usa durante la autenticación de notificaciones EMS que se reciben de ONTAP.

  Certificados para la comunicación mutua con TLS: Se utiliza durante la comunicación mutua con TLS entre Unified Manager y ONTAP. La autenticación basada en certificados está habilitada para un clúster de acuerdo con la versión de ONTAP. Si el clúster que ejecuta la versión de ONTAP es inferior a la versión 9.5, la autenticación basada en certificados no está habilitada.

  La autenticación basada en certificado no se habilita automáticamente para un clúster, si va a actualizar una versión anterior de Unified Manager. Sin embargo, puede habilitarla mediante la modificación y el guardado de los detalles del clúster. Si el certificado caduca, debe regenerarlo para incorporar el nuevo certificado. Para obtener más información sobre la visualización y regeneración del certificado, consulte "Editar clústeres".

  - Puede añadir un clúster desde la interfaz de usuario web y la autenticación basada en certificado se habilita automáticamente.
  - Puede añadir un clúster mediante la CLI de Unified Manager, la autenticación basada en certificado no está habilitada de forma predeterminada. Si se añade un clúster mediante la CLI de Unified Manager, se deberá editar el clúster mediante la interfaz de usuario de Unified Manager. Puede "Comandos de CLI de Unified Manager compatibles" ver para añadir un clúster mediante la CLI de Unified Manager.
  - Si la autenticación basada en certificados está habilitada para un clúster, y realiza el backup de Unified Manager desde un servidor y la restauración a otro servidor de Unified Manager donde se cambia el nombre de host o la dirección IP, la supervisión del clúster puede fallar. Para evitar el error, edite y guarde los detalles del clúster. Para obtener más información sobre la edición de detalles del clúster, consulte "Editar clústeres".

+ **Certificados de clúster**: Este certificado es propiedad de ONTAP. No es posible añadir un clúster a Unified Manager con un certificado caducado y si el certificado ya ha caducado, debe volver a generarlo antes de añadir el clúster. Para obtener información sobre la generación de certificados, consulte el artículo de la base de conocimientos (KB) "Cómo renovar un certificado autofirmado de ONTAP en la interfaz de usuario de System Manager" .

- Debe tener espacio suficiente en el servidor de Unified Manager. Se le impide agregar un clúster al servidor cuando ya se consume más del 90% del espacio en el directorio de la base de datos.

Para una configuración de MetroCluster, debe añadir los clústeres local y remoto, y los clústeres deben configurarse correctamente.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Cluster Setup**.
2. En la página Cluster Setup, haga clic en **Add**.
3. En el cuadro de diálogo Add Cluster, especifique los valores requeridos, como el nombre de host o la dirección IP del clúster, el nombre de usuario, la contraseña y el número de puerto.

   Es posible cambiar la dirección IP de gestión del clúster de IPv6 a IPv4 o de IPv4 a IPv6. La nueva dirección IP se refleja en la cuadrícula del clúster y en la página de configuración del clúster una vez completado el siguiente ciclo de supervisión.
4. Haga clic en **Enviar**.
5. En el cuadro de diálogo autorizar host, haga clic en **Ver certificado** para ver la información del certificado sobre el clúster.
6. Haga clic en **Sí**.

   Después de guardar los detalles del clúster, puede ver el certificado para la comunicación TLS mutua para un clúster.

   Si la autenticación basada en certificados no está habilitada, Unified Manager comprueba el certificado solo cuando se añade el clúster inicialmente. Unified Manager no comprueba el certificado para cada llamada API a ONTAP.

Después de detectar todos los objetos de un clúster nuevo, Unified Manager comienza a recopilar datos históricos de rendimiento de los 15 días anteriores. Estas estadísticas se recopilan mediante la funcionalidad de recogida de continuidad de datos. Esta función le proporciona más de dos semanas de información sobre el rendimiento de un clúster inmediatamente después de añadir. Una vez completado el ciclo de recogida de continuidad de datos, se recogen datos de rendimiento del clúster en tiempo real, de forma predeterminada, cada cinco minutos.

Dado que la recogida de 15 días de datos de rendimiento requiere un uso intensivo de la CPU, se sugiere escalonar la adición de nuevos clústeres de manera que las encuestas de recogida de continuidad de datos no se ejecuten en demasiados clústeres al mismo tiempo. Además, si reinicia Unified Manager durante el período de recogida de continuidad de datos, la recogida se detiene y verá vacíos en los gráficos de rendimiento correspondientes al periodo que falta.

Si recibe un mensaje de error que no puede añadir el clúster, compruebe si los relojes de los dos sistemas no están sincronizados y la fecha de inicio del certificado HTTPS de Unified Manager es posterior a la fecha del clúster. Debe asegurarse de que los relojes se sincronicen con NTP o un servicio similar.

Información relacionada

"Instalar una CA firmada y devolvió un certificado HTTPS"

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 se rellena previamente con la dirección «ActiveIQUnifiedManager@localhost.com», debe cambiarla a una dirección de correo electrónico real y funcional para asegurarse de que todas las notificaciones de correo electrónico se envíen 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: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Usando la notación LDAP apropiada) • 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).

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. b. Especifique el nombre completo base del 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**.

Si selecciona…	Realice lo siguiente…
OpenLDAP	a. Introduzca el nombre distintivo del enlace y la contraseña de enlace. b. Especifique el nombre completo base del 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**.
Otros	a. Introduzca el nombre distintivo del enlace y la contraseña de enlace. b. Especifique el nombre completo base del 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**. c. Especifique la versión de protocolo LDAP que admite el servidor de autenticación. 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**. b. En el área servidores de autenticación, haga clic en **Agregar**. c. En el cuadro de diálogo Add Authentication Server, introduzca el nombre o la dirección IP de autenticación (IPv4 o IPv6) del servidor. d. En el cuadro de diálogo autorizar host, haga clic en Ver certificado. e. En el cuadro de diálogo Ver certificado, compruebe la información del certificado y, a continuación, haga clic en **Cerrar**. f. 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	a. Desactive la opción **utilizar conexión segura**. b. En el área servidores de autenticación, haga clic en **Agregar**. 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. 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 muévalo 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**.

Cambiando la contraseña de usuario local

Es posible cambiar la contraseña de inicio de sesión de usuario local para evitar riesgos potenciales para la seguridad.

Lo que necesitará

Debe iniciar sesión como usuario local.

Las contraseñas del usuario de mantenimiento y de los usuarios remotos no se pueden cambiar mediante estos pasos. Para cambiar una contraseña de usuario remoto, póngase en contacto con el administrador de contraseñas. Para cambiar la contraseña de usuario de mantenimiento, consulte "Mediante la consola de mantenimiento".

Pasos

1. Inicie sesión en Unified Manager.
2. En la barra de menús superior, haga clic en el icono de usuario y, a continuación, haga clic en **Cambiar contraseña**.

   La opción **Cambiar contraseña** no se muestra si es un usuario remoto.

3. En el cuadro de diálogo Change Password, introduzca la contraseña actual y la contraseña nueva.
4. Haga clic en **Guardar**.

Si Unified Manager se configura en una configuración de alta disponibilidad, debe cambiar la contraseña en el segundo nodo de la configuración. Ambas instancias deben tener la misma contraseña.

Configurar el tiempo de espera de inactividad de la sesión

Es posible especificar el valor de tiempo de espera de inactividad para Unified Manager a fin de que la sesión se finalice automáticamente después de un cierto periodo de tiempo. De manera predeterminada, el tiempo de espera está configurado en 4,320 minutos (72 horas).

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Esta configuración afecta a todas las sesiones de usuario que han iniciado sesión.

Esta opción no está disponible si tiene habilitada la autenticación del lenguaje de marcado de aserción de seguridad (SAML).

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Configuración de funciones**.
2. En la página **Configuración de característica**, especifique el tiempo de espera de inactividad seleccionando una de las siguientes opciones:

Si desea…	Realice lo siguiente…
No tener tiempo de espera configurado para que la sesión nunca se cierre automáticamente	En el panel **tiempo de espera de inactividad**, mueva el botón deslizante hacia la izquierda (OFF) y haga clic en **aplicar**.
Establezca un número específico de minutos como valor de tiempo de espera	En el panel **tiempo de espera de inactividad**, mueva el botón deslizante hacia la derecha (Activado), especifique el valor de tiempo de espera de inactividad en minutos y haga clic en **aplicar**.

Cambie el nombre de host de Unified Manager

En algún momento, es posible que desee cambiar el nombre de host del sistema en el que instaló Unified Manager. Por ejemplo, quizás desee cambiar el nombre del host para identificar más fácilmente los servidores de Unified Manager por tipo, grupo de trabajo o grupo de clústeres supervisado.

Los pasos necesarios para cambiar el nombre de host varían en función de si Unified Manager se ejecuta en un servidor VMware ESXi, en un servidor Red Hat o CentOS Linux o en un servidor Microsoft Windows.

Cambiar el nombre de host de la aplicación virtual de Unified Manager

El host de red se asigna un nombre cuando se pone en marcha el dispositivo virtual de Unified Manager por primera vez. Es posible cambiar el nombre de host después de la implementación. Si cambia el nombre de host, también debe volver a generar el certificado HTTPS.

Lo que necesitará

Debe iniciar sesión en Unified Manager como usuario de mantenimiento o tener asignado la función de administrador de aplicaciones para realizar estas tareas.

Puede usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web de Unified Manager. Si configuró una dirección IP estática para la red durante la implementación, debería haber designado un nombre para el host de red. Si configuró la red mediante DHCP, el nombre de host debe tomarse del DNS. Si DHCP o DNS no están configurados correctamente, el nombre de host "'Unified Manager'" se asigna y se asocia automáticamente con el certificado de seguridad.

Independientemente de cómo se asignó el nombre de host, si cambia el nombre de host y piensa usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debe generar un nuevo certificado de seguridad.

Si accede a la interfaz de usuario web mediante la dirección IP del servidor en lugar del nombre de host, no es necesario generar un nuevo certificado si cambia el nombre de host. Sin embargo, se recomienda actualizar el certificado de forma que el nombre de host del certificado coincida con el nombre de host real.

Si cambia el nombre de host en Unified Manager, debe actualizar manualmente el nombre de host en OnCommand Workflow Automation (WFA). El nombre de host no se actualiza automáticamente en WFA.

El nuevo certificado no se aplicará hasta que se reinicie la máquina virtual de Unified Manager.

Pasos

1. Genere un certificado de seguridad HTTPS

   Si desea usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debe volver a generar el certificado HTTPS para asociarlo con el nuevo nombre de host.

2. Reinicie la máquina virtual de Unified Manager

   Después de volver a generar el certificado HTTPS, debe reiniciar la máquina virtual de Unified Manager.

Generar un certificado de seguridad HTTPS

Cuando se instala Active IQ Unified Manager por primera vez, se instala un certificado HTTPS predeterminado. Es posible generar un nuevo certificado de seguridad HTTPS que reemplace el certificado existente.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Puede haber varios motivos para regenerar el certificado, como si desea tener mejores valores para el nombre distintivo (DN) o si desea un tamaño de clave mayor, o un período de caducidad más largo o si el certificado actual ha caducado.

Si no tiene acceso a la interfaz de usuario web de Unified Manager, puede volver a generar el certificado HTTPS con los mismos valores mediante la consola de mantenimiento. Al regenerar los certificados, puede definir el tamaño de la clave y la duración de validez de la clave. Si usa `Reset Server Certificate` la opción de la consola de mantenimiento, se creará un nuevo certificado HTTPS que es válido durante 397 días. Este certificado tendrá una clave RSA de tamaño 2048 bits.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.
2. Haga clic en **regenerar certificado HTTPS**.

   Aparece el cuadro de diálogo Regenerate HTTPS Certificate.

3. Seleccione una de las siguientes opciones en función de cómo desee generar el certificado:

Si desea…	**Realice lo siguiente…**
Regenere el certificado con los valores actuales	Haga clic en la opción **Regenerate usando atributos de certificado actuales**.

Si desea…	Realice lo siguiente…
Genere el certificado con diferentes valores	Haga clic en la opción **Actualizar atributos de certificado actuales**. Los campos Nombre común y nombres alternativos utilizarán los valores del certificado existente si no introduce nuevos valores. El "'Nombre común'" debe ajustarse al FQDN del host. Los demás campos no requieren valores, pero puede introducir valores, por ejemplo, PARA EL CORREO ELECTRÓNICO, LA EMPRESA, EL DEPARTAMENTO, Ciudad, provincia y país si desea que esos valores se rellenen en el certificado. También puede seleccionar EL TAMAÑO de CLAVE disponible (el algoritmo de clave es "'RSA'"). Y PERÍODO DE VALIDEZ. • Los valores permitidos para el tamaño de clave son `2048`, `3072` y `4096`. • Los períodos de validez son como mínimo de 1 día a un máximo de 36500 días. Aunque se permita un período de validez de 36500 días, se recomienda que utilice un período de validez de no más de 397 días o 13 meses. Como si selecciona un periodo de validez de más de 397 días y piensa exportar una CSR para este certificado y conseguir que la firme una CA bien conocida, la validez del certificado firmado que la CA le devolvió se reducirá a 397 días. • Puede seleccionar la casilla de verificación “excluir información de identificación local (p. ej., localhost)” si desea quitar la información de identificación local del campo nombres alternativos del certificado. Cuando se selecciona esta casilla de verificación, sólo se utiliza lo que se introduce en el campo nombres alternativos. Cuando se deja en blanco, el certificado resultante no tendrá ningún campo nombres alternativos.

4. Haga clic en **Sí** para regenerar el certificado.
5. Reinicie el servidor de Unified Manager para que el nuevo certificado surta efecto.
6. Compruebe la información del nuevo certificado; para ello, consulte el certificado HTTPS.

Reiniciar la máquina virtual de Unified Manager

Puede reiniciar el equipo virtual desde la consola de mantenimiento de Unified Manager. Debe reiniciar después de generar un nuevo certificado de seguridad o si hay un problema con la máquina virtual.

Lo que necesitará

El dispositivo virtual está encendido.

Ha iniciado sesión en la consola de mantenimiento como usuario de mantenimiento.

También puede reiniciar la máquina virtual desde vSphere mediante la opción **Restart Guest**. Para obtener más información, consulte la documentación de VMware.

Pasos

1. Acceda a la consola de mantenimiento.
2. Seleccione **Configuración del sistema** > **Reiniciar Virtual Machine**.

Cambiar el nombre de host de Unified Manager en sistemas Linux

En algún momento, puede que desee cambiar el nombre de host del equipo Red Hat Enterprise Linux o CentOS en el que ha instalado Unified Manager. Por ejemplo, quizás desee cambiar el nombre del host para identificar más fácilmente los servidores de Unified Manager por tipo, grupo de trabajo o grupo de clústeres supervisado cuando enumere las máquinas Linux.

Lo que necesitará

Debe tener acceso de usuario raíz al sistema Linux en el que está instalado Unified Manager.

Puede usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web de Unified Manager. Si configuró una dirección IP estática para la red durante la implementación, debería haber designado un nombre para el host de red. Si configuró la red mediante DHCP, el nombre de host debe tomarse del servidor DNS.

Independientemente de cómo se asignó el nombre de host, si cambia el nombre de host y piensa usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debe generar un nuevo certificado de seguridad.

Si accede a la interfaz de usuario web mediante la dirección IP del servidor en lugar del nombre de host, no es necesario generar un nuevo certificado si cambia el nombre de host. Sin embargo, se recomienda actualizar el certificado de forma que el nombre de host del certificado coincida con el nombre de host real. El nuevo certificado no se aplicará hasta que se reinicie el equipo Linux.

Si cambia el nombre de host en Unified Manager, debe actualizar manualmente el nombre de host en OnCommand Workflow Automation (WFA). El nombre de host no se actualiza automáticamente en WFA.

Pasos

1. Inicie sesión como usuario raíz en el sistema Unified Manager que desee modificar.
2. Detenga el software Unified Manager y el software MySQL asociado introduciendo el comando siguiente:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Cambie el nombre de host mediante el comando Linux `hostnamectl`:

   ```
   hostnamectl set-hostname new_FQDN

   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Regenere el certificado HTTPS para el servidor:

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. Reinicie el servicio de red:

   ```
   systemctl restart NetworkManager.service
   ```

6. Después de reiniciar el servicio, compruebe si el nuevo nombre de host puede hacer ping a sí mismo:

   ```
   ping new_hostname

   ping nuhost
   ```

   Este comando debe devolver la misma dirección IP que se configuró con anterioridad para el nombre de host original.

7. Después de completar y verificar el cambio de nombre de host, reinicie Unified Manager introduciendo el comando siguiente:

   ```
   systemctl start mysqld ocie ocieau
   ```

Habilitar y deshabilitar la gestión del almacenamiento basada en políticas

A partir de Unified Manager 9.7, puede aprovisionar cargas de trabajo de almacenamiento (volúmenes y LUN) en los clústeres de ONTAP y gestionar esas cargas de trabajo en función de los niveles de servicio de rendimiento asignados. Esta funcionalidad es similar a crear cargas de trabajo en ONTAP System Manager y asociar políticas de calidad de servicio, pero cuando se aplica mediante Unified Manager, puede aprovisionar y gestionar cargas de trabajo en todos los clústeres que supervisa la instancia de Unified Manager.

Debe tener la función Administrador de aplicaciones.

Esta opción está habilitada de forma predeterminada, pero puede deshabilitarla si no se desean aprovisionar y gestionar cargas de trabajo mediante Unified Manager.

Cuando está activada, esta opción proporciona muchos elementos nuevos en la interfaz de usuario:

Nuevo contenido	Ubicación
Una página para aprovisionar nuevas cargas de trabajo	Disponible en **tareas comunes** > **aprovisionamiento**
Página para crear políticas de nivel de servicio de rendimiento	Disponible en **Ajustes** > **políticas** > **niveles de servicio de rendimiento**
Página para crear políticas de eficiencia del almacenamiento de rendimiento	Disponible en **Ajustes** > **políticas** > **eficiencia del almacenamiento**
Paneles que describen el rendimiento de su carga de trabajo actual y las IOPS de su carga de trabajo	Disponible en la consola

Consulte la ayuda en línea del producto para obtener más información sobre estas páginas y sobre esta función.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Configuración de funciones**.
2. En la página **Configuración de función**, desactive o habilite la administración del almacenamiento basada en políticas eligiendo una de las siguientes opciones:

Si desea…	Realice lo siguiente…
Desactive la administración del almacenamiento basada en políticas	En el panel **Administración de almacenamiento basada en directivas**, mueva el botón deslizante hacia la izquierda.
Gestión del almacenamiento basada en normativas	En el panel **Administración de almacenamiento basada en directivas**, mueva el botón deslizante hacia la derecha.

Configuración de backup de Unified Manager

Puede configurar la funcionalidad de backup en Unified Manager mediante un conjunto de pasos de configuración que se realizarán en los sistemas host y en la consola de mantenimiento.

Para obtener información sobre los pasos de configuración, consulte "Gestión de operaciones de backup y restauración".

Gestión de la configuración de funciones

La página Configuración de la función permite habilitar y deshabilitar funciones específicas en Active IQ Unified Manager. Esto incluye la creación y gestión de objetos de almacenamiento basados en políticas, la habilitación de la puerta de enlace de la API y el banner de inicio de sesión, la carga de scripts para gestionar alertas, el

establecimiento de un tiempo de sesión de la interfaz de usuario web basado en el tiempo de inactividad y la deshabilitación de la recepción de eventos de la plataforma de Active IQ.

> La página Configuración de funciones sólo está disponible para usuarios con la función Administrador de aplicaciones.

Para obtener más información sobre la carga de scripts, consulte "Habilitar y deshabilitar la carga de scripts".

Permitir la gestión del almacenamiento basada en políticas

La opción **Gestión de almacenamiento basada en normativas** permite la administración del almacenamiento en función de los objetivos de nivel de servicio (SLO). Esta opción está habilitada de forma predeterminada.

Al activar esta función, puede aprovisionar cargas de trabajo de almacenamiento en los clústeres de ONTAP añadidos a la instancia de Active IQ Unified Manager y gestionar estas cargas de trabajo en función de los niveles de servicio de rendimiento y las políticas de eficiencia del almacenamiento asignados.

Puede activar o desactivar esta función en **General** > **Configuración de funciones** > **Administración de almacenamiento basada en directivas**. Al activar esta función, están disponibles las siguientes páginas para su funcionamiento y supervisión:

- Aprovisionamiento (aprovisionamiento de carga de trabajo de almacenamiento)
- **Políticas** > **niveles de servicio de rendimiento**
- **Políticas** > **eficiencia del almacenamiento**
- Columna Workloads by Performance Service Level en la página Clusters Setup
- Panel de rendimiento de la carga de trabajo en **Dashboard**

Puede utilizar las pantallas para crear niveles de servicio de rendimiento y políticas de eficiencia del almacenamiento, así como para aprovisionar las cargas de trabajo de almacenamiento. También puede supervisar las cargas de trabajo de almacenamiento que cumplen los niveles de servicio de rendimiento asignados, así como las no conformes. El panel IOPS de carga de trabajo y rendimiento de cargas de trabajo también le permite evaluar la capacidad y el rendimiento (IOPS) totales, disponibles y utilizados de los clústeres en todo el centro de datos en función de las cargas de trabajo de almacenamiento que se aprovisionen en ellos.

Después de activar esta función, puede ejecutar las API REST de Unified Manager para realizar algunas de estas funciones desde **barra de menús** > **botón de ayuda** > **Documentación de API** > **proveedor de almacenamiento**. También es posible introducir el nombre de host o la dirección IP y la URL para acceder a la página de API DE REST en el formato https://<hostname>/docs/api/

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

Habilitar API Gateway

La función de puerta de enlace de API permite a Active IQ Unified Manager ser un único plano de control desde el cual puede gestionar varios clústeres de ONTAP sin iniciar sesión de forma individual.

Puede habilitar esta función en las páginas de configuración que aparecen cuando se inicia sesión por primera vez en Unified Manager. También puede activar o desactivar esta función en **General** > **Configuración de funciones** > **Puerta de enlace API**.

Las API DE REST de Unified Manager son diferentes de las API de REST de ONTAP. No todas las funcionalidades de las API DE REST de ONTAP se pueden obtener usando LAS API DE REST de Unified Manager. Sin embargo, si tiene un requisito empresarial específico de acceso a las API de ONTAP para gestionar funciones específicas que no se exponen a Unified Manager, puede habilitar la función API Gateway y ejecutar las API de ONTAP. La puerta de enlace actúa como proxy para tunear las solicitudes de API manteniendo las solicitudes de encabezado y cuerpo en el mismo formato que en las API de ONTAP. Puede usar sus credenciales de Unified Manager y ejecutar las API específicas para acceder a los clústeres de ONTAP y gestionarlos sin aprobar las credenciales de un clúster individual. Unified Manager se realiza como un único punto de gestión para ejecutar las API en los clústeres de ONTAP gestionados por la instancia de Unified Manager. La respuesta que devuelven las API es la misma que la respuesta que devuelven las respectivas API DE REST de ONTAP ejecutadas directamente desde ONTAP.

Después de activar esta función, puede ejecutar las API REST de Unified Manager desde **barra de menús** > **botón de ayuda** > **Documentación de API** > **categoría de puerta de enlace**. También es posible introducir el nombre de host o la dirección IP y la URL para acceder a la página API DE REST en formato `https://<hostname>/docs/api/`

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

Especificación del tiempo de espera de inactividad

Puede especificar el valor de tiempo de espera de inactividad para Active IQ Unified Manager. Tras una inactividad de la hora especificada, la aplicación se cierra automáticamente. Esta opción está habilitada de forma predeterminada.

Puede desactivar esta función o modificar el tiempo desde **General** > **Configuración de función** > **tiempo de espera de inactividad**. Una vez que active esta función, deberá especificar el límite de tiempo de inactividad (en minutos) en el campo **LOGOUT AFTER**, después de lo cual el sistema cerrará automáticamente la sesión. El valor predeterminado es 4320 minutos (72 horas).

Esta opción no está disponible si tiene habilitada la autenticación del lenguaje de marcado de aserción de seguridad (SAML).

Habilitar los eventos del portal de Active IQ

Puede especificar si desea habilitar o deshabilitar los eventos del portal Active IQ. Este ajuste permite al portal de Active IQ detectar y mostrar eventos adicionales sobre la configuración del sistema, el cableado, etc. Esta opción está habilitada de forma predeterminada.

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

Puede activar o desactivar esta función en **General** > **Configuración de funciones** > **Eventos del portal**

Active IQ. En los sitios sin acceso a la red externa, debe cargar las reglas manualmente desde **Storage Management** > **Event Setup** > **Upload Rules**.

Esta función está habilitada de forma predeterminada. Al deshabilitar esta función, se detienen los eventos de Active IQ no se detectan o se muestran en Unified Manager. Cuando está deshabilitada, al habilitar esta función, Unified Manager puede recibir los eventos de Active IQ en un clúster a una hora predefinida de 00:15 para esa zona horaria del clúster.

Activación y desactivación de la configuración de seguridad para cumplir las normativas

Mediante el botón **Personalizar** del panel **Panel de seguridad** de la página Configuración de características, puede habilitar o deshabilitar los parámetros de seguridad para la supervisión de cumplimiento en Unified Manager.

La configuración que se habilita o se deshabilita en esta página rige el estado de cumplimiento general de los clústeres y las máquinas virtuales de almacenamiento en Unified Manager. Según las selecciones, las columnas correspondientes se pueden ver en la vista **Seguridad: Todos los clústeres** de la página de inventario Clusters y la vista **Seguridad: Todos los equipos virtuales de almacenamiento** de la página de inventario de máquinas virtuales de almacenamiento.

Solo los usuarios con rol de administrador pueden editar esta configuración.

Los criterios de seguridad de los clústeres de ONTAP, las máquinas virtuales de almacenamiento y los volúmenes se evalúan según las recomendaciones definidas en la "Guía de fortalecimiento de la seguridad para NetApp ONTAP 9". El panel Seguridad de la consola y la página Seguridad muestran el estado de cumplimiento de normativas de seguridad predeterminado de los clústeres, las máquinas virtuales de almacenamiento y los volúmenes. Asimismo, se generan eventos de seguridad y se habilitan las acciones de gestión para los clústeres y las máquinas virtuales de almacenamiento que tienen infracciones de seguridad.

Personalización de los ajustes de seguridad

Para personalizar la configuración para fines de supervisión de cumplimiento según corresponda a su entorno de ONTAP, siga estos pasos:

Pasos

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

   Los parámetros de cumplimiento de normativas de seguridad que se habilitan o deshabilitar pueden afectar directamente a las vistas de seguridad predeterminadas, los informes y los informes programados en las pantallas Clusters and Storage VMs. Si ha cargado un informe de Excel desde estas pantallas antes de modificar los parámetros de seguridad, es posible que los informes de Excel descargados estén defectuosos.

2. Para activar o desactivar la configuración personalizada de los clústeres de ONTAP, seleccione la configuración general necesaria en **clúster**. Para obtener información sobre las opciones para personalizar el cumplimiento del clúster, consulte "Categorías de cumplimiento de clusters".
3. Para activar o desactivar la configuración personalizada de los equipos virtuales de almacenamiento, seleccione la configuración general necesaria en **Storage VM**. Para obtener más información acerca de las opciones para personalizar el cumplimiento de las VM de almacenamiento, consulte "Categorías de cumplimiento de normativas para máquinas virtuales de almacenamiento".

Personalización de los ajustes de AutoSupport y autenticación

En la sección **Configuración de AutoSupport**, puede especificar si se va a utilizar el transporte HTTPS para enviar mensajes AutoSupport desde ONTAP.

En la sección **Configuración de autenticación**, puede habilitar alertas de Unified Manager que se elevarán para el usuario administrador de ONTAP predeterminado.

Habilitar y deshabilitar la carga de scripts

La capacidad de cargar scripts en Unified Manager y ejecutarlas está habilitada de forma predeterminada. Si la organización no desea permitir esta actividad debido a motivos de seguridad, puede desactivar esta funcionalidad.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Configuración de funciones**.
2. En la página **Configuración de característica**, desactive o habilite la secuencia de comandos eligiendo una de las siguientes opciones:

Si desea…	Realice lo siguiente…
Desactivar scripts	En el panel **carga de secuencia de comandos**, mueva el botón deslizante hacia la izquierda.
Activar scripts	En el panel **carga de secuencia de comandos**, mueva el botón deslizante hacia la derecha.

Adición de un banner de inicio de sesión

Al añadir un banner de inicio de sesión, su organización puede mostrar cualquier información, como, por ejemplo, quién puede acceder al sistema y los términos y condiciones de uso durante el inicio de sesión y el cierre de sesión.

Cualquier usuario, como operadores de almacenamiento o administradores, puede ver la ventana emergente de este banner de inicio de sesión durante el inicio de sesión, el cierre de sesión y el tiempo de espera de la sesión.

Mediante la consola de mantenimiento

Puede utilizar la consola de mantenimiento para configurar los ajustes de red, configurar y gestionar el sistema donde está instalado Unified Manager y realizar otras tareas de mantenimiento que le ayuden a evitar y solucionar los posibles problemas.

Qué funcionalidad proporciona la consola de mantenimiento

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

Según el sistema operativo en el que instaló Unified Manager, la consola de mantenimiento incorpora las siguientes funciones:

- Solucione cualquier problema que pueda haber con su dispositivo virtual, especialmente si la interfaz web de Unified Manager no está disponible
- Actualice a las versiones más recientes de Unified Manager
- Genere paquetes de soporte para su envío al soporte técnico
- Configure los ajustes de red
- Cambie la contraseña del usuario de mantenimiento
- Conéctese a un proveedor de datos externo para enviar estadísticas de rendimiento
- Cambie la recopilación de datos de rendimiento interna
- Restaure las opciones de configuración y base de datos de Unified Manager desde una versión de backup anterior.

Lo que hace el usuario de mantenimiento

El usuario de mantenimiento se crea durante la instalación de Unified Manager en un sistema Red Hat Enterprise Linux o CentOS. El nombre de usuario de mantenimiento es el usuario "'umadmin'". El usuario de mantenimiento tiene la función Administrador de aplicaciones en la interfaz de usuario web, y ese usuario puede crear usuarios posteriores y asignarles roles.

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

Capacidades de diagnóstico del usuario

El objetivo del acceso de diagnóstico es habilitar el soporte técnico para ayudarle a solucionar problemas, y solo se debe utilizar cuando lo indique el soporte técnico.

El usuario de diagnóstico puede ejecutar comandos de nivel de sistema operativo cuando así lo indique el soporte técnico, con fines de solución de problemas.

Acceso a la consola de mantenimiento

Si la interfaz de usuario de Unified Manager no está en funcionamiento o si necesita ejecutar funciones que no están disponibles en la interfaz de usuario, puede acceder a la consola de mantenimiento para gestionar el sistema de Unified Manager.

Lo que necesitará

Debe haber instalado y configurado Unified Manager.

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

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

Paso

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

En este sistema operativo…	Siga estos pasos…
VMware	a. Mediante Secure Shell, conéctese a la dirección IP o al nombre de dominio completo del dispositivo virtual de Unified Manager. b. Inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña de mantenimiento.
Linux	a. Mediante Secure Shell, conéctese a la dirección IP o al nombre de dominio completo del sistema Unified Manager. b. Inicie sesión en el sistema con el nombre y la contraseña del usuario de mantenimiento (umadmin). c. Introduzca el comando `maintenance_console` y pulse Intro.
Windows	a. Inicie sesión en el sistema Unified Manager con credenciales de administrador. b. Inicie PowerShell como administrador de Windows. c. Introduzca el comando `maintenance_console` y pulse Intro.

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

Acceder a la consola de mantenimiento mediante la consola de la máquina virtual de vSphere

Si la interfaz de usuario de Unified Manager no está en funcionamiento o si necesita realizar funciones que no están disponibles en la interfaz de usuario, puede acceder a la consola de mantenimiento para volver a configurar el dispositivo virtual.

Lo que necesitará

- Debe ser el usuario de mantenimiento.
- El dispositivo virtual debe estar encendido para acceder a la consola de mantenimiento.

Pasos

1. En vSphere Client, busque el dispositivo virtual Unified Manager.
2. Haga clic en la ficha **Consola**.
3. Haga clic dentro de la ventana de la consola para iniciar sesión.
4. Inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña.

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

Menús de la consola de mantenimiento

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

Según el sistema operativo en el que instaló Unified Manager, la consola de mantenimiento consta de los siguientes menús:

- Actualización de Unified Manager (solo VMware)
- Configuración de red (solo VMware)
- Configuración del sistema (sólo VMware)
  a. Soporte/Diagnóstico
  b. Restablecer certificado de servidor
  c. Proveedor de datos externos
  d. Restaurar copia de seguridad
  e. Configuración del intervalo de sondeo de rendimiento
  f. Deshabilitar la autenticación SAML
  g. Ver/cambiar puertos de aplicación
  h. Depurar configuración de registro
  i. Controlar el acceso al puerto MySQL 3306
  j. Salga

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

Menú Configuración de red

El menú Configuración de red le permite administrar los ajustes de red. Debe usar este menú cuando la interfaz de usuario de Unified Manager no esté disponible.

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

Están disponibles las siguientes opciones de menú.

- **Mostrar configuración de dirección IP**

Muestra la configuración de red actual del dispositivo virtual, incluida la dirección IP, la red, la dirección de retransmisión, la máscara de red, la puerta de enlace, Y servidores DNS.

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

  Permite cambiar cualquier configuración de red del dispositivo virtual, incluidos la dirección IP, la máscara de red, la puerta de enlace o los servidores DNS. Si cambia la configuración de red desde DHCP a la red estática mediante la consola de mantenimiento, no puede editar el nombre de host. Debe seleccionar **commit Changes** para que se realicen los cambios.

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

  Muestra la lista de búsqueda de nombres de dominio utilizada para resolver nombres de host.

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

  Permite cambiar los nombres de dominio en los que se desea buscar al resolver nombres de host. Debe seleccionar **commit Changes** para que se realicen los cambios.

- **Mostrar rutas estáticas**

  Muestra las rutas de red estáticas actuales.

- **Cambiar rutas estáticas**

  Permite agregar o eliminar rutas de red estáticas. Debe seleccionar **commit Changes** para que se realicen los cambios.

  - **Añadir ruta**

    Permite agregar una ruta estática.

  - **Eliminar ruta**

    Permite eliminar una ruta estática.

  - **Atrás**

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

  - **Salida**

    Sale de la consola de mantenimiento.

- **Desactivar la interfaz de red**

  Deshabilita las interfaces de red disponibles. Si solo hay disponible una interfaz de red, no puede deshabilitarla. Debe seleccionar **commit Changes** para que se realicen los cambios.

- **Activar interfaz de red**

  Habilita las interfaces de red disponibles. Debe seleccionar **commit Changes** para que se realicen los cambios.

- **Commit Changes**

Aplica los cambios realizados en la configuración de red del dispositivo virtual. Debe seleccionar esta opción para promulgar cualquier cambio realizado o no se producirán los cambios.

- **Hacer ping a un Host**

  Hace ping en un host de destino para confirmar cambios en la dirección IP o la configuración DNS.

- **Restaurar valores predeterminados**

  Restablece todos los ajustes a los valores predeterminados de fábrica. Debe seleccionar **commit Changes** para que se realicen los cambios.

- **Atrás**

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

- **Salida**

  Sale de la consola de mantenimiento.

Menú Configuración del sistema

El menú Configuración del sistema le permite administrar su dispositivo virtual proporcionando diversas opciones, como ver el estado del servidor y reiniciar y apagar la máquina virtual.

Cuando Unified Manager se instala en un sistema Linux o Microsoft Windows, en este menú solo está disponible la opción «'Restaurar desde un backup de Unified Manager'».

Están disponibles las siguientes opciones de menú:

- **Estado del servidor de visualización**

  Muestra el estado actual del servidor. Las opciones de estado incluyen en ejecución o no en ejecución.

  Si el servidor no está en ejecución, es posible que deba ponerse en contacto con el soporte técnico.

- **Reiniciar máquina virtual**

  Reinicia la máquina virtual, deteniendo todos los servicios. Tras reiniciar, la máquina virtual y los servicios se reinician.

- **Apagar máquina virtual**

  Apaga la máquina virtual, deteniendo todos los servicios.

  Solo puede seleccionar esta opción desde la consola de máquinas virtuales.

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

  Cambia la contraseña del usuario que está conectado actualmente, que sólo puede ser el usuario de mantenimiento.

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

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

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

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

- **Cambiar zona horaria**

  Cambia la zona horaria a su ubicación.

- **Cambiar servidor NTP**

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

- **Cambiar el servicio NTP**

  Cambia entre `ntp` los servicios y. `systemd-timesyncd`

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

  Restaura los ajustes de configuración y base de datos de Unified Manager desde una versión de backup anterior.

- **Restablecer certificado de servidor**

  Restablece el certificado de seguridad del servidor.

- **Cambiar nombre de host**

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

- **Atrás**

  Sale del menú Configuración del sistema y vuelve al menú principal.

- **Salida**

  Sale del menú de la consola de mantenimiento.

Menú de soporte y diagnóstico

El menú Soporte y diagnóstico permite generar un bundle de soporte que puede enviar al soporte técnico para la ayuda de solución de problemas.

Están disponibles las siguientes opciones de menú:

- **Generar paquete de soporte ligero**

  Permite producir un paquete de soporte ligero que contiene sólo 30 días de registros y registros de la base de datos de configuración, lo que excluye datos de rendimiento, archivos de registro de adquisición y volcado de pila del servidor.

- **Generar paquete de soporte**

  Permite crear un bundle de soporte completo (archivo 7-Zip) que contiene información de diagnóstico en el

directorio inicial del usuario de diagnóstico. Si el sistema está conectado a Internet, también puede cargar el paquete de soporte a NetApp.

El archivo incluye información generada por un mensaje de AutoSupport, el contenido de la base de datos de Unified Manager, los datos detallados sobre las redes internas del servidor de Unified Manager y los registros a nivel detallado que normalmente no se incluyen en los mensajes de AutoSupport o en el paquete de soporte ligero.

Opciones de menú adicionales

Las siguientes opciones de menú le permiten realizar varias tareas administrativas en el servidor de Unified Manager.

Están disponibles las siguientes opciones de menú:

- **Restablecer certificado de servidor**

  Regenera el certificado del servidor HTTPS.

  Puede regenerar el certificado de servidor en la GUI de Unified Manager haciendo clic en **General** > **certificados HTTPS** > **regenerar certificado HTTPS**.

- **Deshabilitar autenticación SAML**

  Deshabilita la autenticación SAML de modo que el proveedor de identidades (IDP) ya no proporcione autenticación de inicio de sesión para los usuarios que acceden a la interfaz gráfica de usuario de Unified Manager. Normalmente, esta opción de consola se usa cuando un problema con la configuración de servidor IDP o SAML impide que los usuarios accedan a la interfaz gráfica de usuario de Unified Manager.

- **Proveedor de datos externos**

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

  - **Configuración del servidor de visualización**--muestra los valores actuales de conexión y configuración para un proveedor de datos externo.
  - **Agregar / Modificar conexión del servidor**--le permite introducir nuevos ajustes de conexión para un proveedor de datos externo, o cambiar la configuración existente.
  - **Modificar la configuración del servidor**--le permite introducir nuevos valores de configuración para un proveedor de datos externo, o cambiar los valores existentes.
  - **Eliminar conexión del servidor**--elimina la conexión a un proveedor de datos externo.

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

- **Restauración de copia de seguridad**

  Para obtener más información, consulte los temas en "Gestión de operaciones de backup y restauración".

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

  Proporciona una opción para configurar la frecuencia con la que Unified Manager recopila datos

estadísticos de rendimiento de clústeres. El intervalo de recopilación predeterminado es de 5 minutos.

Puede cambiar este intervalo a 10 o 15 minutos si descubre que las colecciones de clústeres grandes no se están completando a tiempo.

- **Ver/cambiar puertos de aplicación**

  Proporciona una opción para cambiar los puertos predeterminados que Unified Manager utiliza para los protocolos HTTP y HTTPS, si corresponde a la seguridad. Los puertos predeterminados son 80 para HTTP y 443 para HTTPS.

- **Control del acceso al puerto MySQL 3306**

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

- **Salida**

  Sale del menú de la consola de mantenimiento.

Cambiar la contraseña del usuario de mantenimiento en Windows

Es posible cambiar la contraseña de usuario de mantenimiento de Unified Manager si es necesario.

Pasos

1. En la página de inicio de sesión de la interfaz de usuario web de Unified Manager, haga clic en **Contraseña olvidada**.

   Aparece una página que solicita el nombre del usuario cuya contraseña desea restablecer.

2. Introduzca el nombre de usuario y haga clic en **Enviar**.

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

3. Haga clic en el enlace **restablecer contraseña** del correo electrónico y defina la nueva contraseña.
4. Vuelva a la interfaz de usuario web e inicie sesión en Unified Manager con la nueva contraseña.

Cambiar la contraseña de umadmin en sistemas Linux

Por motivos de seguridad, debe cambiar la contraseña predeterminada del usuario umadmin de Unified Manager inmediatamente después de completar el proceso de instalación. Si es necesario, puede cambiar la contraseña de nuevo en cualquier

momento.

Lo que necesitará

- Unified Manager debe estar instalado en un sistema Red Hat Enterprise Linux o CentOS de Linux.
- Debe tener las credenciales de usuario raíz del sistema Linux en el que está instalado Unified Manager.

Pasos

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

   ```
   passwd umadmin
   ```

   El sistema le pide que introduzca una nueva contraseña para el usuario umadmin.

Cambiar los puertos Unified Manager utiliza para los protocolos HTTP y HTTPS

Los puertos predeterminados que Unified Manager utiliza para los protocolos HTTP y HTTPS se pueden cambiar después de la instalación si es necesario para la seguridad. Los puertos predeterminados son 80 para HTTP y 443 para HTTPS.

Lo que necesitará

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

> Hay algunos puertos que se consideran no seguros cuando se utilizan los navegadores Mozilla Firefox o Google Chrome. Consulte con el navegador antes de asignar un nuevo número de puerto para el tráfico HTTP y HTTPS. La selección de un puerto no seguro podría hacer que el sistema no sea accesible, lo que requeriría que se pusiera en contacto con el servicio de atención al cliente para obtener una resolución.

La instancia de Unified Manager se reinicia automáticamente después de cambiar el puerto, por lo que debe asegurarse de que es bueno momento para dejar el sistema inactivo durante un breve período de tiempo.

1. Inicie sesión con SSH como usuario de mantenimiento en el host de Unified Manager.

   Se muestran los mensajes de la consola de mantenimiento de Unified Manager.

2. Escriba el número de la opción de menú con la etiqueta **Ver/Cambiar puertos de aplicación** y, a continuación, pulse Intro.
3. Si se le solicita, vuelva a introducir la contraseña de usuario de mantenimiento.
4. Escriba los números de puerto nuevos para los puertos HTTP y HTTPS y, a continuación, pulse Intro.

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

   Se le pregunta si desea cambiar los puertos y reiniciar Unified Manager ahora.

5. Escriba **y** para cambiar los puertos y reinicie Unified Manager.
6. Salga de la consola de mantenimiento.

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

Se añaden interfaces de red

Puede agregar nuevas interfaces de red si necesita separar el tráfico de red.

Lo que necesitará

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

El dispositivo virtual debe estar encendido.

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

Pasos

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

   Después de reiniciarse, la consola de mantenimiento puede detectar la interfaz de red recién añadida.

2. Acceda a la consola de mantenimiento.
3. Seleccione **Configuración de red** > **Activar interfaz de red**.
4. Seleccione la nueva interfaz de red y pulse **Intro**.

   Seleccione **eth1** y pulse **Intro**.

5. Escriba **y** para activar la interfaz de red.
6. Introduzca los ajustes de red.

   Se le pedirá que introduzca la configuración de red si se utiliza una interfaz estática o si no se detecta DHCP.

   Tras introducir los ajustes de red, volverá automáticamente al menú **Configuración de red**.

7. Seleccione **Commit Changes**.

   Debe confirmar los cambios para añadir la interfaz de red.

Agregar espacio en disco al directorio de la base de datos de Unified Manager

El directorio de bases de datos de Unified Manager contiene todos los datos de estado y rendimiento que se recopilan en los sistemas ONTAP. Algunas circunstancias pueden requerir que aumente el tamaño del directorio de la base de datos.

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

No se recopilan datos adicionales de los clústeres después de que el directorio se encuentra lleno al 95 %.

Los pasos necesarios para añadir capacidad al directorio de datos son distintos en función de si Unified Manager se ejecuta en un servidor VMware ESXi, en un servidor Red Hat o CentOS Linux o en un servidor Microsoft Windows.

Adición de espacio al directorio de datos del host Linux

Si asignó espacio en disco insuficiente al `/opt/netapp/data` directorio para que sea compatible con Unified Manager cuando configuró originalmente el host Linux y luego instaló Unified Manager, puede añadir espacio en disco después de la instalación aumentando el espacio en disco en el `/opt/netapp/data` directorio.

Lo que necesitará

Debe tener acceso de usuario raíz a la máquina Red Hat Enterprise Linux o CentOS Linux en la que está instalado Unified Manager.

Le recomendamos que realice un backup de la base de datos de Unified Manager antes de aumentar el tamaño del directorio de datos.

Pasos

1. Inicie sesión como usuario root en el equipo Linux en el que desea agregar espacio en disco.
2. Detenga el servicio Unified Manager y el software MySQL asociado en el orden que se muestra:

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

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

5. Si se Linux está habilitado:

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

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

      El sistema devuelve una confirmación similar a la siguiente:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Ejecute el comando chcon para establecer el tipo de Linux se para el directorio de copia de seguridad:

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

6. Elimine el contenido `/opt/netapp/data` del directorio:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Expanda el tamaño `/opt/netapp/data` del directorio a un mínimo de 150 GB a través de comandos LVM o agregando discos adicionales.

> Si ha creado `/opt/netapp/data` desde un disco, no debe intentar montarlo `/opt/netapp/data` como un recurso compartido NFS o CIFS. Porque, en este caso, si intenta expandir el espacio en disco, algunos comandos LVM, `resize` como y `extend` podrían no funcionar como se esperaba.

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

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

   El sistema devuelve una confirmación similar a la siguiente:

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

9. Si SE Linux está activado, confirme que el contexto `/opt/netapp/data` del directorio sigue definido en mysqld_db_t:
   a. `touch /opt/netapp/data/abc`
   b. `ls -Z /opt/netapp/data/abc`

      El sistema devuelve una confirmación similar a la siguiente:

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

10. Elimine el archivo abc de modo que este archivo no provoque un error en la base de datos en el futuro.
11. Vuelva a copiar el contenido de los datos de copia de seguridad en el directorio ampliado `/opt/netapp/data`:

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

12. Si se Linux está habilitado, ejecute el siguiente comando:

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

13. Inicie el servicio MySQL:

    ```
    systemctl start mysqld
    ```

14. Una vez iniciado el servicio MySQL, inicie los servicios ocie y ocieau en el orden que se muestra:

    ```
    systemctl start ocie ocieau
    ```

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

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

Adición de espacio al disco de datos de la máquina virtual de VMware

Si necesita aumentar la cantidad de espacio en el disco de datos de la base de datos de Unified Manager, puede añadir capacidad después de la instalación aumentando el espacio en disco mediante la consola de mantenimiento de Unified Manager.

Lo que necesitará

- Debe tener acceso a vSphere Client.
- La máquina virtual no debe tener instantáneas almacenadas localmente.
- Debe tener las credenciales de usuario de mantenimiento.

Le recomendamos que haga una copia de seguridad de su máquina virtual antes de aumentar el tamaño de los discos virtuales.

Pasos

1. En el cliente vSphere, seleccione la máquina virtual de Unified Manager y, a continuación, agregue más capacidad de disco a los datos `disk 3`. Consulte la documentación de VMware para obtener más detalles.

   En algunos casos excepcionales, la puesta en funcionamiento de Unified Manager utiliza «disco duro 2» para el disco de datos en lugar de «disco duro 3». Si esto se ha producido en la implementación, aumente el espacio del disco que sea mayor. El disco de datos siempre tendrá más espacio que el otro disco.

2. En el cliente vSphere, seleccione la máquina virtual de Unified Manager y, a continuación, seleccione la pestaña **Console**.
3. Haga clic en en la ventana de la consola y, a continuación, inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña.
4. En el menú principal, introduzca el número de la opción **Configuración del sistema**.
5. En el menú Configuración del sistema, introduzca el número de la opción **aumentar tamaño del disco de datos**.

Agregar espacio a la unidad lógica del servidor Microsoft Windows

Si necesita aumentar la cantidad de espacio en disco para la base de datos de Unified Manager, puede añadir capacidad a la unidad lógica en la que está instalado Unified Manager.

Lo que necesitará

Debe tener privilegios de administrador de Windows.

Le recomendamos que realice un backup de la base de datos de Unified Manager antes de agregar espacio en disco.

Pasos

1. Inicie sesión como administrador en el servidor Windows en el que desea agregar espacio en disco.
2. Siga el paso correspondiente al método que desea utilizar para agregar más espacio:

Opción	Descripción
En un servidor físico, añada capacidad a la unidad lógica en la que se ha instalado el servidor de Unified Manager.	Siga los pasos del tema de Microsoft: "Extender un volumen básico"
En un servidor físico, agregue una unidad de disco duro.	Siga los pasos del tema de Microsoft: "Agregar unidades de disco duro"
En un equipo virtual, aumente el tamaño de una partición de disco.	Siga los pasos del tema de VMware: "Aumentar el tamaño de una partición de disco"

Gestión del acceso de usuarios

Es posible crear roles y asignar capacidades para controlar el acceso de los usuarios a Active IQ Unified Manager. Puede identificar los usuarios que tienen las funcionalidades necesarias para acceder a los objetos seleccionados en Unified Manager. Solo los usuarios que tienen estos roles y funcionalidades pueden gestionar los objetos en Unified Manager.

Adición de usuarios

Puede agregar usuarios locales o usuarios de bases de datos mediante la página Users. También puede agregar usuarios o grupos remotos que pertenecen a un servidor de autenticación. Es posible asignar roles a esos usuarios y, según los privilegios de los roles, los usuarios pueden gestionar los objetos de almacenamiento y los datos con Unified Manager, o ver los datos en una base de datos.

Lo que necesitará

- Debe tener la función Administrador de aplicaciones.
- Para agregar un usuario o grupo remoto, debe haber habilitado la autenticación remota y configurado el servidor de autenticación.
- Si planea configurar la autenticación SAML de modo que un proveedor de identidades (IDP) autentique usuarios que acceden a la interfaz gráfica, asegúrese de que estos usuarios se definen como usuarios "relativamente".

  No se permite el acceso a la interfaz de usuario para usuarios de tipo "'local'" o "mantenimiento" cuando se activa la autenticación SAML.

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página usuarios, haga clic en **Agregar**.
3. En el cuadro de diálogo Agregar usuario, seleccione el tipo de usuario que desea agregar e introduzca la información necesaria.

   Al introducir la información de usuario requerida, debe especificar una dirección de correo electrónico que sea exclusiva para el usuario. Debe evitar especificar las direcciones de correo electrónico compartidas por varios usuarios.

4. Haga clic en **Agregar**.

Creación de un usuario de base de datos

Para admitir una conexión entre Workflow Automation y Unified Manager, o bien para acceder a las vistas de la base de datos, primero debe crear un usuario de base de datos con los roles Integration Schema o Report Schema en la interfaz de usuario web de Unified Manager.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página Users (usuarios), haga clic en **Add**.
3. En el cuadro de diálogo Agregar usuario, seleccione **Usuario de base de datos** en la lista desplegable **Tipo**.
4. Escriba un nombre y una contraseña para el usuario de la base de datos.
5. En la lista desplegable **rol**, seleccione el rol apropiado.

Si está…	Elija este rol
Conexión de Unified Manager con Workflow Automation	Esquema de integración
Acceso a las vistas Informes y otras vistas de bases de datos	Esquema de informes

6. Haga clic en **Agregar**.

Edición de la configuración de usuario

Puede editar la configuración de usuario, como la dirección de correo electrónico y el rol, que se especifican a cada usuario. Por ejemplo, se recomienda cambiar el rol de un usuario que es un operador de almacenamiento y asignar privilegios de administrador de almacenamiento al usuario.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

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

- El usuario cierra la sesión y vuelve a iniciar sesión en Unified Manager.
- Se alcanza un tiempo de espera de sesión de 24 horas.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página Users (usuarios), seleccione el usuario para el que desea editar la configuración y haga clic en **Edit**.
3. En el cuadro de diálogo Editar usuario, edite la configuración adecuada que se ha especificado para el usuario.
4. Haga clic en **Guardar**.

Ver usuarios

Puede utilizar la página Users para ver la lista de usuarios que gestionan objetos de almacenamiento y datos mediante Unified Manager. Es posible ver detalles sobre los usuarios, como el nombre de usuario, el tipo de usuario, la dirección de correo electrónico y el rol asignado a los usuarios.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Paso

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.

Eliminación de usuarios o grupos

Puede eliminar uno o varios usuarios de la base de datos del servidor de gestión para evitar que usuarios específicos accedan a Unified Manager. También puede eliminar grupos para que todos los usuarios del grupo ya no puedan acceder al servidor de administración.

Lo que necesitará

- Cuando se eliminan grupos remotos, debe haber reasignado los eventos que se asignan a los usuarios de

los grupos remotos.

Si va a eliminar usuarios locales o usuarios remotos, los eventos asignados a estos usuarios se asignarán automáticamente.

- Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página Users (usuarios), seleccione los usuarios o grupos que desea eliminar y, a continuación, haga clic en **Delete**.
3. Haga clic en **Sí** para confirmar la eliminación.

Qué es RBAC

El control de acceso basado en roles (RBAC) ofrece la capacidad de controlar quién tiene acceso a diversas funciones y recursos en el servidor Active IQ Unified Manager.

Qué hace el control de acceso basado en roles

El control de acceso basado en roles permite a los administradores gestionar grupos de usuarios definiendo roles. Si necesita restringir el acceso a funciones específicas para administradores seleccionados, debe configurar cuentas de administrador para ellos. Si desea restringir la información que los administradores pueden ver y las operaciones que pueden realizar, debe aplicar roles a las cuentas de administrador que cree.

El servidor de gestión utiliza RBAC para los permisos de inicio de sesión de usuario y roles. Si no ha cambiado la configuración predeterminada del servidor de administración para el acceso de usuarios administrativos, no es necesario iniciar sesión para verlos.

Cuando inicia una operación que requiere un Privileges específico, el servidor de gestión le solicita que inicie sesión. Por ejemplo, para crear cuentas de administrador, debe iniciar sesión con acceso a la cuenta de administrador de aplicaciones.

Definiciones de tipos de usuario

Un tipo de usuario especifica el tipo de cuenta que contiene el usuario e incluye usuarios remotos, grupos remotos, usuarios locales, usuarios de base de datos y usuarios de mantenimiento. Cada uno de estos tipos tiene su propia función, que asigna un usuario con la función Administrador.

Los tipos de usuario de Unified Manager son los siguientes:

- **Usuario de mantenimiento**

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

- **Usuario local**

  Accede a la interfaz de usuario de Unified Manager y realiza funciones según el rol dado por el usuario de mantenimiento o un usuario con el rol de administrador de aplicaciones.

- **Grupo remoto**

  Un grupo de usuarios que acceden a la interfaz de usuario de Unified Manager con las credenciales almacenadas en el servidor de autenticación. El nombre de esta cuenta debe coincidir con el nombre de un grupo almacenado en el servidor de autenticación. Todos los usuarios del grupo remoto reciben acceso a la interfaz de usuario de Unified Manager usando sus credenciales de usuario individuales. Los grupos remotos pueden realizar funciones según sus roles asignados.

- **Usuario remoto**

  Accede a la interfaz de usuario de Unified Manager con las credenciales almacenadas en el servidor de autenticación. Un usuario remoto realiza funciones basadas en la función proporcionada por el usuario de mantenimiento o un usuario con la función Administrador de aplicaciones.

- **Usuario de base de datos**

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

Definiciones de roles de usuario

El usuario de mantenimiento o el administrador de aplicaciones asigna una función a todos los usuarios. Cada rol contiene ciertos privilegios. El ámbito de las actividades que se pueden realizar en Unified Manager depende del rol que se tenga asignado y de los privilegios que contiene el rol.

Unified Manager incluye los siguientes roles de usuario predefinidos:

- **Operador**

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

- **Administrador de almacenamiento**

  Configura las operaciones de gestión del almacenamiento en Unified Manager. Este rol permite al administrador de almacenamiento configurar umbrales y crear alertas, así como otras opciones y políticas específicas de la gestión del almacenamiento.

- **Administrador de aplicaciones**

  Configura ajustes que no están relacionados con la administración del almacenamiento. Esta función permite la gestión de usuarios, certificados de seguridad, acceso a la base de datos y opciones administrativas, incluida la autenticación, SMTP, redes y AutoSupport.

  Cuando Unified Manager se instala en sistemas Linux, el usuario inicial con la función de administrador de aplicaciones se denomina automáticamente «'umadmin'».

- **Esquema de integración**

  Este rol permite el acceso de solo lectura a las vistas de la base de datos de Unified Manager con la integración de Unified Manager con OnCommand Workflow Automation (WFA).

- **Esquema del informe**

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

  - vista_modelo_netapp
  - rendimiento_netapp
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - escalemador

Roles y funcionalidades de usuario de Unified Manager

Según el rol de usuario asignado, puede determinar qué operaciones puede realizar en Unified Manager.

En la siguiente tabla, se muestran las funciones que puede realizar cada rol de usuario:

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informes
Ver la información del sistema de almacenamiento	•	•	•	•	•
Ver otros datos, como historiales y tendencias de capacidad	•	•	•	•	•
Ver, asignar y resolver eventos	•	•	•		

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informes
Ver los objetos de servicio de almacenamiento, como las asociaciones de SVM y los pools de recursos	•	•	•		
Ver políticas de umbral	•	•	•		
Gestionar objetos de servicio de almacenamiento, como asociaciones de SVM y pools de recursos		•	•		
Defina las alertas		•	•		
Gestione las opciones de gestión del almacenamiento		•	•		
Gestione las políticas de gestión del almacenamiento		•	•		
Gestionar usuarios			•		
Administrar opciones administrativas			•		
Defina las políticas de umbral			•		

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informes
Gestionar el acceso a las bases de datos			•		
Gestione la integración con WFA y proporcione acceso a las vistas de la base de datos				•	
Programar y guardar informes		•	•		
Ejecutar las operaciones «'Fix it'» de las acciones de gestión		•	•		
Proporcione acceso de sólo lectura a las vistas de base de datos					•

Gestión de la configuración de autenticación SAML

Después de configurar la configuración de autenticación remota, puede habilitar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para que los usuarios remotos estén autenticados por un proveedor de identidades (IDP) seguro antes de que puedan acceder a la interfaz de usuario web de Unified Manager.

Tenga en cuenta que 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.

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.

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.

Lo que necesitará

- 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.

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.

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.

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**.

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.

Lo que necesitará

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

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 **OK**.

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.

Actualizar la configuración de autenticación SAML después de cambiar el certificado de seguridad de Unified Manager

Cualquier cambio en el certificado de seguridad HTTPS instalado en Unified Manager Server requiere actualizar los ajustes de configuración de la autenticación SAML. El certificado se actualiza si cambia el nombre del sistema host, asigna una dirección IP nueva al sistema host o cambia manualmente el certificado de seguridad del sistema.

Después de modificar el certificado de seguridad y se reinicia el servidor de Unified Manager, la autenticación SAML no funcionará y los usuarios no podrán acceder a la interfaz gráfica de Unified Manager. Debe actualizar la configuración de autenticación SAML tanto en el servidor IDP como en el servidor de Unified Manager para volver a habilitar el acceso a la interfaz de usuario.

Pasos

1. Inicie sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduzca el número de la opción **Desactivar autenticación SAML**.

   Aparece un mensaje para confirmar que desea deshabilitar la autenticación SAML y reiniciar Unified Manager.

3. Inicie la interfaz de usuario de Unified Manager con el FQDN o la dirección IP actualizados, acepte el certificado de servidor actualizado en el explorador e inicie sesión con las credenciales de usuario de mantenimiento.
4. En la página **Configuración/autenticación**, seleccione la ficha **autenticación SAML** y configure la conexión IDP.
5. Copie el URI de metadatos de host de Unified Manager o guarde los metadatos del host en un archivo de texto XML.
6. Haga clic en **Guardar**.

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

7. Haga clic en **Confirmar y cerrar sesión** y se reiniciará Unified Manager.
8. Acceda al servidor IDP e introduzca el URI del servidor de Unified Manager y los metadatos para completar la configuración.

Proveedor de identidades	Pasos de configuración
ADFS	a. Elimine la entrada de confianza de la parte de confianza existente en la GUI de administración de ADFS. b. Agregue una nueva entrada de confianza de parte de confianza mediante el `saml_sp_metadata.xml` desde el servidor de Unified Manager actualizado. c. Defina las tres reglas de reclamación necesarias para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de parte fiable. d. Reinicie el servicio de Windows de ADFS.
Shibboleth	a. Actualice el nuevo FQDN del servidor de Unified Manager en `attribute-filter.xml` los archivos y `relying-party.xml`. b. Reinicie el servidor Web Apache Tomcat y espere a que el puerto 8005 se vuelva a conectar.

9. Inicie sesión en Unified Manager y verifique que la autenticación SAML funcione como se espera en el IDP.

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.

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.

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.

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

Deshabilitar la autenticación SAML de la consola de mantenimiento

Es posible que deba deshabilitar la autenticación SAML desde la consola de mantenimiento cuando no existe acceso a la interfaz gráfica de usuario de Unified Manager. Esto puede suceder en casos de configuración errónea o si no se puede acceder al IDP.

Lo que necesitará

Debe tener acceso a la consola de mantenimiento como usuario de mantenimiento.

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. Los usuarios locales y los usuarios de mantenimiento podrán acceder a la interfaz gráfica de usuario además de los usuarios remotos configurados.

También se puede deshabilitar la autenticación SAML desde la página Setup/Authentication en la interfaz de usuario.

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

Pasos

1. Inicie sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduzca el número de la opción **Desactivar autenticación SAML**.

   Aparece un mensaje para confirmar que desea deshabilitar la autenticación SAML y reiniciar Unified Manager.

3. Escriba **y** y, a continuación, pulse Intro y se reiniciará Unified Manager.

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.

Si se requiere, acceda a IDP y elimine la URL del servidor de Unified Manager y los metadatos.

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.

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.

Puede utilizar **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.
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.

Estado	Descripción
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 como “NORMAL” o “MANIPULADOS” se descargan en formato comprimido `.gzip`.

Los archivos de registro de auditoría se archivan periódicamente y se guardan en la base de datos a modo de referencia. Antes del archivado, los registros de auditoría se firman digitalmente para mantener la seguridad y la integridad.

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 `.pem` en formato. Este certificado debe obtenerse del servidor de syslog de destino y no debe haber caducado. El certificado debe contener el nombre de host seleccionado como parte del `SubjectAltName` atributo (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 un <hash> del certificado mediante el comando `openssl x509 -noout -hash -in cert.pem`y, a continuación, debe vincular simbólicamente el certificado de autenticación de cliente a un archivo llamado 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.

El valor **Connection Timeout** puede afectar la configuración. Si la configuración tarda más tiempo en responder que el valor definido, puede provocar un fallo de configuración debido a un error de conexión. Para establecer una conexión correcta, aumente el valor de **Connection Timeout** e intente la configuración de nuevo.

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 utiliza para comunicarse con servidores de autenticación LDAP.

◦ **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.

> Los valores que especifique para los atributos *Member*, *User Object Class* y *Group Object Class* deben ser los mismos que los agregados en las configuraciones de Active Directory, OpenLDAP y LDAP. De lo contrario, es posible que se produzca un error en la autenticación.

- 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.

Gestión de certificados de seguridad

Puede configurar HTTPS en el servidor de Unified Manager para supervisar y gestionar los clústeres a través de una conexión segura.

Visualizar el certificado de seguridad HTTPS

Es posible comparar los detalles del certificado HTTPS con el certificado recuperado en el explorador para asegurarse de que la conexión cifrada del explorador con Unified Manager no se intercepte.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

La visualización del certificado permite verificar el contenido de un certificado regenerado o ver los nombres Alt (SAN) sujetos desde los que puede acceder a Unified Manager.

Paso

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.

   El certificado HTTPS se muestra en la parte superior de la página

Si necesita ver información más detallada sobre el certificado de seguridad que la que aparece en la página Certificado HTTPS, puede ver el certificado de conexión en el explorador.

Descargar una solicitud de firma de certificación HTTPS

Puede descargar una solicitud de firma de certificación para el certificado de seguridad HTTPS actual para poder proporcionar el archivo a una entidad de certificación para

firmar. Un certificado firmado por CA ayuda a evitar ataques de tipo "man in the middle" y proporciona una mejor protección de seguridad que un certificado autofirmado.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.
2. Haga clic en **Descargar la solicitud de firma de certificado HTTPS**.
3. Guarde el `<hostname>.csr` archivo.

Puede proporcionar el archivo a una entidad de certificación para firmar e instalar el certificado firmado.

Instalar una CA firmada y devolvió un certificado HTTPS

Puede cargar e instalar un certificado de seguridad después de que una entidad de certificación lo haya firmado y devuelto. El archivo que cargue e instale debe ser una versión firmada del certificado autofirmado existente. Un certificado firmado por CA ayuda a evitar los ataques de tipo "man in the middle" y ofrece una mejor protección de seguridad que un certificado autofirmado.

Lo que necesitará

Debe haber completado las siguientes acciones:

- Descargó el archivo de solicitud de firma de certificado y lo firmó una entidad de certificación
- Se guardó la cadena de certificados en formato PEM
- Se incluyeron todos los certificados en la cadena, desde el certificado de servidor de Unified Manager hasta el certificado de firma raíz, incluidos los certificados intermedios presentes

Debe tener la función Administrador de aplicaciones.

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.
2. Haga clic en **instalar certificado HTTPS**.
3. En el cuadro de diálogo que aparece, haga clic en **elegir archivo…** para localizar el archivo que se va a cargar.
4. Seleccione el archivo y haga clic en **instalar** para instalarlo.

   Para obtener más información, consulte "Instalar un certificado HTTPS generado con herramientas externas".

Ejemplo de cadena de certificados

El siguiente ejemplo muestra cómo puede aparecer el archivo de cadena de certificados:

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

Instalar un certificado HTTPS generado con herramientas externas

Puede instalar certificados que están autofirmados o firmados por CA y que se generan con una herramienta externa como OpenSSL, BoringSSL o LetsEncrypt.

Debe cargar la clave privada junto con la cadena de certificados porque estos certificados son pares de claves pública-privada generados externamente. Los algoritmos de pares de claves permitidos son «'RSA'» y «'EC'». La opción **instalar certificado HTTPS** está disponible en la página certificados HTTPS de la sección General. El archivo que cargue debe tener el siguiente formato de entrada.

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

Formato para cargar un certificado con un par de claves EC

Las curvas permitidas son «'prime256v1» y «slecp384r1». Ejemplo de certificado con un par de EC generado externamente:

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

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

Formato para cargar un certificado con un par de claves RSA

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

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

Una vez cargado el certificado, debe reiniciar la instancia de Active IQ Unified Manager para que los cambios se apliquen.

Comprueba la carga de certificados generados externamente

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

- La clave privada de la entrada se valida contra el certificado de host en la entrada.
- El nombre común (CN) del certificado de host se comprueba con el FQDN del host.

- El nombre común (CN) del certificado de host no debe estar vacío ni en blanco y no debe establecerse en localhost.
- La fecha de inicio de la validez no debe ser posterior y la fecha de caducidad del certificado no debe ser pasada.
- Si existe CA intermedia o CA, la fecha de inicio de validez del certificado no debe ser futura y la fecha de caducidad de validez no debe ser pasada.

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

Ejemplo 1

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

Ejemplo 2

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

Ejemplo 3

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

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

Descripciones de página para la gestión de certificados

Puede usar la página HTTPS Certificate para ver los certificados de seguridad actuales y generar certificados HTTPS nuevos.

Página HTTPS Certificate

En la página HTTPS Certificate, puede ver el certificado de seguridad actual, descargar una solicitud de firma de certificación, generar un certificado HTTPS autofirmado nuevo o instalar un certificado HTTPS nuevo.

Si no generó un certificado HTTPS autofirmado nuevo, el certificado que aparece en esta página es el

certificado que se generó durante la instalación.

Botones de comando

Los botones de comando le permiten realizar las siguientes operaciones:

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

  Descarga una solicitud de certificación para el certificado HTTPS instalado actualmente. El explorador le solicita que guarde el archivo <hostname>.csr para poder proporcionar el archivo a una entidad de certificación que desea firmar.

- **Instalar certificado HTTPS**

  Permite cargar e instalar un certificado de seguridad después de que una entidad de certificación lo haya firmado y devuelto. El nuevo certificado se aplicará después de reiniciar el servidor de gestión.

- **Regenerar certificado HTTPS**

  Permite generar un certificado HTTPS autofirmado nuevo, que reemplaza el certificado de seguridad actual. El nuevo certificado se aplica después de reiniciar Unified Manager.

Cuadro de diálogo Regenerate HTTPS Certificate

El cuadro de diálogo Regenerate HTTPS Certificate permite personalizar la información de seguridad y, a continuación, generar un nuevo certificado HTTPS con esa información.

La información del certificado actual aparece en esta página.

La selección "'Regenerate usando atributos de certificado actuales'" y "'Actualizar atributos de certificado actuales'" le permite regenerar el certificado con la información actual o generar un certificado con nueva información.

- **Nombre común**

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

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

- **Correo electrónico**

  Opcional. Una dirección de correo electrónico para ponerse en contacto con su empresa; normalmente, la dirección de correo electrónico del administrador del certificado o del departamento DE TI.

- **Empresa**

  Opcional. Normalmente el nombre incorporado de su empresa.

- **Departamento**

  Opcional. El nombre del departamento de su empresa.

- * Ciudad*

Opcional. Ubicación de la ciudad de su empresa.

- **Estado**

  Opcional. La ubicación del estado o provincia, no abreviada, de la compañía.

- **País**

  Opcional. Ubicación del país de su empresa. Este es típicamente un código ISO de dos letras del país.

- **Nombres alternativos**

  Obligatorio. Nombres de dominio adicionales no primarios que se pueden utilizar para tener acceso a este servidor además del host local u otras direcciones de red existentes. Cada nombre alternativo debe separarse con comas.

  Seleccione la casilla de verificación "'excluir información de identificación local (p. ej., localhost)'" si desea eliminar la información de identificación local del campo nombres alternativos del certificado. Cuando se selecciona esta casilla de verificación, sólo se utiliza el campo nombres alternativos lo que se introduce en el campo. Cuando se deja en blanco, el certificado resultante no tendrá ningún campo nombres alternativos.

- **TAMAÑO DE CLAVE (ALGORITMO DE CLAVE: RSA)**

  El algoritmo de clave está establecido en RSA. Puede seleccionar uno de los tamaños de clave: 2048, 3072 ó 4096 bits. El tamaño de clave predeterminado es de 2048 bits.

- **PERÍODO DE VALIDEZ**

  El período de validez predeterminado es de 397 días. Si ha actualizado desde una versión anterior, es posible que la validez del certificado anterior no cambie.

Para obtener más información, consulte "Generación de certificados HTTPS".