Configurar Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

Tabla de contenidos

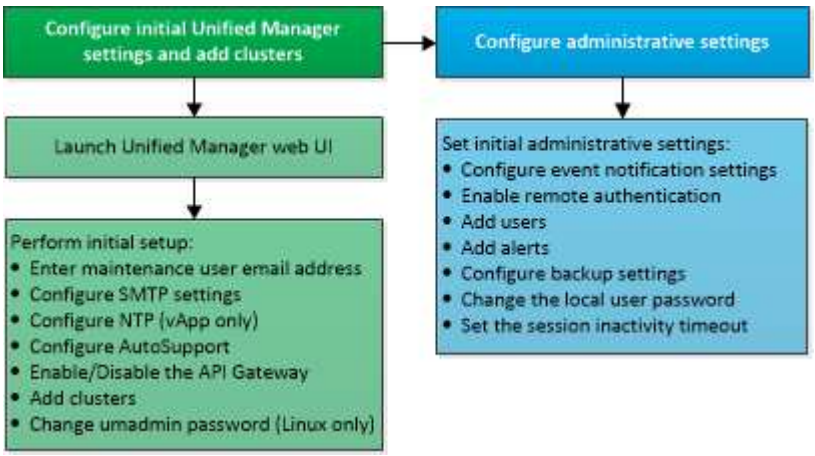
Configurar Active IQ Unified Manager

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

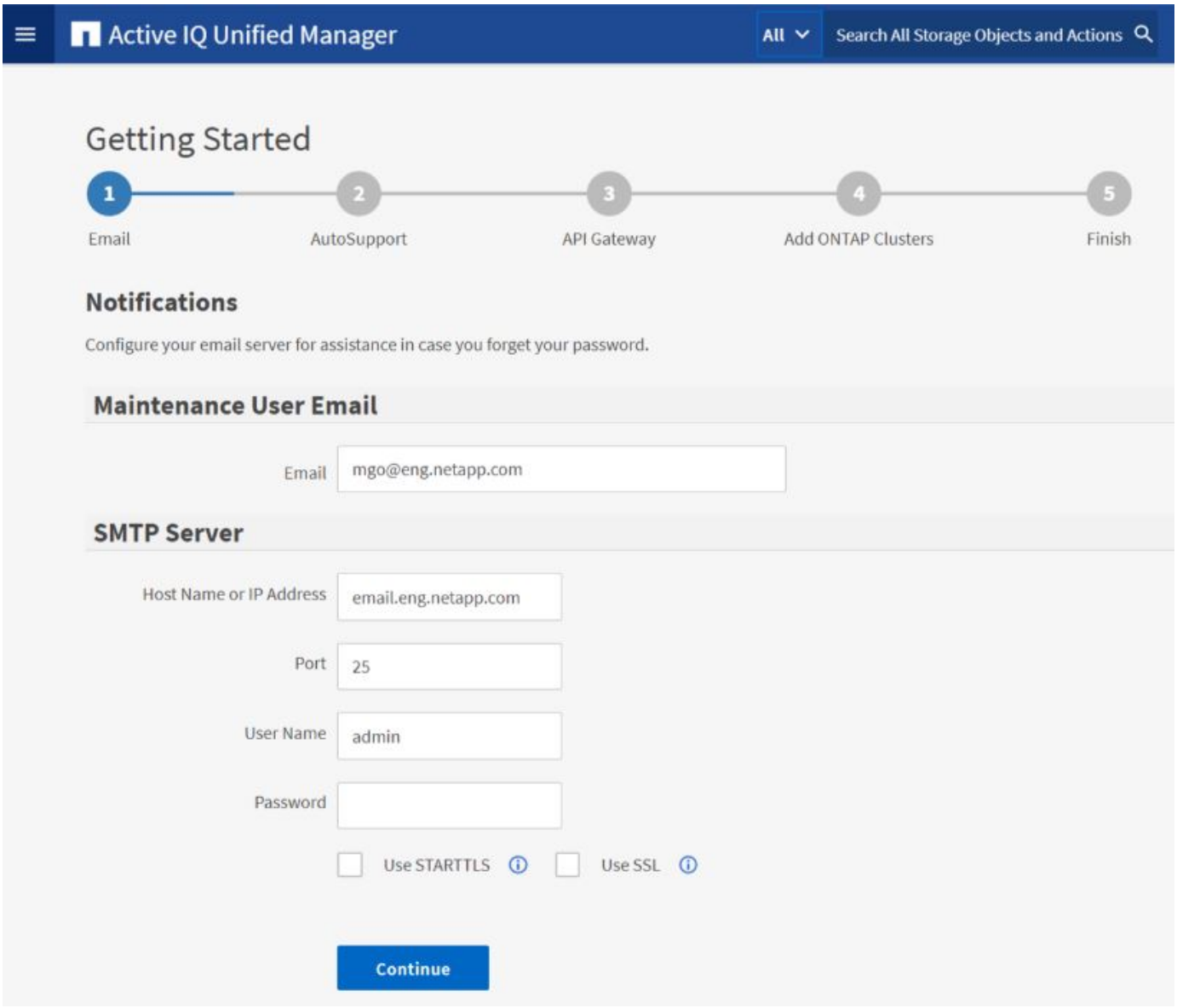
Para utilizar Unified Manager, primero debe configurar las opciones de configuración inicial, incluido el servidor NTP, la dirección de correo electrónico del usuario de mantenimiento, el host del servidor SMTP y la adición de clústeres ONTAP .

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.