Realizar tareas administrativas y de configuración

Active IQ Unified Manager

NetApp
April 02, 2025

This PDF was generated from https://docs.netapp.com/es-es/active-iq-unified-manager-97/config/concept-overview-of-the-configuration-sequence.html on April 02, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Realizar tareas administrativas y de configuración . . . 1
Configurando Active IQ Unified Manager . . . 1
Descripción general de la secuencia de configuración . . . 1
Acceder a la interfaz de usuario web de Unified Manager . . . 1
Realizando la configuración inicial de la interfaz de usuario web de Unified Manager . . . 2
Añadir clústeres . . . 4
Configuración de Unified Manager para enviar notificaciones de alerta . . . 6
Eventos de EMS que se añaden automáticamente a Unified Manager . . . 14
Suscripción a eventos de EMS de ONTAP . . . 18
Gestión de la configuración de autenticación SAML . . . 19
Configurar los ajustes de backup de la base de datos . . . 22
Cambiando la contraseña de usuario local . . . 23
Configurar el tiempo de espera de inactividad de la sesión . . . 23
Cambie el nombre de host de Unified Manager . . . 24
Habilitar y deshabilitar la gestión del almacenamiento basada en políticas . . . 28
Mediante la consola de mantenimiento . . . 29
Qué funcionalidad proporciona la consola de mantenimiento . . . 29
Lo que hace el usuario de mantenimiento . . . 30
Capacidades de diagnóstico del usuario . . . 30
Acceso a la consola de mantenimiento . . . 30
Acceder a la consola de mantenimiento mediante la consola de la máquina virtual de vSphere . . . 31
Menús de la consola de mantenimiento . . . 32
Cambiar la contraseña del usuario de mantenimiento en Windows . . . 36
Cambiar la contraseña de umadmin en sistemas Linux . . . 37
Cambiar los puertos Unified Manager utiliza para los protocolos HTTP y HTTPS . . . 37
Se añaden interfaces de red . . . 38
Agregar espacio en disco al directorio de la base de datos de Unified Manager . . . 39

Realizar tareas administrativas y de configuración

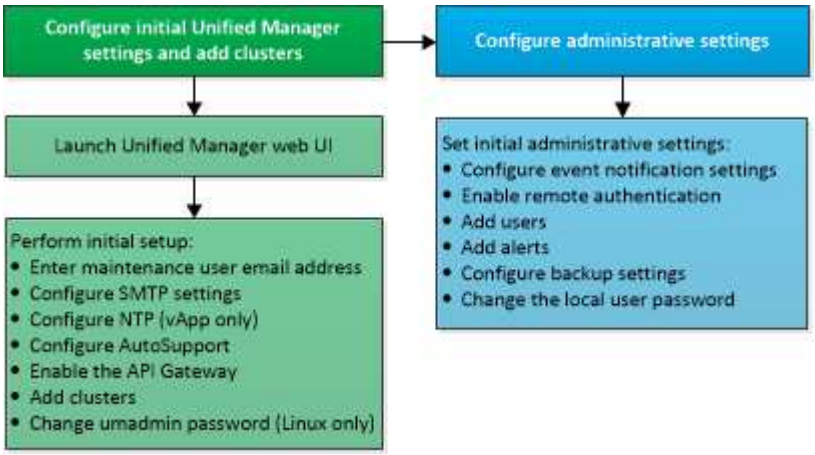
Configurando Active IQ Unified Manager

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

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

Descripción general de la secuencia de configuración

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



Acceder a la interfaz de usuario web de Unified Manager

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

Antes de empezar

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

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

Pasos

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

   El enlace tiene el formato siguiente: https://`URL`.

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

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

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

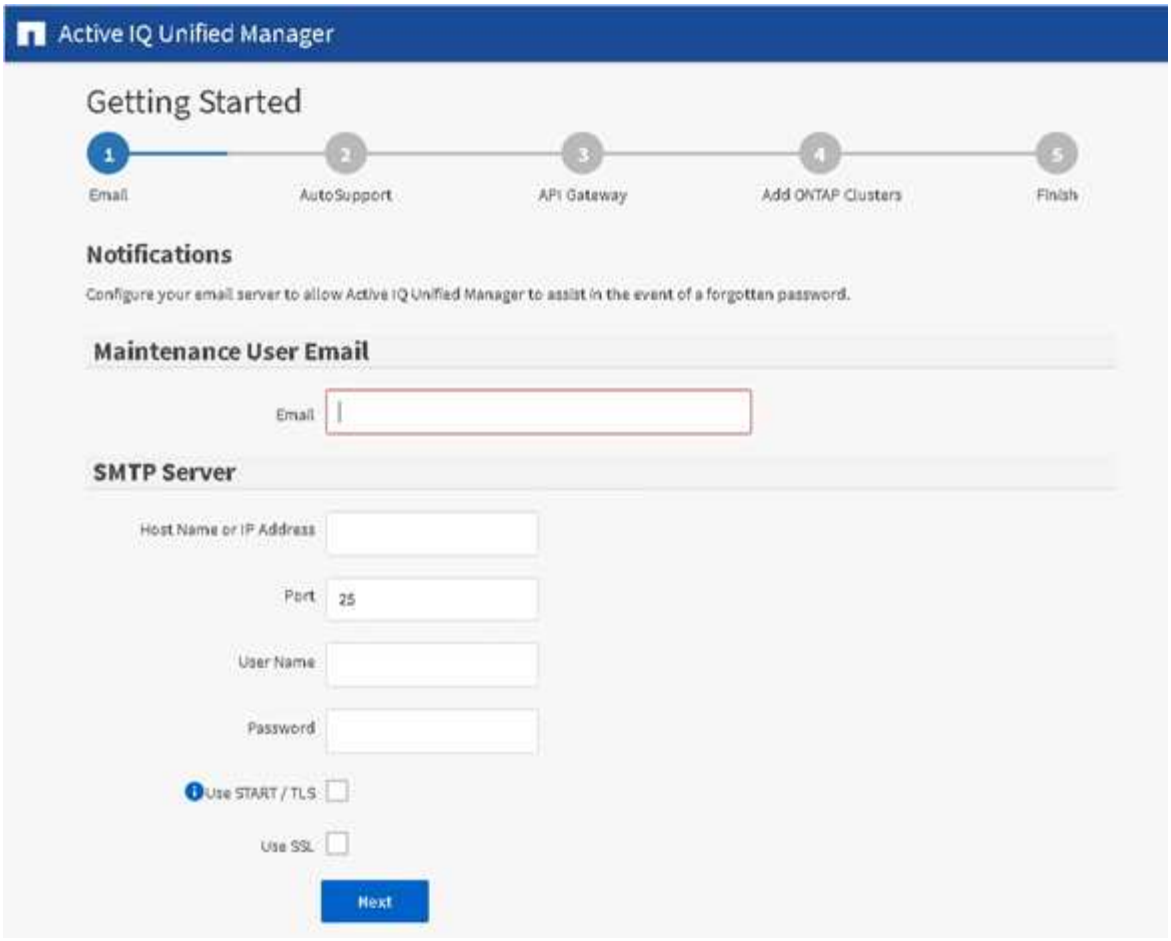
Antes de empezar

Debe haber realizado las siguientes operaciones:

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

Acerca de esta tarea

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



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

Pasos

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

   Si necesita designar un proxy para proporcionar acceso a Internet con el fin de enviar contenido AutoSupport, o si desea desactivar AutoSupport, utilice la opción **General** > **AutoSupport** de la interfaz de usuario web.

3. En los sistemas Red Hat y CentOS puede cambiar la contraseña de usuario umadmin de la cadena "'admin'" predeterminada a una cadena personalizada.
4. En la página **Configurar puerta de enlace de API**, seleccione si desea utilizar la función API Gateway que permite a Unified Manager administrar los clústeres de ONTAP que está planeando supervisar mediante API DE REST de ONTAP. A continuación, haga clic en **continuar**.

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

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

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

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

Resultados

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

Añadir clústeres

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

Antes de empezar

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe tener la siguiente información:
  - El nombre de host o la dirección IP de administración del clúster

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

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

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

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

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

    Puede agregar clústeres que están detrás de un servidor de seguridad/NAT utilizando la dirección IP NAT de Unified Manager. Los sistemas SnapProtect o de automatización de flujo de trabajo conectados también deben estar detrás del servidor de seguridad NAT y las llamadas API de SnapProtect deben utilizar la dirección IP NAT para identificar el clúster.

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

Acerca de esta tarea

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

Puede supervisar un único clúster mediante dos instancias de Unified Manager siempre que haya configurado una segunda LIF de gestión del clúster para que cada instancia de Unified Manager se conecte a través de un LIF diferente.

Pasos

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

   Es posible cambiar la dirección IP de gestión del clúster de IPv6 a IPv4 o de IPv4 a IPv6. La nueva dirección IP se refleja en la cuadrícula del clúster y en la página de configuración del clúster una vez completado el siguiente ciclo de supervisión.

4. Haga clic en **Enviar**.
5. En el cuadro de diálogo **autorizar host**, haga clic en **Ver certificado** para ver la información del certificado sobre el clúster.
6. Haga clic en **Sí**.

   Unified Manager comprueba el certificado solo cuando se añade inicialmente el clúster. Unified Manager no comprueba el certificado para cada llamada API a ONTAP.

   Si el certificado ha caducado, no puede añadir un clúster nuevo. Primero debe renovar el certificado SSL y, a continuación, añadir el clúster.

Resultados

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

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

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

Configuración de Unified Manager para enviar notificaciones de alerta

Puede configurar Unified Manager para que envíe notificaciones que le alertan de los eventos de su entorno. Antes de que las notificaciones se puedan enviar, debe configurar varias otras opciones de Unified Manager.

Antes de empezar

Debe tener la función Administrador de aplicaciones.

Acerca de esta tarea

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

Pasos

1. "Configure los ajustes de notificación de eventos"

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

2. "Habilite la autenticación remota"

   Si desea que los usuarios remotos de LDAP o Active Directory accedan a la instancia de Unified Manager y reciban notificaciones de alerta, debe habilitar la autenticación remota.

3. Agregue servidores de autenticación

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

4. "Añadir usuarios"

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

5. "Añadir alertas"

   Después de añadir la dirección de correo electrónico para enviar notificaciones, se añadieron usuarios para recibir las notificaciones, configurar los ajustes de red y configurar las opciones SMTP y SNMP necesarias para el entorno, y después puede asignar alertas.

Configuración de los ajustes de notificación de eventos

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

Antes de empezar

Debe tener la siguiente información:

- Dirección de correo electrónico desde la cual se envía la notificación de alertas

  La dirección de correo electrónico aparece en el campo «'de'» en las notificaciones de alerta enviadas. Si el correo electrónico no se puede entregar por cualquier motivo, esta dirección de correo electrónico también se utiliza como destinatario para el correo no entregable.

- El nombre de host del servidor SMTP, así como el nombre de usuario y la contraseña para acceder al servidor
- Nombre de host o dirección IP del host de destino de captura que recibirá la captura SNMP, junto con la versión SNMP, el puerto de capturas saliente, la comunidad y otros valores de configuración SNMP requeridos

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

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

Pasos

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

```
**If the From Address is pre-filled with the address
"ActiveIQUnifiedManager@localhost.com", you should change it
to a real, working email address to make sure that all email
notifications are delivered successfully.
** If the host name of the SMTP server cannot be resolved,
you can specify the IP address (IPv4 or IPv6) of the SMTP
server instead of the host name.
```

Habilitación de la autenticación remota

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

Antes de empezar

Debe tener la función Administrador de aplicaciones.

El servidor de Unified Manager debe estar conectado directamente con el servidor de autenticación. Debe deshabilitar cualquier cliente LDAP local, como SSSD (demonio de servicios de seguridad del sistema) o NSLCD (demonio de almacenamiento en caché LDAP del servicio de nombres).

Acerca de esta tarea

Puede habilitar la autenticación remota mediante Open LDAP o Active Directory. Si la autenticación remota está deshabilitada, los usuarios remotos no pueden acceder a Unified Manager.

La autenticación remota es compatible con LDAP y LDAPS (LDAP seguro). Unified Manager utiliza 389 como puerto predeterminado para la comunicación no segura y 636 como puerto predeterminado para la comunicación segura.

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

Pasos

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

Para tipo de autenticación…	Introduzca la siguiente información…
Active Directory	• Nombre del administrador del servidor de autenticación en uno de los siguientes formatos: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Usando la notación LDAP adecuada) • Contraseña de administrador • Nombre completo base (con la notación LDAP adecuada)
Abra LDAP	• Enlazar nombre distintivo (en la notación LDAP correspondiente) • Enlazar contraseña • Nombre distintivo de base

Si la autenticación de un usuario de Active Directory tarda mucho tiempo o agota el tiempo de espera, es probable que el servidor de autenticación tarde mucho tiempo en responder. Al deshabilitar la compatibilidad con los grupos anidados en Unified Manager, es posible que se reduzca el tiempo de autenticación.

Si selecciona la opción Use Secure Connection para el servidor de autenticación, Unified Manager se comunica con el servidor de autenticación mediante el protocolo Secure Sockets Layer (SSL).

4. Añada servidores de autenticación y pruebe la autenticación.
5. Haga clic en **Guardar**.

Deshabilitar grupos anidados de la autenticación remota

Si tiene habilitada la autenticación remota, puede deshabilitar la autenticación de grupos anidados para que solo los usuarios individuales y no los miembros de grupos se puedan autenticar de forma remota a Unified Manager. Puede deshabilitar los grupos anidados cuando desee mejorar el tiempo de respuesta de autenticación de Active Directory.

Antes de empezar

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

Acerca de esta tarea

Al deshabilitar la compatibilidad con los grupos anidados en Unified Manager, es posible que se reduzca el tiempo de autenticación. Si la compatibilidad de grupos anidados está deshabilitada y, si se añade un grupo remoto a Unified Manager, los usuarios individuales deben ser miembros del grupo remoto para autenticarse en Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Active la casilla de verificación **Desactivar búsqueda de grupo anidada**.
3. Haga clic en **Guardar**.

Añadiendo servidores de autenticación

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

Antes de empezar

- Debe estar disponible la siguiente información:
  - Nombre de host o dirección IP del servidor de autenticación
  - Número de puerto del servidor de autenticación
- Debe haber habilitado la autenticación remota y configurado el servicio de autenticación para que el servidor de administración pueda autenticar usuarios o grupos remotos en el servidor de autenticación.
- Debe tener la función Administrador de aplicaciones.

Acerca de esta tarea

Si el servidor de autenticación que va a añadir forma parte de un par de alta disponibilidad (ha) (con la misma base de datos), también puede añadir el servidor de autenticación asociado. Esto permite que el servidor de administración se comunique con el asociado cuando no se puede acceder a uno de los servidores de autenticación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Activar o desactivar la opción **utilizar conexión segura**:

Si desea…	Realice lo siguiente…
Habilite	a. Seleccione la opción **utilizar conexión segura**. b. En el área servidores de autenticación, haga clic en **Agregar**. c. En el cuadro de diálogo Add Authentication Server, introduzca el nombre o la dirección IP de autenticación (IPv4 o IPv6) del servidor. d. En el cuadro de diálogo autorizar host, haga clic en Ver certificado. e. En el cuadro de diálogo Ver certificado, compruebe la información del certificado y, a continuación, haga clic en **Cerrar**. f. En el cuadro de diálogo autorizar host, haga clic en **Sí**. Al activar la opción **usar autenticación de conexión segura**, Unified Manager se comunica con el servidor de autenticación y muestra el certificado. Unified Manager utiliza 636 como puerto predeterminado para una comunicación segura y el número de puerto 389 para una comunicación no segura.
Deshabilitarla	a. Desactive la opción **utilizar conexión segura**. b. En el área servidores de autenticación, haga clic en **Agregar**. c. En el cuadro de diálogo Add Authentication Server, especifique el nombre de host o la dirección IP (IPv4 o IPv6) del servidor y los detalles del puerto. d. Haga clic en **Agregar**.

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

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

Prueba de la configuración de los servidores de autenticación

Puede validar la configuración de los servidores de autenticación para garantizar que el servidor de gestión pueda comunicarse con ellos. Puede validar la configuración buscando un usuario remoto o un grupo remoto desde los servidores de autenticación y autentificándolos con la configuración configurada.

Antes de empezar

- Usted debe haber habilitado la autenticación remota y configurado el servicio de autenticación para que el servidor de Unified Manager pueda autenticar el usuario remoto o el grupo remoto.
- Debe haber agregado los servidores de autenticación para que el servidor de administración pueda buscar el usuario remoto o el grupo remoto desde estos servidores y autentificarlos.
- Debe tener la función Administrador de aplicaciones.

Acerca de esta tarea

Si el servicio de autenticación está establecido en Active Directory y si está validando la autenticación de usuarios remotos que pertenecen al grupo principal del servidor de autenticación, la información sobre el grupo principal no se muestra en los resultados de la autenticación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Haga clic en **probar autenticación**.
3. En el cuadro de diálogo **Usuario de prueba**, especifique el nombre de usuario y la contraseña del usuario remoto o el nombre de usuario del grupo remoto y, a continuación, haga clic en **Prueba**.

   Si va a autenticar un grupo remoto, no debe introducir la contraseña.

Adición de usuarios

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

Antes de empezar

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

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

Acerca de esta tarea

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

Pasos

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

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

4. Haga clic en **Agregar**.

Adición de alertas

Puede configurar alertas para que le notifiquen un evento determinado. Es posible configurar alertas para un solo recurso, para un grupo de recursos o para eventos de un tipo de gravedad determinado. Puede especificar la frecuencia con la que desea que se le notifique y asociar un script a la alerta.

Antes de empezar

- Debe haber configurado los ajustes de notificación, como la dirección de correo electrónico de usuario, el servidor SMTP y el host de captura SNMP, con el fin de permitir que el servidor Active IQ Unified Manager utilice estos ajustes para enviar notificaciones a los usuarios cuando se genera un evento.
- Debe conocer los recursos y los eventos sobre los que desea activar la alerta, así como los nombres de usuario o las direcciones de correo electrónico de los usuarios a los que desea notificar.
- Si desea que un script se ejecute según el evento, debe haber añadido el script a Unified Manager mediante la página Scripts.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Acerca de esta tarea

Puede crear una alerta directamente desde la página de detalles Event después de recibir un evento además de crear una alerta desde la página Alert Setup, tal y como se describe aquí.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar alerta**, haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.

4. Haga clic en **Recursos** y seleccione los recursos que se incluirán o excluirán de la alerta.

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

   Si un recurso cumple las reglas de inclusión y exclusión especificadas, la regla de exclusión tiene prioridad sobre la regla de inclusión y no se genera la alerta para los eventos relacionados con el recurso excluido.

5. Haga clic en **Eventos** y seleccione los eventos según el nombre del evento o el tipo de gravedad del evento para el que desea activar una alerta.

   Para seleccionar más de un evento, pulse la tecla Ctrl mientras realiza las selecciones.

6. Haga clic en **acciones** y seleccione los usuarios a los que desea notificar, elija la frecuencia de notificación, elija si se enviará una captura SNMP al receptor de capturas y asigne una secuencia de comandos para que se ejecute cuando se genere una alerta.

   Si modifica la dirección de correo electrónico especificada para el usuario y vuelve a abrir la alerta para su edición, el campo Nombre aparecerá en blanco porque la dirección de correo electrónico modificada ya no está asignada al usuario que se seleccionó previamente. Además, si modificó la dirección de correo electrónico del usuario seleccionado desde la página usuarios, la dirección de correo electrónico modificada no se actualizará para el usuario seleccionado.

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

7. Haga clic en **Guardar**.

Ejemplo de añadir una alerta

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

- Nombre de alerta: HealthTest
- Recursos: Incluye todos los volúmenes cuyo nombre contenga «'abc'» y excluye todos los volúmenes cuyo nombre contenga «'xyz'».
- Eventos: Incluye todos los eventos críticos de salud
- Acciones: Incluye «ample@domain.com», un guión «Prueba» y el usuario deberá ser notificado cada 15 minutos

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

1. Haga clic en **Nombre** e introduzca `HealthTest` En el campo **Nombre de alerta**.
2. Haga clic en **Recursos** y, en la ficha incluir, seleccione **volúmenes** en la lista desplegable.
   a. Introduzca `abc` En el campo **Nombre contiene** para mostrar los volúmenes cuyo nombre contiene "'abc'".
   b. Seleccione **todos los volúmenes cuyo nombre contenga 'abc'** en el área Available Resources y muévalos al área Selected Resources.
   c. Haga clic en **excluir** e introduzca `xyz` En el campo **Nombre contiene** y, a continuación, haga clic en

Agregar.

3. Haga clic en **Eventos** y seleccione **críticos** en el campo gravedad del evento.
4. Seleccione **todos los eventos críticos** en el área Eventos coincidentes y muévalos al área Eventos seleccionados.
5. Haga clic en **acciones** e introduzca `sample@domain.com` En el campo Alerta a estos usuarios.
6. Seleccione **Recordar cada 15 minutos** para notificar al usuario cada 15 minutos.

   Puede configurar una alerta para que envíe repetidamente notificaciones a los destinatarios durante un período de tiempo específico. Debe determinar la hora desde la cual está activa la notificación de eventos para la alerta.

7. En el menú Select Script to Execute, seleccione **Test** script.
8. Haga clic en **Guardar**.

Eventos de EMS que se añaden automáticamente a Unified Manager

Los siguientes eventos de EMS de ONTAP se añaden automáticamente a Unified Manager. Estos eventos se generarán cuando se active en cualquier clúster que Unified Manager supervise.

Los siguientes eventos de EMS están disponibles cuando se supervisan clústeres que ejecutan ONTAP 9.5 o una versión posterior del software:

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
Acceso al nivel de cloud denegado para la reubicación de agregados	arl.netra.ca.check.failed	Agregado	Error
Acceso al nivel de cloud denegado para la reubicación de agregados durante la conmutación al nodo de respaldo del almacenamiento	gb.netra.ca.check.failed	Agregado	Error
Se completó la resincronización de replicación de mirroring de FabricPool	wafl.ca.resync.complete	Clúster	Error
Espacio de FabricPool casi completo	fabricpool.casi.lleno	Clúster	Error
Se inició el periodo de gracia de NVMe-of	nvmf.graceperiod.start	Clúster	Advertencia

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
NVMe-of Grace Period activo	nvmf.graceperiod.active	Clúster	Advertencia
NVMe-of Grace caducó	nvmf.graceperiod.expired	Clúster	Advertencia
LUN destruida	lun.destroy	LUN	Información
MetaDataConnFail de Cloud AWS	Cloud.aws.metadataConnFail	Nodo	Error
Cloud AWS IAMCredsExpired	Cloud.aws.iamCredsExpired	Nodo	Error
IAMCredsInvalid de Cloud AWS	Cloud.aws.iamCredsInvalid	Nodo	Error
Cloud AWS IAMCredsNotFound	Cloud.aws.iamCredsNotFound	Nodo	Error
IAMCredsNotInitialized Cloud de AWS	Cloud.aws.iamNotInitialized	Nodo	Información
Cloud AWS IAMRoleinválido	Cloud.aws.iamRoleInvalid	Nodo	Error
Cloud AWS IAMRoleNotFound	Cloud.aws.iamRoleNotFound	Nodo	Error
Organización de hosts de nivel cloud sin resolver	objstore.host.no se puede resolver	Nodo	Error
LIF de interconexión de clústeres por niveles en el cloud inactivo	objstore.interclusterlifDown	Nodo	Error
La solicitud no coincide con la firma del nivel de cloud	osc.signaturediscordancia	Nodo	Error
Una de las agrupaciones de NFSv4 agotadas	Nblade.nfsV4PoolEscape	Nodo	Crítico
La memoria del monitor QoS se enceró	qos.monitor.memory.mutile	Nodo	Error

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
Memoria de monitor QoS abated	qos.monitor.memory.abated	Nodo	Información
Destrucción NVMeNS	NVMeNS.destroy	Espacio de nombres	Información
NVMeNS en línea	NVMeNS.offline	Espacio de nombres	Información
NVMeNS sin conexión	NVMeNS.online	Espacio de nombres	Información
NVMeNS fuera espacio	NVMeNS.out.of.space	Espacio de nombres	Advertencia
Replicación síncrona fuera de sincronización	sms.status.out.of.sync	Relación de SnapMirror	Advertencia
Replicación síncrona restaurada	sms.status.in.sync	Relación de SnapMirror	Información
Error en la resincronización automática de replicación síncrona	sms.resync.intento.error	Relación de SnapMirror	Error
Muchas conexiones CIFS	Nblade.cifsManyAutos	SVM	Error
Se superó la conexión CIFS máxima	Nblade.cifsMaxOpenSameFile	SVM	Error
Se ha excedido el número máximo de conexiones CIFS por usuario	Nblade.cifsMaxSessPerUsrConn	SVM	Error
Conflicto con los nombres NetBIOS de CIFS	Nblade.cifsNbNameConflict	SVM	Error
Intentos de conexión de recursos compartidos CIFS no existentes	Nblade.cifsNoPrivShare	SVM	Crítico
Error en la operación de copia de volúmenes redundantes de CIFS	cifs.shadowcopy.error	SVM	Error
Virus detectado por el servidor AV	Nblade.vscanVirusDetected	SVM	Error

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
No hay conexión con el servidor AV para el análisis de virus	Nblade.vscanNoScannerConn	SVM	Crítico
No hay ningún servidor AV registrado	Nblade.vscanNoRegdScanner	SVM	Error
Conexión del servidor AV sin respuesta	Nblade.vscanConnInactive	SVM	Información
El servidor AV está muy ocupado para aceptar una nueva solicitud de análisis	Nblade.vscanConnBackPressure	SVM	Error
Un usuario no autorizado intenta utilizar el servidor AV	Nblade.vscanBadUserPrivAccess	SVM	Error
Los componentes de FlexGroup tienen problemas de espacio	flexgroup.constituyentes.have.space.problemas	Volumen	Error
El estado del espacio de los componentes de FlexGroup es correcto	flexgroup.constituyentes.space.status.all.ok	Volumen	Información
Los componentes de FlexGroup tienen problemas de inodos	flexgroup.constituents.have.inodes.issues	Volumen	Error
Los componentes de FlexGroup inodos Estado todo OK	flexgroup.constituents.inodes.status.all.ok	Volumen	Información
Espacio lógico del volumen casi lleno	monitor.vol.nearFull.inc.sav	Volumen	Advertencia
Espacio lógico del volumen lleno	monitor.vol.full.inc.sav	Volumen	Error
Espacio lógico del volumen normal	monitor.vol.one.ok.inc.sav	Volumen	Información
Error al ajustar el tamaño automático del volumen de WAFL	wafl.vol.autoSize.fail	Volumen	Error

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
Se ha completado el tamaño automático de volúmenes de WAFL	wafl.vol.autoSize.done	Volumen	Información
Tiempo de espera de operación de archivo DE READDIR de WAFL	wafl.readdir.expiraba	Volumen	Error

Suscripción a eventos de EMS de ONTAP

Puede suscribirse para recibir eventos del sistema de gestión de eventos (EMS) generados por sistemas instalados con el software ONTAP. Un subconjunto de eventos de EMS se informa automáticamente a Unified Manager, pero solo se informan eventos de EMS adicionales si se ha suscrito a estos eventos.

Antes de empezar

No suscribirse a eventos de EMS que ya se hayan añadido a Unified Manager automáticamente, ya que esto puede provocar confusión al recibir dos eventos por el mismo problema.

Acerca de esta tarea

Puede suscribirse a cualquier número de eventos de EMS. Todos los eventos a los que se suscribe están validados y solo se aplican los eventos validados a los clústeres que supervisa en Unified Manager. El *ONTAP 9 Catálogo de eventos EMS* proporciona información detallada para todos los mensajes EMS de la versión especificada del software ONTAP 9. Busque la versión adecuada del *Catálogo de eventos EMS* en la página Documentación del producto de ONTAP 9 para obtener una lista de los eventos aplicables.

"Biblioteca de productos de ONTAP 9"

Es posible configurar alertas para los eventos de EMS de ONTAP a los que se suscribe, y puede crear scripts personalizados para su ejecución.

> Si no recibe los eventos de EMS de ONTAP a los que se ha suscrito, puede haber un problema con la configuración de DNS del clúster, lo que impide que el clúster llegue al servidor de Unified Manager. Para resolver este problema, el administrador de clúster debe corregir la configuración de DNS del clúster y, a continuación, reiniciar Unified Manager. Si lo hace, se vacíe los eventos de EMS pendientes en Unified Manager Server.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de eventos**.
2. En la página **Event Setup**, haga clic en el botón **Subscribe to EMS events**.
3. En el cuadro de diálogo **Suscribirse a eventos EMS**, introduzca el nombre del evento EMS de ONTAP al que desea suscribirse.

Para ver los nombres de los eventos de EMS a los que se puede suscribir, desde el shell del clúster de ONTAP, puede usar la `event route show` (Anterior a ONTAP 9) o el `event catalog show` (ONTAP 9 o posterior).

"Cómo configurar las suscripciones a eventos de EMS de ONTAP en OnCommand Unified Manager / Active IQ Unified Manager"

4. Haga clic en **Agregar**.

   El evento EMS se agrega a la lista de eventos EMS suscritos, pero la columna aplicable al clúster muestra el estado como "'Desconocido'" para el evento EMS que ha agregado.

5. Haga clic en **Guardar y cerrar** para registrar la suscripción al evento EMS con el clúster.
6. Haga clic en **Subscribe to EMS events** de nuevo.

   El estado «'Yes'» aparece en la columna aplicable al clúster del evento EMS que ha añadido.

   Si el estado no es "'Yes'", compruebe la ortografía del nombre del evento de EMS de ONTAP. Si el nombre se introduce de forma incorrecta, deberá eliminar el evento incorrecto y, a continuación, volver a añadir el evento.

Después de terminar

Cuando se produce el evento de ONTAP EMS, el evento se muestra en la página Events. Es posible seleccionar el evento para ver detalles sobre el evento de EMS en la página de detalles Event. También puede gestionar la disposición del evento o crear alertas para el evento.

Gestión de la configuración de autenticación SAML

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

Tenga en cuenta que solo los usuarios remotos tendrán acceso a la interfaz gráfica de usuario de Unified Manager después de habilitar la autenticación SAML. Los usuarios locales y los usuarios de mantenimiento no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento.

Requisitos del proveedor de identidades

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

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

Estándares de cifrado compatibles

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

Proveedores de identidades validados

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

Requisitos de configuración de ADFS

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

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

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

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

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

Otros requisitos de configuración

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

Habilitación de la autenticación SAML

Puede habilitar la autenticación del lenguaje de marcado de aserción de seguridad

(SAML) para que los usuarios remotos se autentiquen mediante un proveedor de identidad seguro (IDP) antes de poder acceder a la interfaz de usuario web de Unified Manager.

Antes de empezar

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

Acerca de esta tarea

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

Solo los usuarios remotos tendrán acceso a la interfaz gráfica de usuario de Unified Manager después de habilitar la autenticación SAML. Los usuarios locales y los usuarios de mantenimiento no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento, los comandos de Unified Manager o las ZAPI.

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

Pasos

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

   Se mostrarán los campos necesarios para configurar la conexión IDP.

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

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

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

   Ahora es posible configurar el servidor IDP con esta información.

5. Haga clic en **Guardar**.

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

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

Resultados

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

Después de terminar

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

Cuando se utiliza ADFS como proveedor de identidades, la interfaz gráfica de usuario de Unified Manager no cumple el tiempo de espera de ADFS y continúa funcionando hasta que se alcanza el tiempo de espera de la sesión de Unified Manager. Cuando Unified Manager se pone en marcha en Windows, Red Hat o CentOS, puede cambiar el tiempo de espera de sesión de la interfaz gráfica de usuario mediante el siguiente comando CLI de Unified Manager: `um option set absolute.session.timeout=00:15:00`Este comando configura el tiempo de espera de sesión de la interfaz gráfica de usuario de Unified Manager en 15 minutos.

Configurar los ajustes de backup de la base de datos

Puede configurar los ajustes de backup de la base de datos de Unified Manager para establecer la ruta de backup de la base de datos, el número de retención y las programaciones de backup. Se pueden habilitar backups programados diarios o semanales. De manera predeterminada, las copias de seguridad programadas están deshabilitadas.

Antes de empezar

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe tener un mínimo de 150 GB de espacio disponible en la ubicación que defina como ruta de backup.

  Se recomienda que utilice una ubicación remota externa al sistema host de Unified Manager.

- Cuando Unified Manager esté instalado en un sistema Linux, compruebe que el usuario "'jboss'" tiene permisos de escritura en el directorio de copia de seguridad.
- No se deben programar operaciones de backup para que se produzcan inmediatamente después de añadir un clúster nuevo mientras Unified Manager recoge 15 días de datos de rendimiento históricos.

Acerca de esta tarea

Se requiere más tiempo la primera vez que se realiza un backup que para backups posteriores, ya que el primer backup es un backup completo. Un backup completo puede tener más de 1 GB y puede tardar entre tres y cuatro horas. Los backups posteriores son incrementales y requieren menos tiempo.

Si encuentra que el número de archivos de copia de seguridad incremental es demasiado grande para el espacio que ha asignado para las copias de seguridad, puede crear una nueva copia de seguridad completa periódicamente para reemplazar la copia de seguridad completa antigua y todos sus archivos incrementales secundarios.

"Cómo iniciar una nueva cadena de backup incremental en Active IQ Unified Manager"

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **copia de seguridad de la base de datos**.
2. En la página **copia de seguridad de la base de datos**, haga clic en **Configuración de copia de seguridad**.
3. Configure los valores adecuados para una ruta de backup, un recuento de retención y una programación.

   El valor predeterminado para el número de retención es 10; se puede usar 0 para crear copias de seguridad ilimitadas.

4. Seleccione el botón **Diario programado** o **Semanal programado** y, a continuación, especifique los detalles del programa.
5. Haga clic en **aplicar**.

Cambiando la contraseña de usuario local

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

Antes de empezar

Debe iniciar sesión como usuario local.

Acerca de esta tarea

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

Pasos

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

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

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

Después de terminar

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

Configurar el tiempo de espera de inactividad de la sesión

Es posible especificar el valor de tiempo de espera de inactividad para Unified Manager

a fin de que la sesión se finalice automáticamente después de un cierto periodo de tiempo. De manera predeterminada, el tiempo de espera está configurado en 4,320 minutos (72 horas).

Antes de empezar

Debe tener la función Administrador de aplicaciones.

Acerca de esta tarea

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

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

Pasos

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

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

Cambie el nombre de host de Unified Manager

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

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

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

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

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

Pasos

1. Genere un certificado de seguridad HTTPS

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

2. Reinicie la máquina virtual de Unified Manager

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

Generar un certificado de seguridad HTTPS

Puede generar un nuevo certificado de seguridad HTTPS por varios motivos, como si desea firmar con otra entidad emisora de certificados o si el certificado de seguridad actual ha caducado. El nuevo certificado sustituye al certificado existente.

Antes de empezar

Debe tener la función Administrador de aplicaciones.

Acerca de esta tarea

Si no tiene acceso a la interfaz de usuario web de Unified Manager, puede volver a generar el certificado HTTPS con los mismos valores mediante la consola de mantenimiento.

Pasos

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

   Aparece el cuadro de diálogo Regenerate HTTPS Certificate.

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

Si desea…	Realice lo siguiente…
Regenere el certificado con los valores actuales	Haga clic en la opción **Regenerate usando atributos de certificado actuales**.
Genere el certificado con diferentes valores	`Click the *Update the Current Certificate Attributes* option. Los campos Nombre común y nombres alternativos utilizarán los valores del certificado existente si no introduce nuevos valores. Los demás campos no requieren valores, pero puede introducir valores, por ejemplo, para la ciudad, el estado y el país si desea que dichos valores se rellenen en el certificado.` Puede seleccionar la casilla de verificación "'excluir información de identificación local (p. ej., localhost)'" si desea eliminar la información de identificación local del campo nombres alternativos del certificado. Cuando se selecciona esta casilla de verificación, sólo se utiliza el campo nombres alternativos lo que se introduce en el campo. Cuando se deja en blanco, el certificado resultante no tendrá ningún campo nombres alternativos.

4. Haga clic en **Sí** para regenerar el certificado.
5. Reinicie el servidor de Unified Manager para que el nuevo certificado surta efecto.

Después de terminar

Compruebe la información del nuevo certificado; para ello, consulte el certificado HTTPS.

Reiniciar la máquina virtual de Unified Manager

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

Antes de empezar

El dispositivo virtual está encendido.

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

Acerca de esta tarea

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

Pasos

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

Cambiar el nombre de host de Unified Manager en sistemas Linux

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

Pasos

1. Inicie sesión como usuario raíz en el sistema Unified Manager que desee modificar.
2. Detenga el software Unified Manager y el software MySQL asociado introduciendo el comando siguiente: `systemctl stop ocieau ocie mysqld`
3. Cambie el nombre de host con Linux `hostnamectl` comando: `hostnamectl set-hostname new_FQDN`

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

4. Regenere el certificado HTTPS para el servidor:`/opt/netapp/essentials/bin/cert.sh create`
5. Reinicie el servicio de red: `service network restart`
6. Después de reiniciar el servicio, compruebe si el nuevo nombre de host puede hacer ping a sí mismo: `ping new_hostname`

   ```
   ping nuhost
   ```

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

7. Después de completar y verificar el cambio de nombre de host, reinicie Unified Manager introduciendo el comando siguiente: `systemctl start mysqld ocie ocieau`

Habilitar y deshabilitar la gestión del almacenamiento basada en políticas

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

Antes de empezar

Debe tener la función Administrador de aplicaciones.

Acerca de esta tarea

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

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

Nuevo contenido	Ubicación
Una página para aprovisionar nuevas cargas de trabajo	Disponible en **tareas comunes** > **aprovisionamiento**

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

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

Pasos

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

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

Mediante la consola de mantenimiento

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

Qué funcionalidad proporciona la consola de mantenimiento

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

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

- Solucione cualquier problema que pueda haber con su dispositivo virtual, especialmente si la interfaz web de Unified Manager no está disponible

- Actualice a las versiones más recientes de Unified Manager
- Genere paquetes de soporte para su envío al soporte técnico
- Configure los ajustes de red
- Cambie la contraseña del usuario de mantenimiento
- Conéctese a un proveedor de datos externo para enviar estadísticas de rendimiento
- Cambie la recopilación de datos de rendimiento interna
- Restaure las opciones de configuración y base de datos de Unified Manager desde una versión de backup anterior.

Lo que hace el usuario de mantenimiento

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

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

Capacidades de diagnóstico del usuario

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

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

Acceso a la consola de mantenimiento

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

Antes de empezar

Debe haber instalado y configurado Unified Manager.

Acerca de esta tarea

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

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

Pasos

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

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

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

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

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

Antes de empezar

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

Acerca de esta tarea

Pasos

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

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

Menús de la consola de mantenimiento

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

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

- Actualización de Unified Manager (solo VMware)
- Configuración de red (solo VMware)
- Configuración del sistema (sólo VMware)
- Soporte / Diagnóstico
- Restablecer certificado de servidor
- Proveedor de datos externos
- Configuración del intervalo de sondeo de rendimiento

Menú Configuración de red

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

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

Están disponibles las siguientes opciones de menú.

- **Mostrar configuración de dirección IP**

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

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

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

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

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

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

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

- **Mostrar rutas estáticas**

  Muestra las rutas de red estáticas actuales.

- **Cambiar rutas estáticas**

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

  - **Añadir ruta**

    Permite agregar una ruta estática.

  - **Eliminar ruta**

    Permite eliminar una ruta estática.

  - **Atrás**

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

  - **Salida**

    Sale de la consola de mantenimiento.

- **Desactivar la interfaz de red**

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

- **Activar interfaz de red**

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

- **Commit Changes**

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

- **Hacer ping a un Host**

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

- **Restaurar valores predeterminados**

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

- **Atrás**

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

- **Salida**

  Sale de la consola de mantenimiento.

Menú Configuración del sistema

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

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

Están disponibles las siguientes opciones de menú:

- **Estado del servidor de visualización**

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

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

- **Reiniciar máquina virtual**

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

- **Apagar máquina virtual**

  Apaga la máquina virtual, deteniendo todos los servicios.

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

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

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

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

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

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

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

- **Cambiar zona horaria**

  Cambia la zona horaria a su ubicación.

- **Cambiar servidor NTP**

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

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

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

- **Restablecer certificado de servidor**

Restablece el certificado de seguridad del servidor.

- **Cambiar nombre de host**

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

- **Atrás**

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

- **Salida**

  Sale del menú de la consola de mantenimiento.

Menú de soporte y diagnóstico

El menú Soporte y Diagnóstico permite generar un bundle de soporte.

Está disponible la siguiente opción de menú:

- **Generar paquete de soporte**

  Permite crear un archivo 7-Zip que contenga información completa de diagnóstico en el directorio principal del usuario de diagnóstico. El archivo incluye información generada por un mensaje de AutoSupport, el contenido de la base de datos de Unified Manager, los datos detallados sobre las redes internas del servidor de Unified Manager y los registros a nivel detallado que no se incluyen normalmente en los mensajes de AutoSupport.

Opciones de menú adicionales

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

Están disponibles las siguientes opciones de menú:

- **Restablecer certificado de servidor**

  Regenera el certificado del servidor HTTPS.

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

- **Deshabilitar autenticación SAML**

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

- **Proveedor de datos externos**

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

muestran las siguientes opciones:

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

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

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

  Proporciona una opción para configurar la frecuencia con la que Unified Manager recopila datos estadísticos de rendimiento de clústeres. El intervalo de recopilación predeterminado es de 5 minutos.

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

- **Ver/cambiar puertos de aplicación**

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

- **Salida**

  Sale del menú de la consola de mantenimiento.

Cambiar la contraseña del usuario de mantenimiento en Windows

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

Pasos

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

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

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

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

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

Cambiar la contraseña de umadmin en sistemas Linux

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

Antes de empezar

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

Pasos

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

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

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

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

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

Acerca de esta tarea

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

Pasos

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

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

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

4. Escriba los números de puerto nuevos para los puertos HTTP y HTTPS y, a continuación, pulse Intro.

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

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

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

Resultados

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

Se añaden interfaces de red

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

Antes de empezar

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

El dispositivo virtual debe estar encendido.

Acerca de esta tarea

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

Pasos

1. En vSphere Console **Main Menu**, seleccione **Configuración del sistema** > **Reiniciar el sistema operativo**.

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

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

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

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

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

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

7. Seleccione **Commit Changes**.

Debe confirmar los cambios para añadir la interfaz de red.

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

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

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

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

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

Adición de espacio al directorio de datos del host Linux

Si ha asignado poco espacio en disco a `/opt/netapp/data` directorio para admitir Unified Manager cuando originalmente configuró el host Linux y después instaló Unified Manager, es posible añadir espacio en disco después de la instalación aumentando espacio en disco en la `/opt/netapp/data` directorio.

Antes de empezar

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

Acerca de esta tarea

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

Pasos

1. Inicie sesión como usuario root en el equipo Linux en el que desea agregar espacio en disco.
2. Detenga el servicio Unified Manager y el software MySQL asociado en el orden que se muestra: `systemctl stop ocieau ocie mysqld`
3. Crear una carpeta de copia de seguridad temporal (por ejemplo, `/backup-data`) con suficiente espacio en disco para contener los datos de la corriente `/opt/netapp/data` directorio.
4. Copie la configuración de contenido y privilegios de la existente `/opt/netapp/data` directorio en el directorio de datos de copia de seguridad: `cp -arp /opt/netapp/data/* /backup-data`
5. Si se Linux está habilitado:

    a. Obtenga el tipo de Linux de se para las 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 `chcon` Comando para establecer el tipo de Linux de se para el directorio de copia de seguridad: `chcon -R --type=mysqld_db_t /backup-data`

6. Elimine el contenido del `/opt/netapp/data` directorio:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`. Expanda el tamaño de `/opt/netapp/data` directorio a un mínimo de 750 GB a través de comandos de LVM o mediante la adición de discos adicionales.

> Montar el `/opt/netapp/data` No se admite el directorio de un recurso compartido NFS o CIFS.

7. Confirme 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
```

8. Si se activa Linux, confirme que el contexto del `/opt/netapp/data` el directorio todavía está establecido en mysqld_db_t:
   a. `touch /opt/netapp/data/abc`
   b. `ls -Z /opt/netapp/data/abc`

      El sistema devuelve una confirmación similar a la siguiente:

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

9. Elimine el archivo `abc` de forma que este archivo no causa un error de base de datos en el futuro.
10. Copie el contenido de `backup-data` volver al expandido `/opt/netapp/data` directorio: `cp -arp /backup-data/* /opt/netapp/data/`
11. Si se Linux está habilitado, ejecute el siguiente comando: `chcon -R --type=mysqld_db_t /opt/netapp/data`
12. Inicie el servicio MySQL: `systemctl start mysqld`

13. Una vez iniciado el servicio MySQL, inicie los servicios ocie y ocieau en el orden que se muestra: `systemctl start ocie ocieau`
14. Después de iniciar todos los servicios, elimine la carpeta de copia de seguridad `/backup-data`: `rm -rf /backup-data`

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

Si necesita aumentar la cantidad de espacio en el disco de datos para la base de datos de Unified Manager, puede añadir capacidad después de la instalación aumentando el espacio en disco `disk 3`.

Antes de empezar

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

Acerca de esta tarea

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 de vSphere, seleccione la máquina virtual de Unified Manager y, a continuación, añada más capacidad de disco a los datos `disk 3`. Consulte la documentación de VMware para obtener más detalles.
2. En el cliente vSphere, seleccione la máquina virtual de Unified Manager y, a continuación, seleccione la pestaña **Console**.
3. Haga clic en en la ventana de la consola y, a continuación, inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña.
4. En **Menú principal**, introduzca el número de la opción **Configuración del sistema**.
5. En **Menú de configuración del sistema**, introduzca el número de la opción **aumentar tamaño del disco de datos**.

Agregar espacio a la unidad lógica del servidor Microsoft Windows

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

Antes de empezar

Debe tener privilegios de administrador de Windows.

Acerca de esta tarea

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

Pasos

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

Opción	Descripción
En un servidor físico, añada capacidad a la unidad lógica en la que se ha instalado el servidor de Unified Manager.	Follow the steps in the Microsoft topic: https://technet.microsoft.com/en-us/library/cc771473(v=ws.11).aspx ["Extender un volumen básico"]
En un servidor físico, agregue una unidad de disco duro.	Follow the steps in the Microsoft topic: https://msdn.microsoft.com/en-us/library/dd163551.aspx["Agregar unidades de disco duro"]
En un equipo virtual, aumente el tamaño de una partición de disco.	Follow the steps in the VMware topic: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004071["Aumentar el tamaño de una partición de disco"]

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.