Realizar tareas de configuración y administración

Active IQ Unified Manager

NetApp
October 15, 2025

Tabla de contenidos

Realizar tareas de configuración y administración

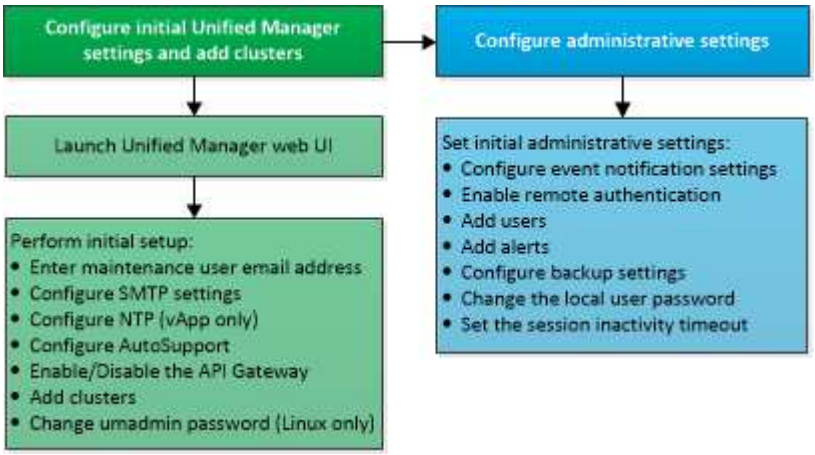
Configurar Active IQ Unified Manager

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

Algunos de los procedimientos descritos en este manual son necesarios para completar la configuración inicial de su instancia de Unified Manager. Se recomiendan otros procedimientos de configuración que son útiles para configurar en su nueva instancia o que es bueno conocer antes de comenzar el monitoreo regular de sus sistemas ONTAP .

Descripción general de la secuencia de configuración

El flujo de trabajo de configuración describe las tareas que debe realizar antes de poder utilizar Unified Manager.



Acceda a la interfaz web de Unified Manager

Después de haber instalado Unified Manager, puede acceder a la interfaz de usuario web para configurar Unified Manager y así poder comenzar a monitorear sus sistemas ONTAP .

Antes de empezar

- Si es la primera vez que accede a la interfaz de usuario web, debe iniciar sesión como usuario de mantenimiento (o usuario umadmin para instalaciones de Linux).
- Si planea permitir que los usuarios accedan a Unified Manager usando el nombre corto en lugar de usar el nombre de dominio completo (FQDN) o la dirección IP, entonces su configuración de red debe resolver este nombre corto en un FQDN válido.
- Si el servidor utiliza un certificado digital autofirmado, el navegador podría mostrar una advertencia

indicando que el certificado no es confiable. Puede reconocer el riesgo para continuar con el acceso o instalar un certificado digital firmado por una autoridad de certificación (CA) para la autenticación del servidor.

Pasos

1. Inicie la interfaz web de Unified Manager desde su navegador utilizando 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 tiene 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 realiza tres intentos fallidos consecutivos de iniciar sesión en la interfaz de usuario web dentro de una hora, quedará bloqueado del sistema y deberá comunicarse con el administrador del sistema. Esto es aplicable únicamente para usuarios locales.

Realice la configuración inicial de la interfaz web de Unified Manager

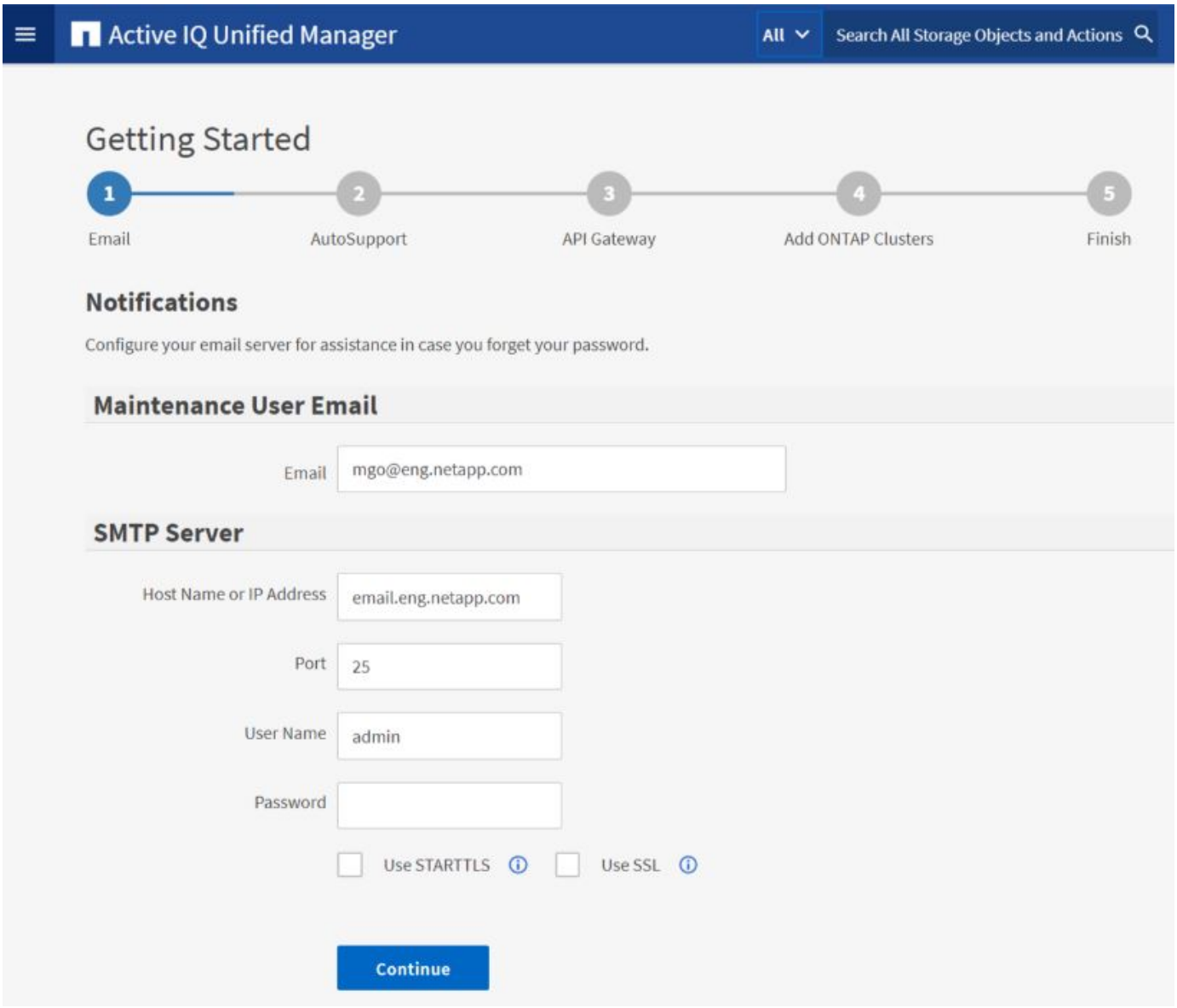
Para utilizar Unified Manager, primero debe configurar las opciones de configuración inicial, incluido el servidor NTP, la dirección de correo electrónico del usuario de mantenimiento, el host del servidor SMTP y la adición de clústeres ONTAP .

Antes de empezar

Debes haber realizado las siguientes operaciones:

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

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



Si desea cambiar alguna de estas opciones más adelante, puede seleccionar su elección en las opciones Generales en el 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 mediante la consola de mantenimiento de Unified Manager.

Pasos

1. En la página de configuración inicial de Active IQ Unified Manager , ingrese la dirección de correo electrónico del usuario de mantenimiento, el nombre de host del servidor SMTP y cualquier opción SMTP adicional, y el servidor NTP (solo instalaciones de VMware). Luego 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**. Verifique los detalles del certificado y acéptelo para continuar con la configuración inicial de la interfaz de usuario web.

2. En la página AutoSupport , haga clic en **Aceptar y continuar** para habilitar el envío de mensajes de AutoSupport desde Unified Manager a NetAppActive IQ.

   Si necesita designar un proxy para proporcionar acceso a Internet para enviar contenido de AutoSupport , o si desea deshabilitar AutoSupport, utilice la opción **General** > * AutoSupport* de la interfaz de usuario

web.

3. En los sistemas Red Hat, cambie la contraseña del usuario umadmin de la cadena predeterminada “admin” a una cadena personalizada.
4. En la página Configurar API Gateway, seleccione si desea utilizar la función API Gateway que permite a Unified Manager administrar los clústeres de ONTAP que planea monitorear mediante las API REST de ONTAP . Luego haga clic en **Continuar**.

   Puede habilitar o deshabilitar esta configuración más adelante en la interfaz de usuario web desde **General** > **Configuración de funciones** > **API Gateway**. Para obtener más información sobre las API, consulte"Introducción a las API REST de Active IQ Unified Manager" .

5. Agregue los clústeres que desea que Unified Manager administre y luego haga clic en **Siguiente**. Para cada clúster que planea 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 tarde en la interfaz de usuario web desde **Administración de almacenamiento** > **Configuración de clúster**.

6. En la página Resumen, verifique que todas las configuraciones sean correctas y haga clic en **Finalizar**.

La página Primeros pasos se cierra y se muestra la página Panel de control de Unified Manager.

Agregar clústeres

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

Antes de empezar

- Debe tener el rol de Administrador de aplicaciones o Administrador de almacenamiento.
- Debes tener la siguiente información:
  - Unified Manager admite clústeres ONTAP locales, ONTAP Select y Cloud Volumes ONTAP.
  - Nombre de host o dirección IP de administración del clúster

    El nombre de host es el FQDN o nombre corto que Unified Manager utiliza para conectarse al clúster. El nombre del host debe resolverse en la dirección IP de administración del clúster.

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

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

    Esta cuenta debe tener el rol *admin* con acceso a la aplicación establecido en *ontapi*, *console* y *http*.

  - El número de puerto para conectarse al clúster mediante el protocolo HTTPS (normalmente el puerto 443)

◦ Tienes los certificados requeridos:

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

Certificado EMS: Este certificado es propiedad de Unified Manager. Se utiliza durante la autenticación de las notificaciones EMS recibidas de ONTAP.

Certificados para comunicación TLS mutua: se utilizan durante la comunicación TLS mutua entre Unified Manager y ONTAP. La autenticación basada en certificado está habilitada para un clúster, según la versión de ONTAP . Si el clúster que ejecuta la versión de ONTAP es inferior a la 9.5, la autenticación basada en certificados no estará habilitada.

La autenticación basada en certificados no se habilita automáticamente para un clúster si está actualizando una versión anterior de Unified Manager. Sin embargo, puedes habilitarlo modificando y guardando los detalles del clúster. Si el certificado caduca, deberá regenerarlo para incorporar el nuevo certificado. Para obtener más información sobre cómo ver y regenerar el certificado, consulte"Edición de clústeres" .

- Puede agregar un clúster desde la interfaz de usuario web y la autenticación basada en certificados se habilita automáticamente.
- Puede agregar un clúster a través de la CLI de Unified Manager, la autenticación basada en certificado no está habilitada de forma predeterminada. Si agrega un clúster mediante la CLI de Unified Manager, será necesario editar el clúster mediante la UI de Unified Manager. Ya puedes ver"Comandos CLI de Unified Manager compatibles" para agregar un clúster mediante la CLI de Unified Manager.
- Si la autenticación basada en certificados está habilitada para un clúster y usted toma la copia de seguridad de Unified Manager desde un servidor y la restaura en otro servidor de Unified Manager donde se modifica el nombre de host o la dirección IP, entonces la supervisión del clúster puede fallar. Para evitar el error, edite y guarde los detalles del clúster. Para obtener más información sobre cómo editar los detalles del clúster, consulte"Edición de clústeres" .

+ **Certificados de clúster**: este certificado es propiedad de ONTAP. No puede agregar un clúster a Unified Manager con un certificado vencido y, si el certificado ya venció, debe regenerarlo antes de agregar 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 del Administrador del sistema" .

- Debe tener espacio suficiente en el servidor de Unified Manager. No se le permite agregar un clúster al servidor cuando ya se ha consumido más del 90 % del espacio en el directorio de la base de datos.

Para una configuración de MetroCluster , debe agregar los clústeres locales y remotos, y los clústeres deben estar configurados correctamente.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración del clúster**.

2. En la página Configuración del clúster, haga clic en **Agregar**.
3. En el cuadro de diálogo Agregar clúster, 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.

   Puede cambiar la dirección IP de administración 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 que se completa el siguiente ciclo de monitoreo.

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 certificado no está habilitada, Unified Manager verifica el certificado solo cuando se agrega el clúster inicialmente. Unified Manager no verifica el certificado para cada llamada API a ONTAP.

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

Debido a que la recopilación de 15 días de datos de rendimiento consume muchos recursos de la CPU, se sugiere escalonar la incorporación de nuevos clústeres para que las encuestas de recopilación de continuidad de datos no se ejecuten en demasiados clústeres al mismo tiempo. Además, si reinicia Unified Manager durante el período de recopilación de continuidad de datos, la recopilación se detendrá y verá brechas en los gráficos de rendimiento correspondientes al período de tiempo faltante.

Si recibe un mensaje de error que indica que no puede agregar el clúster, verifique si los relojes de los dos sistemas no están sincronizados y si la fecha de inicio del certificado HTTPS de Unified Manager es posterior a la fecha del clúster. Debe asegurarse de que los relojes estén sincronizados mediante NTP o un servicio similar.

Información relacionada

"Instalación de un certificado HTTPS firmado y devuelto por una CA"

Configurar Unified Manager para enviar notificaciones de alerta

Puede configurar Unified Manager para enviar notificaciones que le alerten sobre eventos en su entorno. Antes de poder enviar notificaciones, debe configurar varias otras opciones de Unified Manager.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

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

Pasos

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

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

2. "Habilitar 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. "Agregar servidores de autenticación".

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

4. "Agregar usuarios".

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

5. "Agregar alertas".

   Una vez que haya agregado la dirección de correo electrónico para enviar notificaciones, agregado usuarios para recibir las notificaciones, configurado los ajustes de red y configurado las opciones SMTP y SNMP necesarias para su entorno, podrá asignar alertas.

Configurar los ajustes de notificación de eventos

Puede configurar Unified Manager para enviar notificaciones de alerta cuando se genera un evento o cuando se asigna un evento a un usuario. Puede configurar el servidor SMTP que se utiliza para enviar la alerta y puede establecer varios mecanismos de notificación; por ejemplo, las notificaciones de alerta se pueden enviar como correos electrónicos o trampas SNMP.

Antes de empezar

Debes tener la siguiente información:

- Dirección de correo electrónico desde la que se envía la notificación de alerta

  La dirección de correo electrónico aparece en el campo "De" en las notificaciones de alerta enviadas. Si por algún motivo no se puede entregar el correo electrónico, esta dirección de correo electrónico también se utiliza como destinatario del correo no entregado.

- Nombre de host del servidor SMTP y el nombre de usuario y la contraseña para acceder al servidor
- Nombre de host o dirección IP para el host de destino de la trampa que recibirá la trampa SNMP, junto con la versión de SNMP, el puerto de trampa de salida, la comunidad y otros valores de configuración de

SNMP requeridos

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

Debe tener el rol de Administrador de aplicaciones o Administrador de almacenamiento.

Pasos

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

   Notas:

   - Si la dirección de remitente está precargada con la dirección "ActiveIQUnifiedManager@localhost.com", debe cambiarla a una dirección de correo electrónico real y funcional para asegurarse de que todas las notificaciones por 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**. Verifique los detalles del certificado y acéptelo 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 está vencido, desmarque 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.

Habilitar la autenticación remota

Puede habilitar la autenticación remota para que el servidor de Unified Manager pueda comunicarse con sus servidores de autenticación. Los usuarios del servidor de autenticación pueden acceder a la interfaz gráfica de Unified Manager para administrar objetos de almacenamiento y datos.

Antes de empezar

Debe tener el rol de 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 (System Security Services Daemon) o NSLCD (Name Service LDAP Caching Daemon).

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 el puerto predeterminado para la comunicación no segura y 636 como el puerto predeterminado para la comunicación segura.

El certificado que se utiliza para autenticar a los usuarios debe cumplir con el formato X.509.

Pasos

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

Para el tipo de autenticación…	Introduzca la siguiente información…
Directorio activo	• Nombre del administrador del servidor de autenticación en uno de los siguientes formatos: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name`(utilizando la notación LDAP apropiada) • Contraseña de administrador • Nombre distinguido base (utilizando la notación LDAP apropiada)
Abrir LDAP	• Vincular nombre distinguido (en la notación LDAP apropiada) • Vincular contraseña • Nombre distinguido base

Si la autenticación de un usuario de Active Directory tarda mucho tiempo o se agota el tiempo de espera, es probable que el servidor de autenticación tarde mucho en responder. Deshabilitar la compatibilidad con grupos anidados en Unified Manager podría reducir el tiempo de autenticación.

Si selecciona la opción Usar conexión segura 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 grupo anidado para que solo los usuarios individuales, y no los miembros del grupo, puedan autenticarse de forma remota en Unified Manager. Puede deshabilitar los grupos anidados cuando desee mejorar el tiempo de respuesta de la autenticación de Active Directory.

Antes de empezar

- Debe tener el rol de Administrador de aplicaciones.

- La deshabilitación de grupos anidados solo se aplica cuando se utiliza Active Directory.

Deshabilitar la compatibilidad con grupos anidados en Unified Manager podría reducir el tiempo de autenticación. Si la compatibilidad con grupos anidados está deshabilitada y se agrega 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. Marque la casilla para **Deshabilitar búsqueda de grupo anidado**.
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 proporcionarles acceso a Unified Manager. Puede autenticar usuarios mediante servicios de autenticación predefinidos (como Active Directory o OpenLDAP) o configurando su propio mecanismo de autenticación.

Antes de empezar

- Debe tener habilitada la autenticación remota.
- Debe tener el rol de 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 seleccionas…	Entonces haz esto…
Directorio activo	a. Introduzca el nombre y la contraseña del administrador. b. Especifique el nombre distinguido base del servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre distinguido base es **cn=ou,dc=domain,dc=com**.

Si seleccionas…	Entonces haz esto…
OpenLDAP	a. Introduzca el nombre distinguido del enlace y la contraseña del enlace. b. Especifique el nombre distinguido base del servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre distinguido base es **cn=ou,dc=domain,dc=com**.
Otros	a. Introduzca el nombre distinguido del enlace y la contraseña del enlace. b. Especifique el nombre distinguido base del servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre distinguido base es **cn=ou,dc=domain,dc=com**. c. Especifique la versión del protocolo LDAP compatible con el servidor de autenticación. d. Ingrese el nombre de usuario, la membresía del grupo, el grupo de usuario y los atributos del miembro.

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

3. Haga clic en **Guardar**.

Agregar servidores de autenticación

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

Antes de empezar

- La siguiente información debe estar disponible:
  - 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 su servicio de autenticación para que el servidor de administración pueda autenticar usuarios o grupos remotos en el servidor de autenticación.
- Debe tener el rol de Administrador de aplicaciones.

Si el servidor de autenticación que está agregando es parte de un par de alta disponibilidad (HA) (que usa la

misma base de datos), también puede agregar el servidor de autenticación asociado. Esto permite que el servidor de administración se comunique con el socio cuando uno de los servidores de autenticación no está disponible.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Autenticación remota**.
2. Habilitar o deshabilitar la opción **Usar conexión segura**:

Si quieres…	Entonces haz esto…
Habilitarlo	a. Seleccione la opción **Usar conexión segura**. b. En el área Servidores de autenticación, haga clic en **Agregar**. c. En el cuadro de diálogo Agregar servidor de autenticación, ingrese el nombre de autenticación o la dirección IP (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, verifique la información del certificado y luego haga clic en **Cerrar**. f. En el cuadro de diálogo Autorizar host, haga clic en **Sí**. Cuando habilita 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 la comunicación segura y el puerto número 389 para la comunicación no segura.
Deshabilitarlo	a. Desmarque la opción **Usar conexión segura**. b. En el área Servidores de autenticación, haga clic en **Agregar**. c. En el cuadro de diálogo Agregar servidor de autenticación, 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 agregó se muestra en el área Servidores.

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

Probar la configuración de los servidores de autenticación

Puede validar la configuración de sus servidores de autenticación para asegurarse de que el servidor de administración pueda comunicarse con ellos. Puede validar la configuración buscando un usuario remoto o un grupo remoto desde sus servidores de autenticación y autenticándolos utilizando las configuraciones.

Antes de empezar

- Debe haber habilitado la autenticación remota y configurado su servicio de autenticación para que el servidor de Unified Manager pueda autenticar al usuario remoto o al grupo remoto.
- Debe haber agregado sus servidores de autenticación para que el servidor de administración pueda buscar al usuario remoto o al grupo remoto desde estos servidores y autenticarlos.
- Debe tener el rol de Administrador de aplicaciones.

Si el servicio de autenticación está configurado en Active Directory y 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 **Probar**.

   Si está autenticando un grupo remoto, no debe ingresar la contraseña.

Agregar alertas

Puede configurar alertas para que le notifiquen cuando se genera un evento en particular. Puede configurar alertas para un solo recurso, para un grupo de recursos o para eventos de un tipo de gravedad particular. Puede especificar la frecuencia con la que desea recibir notificaciones y asociar un script a la alerta.

Antes de empezar

- Debe haber configurado ajustes de notificación como la dirección de correo electrónico del usuario, el servidor SMTP y el host de trampa SNMP para permitir que el servidor Active IQ Unified Manager use estos ajustes para enviar notificaciones a los usuarios cuando se genera un evento.
- Debe conocer los recursos y eventos para los que desea activar la alerta, y los nombres de usuario o direcciones de correo electrónico de los usuarios a los que desea notificar.
- Si desea que se ejecute un script en función del evento, debe haber agregado el script a Unified Manager mediante la página Scripts.
- Debe tener el rol de Administrador de aplicaciones o Administrador de almacenamiento.

Puede crear una alerta directamente desde la página de Detalles del evento después de recibir un evento, además de crear una alerta desde la página Configuración de alertas, 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 ingrese un nombre y una descripción para la alerta.
4. Haga clic en **Recursos** y seleccione los recursos que desea incluir o excluir de la alerta.

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

   Si un recurso cumple con las reglas de inclusión y exclusión que ha especificado, la regla de exclusión tiene prioridad sobre la regla de inclusión y la alerta no se genera para 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 cual desea activar una alerta.

   Para seleccionar más de un evento, presione la tecla Ctrl mientras realiza sus selecciones.

6. Haga clic en **Acciones** y seleccione los usuarios que desea notificar, elija la frecuencia de notificación, elija si se enviará una trampa SNMP al receptor de trampa y asigne un script 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 editarla, el campo Nombre aparece en blanco porque la dirección de correo electrónico modificada ya no está asignada al usuario que se seleccionó anteriormente. Además, si modificó la dirección de correo electrónico del usuario seleccionado desde la página Usuarios, la dirección de correo electrónico modificada no se actualiza para el usuario seleccionado.

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

7. Haga clic en **Guardar**.

Ejemplo de cómo añadir una alerta

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

- Nombre de la alerta: HealthTest
- Recursos: incluye todos los volúmenes cuyo nombre contiene “abc” y excluye todos los volúmenes cuyo nombre contiene “xyz”
- Eventos: incluye todos los eventos críticos de salud
- Acciones: incluye "sample@domain.com", un script “Test” y se debe notificar al usuario cada 15 minutos

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

Pasos

1. Haga clic en **Nombre** e ingrese **HealthTest** en el campo **Nombre de alerta**.
2. Haga clic en **Recursos** y, en la pestaña Incluir, seleccione **Volúmenes** de la lista desplegable.
   a. Ingrese **abc** en el campo **El nombre contiene** para mostrar los volúmenes cuyo nombre contiene “abc”.
   b. Seleccionar **+[All Volumes whose name contains 'abc'] +** del área Recursos disponibles y muévalo al área Recursos seleccionados.
   c. Haga clic en **Excluir**, ingrese **xyz** en el campo **El nombre contiene** y luego haga clic en **Agregar**.
3. Haga clic en **Eventos** y seleccione **Crítico** en el campo Gravedad del evento.
4. Seleccione **Todos los eventos críticos** del área Eventos coincidentes y muévalo al área Eventos seleccionados.
5. Haga clic en **Acciones** e ingrese **sample@domain.com** en el campo Alertar a estos usuarios.
6. Seleccione **Recordar cada 15 minutos** para notificar al usuario cada 15 minutos.

   Puede configurar una alerta para enviar notificaciones repetidamente a los destinatarios durante un tiempo específico. Debe determinar la hora a partir de la cual la notificación del evento está activa para la alerta.
7. En el menú Seleccionar script para ejecutar, seleccione Script **Prueba**.
8. Haga clic en **Guardar**.

Cambiar la contraseña del usuario local

Puede cambiar su contraseña de inicio de sesión de usuario local para evitar posibles riesgos de seguridad.

Antes de empezar

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, comuníquese con su administrador de contraseñas. Para cambiar la contraseña del usuario de mantenimiento, consulte"Uso de la consola de mantenimiento" .

Pasos

1. Inicie sesión en Unified Manager.
2. Desde la barra de menú superior, haga clic en el ícono de usuario y luego haga clic en **Cambiar contraseña**.

   La opción **Cambiar contraseña** no se muestra si eres un usuario remoto.
3. En el cuadro de diálogo Cambiar contraseña, ingrese la contraseña actual y la nueva contraseña.
4. Haga clic en **Guardar**.

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

Establecer el tiempo de espera de inactividad de la sesión

Puede especificar el valor de tiempo de espera de inactividad para Unified Manager para

que la sesión finalice automáticamente después de un cierto período de inactividad. De forma predeterminada, el tiempo de espera se establece en 4320 minutos (72 horas).

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

Esta configuración afecta a todas las sesiones de usuario iniciadas sesión.

Esta opción no está disponible si ha habilitado 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 funciones**, especifique el tiempo de espera de inactividad eligiendo una de las siguientes opciones:

Si quieres…	Entonces haz esto…
No establezca ningún tiempo de espera para que la sesión nunca se cierre automáticamente	En el panel **Tiempo de espera por inactividad**, mueva el botón deslizante hacia la izquierda (desactivado) y haga clic en **Aplicar**.
Establezca un número específico de minutos como valor de tiempo de espera	En el panel **Tiempo de espera por inactividad**, mueva el botón deslizante hacia la derecha (activado), especifique el valor del tiempo de espera por inactividad en minutos y haga clic en **Aplicar**.

Establezca el tiempo de espera de la sesión a través de CLI

Puede establecer un valor de tiempo de espera máximo de sesión para Unified Manager mediante la CLI para que la sesión finalice automáticamente después de un cierto período de tiempo. De forma predeterminada, el tiempo de espera de su sesión se establece en el valor máximo, que es 4320 minutos (72 horas). Esto significa que su sesión finaliza automáticamente después de 72 horas, incluso si ha iniciado sesión y utiliza activamente Unified Manager.

Acerca de esta tarea

Debe tener el rol de Administrador de aplicaciones.

La configuración del tiempo de espera de la sesión afecta a todas las sesiones de usuario iniciadas sesión.

Pasos

1. Inicie sesión en la CLI de Unified Manager ingresando el `um cli login` dominio. Utilice un nombre de usuario y contraseña válidos para la autenticación.
2. Entra en el `um option set max.session.timeout.value=<in mins>` Comando para modificar el valor del tiempo de espera de la sesión.

Cambiar el nombre de host de Unified Manager

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

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

Cambiar el nombre del host del dispositivo virtual Unified Manager

Al host de red se le asigna un nombre cuando se implementa por primera vez el dispositivo virtual Unified Manager. Puede cambiar el nombre del host después de la implementación. Si cambia el nombre del host, también deberá regenerar el certificado HTTPS.

Antes de empezar

Debe iniciar sesión en Unified Manager como usuario de mantenimiento o tener asignado el rol de Administrador de aplicaciones para realizar estas tareas.

Puede utilizar 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 su red durante la implementación, entonces deberá designar un nombre para el host de la red. Si configuró la red usando 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 automáticamente y se asocia con el certificado de seguridad.

Independientemente de cómo se asignó el nombre de host, si cambia el nombre de host y pretende utilizar 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 utilizando la dirección IP del servidor en lugar del nombre de host, no tendrá que generar un nuevo certificado si cambia el nombre de host. Sin embargo, la mejor práctica es actualizar el certificado para que el nombre de host en el certificado coincida con el nombre de host real.

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

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

Pasos

1. Generar un certificado de seguridad HTTPS

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

2. Reinicie la máquina virtual de Unified Manager

   Después de regenerar 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. Puede generar un nuevo certificado de seguridad HTTPS que reemplace el certificado existente.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

Puede haber varias razones para regenerar el certificado, por ejemplo, si desea tener mejores valores para el nombre distinguido (DN), si desea un tamaño de clave mayor, un período de vencimiento más largo o si el certificado actual ha vencido.

Si no tiene acceso a la interfaz de usuario web de Unified Manager, puede regenerar el certificado HTTPS con los mismos valores utilizando la consola de mantenimiento. Al regenerar certificados, puede definir el tamaño de la clave y la duración de validez de la clave. Si utiliza el `Reset Server Certificate` opción desde la consola de mantenimiento, luego se crea un nuevo certificado HTTPS que es válido por 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**.

   Se muestra el cuadro de diálogo Regenerar certificado HTTPS.

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

Si quieres…	Haz esto…
Regenerar el certificado con los valores actuales	Haga clic en la opción **Regenerar usando los atributos del certificado actual**.

Si quieres…	Haz esto…
Generar el certificado utilizando diferentes valores	Haga clic en la opción **Actualizar los atributos del certificado actual**. Los campos Nombre común y Nombres alternativos utilizarán los valores del certificado existente si no ingresa valores nuevos. El "Nombre común" debe establecerse en el FQDN del host. Los demás campos no requieren valores, pero puede ingresar valores, por ejemplo, para CORREO ELECTRÓNICO, EMPRESA, DEPARTAMENTO, Ciudad, Estado y País si desea que esos valores se completen en el certificado. También puede seleccionar entre el TAMAÑO DE CLAVE disponible (el algoritmo de clave es “RSA”.) y el PERÍODO DE VALIDEZ. • Los valores permitidos para el tamaño de la clave son `2048` , `3072` y `4096` . • Los períodos de validez son mínimo de 1 día y máximo de 36500 días. Aunque se permite un período de validez de 36.500 días, se recomienda utilizar un período de validez de no más de 397 días o 13 meses. Porque si selecciona un período de validez de más de 397 días y planea exportar un CSR para este certificado y hacer que lo firme una CA conocida, la validez del certificado firmado que le devuelva la CA se reducirá a 397 días. • Puede seleccionar la casilla de verificación “Excluir información de identificación local (por ejemplo, localhost)” si desea eliminar la información de identificación local del campo Nombres alternativos en el certificado. Cuando esta casilla de verificación está seleccionada, solo lo que ingrese en el campo se utilizará en el campo Nombres alternativos. Si se deja en blanco, el certificado resultante no tendrá ningún campo de 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. Verifique la información del nuevo certificado viendo el certificado HTTPS.

Reinicie la máquina virtual de Unified Manager

Puede reiniciar la máquina 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.

Antes de empezar

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 utilizando la opción **Reiniciar invitado**. Consulte la documentación de VMware para obtener más información.

Pasos

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

Cambiar el nombre de host de Unified Manager en sistemas Linux

En algún momento, es posible que desee cambiar el nombre de host de la máquina Red Hat Enterprise Linux en la que ha instalado Unified Manager. Por ejemplo, es posible que desee cambiar el nombre del host para identificar más fácilmente sus servidores Unified Manager por tipo, grupo de trabajo o grupo de clúster monitoreado cuando enumera sus máquinas Linux.

Antes de empezar

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

Puede utilizar 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 su red durante la implementación, entonces deberá designar un nombre para el host de la red. Si configuró la red usando 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 pretende utilizar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, deberá generar un nuevo certificado de seguridad.

Si accede a la interfaz de usuario web utilizando la dirección IP del servidor en lugar del nombre de host, no tendrá que generar un nuevo certificado si cambia el nombre de host. Sin embargo, la mejor práctica es actualizar el certificado para que el nombre de host en el certificado coincida con el nombre de host real. El nuevo certificado no tendrá efecto hasta que se reinicie la máquina Linux.

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

Pasos

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

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Cambiar el nombre del host usando Linux `hostnamectl` dominio:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Regenerar el certificado HTTPS para el servidor:

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

5. Reiniciar el servicio de red:

   ```
   systemctl restart NetworkManager.service
   ```

6. Después de reiniciar el servicio, verifique 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 estableció anteriormente para el nombre de host original.

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

   ```
   systemctl start mysqld ocie ocieau
   ```

Habilitar y deshabilitar la administración de almacenamiento basada en políticas

A partir de Unified Manager 9.7, puede aprovisionar cargas de trabajo de almacenamiento (volúmenes y LUN) en sus clústeres ONTAP y administrar esas cargas de trabajo en función de los niveles de servicio de rendimiento asignados. Esta funcionalidad es similar a la creación de cargas de trabajo en ONTAP System Manager y la asociación de políticas de QoS, pero cuando se aplica mediante Unified Manager, puede aprovisionar y administrar cargas de trabajo en todos los clústeres que su instancia de Unified Manager está monitoreando.

Debe tener el rol de Administrador de aplicaciones.

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

Cuando está habilitada, 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**
Una página para crear políticas de nivel de servicio de rendimiento	Disponible en **Configuración** > **Políticas** > **Niveles de servicio de rendimiento**
Una página para crear políticas de eficiencia de almacenamiento de rendimiento	Disponible en **Configuración** > **Políticas** > **Eficiencia de almacenamiento**
Paneles que describen el rendimiento de su carga de trabajo actual y las IOPS de su carga de trabajo	Disponible desde el Panel de Control

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

Pasos

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

Si quieres…	Entonces haz esto…
Deshabilitar la administración de almacenamiento basada en políticas	En el panel **Administración de almacenamiento basada en políticas**, mueva el botón deslizante hacia la izquierda.
Habilitar la gestión de almacenamiento basada en políticas	En el panel **Administración de almacenamiento basada en políticas**, mueva el botón deslizante hacia la derecha.

Configurar la copia de seguridad de Unified Manager

Puede configurar la capacidad de respaldo en Unified Manager a través de un conjunto de pasos de configuración que se realizarán en los sistemas host y mediante la consola de mantenimiento.

Para obtener información sobre los pasos de configuración, consulte"Administrar operaciones de copia de seguridad y restauración" .

Administrar la configuración de funciones

La página Configuración de funciones le permite habilitar y deshabilitar funciones específicas en Active IQ Unified Manager. Esto incluye la creación y administración de objetos de almacenamiento basados en políticas, la habilitación de API Gateway y el banner de inicio de sesión, la carga de scripts para administrar alertas, el cronometrar

una sesión de IU web en función del tiempo de inactividad y la deshabilitar la recepción de eventos de la plataforma Active IQ .

> La página Configuración de funciones solo está disponible para usuarios con rol de Administrador de aplicaciones.

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

Habilitar la gestión de almacenamiento basada en políticas

La opción **Administración de almacenamiento basada en políticas** permite la gestión del almacenamiento en función de 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 agregados a su instancia Active IQ Unified Manager y administrar estas cargas de trabajo en función de los niveles de servicio de rendimiento y las políticas de eficiencia de almacenamiento asignados.

Puede elegir activar o desactivar esta función desde **General** > **Configuración de funciones** > **Administración de almacenamiento basada en políticas**. Al activar esta función, las siguientes páginas estarán disponibles para su operación y monitoreo:

- Aprovisionamiento (aprovisionamiento de carga de trabajo de almacenamiento)
- **Políticas** > **Niveles de servicio de rendimiento**
- **Políticas** > **Eficiencia de almacenamiento**
- Columna Cargas de trabajo administradas por el nivel de servicio de rendimiento en la página Configuración de clústeres
- Panel de rendimiento de la carga de trabajo en el **Tablero**

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

Después de activar esta función, puede ejecutar las API REST de Unified Manager para realizar algunas de estas funciones desde **Barra de menú** > **Botón Ayuda** > **Documentación de API** > categoría **proveedor de almacenamiento**. Alternativamente, puede ingresar el nombre del host o la dirección IP y la URL para acceder a la página de la API REST en el formato https://<hostname>/docs/api/

Para obtener más información sobre las API, consulte"Introducción a las API REST de Active IQ Unified Manager" .

Habilitar API Gateway

La función API Gateway permite que Active IQ Unified Manager sea un único plano de control desde el cual puede administrar múltiples clústeres de ONTAP , sin iniciar sesión en ellos individualmente.

Puede habilitar esta función desde las páginas de configuración que aparecen cuando inicia sesión por primera vez en Unified Manager. Alternativamente, puede habilitar o deshabilitar esta función desde **General** > **Configuración de funciones** > **API Gateway**.

Las API REST de Unified Manager son diferentes de las API REST de ONTAP , y no todas las funcionalidades de las API REST de ONTAP se pueden aprovechar mediante el uso de las API REST de Unified Manager. Sin embargo, si tiene un requisito comercial específico para acceder a las API de ONTAP para administrar funciones específicas que no están expuestas a Unified Manager, puede habilitar la función API Gateway y ejecutar las API de ONTAP . La puerta de enlace actúa como un proxy para tunelizar las solicitudes de API manteniendo el encabezado y el cuerpo de las solicitudes en el mismo formato que en las API de ONTAP . Puede usar sus credenciales de Unified Manager y ejecutar las API específicas para acceder y administrar los clústeres de ONTAP sin pasar credenciales de clúster individuales. Unified Manager funciona como un único punto de administración para ejecutar las API en los clústeres de ONTAP administrados por su instancia de Unified Manager. La respuesta devuelta por las API es la misma que la respuesta devuelta por las respectivas API REST de ONTAP ejecutadas directamente desde ONTAP.

Después de habilitar esta función, puede ejecutar las API REST de Unified Manager desde **Barra de menú** > **Botón Ayuda** > **Documentación de API** > categoría **puerta de enlace**. Alternativamente, puede ingresar el nombre del host o la dirección IP y la URL para acceder a la página de la API REST en el formato `https://<hostname>/docs/api/`

Para obtener más información sobre las API, consulte"Introducción a las API REST de Active IQ Unified Manager" .

Especificar el tiempo de espera por inactividad

Puede especificar el valor de tiempo de espera de inactividad para Active IQ Unified Manager. Después de una inactividad del tiempo especificado, la sesión de la aplicación se cierra automáticamente. Esta opción está habilitada de forma predeterminada.

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

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

Habilitar eventos del portal Active IQ

Puede especificar si desea habilitar o deshabilitar los eventos del portal Active IQ . Esta configuración permite que el portal Active IQ descubra y muestre 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 los eventos descubiertos 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 monitoreados. Estos eventos son diferentes de los demás eventos de Unified Manager e identifican incidentes o riesgos relacionados con la configuración del sistema, el cableado, las mejores prácticas y los problemas de disponibilidad.

Puede elegir activar o desactivar esta función desde **General** > **Configuración de funciones** > **Eventos**

Active IQ *. En sitios sin acceso a red externa, debe cargar las reglas manualmente desde *Administración de almacenamiento > **Configuración de eventos** > **Cargar reglas**.

Esta función está habilitada de forma predeterminada. Al deshabilitar esta función, se impide que los eventos de Active IQ se detecten o se muestren en Unified Manager. Cuando está deshabilitada, habilitar esta función permite que Unified Manager reciba los eventos de Active IQ en un clúster a una hora predefinida de 00:15 para esa zona horaria del clúster.

Habilitar y deshabilitar configuraciones de seguridad para el cumplimiento

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

Las configuraciones que se habilitan o deshabilitan desde esta página rigen el estado de cumplimiento general de los clústeres y las máquinas virtuales de almacenamiento en Unified Manager. Según las selecciones, las columnas correspondientes son visibles en la vista **Seguridad: Todos los clústeres** de la página de inventario de clústeres y en la vista **Seguridad: Todas las máquinas virtuales de almacenamiento** de la página de inventario de máquinas virtuales de almacenamiento.

Sólo los usuarios con rol de administrador pueden editar estas configuraciones.

Los criterios de seguridad para sus clústeres de ONTAP , máquinas virtuales de almacenamiento y volúmenes se evalúan en función de las recomendaciones definidas en el"Guía de refuerzo de seguridad para NetApp ONTAP 9" . El panel de Seguridad en el tablero y la página de Seguridad muestran el estado de cumplimiento de seguridad predeterminado de sus clústeres, máquinas virtuales de almacenamiento y volúmenes. También se generan eventos de seguridad y se habilitan acciones de administración para los clústeres y las máquinas virtuales de almacenamiento que tienen violaciones de seguridad.

Personalizar la configuración de seguridad

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

Pasos

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

   Los parámetros de cumplimiento de seguridad que habilite o deshabilite pueden afectar directamente las vistas de seguridad predeterminadas, los informes y los informes programados en las pantallas Clústeres y Máquinas virtuales de almacenamiento. 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 presenten errores.

2. Para habilitar o deshabilitar la configuración personalizada para sus clústeres ONTAP , seleccione la configuración general requerida en **Clúster**. Para obtener información sobre las opciones para personalizar la conformidad del clúster, consulte"Categorías de cumplimiento del clúster" .
3. Para habilitar o deshabilitar la configuración personalizada para sus máquinas virtuales de almacenamiento, seleccione la configuración general requerida en **Máquina virtual de almacenamiento**. Para obtener información sobre las opciones para personalizar la conformidad de las máquinas virtuales de almacenamiento, consulte"Categorías de cumplimiento de máquinas virtuales de almacenamiento" .

Personalizar la configuración de AutoSupport y autenticación

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

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

Habilitar y deshabilitar la carga de scripts

La capacidad de cargar scripts en Unified Manager y ejecutarlos está habilitada de forma predeterminada. Si su organización no desea permitir esta actividad por razones de seguridad, puede deshabilitar esta funcionalidad.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

Pasos

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

Si quieres…	Entonces haz esto…
Deshabilitar scripts	En el panel **Carga de script**, mueva el botón deslizante hacia la izquierda.
Habilitar scripts	En el panel **Carga de script**, mueva el botón deslizante hacia la derecha.

Agregar banner de inicio de sesión

Agregar un banner de inicio de sesión permite a su organización mostrar cualquier información, como quién tiene permiso para acceder al sistema y los términos y condiciones de uso durante el inicio y cierre de sesión.

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

Utilice la consola de mantenimiento

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

¿Qué funcionalidad proporciona la consola de mantenimiento?

La consola de mantenimiento de Unified Manager le permite mantener la configuración de su sistema Unified Manager y realizar los cambios necesarios para evitar que surjan problemas.

Dependiendo del sistema operativo en el que haya instalado Unified Manager, la consola de mantenimiento proporciona las siguientes funciones:

- Solucione cualquier problema con su dispositivo virtual, especialmente si la interfaz web de Unified Manager no está disponible
- Actualice a versiones más nuevas de Unified Manager
- Generar paquetes de soporte para enviar al soporte técnico
- Configurar los ajustes de red
- Cambiar la contraseña del usuario de mantenimiento
- Conéctese a un proveedor de datos externo para enviar estadísticas de rendimiento
- Cambiar la recopilación de datos de rendimiento interna
- Restaurar la base de datos de Unified Manager y la configuración desde una versión previamente respaldada.

Qué hace el usuario de mantenimiento

El usuario de mantenimiento se crea durante la instalación de Unified Manager en un sistema Red Hat Enterprise Linux. El nombre de usuario de mantenimiento es el usuario “umadmin”. El usuario de mantenimiento tiene el rol de administrador de aplicaciones en la interfaz de usuario web y puede crear usuarios posteriores y asignarles roles.

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

Capacidades de diagnóstico del usuario

El propósito del acceso de diagnóstico es permitir que el soporte técnico lo ayude a solucionar problemas, y solo debe usarlo cuando se lo indique el soporte técnico.

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

Acceder a la consola de mantenimiento

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 administrar su sistema Unified Manager.

Antes de empezar

Debe tener instalado y configurado Unified Manager.

Después de 15 minutos de inactividad, la consola de mantenimiento cerrará su sesión.

Cuando se instala en VMware, si ya ha iniciado sesión como usuario de mantenimiento a través de la consola de VMware, no podrá iniciar sesión simultáneamente usando 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 Unified Manager. b. Inicie sesión en la consola de mantenimiento utilizando 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 de usuario de mantenimiento (umadmin) y la contraseña. c. Introduzca el comando `maintenance_console` y presione Enter.
Ventanas	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 presione Enter.

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

Acceda a la consola de mantenimiento mediante la consola de VM 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 reconfigurar su dispositivo virtual.

Antes de empezar

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

Pasos

1. En vSphere Client, ubique el dispositivo virtual Unified Manager.
2. Haga clic en la pestaña **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.

   Después de 15 minutos de inactividad, la consola de mantenimiento cerrará su sesión.

Menús de la consola de mantenimiento

La consola de mantenimiento consta de diferentes menús que le permiten mantener y administrar funciones especiales y configuraciones del servidor Unified Manager.

Dependiendo del sistema operativo en el que haya instalado Unified Manager, la consola de mantenimiento consta de los siguientes menús:

- Actualizar Unified Manager (solo VMware)
- Configuración de red (solo VMware)
- Configuración del sistema (solo VMware)
  a. Soporte/Diagnóstico
  b. Restablecer el certificado del servidor
  c. Proveedor de datos externo
  d. Restauración de copia de seguridad
  e. Configuración del intervalo de sondeo de rendimiento
  f. Deshabilitar la autenticación SAML
  g. Ver/Cambiar puertos de la aplicación
  h. Configuración del registro de depuración
  i. Controlar el acceso al puerto MySQL 3306
  j. Salida

Selecciona el número de la lista para acceder a la opción de menú específica. Por ejemplo, para realizar copias de seguridad y restaurar, seleccione *4*.

Menú de configuración de red

El menú Configuración de red le permite administrar la configuración de red. Debe utilizar 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 o en Microsoft Windows.

Las siguientes opciones de menú están disponibles.

- **Mostrar configuración de dirección IP**

  Muestra la configuración de red actual del dispositivo virtual, incluida la dirección IP, la red, la dirección de transmisión, la máscara de red, la puerta de enlace y los servidores DNS.

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

Le permite cambiar cualquiera de las configuraciones de red del dispositivo virtual, incluida la dirección IP, la máscara de red, la puerta de enlace o los servidores DNS. Si cambia la configuración de red de DHCP a red estática mediante la consola de mantenimiento, no podrá editar el nombre del host. Debes seleccionar **Confirmar cambios** para que los cambios tengan lugar.

- **Mostrar configuración de búsqueda de nombre de dominio**

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

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

  Le permite cambiar los nombres de dominio que desea buscar al resolver nombres de host. Debes seleccionar **Confirmar cambios** para que los cambios tengan lugar.

- **Mostrar rutas estáticas**

  Muestra las rutas de red estáticas actuales.

- **Cambiar rutas estáticas**

  Le permite agregar o eliminar rutas de red estáticas. Debes seleccionar **Confirmar cambios** para que los cambios tengan lugar.

  - **Añadir ruta**

    Le permite agregar una ruta estática.

  - **Eliminar ruta**

    Le permite eliminar una ruta estática.

  - **Atrás**

    Te lleva de regreso al **Menú principal**.

  - **Salida**

    Sale de la consola de mantenimiento.

- **Deshabilitar interfaz de red**

  Desactiva cualquier interfaz de red disponible. Si solo hay una interfaz de red disponible, no podrás desactivarla. Debes seleccionar **Confirmar cambios** para que los cambios tengan lugar.

- **Habilitar interfaz de red**

  Habilita las interfaces de red disponibles. Debes seleccionar **Confirmar cambios** para que los cambios tengan lugar.

- **Confirmar cambios**

  Aplica cualquier cambio realizado en la configuración de red del dispositivo virtual. Debe seleccionar esta opción para aplicar cualquier cambio realizado, de lo contrario los cambios no se realizarán.

- **Hacer ping a un host**

Hace ping a un host de destino para confirmar cambios de dirección IP o configuraciones de DNS.

- **Restaurar configuración predeterminada**

  Restablece todas las configuraciones a los valores predeterminados de fábrica. Debes seleccionar **Confirmar cambios** para que los cambios tengan lugar.

- **Atrás**

  Te lleva de regreso al **Menú principal**.

- **Salida**

  Sale de la consola de mantenimiento.

Menú de configuración del sistema

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

> Cuando Unified Manager está instalado en un sistema Linux o Microsoft Windows, solo la opción "Restaurar desde una copia de seguridad de Unified Manager" está disponible en este menú.

Las siguientes opciones de menú están disponibles:

- **Mostrar estado del servidor**

  Muestra el estado actual del servidor. Las opciones de estado incluyen En ejecución y No en ejecución.

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

- **Reiniciar la máquina virtual**

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

- **Apagar máquina virtual**

  Apaga la máquina virtual y detiene todos los servicios.

  Puede seleccionar esta opción solo desde la consola de la máquina virtual.

- **Cambiar la contraseña de usuario de <usuario registrado>**

  Cambia la contraseña del usuario que está actualmente conectado, el cual 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.

- **Aumentar 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 tu ubicación.

- **Cambiar servidor NTP**

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

- **Cambiar servicio NTP**

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

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

  Restaura la base de datos de Unified Manager y la configuración de una versión respaldada previamente.

- **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 de Configuración del sistema y regresa al Menú principal.

- **Salida**

  Sale del menú de la consola de mantenimiento.

Menú de soporte y diagnóstico

El menú Soporte y diagnóstico le permite generar un paquete de soporte que puede enviar al soporte técnico para obtener asistencia para la resolución de problemas.

Las siguientes opciones de menú están disponibles:

- **Paquete de soporte para generar luz**

  Le permite producir un paquete de soporte liviano que contiene solo 30 días de registros y registros de bases de datos de configuración; excluye datos de rendimiento, archivos de registro de adquisiciones y volcado de montón del servidor.

- **Generar paquete de soporte**

  Le permite crear un paquete de soporte completo (archivo 7-Zip) que contiene información de diagnóstico en el directorio de inicio del usuario de diagnóstico. Si su 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, datos detallados sobre los componentes internos del servidor de Unified Manager y

registros de nivel detallado que normalmente no se incluyen en los mensajes de AutoSupport ni en el paquete de soporte ligero.

Opciones de menú adicionales

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

Las siguientes opciones de menú están disponibles:

- **Restablecer certificado de servidor**

  Regenera el certificado del servidor HTTPS.

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

- **Deshabilitar la autenticación SAML**

  Deshabilita la autenticación SAML para que el proveedor de identidad (IdP) ya no proporcione autenticación de inicio de sesión para los usuarios que acceden a la GUI de Unified Manager. Esta opción de consola generalmente se usa cuando un problema con el servidor IdP o la configuración SAML impide que los usuarios accedan a la GUI de Unified Manager.

- **Proveedor de datos externo**

  Proporciona opciones para conectar Unified Manager a un proveedor de datos externo. Una vez establecida la conexión, los datos de rendimiento se envían a un servidor externo para que los expertos en rendimiento de almacenamiento puedan graficar las métricas de rendimiento utilizando software de terceros. Se muestran las siguientes opciones:

  - **Mostrar configuración del servidor**: muestra la conexión actual y la configuración de un proveedor de datos externo.
  - **Agregar/Modificar conexión de servidor**: le permite ingresar nuevas configuraciones de conexión para un proveedor de datos externo o cambiar configuraciones existentes.
  - **Modificar configuración del servidor**: le permite ingresar nuevas configuraciones para un proveedor de datos externo o cambiar configuraciones existentes.
  - **Eliminar conexión de 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"Administrar operaciones de copia de seguridad 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 los clústeres. El intervalo de recopilación predeterminado es de 5 minutos.

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

- **Ver/Cambiar puertos de la aplicación**

  Proporciona una opción para cambiar los puertos predeterminados que Unified Manager utiliza para los protocolos HTTP y HTTPS, si es necesario por razones de seguridad. Los puertos predeterminados son 80 para HTTP y 443 para HTTPS.

- **Controlar el acceso al puerto MySQL 3306**

  Controla el acceso del host al puerto MySQL predeterminado 3306. Por razones de seguridad, el acceso a través de este puerto está restringido únicamente al host local durante una nueva instalación de Unified Manager en sistemas Linux, Windows y VMware vSphere. Esta opción le permite alternar la visibilidad de este puerto entre el host local y los hosts remotos, es decir, si está habilitado solo para el host local en su entorno, puede hacer que este puerto también esté disponible para los hosts remotos. Alternativamente, cuando está habilitado para todos los hosts, puede restringir el acceso de este puerto solo al host local. Si el acceso se habilitó previamente en hosts remotos, la configuración se conserva en un escenario de actualización. Debe verificar la configuración del firewall en los sistemas Windows después de alternar la visibilidad del puerto y deshabilitar la configuración del firewall si las configuraciones están configuradas 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

Puede cambiar la contraseña del usuario de mantenimiento de Unified Manager cuando sea necesario.

Pasos

1. Desde la página de inicio de sesión de la interfaz web de Unified Manager, haga clic en **Olvidé mi contraseña**.

   Se muestra 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 para restablecer contraseña** en el correo electrónico y defina la nueva contraseña.
4. Regrese 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 razones de seguridad, debe cambiar la contraseña predeterminada para el usuario umadmin de Unified Manager inmediatamente después de completar el proceso de instalación. Si es necesario, puedes cambiar la contraseña nuevamente en cualquier momento más tarde.

Antes de empezar

- Unified Manager debe instalarse en un sistema Linux Red Hat Enterprise Linux.

- Debe tener las credenciales de usuario root para el sistema Linux en el que está instalado Unified Manager.

Pasos

1. Inicie sesión como usuario root en el sistema Linux en el que se ejecuta Unified Manager.
2. Cambiar la contraseña de umadmin:

   ```
   passwd umadmin
   ```

   El sistema le solicita que ingrese una nueva contraseña para el usuario umadmin.

Cambiar los puertos que 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 por razones de seguridad. Los puertos predeterminados son 80 para HTTP y 443 para HTTPS.

Antes de empezar

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 inseguros cuando se utilizan los navegadores Mozilla Firefox o Google Chrome. Consulte su navegador antes de asignar un nuevo número de puerto para el tráfico HTTP y HTTPS. Seleccionar un puerto no seguro podría hacer que el sistema quede inaccesible, por lo que deberá comunicarse con el servicio de atención al cliente para obtener una solución.

La instancia de Unified Manager se reinicia automáticamente después de cambiar el puerto, así que asegúrese de que este sea un buen momento para apagar el sistema por un breve período de tiempo.

1. Inicie sesión utilizando 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 denominada **Ver/Cambiar puertos de aplicación** y luego presione Entrar.
3. Si se le solicita, ingrese nuevamente la contraseña de usuario de mantenimiento.
4. Escriba los nuevos números de puerto para los puertos HTTP y HTTPS y luego presione Entrar.

   Dejar un número de puerto en blanco asigna el puerto predeterminado para el protocolo.

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

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

Después de 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.

Agregar interfaces de red

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

Antes de empezar

Debe haber agregado 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 vSphere, seleccione **Configuración del sistema** > **Reiniciar sistema operativo**.

   Después de reiniciar, la consola de mantenimiento puede detectar la interfaz de red recién agregada.

2. Acceda a la consola de mantenimiento.
3. Seleccione **Configuración de red** > **Habilitar interfaz de red**.
4. Seleccione la nueva interfaz de red y presione **Enter**.

   Seleccione **eth1** y presione **Enter**.

5. Escriba **y** para habilitar la interfaz de red.
6. Ingrese a la configuración de red.

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

   Después de ingresar a la configuración de red, regresará automáticamente al menú **Configuración de red**.

7. Seleccione **Confirmar cambios**.

   Debe confirmar los cambios para agregar la interfaz de red.

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

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

Por ejemplo, el directorio de la base de datos puede llenarse si Unified Manager recopila datos de una gran cantidad de clústeres donde 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 una vez que el directorio alcanza el 95 % de su capacidad.

Los pasos necesarios para agregar capacidad al directorio de datos son diferentes dependiendo de si Unified Manager se ejecuta en un servidor VMware ESXi, en un servidor Red Hat o en un servidor Microsoft Windows.

Agregar espacio al directorio de datos del host Linux

Si no le ha asignado suficiente espacio en disco al `/opt/netapp/data` directorio para admitir Unified Manager cuando configuró originalmente el host Linux y luego instaló Unified Manager, puede agregar espacio en disco después de la instalación aumentando el espacio en disco en el `/opt/netapp/data` directorio.

Antes de empezar

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

Le recomendamos que realice una copia de seguridad 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 la máquina Linux en la 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 respaldo temporal (por ejemplo, `/backup-data`) con suficiente espacio en disco para contener los datos en el sistema actual. `/opt/netapp/data` directorio.
4. Copiar el contenido y la configuración de privilegios del existente `/opt/netapp/data` directorio al directorio de datos de respaldo:

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

5. Si SE Linux está habilitado:

   a. Obtenga el tipo SE Linux para carpetas existentes `/opt/netapp/data` carpeta:

      ```
      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 SE Linux para el directorio de respaldo:

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

6. Retire el contenido del `/opt/netapp/data` directorio:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Ampliar el tamaño de la `/opt/netapp/data` directorio a un mínimo de 150 GB a través de comandos LVM o agregando discos adicionales.

Si has creado `/opt/netapp/data` desde un disco, entonces no deberías intentar montarlo `/opt/netapp/data` como un recurso compartido NFS o CIFS. Porque, en este caso, si intenta ampliar el espacio en disco, algunos comandos LVM, como `resize` y `extend` Podría no funcionar como se esperaba.

8. Confirmar que el `/opt/netapp/data` El propietario del directorio (mysql) y el grupo (root) no cambian:

   ```
   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 habilitado, confirme que el contexto para el `/opt/netapp/data` El directorio todavía está configurado como 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 para que este archivo extraño no provoque un error de base de datos en el futuro.
11. Copiar el contenido de los datos de respaldo de nuevo al archivo expandido `/opt/netapp/data` directorio:

    ```
    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. Iniciar el servicio MySQL:

    ```
    systemctl start mysqld
    ```

14. Después de iniciar 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, elimine la carpeta de respaldo `/backup-data` :

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

Agregar espacio al disco de datos de la máquina virtual VMware

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

Antes de empezar

- Debe tener acceso al cliente vSphere.
- 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 Unified Manager y luego agregue más capacidad de disco a los datos `disk 3` . Consulte la documentación de VMware para obtener más detalles.

   En algunos casos excepcionales, la implementación de Unified Manager utiliza “Disco duro 2” para el disco de datos en lugar de “Disco duro 3”. Si esto ha ocurrido en su implementación, aumente el espacio del disco que sea más grande. El disco de datos siempre tendrá más espacio que el otro disco.

2. En el cliente vSphere, seleccione la máquina virtual Unified Manager y luego seleccione la pestaña **Consola**.
3. Haga clic en la ventana de la consola y luego inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña.
4. En el Menú principal, ingrese el número para la opción **Configuración del sistema**.
5. En el menú de configuración del sistema, ingrese el número para la opción **Aumentar el tamaño del disco de datos**.

Agregar espacio a la unidad lógica del servidor de Microsoft Windows

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

Antes de empezar

Debe tener privilegios de administrador de Windows.

Le recomendamos que haga una copia de seguridad 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 que corresponda al método que desee utilizar para agregar más espacio:

Opción	Descripción
En un servidor físico, agregue capacidad a la unidad lógica en la que está instalado el servidor 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 una máquina virtual, aumente el tamaño de una partición de disco.	Siga los pasos del tema de VMware: "Aumentar el tamaño de una partición de disco"

Administrar el acceso de los usuarios

Puede crear roles y asignar capacidades para controlar el acceso de los usuarios a Active IQ Unified Manager. Puede identificar a los usuarios que tienen las capacidades necesarias para acceder a objetos seleccionados dentro de Unified Manager. Sólo aquellos usuarios que tienen estos roles y capacidades pueden administrar los objetos en Unified Manager.

Agregar usuarios

Puede agregar usuarios locales o usuarios de base de datos utilizando la página Usuarios. También puede agregar usuarios o grupos remotos que pertenezcan a un servidor de autenticación. Puede asignar roles a estos usuarios y, según los privilegios de los roles, los usuarios pueden administrar los objetos de almacenamiento y los datos con Unified Manager, o ver los datos en una base de datos.

Antes de empezar

- Debe tener el rol de Administrador de aplicaciones.
- Para agregar un usuario o grupo remoto, debe haber habilitado la autenticación remota y configurado su servidor de autenticación.
- Si planea configurar la autenticación SAML para que un proveedor de identidad (IdP) autentique a los usuarios que acceden a la interfaz gráfica, asegúrese de que estos usuarios estén definidos como usuarios "remotos".

  No se permite el acceso a la interfaz de usuario a los usuarios de tipo “local” o “maintenance” cuando la autenticación SAML está habilitada.

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

   Al ingresar la información de usuario requerida, debe especificar una dirección de correo electrónico que sea única para ese usuario. Debes evitar especificar direcciones de correo electrónico que sean compartidas por varios usuarios.

4. Haga clic en **Agregar**.

Crear un usuario de base de datos

Para admitir una conexión entre Workflow Automation y Unified Manager, o para acceder a las vistas de la base de datos, primero debe crear un usuario de base de datos con la función Esquema de integración o Esquema de informe en la interfaz de usuario web de Unified Manager.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

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

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 **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 eres…	Elige este rol
Conexión de Unified Manager con la automatización del flujo de trabajo	Esquema de integración
Acceso a informes y otras vistas de bases de datos	Esquema de informe

6. Haga clic en **Agregar**.

Editar la configuración del usuario

Puede editar la configuración de usuario (como la dirección de correo electrónico y el rol) que se especifica para cada usuario. Por ejemplo, es posible que desee cambiar el rol de un usuario que es operador de almacenamiento y asignarle privilegios de administrador de almacenamiento.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

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

- El usuario cierra la sesión y vuelve a iniciarla en Unified Manager.
- Se alcanzó el 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 Usuarios, seleccione el usuario cuya configuración desea editar y haga clic en **Editar**.
3. En el cuadro de diálogo Editar usuario, edite las configuraciones apropiadas especificadas para el usuario.
4. Haga clic en **Guardar**.

Ver usuarios

Puede utilizar la página Usuarios para ver la lista de usuarios que administran objetos de almacenamiento y datos mediante Unified Manager. Puede 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.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

Paso

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

Eliminar usuarios o grupos

Puede eliminar uno o más usuarios de la base de datos del servidor de administración 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.

Antes de empezar

- Al eliminar grupos remotos, debe haber reasignado los eventos que están asignados a los usuarios de los grupos remotos.

  Si está eliminando usuarios locales o usuarios remotos, los eventos asignados a estos usuarios se desasignan automáticamente.

- Debe tener el rol de Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Usuarios**.
2. En la página Usuarios, seleccione los usuarios o grupos que desea eliminar y luego haga clic en **Eliminar**.
3. Haga clic en **Sí** para confirmar la eliminación.

¿Qué es RBAC?

RBAC (control de acceso basado en roles) proporciona 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 (RBAC) permite a los administradores gestionar grupos de usuarios mediante la definición de roles. Si necesita restringir el acceso a una funcionalidad específica a 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 administración utiliza RBAC para el inicio de sesión de usuarios y los permisos de roles. Si no ha cambiado la configuración predeterminada del servidor de administración para el acceso de usuarios administrativos, no necesita iniciar sesión para verla.

Cuando inicia una operación que requiere privilegios específicos, el servidor de administración le solicita que inicie sesión. Por ejemplo, para crear cuentas de administrador, debe iniciar sesión con acceso de cuenta de administrador de aplicaciones.

Definiciones de tipos de usuarios

Un tipo de usuario especifica el tipo de cuenta que tiene el usuario e incluye usuarios remotos, grupos remotos, usuarios locales, usuarios de bases de datos y usuarios de mantenimiento. Cada uno de estos tipos tiene su propio rol, que es asignado por un usuario con el rol de Administrador.

Los tipos de usuarios de Unified Manager son los siguientes:

- **Usuario de mantenimiento**

  Creado durante la configuración inicial de Unified Manager. Luego, el usuario de mantenimiento crea usuarios adicionales y asigna roles. El usuario de mantenimiento también es el único usuario con acceso a la consola de mantenimiento. Cuando Unified Manager se instala en un sistema Red Hat Enterprise Linux, 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 asignado 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 utilizando 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 dentro del grupo remoto tienen 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 utilizando las credenciales almacenadas en el servidor de autenticación. Un usuario remoto realiza funciones según el rol asignado por el usuario de mantenimiento o un usuario con el rol de Administrador de aplicaciones.

- **Usuario de la base de datos**

  Tiene acceso de solo lectura a los datos de 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 API.

Definiciones de roles de usuario

El usuario de mantenimiento o administrador de la aplicación asigna un rol a cada usuario. Cada rol contiene ciertos privilegios. El alcance de las actividades que puede realizar en Unified Manager depende del rol que se le asigne y de los privilegios que contenga el rol.

Unified Manager incluye los siguientes roles de usuario predefinidos:

- **Operador**

  Visualiza información del sistema de almacenamiento y otros datos recopilados por Unified Manager, incluidos historiales y tendencias de capacidad. Esta función permite al operador de almacenamiento ver, asignar, reconocer, resolver y agregar notas para los eventos.

- **Administrador de almacenamiento**

  Configura las operaciones de gestión de almacenamiento dentro de Unified Manager. Esta función permite al administrador de almacenamiento configurar umbrales y crear alertas y otras opciones y políticas específicas de la administración del almacenamiento.

- **Administrador de la aplicación**

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

  > Cuando Unified Manager se instala en sistemas Linux, el usuario inicial con el rol de administrador de aplicaciones se denomina automáticamente “umadmin”.

- **Esquema de integración**

  Esta función permite el acceso de solo lectura a las vistas de la base de datos de Unified Manager para integrar Unified Manager con OnCommand Workflow Automation (WFA).

- **Esquema del informe**

  Esta función permite el acceso de solo lectura a informes y otras vistas de bases de datos directamente desde la base de datos de Unified Manager. Las bases de datos que se pueden visualizar incluyen:

  - vista del modelo de netapp
  - rendimiento de netapp
  - ocum

- informe_ocum
- informe_de_nacimiento_ocum
- opm
- monitor de escala

Funciones y capacidades de usuario de Unified Manager

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

La siguiente tabla muestra las funciones que puede realizar cada rol de usuario:

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informe
Ver información del sistema de almacenamiento	•	•	•	•	•
Ver otros datos, como historiales y tendencias de capacidad	•	•	•	•	•
Ver, asignar y resolver eventos	•	•	•		
Ver objetos de servicio de almacenamiento, como asociaciones de SVM y grupos de recursos	•	•	•		
Ver políticas de umbral	•	•	•		
Administrar objetos de servicio de almacenamiento, como asociaciones SVM y grupos de recursos		•	•		

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informe
Definir alertas		•	•		
Administrar las opciones de gestión de almacenamiento		•	•		
Administrar políticas de gestión de almacenamiento		•	•		
Administrar usuarios			•		
Administrar opciones administrativas			•		
Definir políticas de umbral			•		
Administrar el acceso a la base de datos			•		
Administrar la integración con WFA y proporcionar acceso a las vistas de la base de datos				•	
Programar y guardar informes		•	•		
Ejecutar operaciones "Repararlo" desde Acciones de administración		•	•		

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informe
Proporcionar acceso de solo lectura a las vistas de la base de datos					•

Administrar la configuración de autenticación SAML

Una vez que haya configurado los ajustes de autenticación remota, puede habilitar la autenticación SAML (lenguaje de marcado de aserción de seguridad) para que los usuarios remotos sean autenticados por un proveedor de identidad seguro (IdP) 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 que se haya habilitado 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 identidad

Al configurar Unified Manager para usar un proveedor de identidad (IdP) para realizar la autenticación SAML para todos los usuarios remotos, debe tener en cuenta algunas configuraciones necesarias para que la conexión a Unified Manager sea exitosa.

Debe ingresar la URI y los metadatos de Unified Manager en el servidor IdP. Puede copiar esta información desde la página de autenticación SAML de Unified Manager. Unified Manager se considera el proveedor de servicios (SP) en el estándar Security Assertion Markup Language (SAML).

Estándares de cifrado admitidos

- Estándar de cifrado avanzado (AES): AES-128 y AES-256
- Algoritmo hash seguro (SHA): SHA-1 y SHA-256

Proveedores de identidad validados

- Santo y seña
- Servicios de federación de Active Directory (ADFS)

Requisitos de configuración de ADFS

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

Regla de reclamación	Valor
Nombre de la cuenta SAM	Identificación del nombre
Nombre de la cuenta SAM	urna:oid:0.9.2342.19200300.100.1.1
Grupos de tokens - Nombre no calificado	urna:oid:1.3.6.1.4.1.5923.1.5.1.1

- Debe configurar 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 Políticas de autenticación en la vista de árbol izquierda.
  c. En Acciones, a la derecha, haga clic en Editar política de autenticación primaria global.
  d. Establezca el método de autenticación de intranet en “Autenticación de formularios” en lugar del valor predeterminado “Autenticación de Windows”.
- En algunos casos, se rechaza el inicio de sesión a través del IdP cuando el certificado de seguridad de Unified Manager está firmado por CA. Hay dos soluciones alternativas para resolver este problema:
  - Siga las instrucciones identificadas en el enlace para deshabilitar la verificación de revocación en el servidor ADFS para la parte confiable asociada al certificado de CA encadenado:

    "Deshabilitar la comprobación de revocación por cada confianza de parte autenticada"

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

Otros requisitos de configuración

- La diferencia horaria del Unified Manager está establecida en 5 minutos, por lo que la diferencia horaria entre el servidor IdP y el servidor del Unified Manager no puede ser más de 5 minutos o la autenticación fallará.

Habilitar la autenticación SAML

Puede habilitar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para que los usuarios remotos sean autenticados por un proveedor de identidad seguro (IdP) antes de que puedan acceder a la interfaz de usuario web de Unified Manager.

Antes de empezar

- Debe haber configurado la autenticación remota y verificado que sea exitosa.
- Debe haber creado al menos un Usuario remoto o un Grupo remoto con el rol de Administrador de aplicaciones.
- El proveedor de identidad (IdP) debe ser compatible con Unified Manager y debe estar configurado.
- Debe tener la URL y los metadatos del IdP.
- Debe tener acceso al servidor IdP.

Una vez que haya habilitado la autenticación SAML desde Unified Manager, los usuarios no podrán acceder a

la interfaz gráfica de usuario hasta que el IdP se haya configurado con la información del host del servidor de Unified Manager. Por lo tanto, debe estar preparado para completar ambas partes de la conexión antes de comenzar 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 que se haya habilitado 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, a los comandos de Unified Manager o a 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 muestran los campos necesarios para configurar la conexión IdP.

3. Ingrese la URI del IdP y los metadatos del IdP necesarios para conectar el servidor de Unified Manager al servidor del IdP.

   Si se puede acceder al servidor IdP directamente desde el servidor Unified Manager, puede hacer clic en el botón **Obtener metadatos IdP** después de ingresar el URI del IdP para completar el campo Metadatos IdP automáticamente.

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

   Puede configurar el servidor IdP con esta información en este momento.

5. Haga clic en **Guardar**.

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

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

La próxima vez que usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager, ingresarán 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 aún no lo ha completado, acceda a su IdP e ingrese la URI y los metadatos del servidor Unified Manager para completar la configuración.

Al utilizar ADFS como proveedor de identidad, la GUI de Unified Manager no respeta el tiempo de espera de ADFS y continuará funcionando hasta que se alcance 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 funciones** > **Tiempo de espera de inactividad**.

Cambiar el proveedor de identidad utilizado para la autenticación SAML

Puede cambiar el proveedor de identidad (IdP) que Unified Manager utiliza para

autenticar usuarios remotos.

Antes de empezar

- Debe tener la URL y los metadatos del 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. Ingrese la nueva URI del IdP y los metadatos del IdP necesarios para conectar el servidor Unified Manager al IdP.

   Si se puede acceder al IdP directamente desde el servidor de Unified Manager, puede hacer clic en el botón **Obtener metadatos del IdP** después de ingresar la URL del IdP para completar el campo Metadatos del IdP automáticamente.

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

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

5. Haga clic en **Aceptar**.

Acceda al nuevo IdP e ingrese la URI y los metadatos del servidor Unified Manager para completar la configuración.

La próxima vez que usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager, ingresarán sus credenciales en la nueva página de inicio de sesión de IdP en lugar de la página de inicio de sesión de IdP anterior.

Actualizar la configuración de autenticación SAML después del cambio del certificado de seguridad de Unified Manager

Cualquier cambio en el certificado de seguridad HTTPS instalado en el servidor de Unified Manager requiere que actualice la configuración de autenticación SAML. El certificado se actualiza si cambia el nombre del sistema host, le asigna una nueva dirección IP o cambia manualmente el certificado de seguridad del sistema.

Una vez que se cambia 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 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**, ingrese el número para la opción **Deshabilitar autenticación SAML**.

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

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

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

7. Haga clic en **Confirmar y cerrar sesión** y Unified Manager se reiniciará.
8. Acceda a su servidor IdP e ingrese la URI y los metadatos del servidor Unified Manager para completar la configuración.

Proveedor de identidad	Pasos de configuración
ADFS	a. Eliminar la entrada de confianza de usuario autenticado existente en la GUI de administración de ADFS. b. Agregue una nueva entrada de confianza de usuario confiado utilizando el `saml_sp_metadata.xml` desde el servidor 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 usuario confiable. d. Reinicie el servicio ADFS de Windows.
Santo y seña	a. Actualice el nuevo FQDN del servidor de Unified Manager en el `attribute-filter.xml` y `relying-party.xml` archivos. b. Reinicie el servidor web Apache Tomcat y espere a que el puerto 8005 esté en línea.

9. Inicie sesión en Unified Manager y verifique que la autenticación SAML funcione como se espera a través de su IdP.

Deshabilitar la autenticación SAML

Puede deshabilitar la autenticación SAML cuando desee dejar de autenticar usuarios remotos a través de un proveedor de identidad seguro (IdP) antes de que puedan iniciar sesión en la interfaz de usuario web de Unified Manager. Cuando la autenticación SAML está deshabilitada, 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 mediante 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 SAML.

Pasos

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

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

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

La próxima vez que usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, ingresarán 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 su IdP y elimine la URI y los metadatos del servidor Unified Manager.

Deshabilitar la autenticación SAML desde la consola de mantenimiento

Es posible que deba deshabilitar la autenticación SAML desde la consola de mantenimiento cuando no haya acceso a la GUI de Unified Manager. Esto podría suceder en casos de mala configuración o si el IdP no es accesible.

Antes de empezar

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

Cuando la autenticación SAML está deshabilitada, 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 puede deshabilitar la autenticación SAML desde la página Configuración/Autenticación en la interfaz de usuario.

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

Pasos

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

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

3. Escriba **y** y luego presione Enter y Unified Manager se reiniciará.

La próxima vez que usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, ingresarán 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 es necesario, acceda a su IdP y elimine la URL y los metadatos del servidor Unified Manager.

Página de autenticación SAML

Puede utilizar la página Autenticación SAML para configurar Unified Manager para autenticar usuarios remotos mediante SAML a través de un proveedor de identidad seguro (IdP) antes de 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.

Una vez configurada la autenticación remota y los usuarios remotos, puede seleccionar la casilla de verificación Habilitar autenticación SAML para habilitar la autenticación mediante un proveedor de identidad seguro.

- **URI del proveedor de identidad**

  La URI para acceder al IdP desde el servidor de Unified Manager. A continuación se enumeran ejemplos de URI.

  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 del IdP**

  Los metadatos del IdP en formato XML.

  Si se puede acceder a la URL del IdP desde el servidor de Unified Manager, puede hacer clic en el botón **Obtener metadatos del IdP** para completar este campo.

- **Sistema host (FQDN)**

  El FQDN del sistema host de Unified Manager tal como se definió durante la instalación. Puede cambiar este valor si es necesario.

- **URI del host**

  La URI para acceder al sistema host de Unified Manager desde el IdP.

- **Metadatos del host**

Los metadatos del sistema host en formato XML.

Administrar la autenticación

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

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

Editar servidores de autenticación

Puede cambiar el puerto que utiliza el servidor de Unified Manager para comunicarse con su servidor de autenticación.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Autenticación remota**.
2. Marque la casilla **Deshabilitar búsqueda de grupo anidado**.
3. En el área **Servidores de autenticación**, seleccione el servidor de autenticación que desea editar y luego 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 evitar que el servidor de Unified Manager se comunique con el servidor de autenticación. Por ejemplo, si desea cambiar un servidor de autenticación con el que se comunica el servidor de administración, puede eliminar el servidor de autenticación y agregar uno nuevo.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

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

Pasos

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

   Si la opción **Usar conexión segura** está habilitada, los certificados asociados con el servidor de

autenticación se eliminan junto con el servidor de autenticación.

Autenticación con Active Directory o OpenLDAP

Puede habilitar la autenticación remota en el servidor de administración y configurar el servidor de administración para que se comunique con sus servidores de autenticación para 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:

- Directorio activo de Microsoft

  No puedes utilizar Microsoft Lightweight Directory Services.

- OpenLDAP

Puede seleccionar el servicio de autenticación requerido y agregar los servidores de autenticación adecuados para permitir que los usuarios remotos en el servidor de autenticación accedan a Unified Manager. El servidor de autenticación mantiene las credenciales de los usuarios o grupos remotos. El servidor de administración utiliza el Protocolo ligero de acceso a directorios (LDAP) para autenticar usuarios remotos dentro del servidor de autenticación configurado.

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

Registro de auditoría

Puede detectar si los registros de auditoría se han visto comprometidos mediante el uso de Registros de auditoría. Todas las actividades realizadas por un usuario son monitoreadas y registradas en los Registros de Auditoría. Las auditorías se realizan para todas las interfaces de usuario y las funcionalidades de las API expuestas públicamente de Active IQ Unified Manager.

Puede utilizar la **Vista de archivo de registro de auditoría** para ver y acceder a todos los archivos de registro de auditoría disponibles en su Active IQ Unified Manager. Los archivos en el Registro de auditoría: Vista de archivos se enumeran según su fecha de creación. Esta vista muestra información de todos los registros de auditoría que se capturan desde la instalación o actualización hasta el presente en el sistema. Cada vez 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 utilizando el atributo "Estado de integridad del archivo", que se monitorea activamente para detectar alteraciones o eliminaciones del archivo de registro. Los registros de auditoría pueden tener uno de los siguientes estados cuando están disponibles en el sistema:

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

Estado	Descripción
NORMAL	Archivo inactivo, comprimido y almacenado en el sistema.
MANIPULADO	Archivo que ha sido comprometido por un usuario que lo ha editado manualmente.
ELIMINACIÓN MANUAL	Archivo que fue eliminado por un usuario autorizado.
ROLLOVER_DELETE	Archivo que se eliminó debido a la eliminación gradual según la política de configuración gradual.
ELIMINACIÓN INESPERADA	Archivo que se eliminó por razones desconocidas.

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

- Configurar
- Borrar
- Descargar

El botón **ELIMINAR** le 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, lo que ayudará 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.

Eliminar un archivo de registro provocará la eliminación del archivo del sistema, pero la entrada en la tabla de base de datos no se eliminará.

Puede descargar los registros de auditoría de Active IQ Unified Manager utilizando el botón **DESCARGAR** en la sección Registros de auditoría y exportar los archivos de registro de auditoría. Los archivos que están marcados como "NORMAL" o "MANIPULADOS" se descargan en un formato comprimido. `.gzip` formato.

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

Cuando se genera un paquete de AutoSupport completo, el paquete de soporte incluye archivos de registro de auditoría archivados y activos. Pero cuando se genera un paquete de soporte ligero, solo incluye los registros de auditoría activos. Los registros de auditoría archivados no están incluidos.

Configurar registros de auditoría

Puede utilizar el botón **Configurar** en la sección Registros de auditoría para configurar una política continua para los archivos de registro de auditoría y también para habilitar el registro remoto para los registros de auditoría.

Puede establecer los valores en **TAMAÑO MÁXIMO DE ARCHIVO** y **DÍAS DE RETENCIÓN DEL REGISTRO DE AUDITORÍA** según la cantidad y frecuencia de datos que desee almacenar en el sistema. El valor en el campo **TAMAÑO TOTAL DEL REGISTRO DE AUDITORÍA** es el tamaño total de los datos del registro de

auditoría presentes en el sistema. La política de renovación está determinada por los valores en el campo **DÍAS DE RETENCIÓN DEL REGISTRO DE AUDITORÍA**, **TAMAÑO MÁXIMO DE ARCHIVO** y **TAMAÑO TOTAL DEL REGISTRO DE AUDITORÍA**. Cuando el tamaño de la copia de seguridad del registro de auditoría alcanza el valor configurado en **TAMAÑO TOTAL DEL REGISTRO DE AUDITORÍA**, se elimina el archivo que se archivó primero. Esto significa que se elimina el archivo más antiguo. Pero la entrada del archivo continúa estando disponible en la base de datos y está marcada como "Rollover Delete". El valor **DÍAS DE RETENCIÓN DEL REGISTRO DE AUDITORÍA** corresponde a la cantidad de días que se conservan los archivos del registro de auditoría. Cualquier archivo que sea más antiguo que el valor establecido en este campo se renueva.

Pasos

1. Haga clic en **Registros de auditoría** > > **Configurar**.
2. Introduzca valores en **TAMAÑO MÁXIMO DE ARCHIVO**, **TAMAÑO TOTAL DEL REGISTRO DE AUDITORÍA** y **DÍAS DE RETENCIÓN DEL REGISTRO DE AUDITORÍA**.

   Si desea habilitar el registro remoto, debe seleccionar **Habilitar registro remoto**. /// 2025-6-11, OTHERDOC-133

Habilitar el registro remoto de registros de auditoría

Puede seleccionar la casilla de verificación **Habilitar registro remoto** en el cuadro de diálogo Configurar registros de auditoría para habilitar el registro de auditoría remoto. Puede utilizar esta función para transferir registros de auditoría a un servidor Syslog remoto. Esto le permitirá administrar sus 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 alteren los archivos de registro de auditoría en el servidor Active IQ Unified Manager .

Pasos

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

   Se muestran 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 CA DEL SERVIDOR**, haga clic en **EXAMINAR** para seleccionar un certificado público del servidor de destino.

   El certificado debe cargarse en `.pem` formato. Este certificado debe obtenerse del servidor Syslog de destino y no debe haber expirado. El certificado debe contener el “nombre de host” seleccionado como parte del `SubjectAltName` Atributo (SAN).

4. Introduzca los valores para los siguientes campos: **CHARSET**, **CONNECTION TIMEOUT**, **RETRASO 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 **Habilitar autenticación de cliente** si el servidor Syslog de destino

requiere autenticación basada en certificado.

Necesitará descargar el certificado de autenticación del cliente y cargarlo en el servidor Syslog antes de guardar la configuración del registro de auditoría; de lo contrario, la conexión fallará. Dependiendo del tipo de servidor Syslog, es posible que necesite crear un hash del certificado de autenticación del cliente.

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

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

   Serás redirigido a la página de Registros de auditoría.

> El valor de **Tiempo de espera de conexión** puede afectar la configuración. Si la configuración tarda más tiempo en responder que el valor definido, puede provocar una falla en la configuración debido a un error de conexión. Para establecer una conexión exitosa, aumente el valor de **Tiempo de espera de conexión** e intente la configuración nuevamente.

Página de autenticación remota

Puede utilizar la página Autenticación remota para configurar Unified Manager para que se comunique con su servidor de autenticación para 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 Administrador de almacenamiento.

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

- **Servicio de autenticación**

  Le 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. Puede especificar un servicio de autenticación solo si ha habilitado la autenticación remota.

  - **Directorio Activo**
    - Nombre del administrador

      Especifica el nombre del administrador del servidor de autenticación.

    - Password

      Especifica la contraseña para acceder al servidor de autenticación.

    - Nombre distinguido de la 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 distinguido base es **cn=ou,dc=domain,dc=com**.

    - Deshabilitar la búsqueda de grupos anidados

Especifica si se debe habilitar o deshabilitar la opción de búsqueda de grupo anidado. De forma predeterminada, esta opción está deshabilitada. Si usa Active Directory, puede acelerar la autenticación deshabilitando la compatibilidad con grupos anidados.

- Utilice una conexión segura

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

- **OpenLDAP**
  - Nombre distinguido de Bind

    Especifica el nombre distinguido de enlace que se utiliza junto con el nombre distinguido base para encontrar usuarios remotos en el servidor de autenticación.

  - Vincular contraseña

    Especifica la contraseña para acceder al servidor de autenticación.

  - Nombre distinguido de la 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 distinguido base es **cn=ou,dc=domain,dc=com**.

  - Utilice una conexión segura

    Especifica que se utiliza LDAP seguro para comunicarse con servidores de autenticación LDAP.

- **Otros**
  - Nombre distinguido de Bind

    Especifica el nombre distinguido de enlace que se utiliza junto con el nombre distinguido base para buscar usuarios remotos en el servidor de autenticación que ha configurado.

  - Vincular contraseña

    Especifica la contraseña para acceder al servidor de autenticación.

  - Nombre distinguido de la 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 distinguido base es **cn=ou,dc=domain,dc=com**.

  - Versión del protocolo

    Especifica la versión del Protocolo ligero de acceso a directorios (LDAP) compatible con su servidor de autenticación. Puede especificar si la versión del protocolo debe detectarse automáticamente o establecer la versión en 2 o 3.

  - Atributo de nombre de usuario

    Especifica el nombre del atributo en el servidor de autenticación que contiene los nombres de

inicio de sesión de los usuarios que serán autenticados por el servidor de administración.

- Atributo de membresía de grupo

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

- Identificación de usuario final

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

- Deshabilitar la búsqueda de grupos anidados

  Especifica si se debe habilitar o deshabilitar la opción de búsqueda de grupo anidado. De forma predeterminada, esta opción está deshabilitada. Si usa Active Directory, puede acelerar la autenticación deshabilitando la compatibilidad con grupos anidados.

- Miembro

  Especifica el nombre del atributo que utiliza su servidor de autenticación para almacenar información sobre los miembros individuales de un grupo.

- Clase de objeto de usuario

  Especifica la clase de objeto de un usuario en el servidor de autenticación remoto.

- Clase de objeto de grupo

  Especifica la clase de objeto de todos los grupos en el servidor de autenticación remoto.

> Los valores que ingrese para los atributos *Member*, *User Object Class* y *Group Object Class* deben ser los mismos que los agregados en sus configuraciones de Active Directory, OpenLDAP y LDAP. De lo contrario, la autenticación podría fallar.

- Utilice una 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 todos los servidores de autenticación existentes y agregar servidores de autenticación nuevos.

Área de servidores de autenticación

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

- **Botones de comando**

Le permite agregar, editar o eliminar servidores de autenticación.

- Agregar

  Le permite agregar un servidor de autenticación.

Si el servidor de autenticación que está agregando es parte de un par de alta disponibilidad (que utiliza la misma base de datos), también puede agregar el servidor de autenticación asociado. Esto permite que el servidor de administración se comunique con el socio cuando uno de los servidores de autenticación no está disponible.

- Editar

  Le permite editar la configuración de un servidor de autenticación seleccionado.

- Borrar

  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 utiliza para autenticar al usuario en el servidor de administración.

- **Puerto**

  Muestra el número de puerto del servidor de autenticación.

- **Prueba de autenticación**

  Este botón valida la configuración de su servidor de autenticación al autenticar un usuario o grupo remoto.

  Durante la prueba, si solo especifica el nombre de usuario, el servidor de administración busca al usuario remoto en el servidor de autenticación, pero no autentica al usuario. Si especifica tanto el nombre de usuario como la contraseña, el servidor de administración busca y autentica al usuario remoto.

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

Administrar certificados de seguridad

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

Ver el certificado de seguridad HTTPS

Puede comparar los detalles del certificado HTTPS con el certificado recuperado en su navegador para asegurarse de que la conexión cifrada de su navegador a Unified Manager no esté siendo interceptada.

Antes de empezar

Debe tener el rol de Operador, Administrador de aplicaciones o Administrador de almacenamiento.

Al ver el certificado, podrá verificar el contenido de un certificado regenerado o ver los nombres alternativos

del sujeto (SAN) desde los cuales 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 se muestra en la página Certificado HTTPS, puede ver el certificado de conexión en su navegador.

Descargar una solicitud de firma de certificado HTTPS

Puede descargar una solicitud de firma de certificación para el certificado de seguridad HTTPS actual para poder proporcionar el archivo a una autoridad de certificación para que lo firme. Un certificado firmado por una CA ayuda a prevenir ataques de intermediario y proporciona una mejor protección de seguridad que un certificado autofirmado.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

Pasos

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

Puede proporcionar el archivo a una autoridad de certificación para que lo firme y luego instalar el certificado firmado.

Instalar un certificado HTTPS firmado y devuelto por una CA

Puede cargar e instalar un certificado de seguridad después de que una autoridad certificadora lo haya firmado y devuelto. El archivo que cargue e instale debe ser una versión firmada del certificado autofirmado existente. Un certificado firmado por una CA ayuda a prevenir ataques de intermediario y proporciona una mejor protección de seguridad que un certificado autofirmado.

*¿Qué? Antes de empezar

Debes haber completado las siguientes acciones:

- Descargué el archivo de solicitud de firma de certificado y lo firmé mediante una autoridad de certificación.
- Guardó la cadena de certificados en formato PEM
- Se incluyen todos los certificados de la cadena, desde el certificado del servidor Unified Manager hasta el certificado de firma raíz, incluidos todos los certificados intermedios presentes.

Debe tener el rol de Administrador de aplicaciones.

Si la validez del certificado para el cual se creó un 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 se muestra, haga clic en **Elegir archivo…** para localizar el archivo que desea cargar.
4. Seleccione el archivo y luego haga clic en **Instalar** para instalar el archivo.

   Para obtener más información, consulte"Instalación de un certificado HTTPS generado mediante herramientas externas" .

Ejemplo de cadena de certificados

El siguiente ejemplo muestra cómo podría aparecer el archivo de la 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 mediante herramientas externas

Puede instalar certificados autofirmados o firmados por una CA y generados mediante una herramienta externa como OpenSSL, BoringSSL, 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 en la sección General. El archivo que cargue debe tener el siguiente formato de entrada.

1. Clave privada del servidor que pertenece al host de Active IQ Unified Manager
2. Certificado del servidor que coincide con la clave privada
3. Certificado de las CA en sentido inverso 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 “secp384r1”. Ejemplo de certificado con un par 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 del 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-----
```

Después de cargar el certificado, debe reiniciar la instancia de Active IQ Unified Manager para que los

cambios surtan efecto.

Comprobaciones al cargar certificados generados externamente

El sistema realiza comprobaciones mientras se carga un certificado generado mediante herramientas externas. Si alguna de las comprobaciones falla, el certificado se rechaza. También se incluyen validaciones para los certificados que se generan a partir del CSR dentro del producto y para los certificados que se generan utilizando herramientas externas.

- La clave privada en la entrada se valida con el certificado del host en la entrada.
- El nombre común (CN) en el certificado del host se compara con el FQDN del host.
- El nombre común (CN) del certificado de host no debe estar vacío ni en blanco y no debe configurarse como localhost.
- La fecha de inicio de la validez no debe ser futura y la fecha de vencimiento de la validez del certificado no debe ser pasada.
- Si existe una CA intermedia o CA, la fecha de inicio de validez del certificado no debe ser futura y la fecha de vencimiento de la validez no debe ser pasada.

La clave privada en 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 falla la instalación del certificado, consulte el artículo de la base de conocimientos (KB):https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager no puede instalar un certificado generado externamente"^]

Descripciones de páginas para la gestión de certificados

Puede utilizar la página de Certificado HTTPS para ver los certificados de seguridad actuales y generar nuevos certificados HTTPS.

Página del certificado HTTPS

La página Certificado HTTPS le permite ver el certificado de seguridad actual, descargar una solicitud de firma de certificado, generar un nuevo certificado HTTPS autofirmado o instalar un nuevo certificado HTTPS.

Si no ha generado un nuevo certificado HTTPS autofirmado, 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 solicitud de firma de certificado HTTPS**

  Descarga una solicitud de certificación para el certificado HTTPS actualmente instalado. Su navegador le solicita que guarde el archivo <hostname>.csr para que pueda proporcionarlo a una autoridad de certificación para que lo firme.

- **Instalar certificado HTTPS**

  Le permite cargar e instalar un certificado de seguridad después de que una autoridad certificadora lo haya firmado y devuelto. El nuevo certificado entrará en vigor después de reiniciar el servidor de administración.

- **Regenerar certificado HTTPS**

  Le permite generar un nuevo certificado HTTPS autofirmado, que reemplaza el certificado de seguridad actual. El nuevo certificado entrará en vigor después de reiniciar Unified Manager.

Cuadro de diálogo Regenerar certificado HTTPS

El cuadro de diálogo Regenerar certificado HTTPS le permite personalizar la información de seguridad y luego generar un nuevo certificado HTTPS con esa información.

La información del certificado actual aparece en esta página.

La selección “Regenerar utilizando los atributos del certificado actual” y “Actualizar los atributos del certificado actual” le permite regenerar el certificado con la información actual o generar un certificado con información nueva.

- **Nombre común**

  Requerido. 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 contactar a su organización; normalmente la dirección de correo electrónico del administrador del certificado o del departamento de TI.

- **Compañía**

  Opcional. Normalmente, el nombre incorporado de su empresa.

- **Departamento**

  Opcional. El nombre del departamento de su empresa.

- **Ciudad**

  Opcional. La ubicación de la ciudad de su empresa.

- **Estado**

  Opcional. La ubicación estatal o provincial, no abreviada, de su empresa.

- **País**

  Opcional. La ubicación del país de su empresa. Normalmente se trata de un código ISO de dos letras del país.

- **Nombres alternativos**

  Requerido. Nombres de dominio adicionales, no principales, que se pueden usar para acceder a este servidor además del host local existente u otras direcciones de red. Separe cada nombre alternativo con una coma.

  Seleccione la casilla de verificación "Excluir información de identificación local (por ejemplo, localhost)" si desea eliminar la información de identificación local del campo Nombres alternativos en el certificado. Cuando esta casilla de verificación está seleccionada, solo lo que ingrese en el campo se utilizará en el campo Nombres alternativos. Si se deja en blanco, el certificado resultante no tendrá ningún campo de Nombres alternativos.

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

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

- **PERIODO 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".