



Configurando Active IQ Unified Manager

Active IQ Unified Manager 9.9

NetApp
April 05, 2024

Tabla de contenidos

- 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 20
 - Cambiando la contraseña de usuario local 22
 - 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

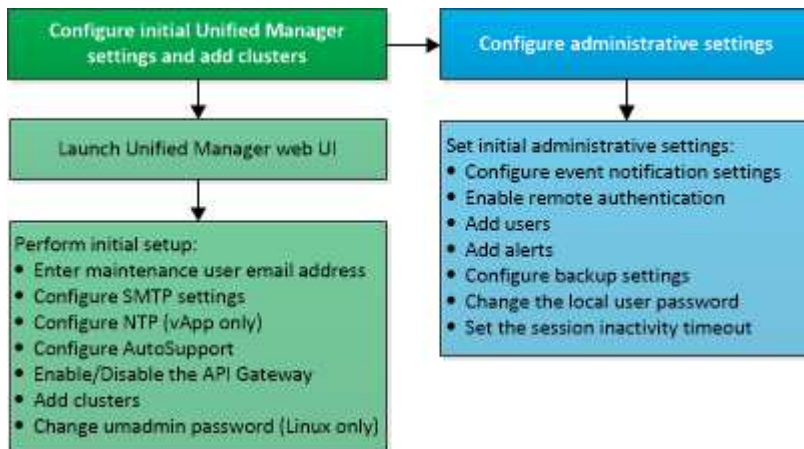
Configurando Active IQ Unified Manager

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`.

1. 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 sobre las API, consulte ["Primeros pasos con 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 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)
- Tiene los certificados necesarios. Se requieren dos tipos de certificados:

Certificados de servidor: Utilizados para el registro. Se requiere un certificado válido para añadir un clúster. Si caduca el certificado de servidor, debe volver a regenerarlo y reiniciar Unified Manager para que los servicios se registren automáticamente. Para obtener información acerca de la generación de certificados, consulte el artículo de la base de conocimientos (KB): ["Cómo renovar un certificado SSL en ONTAP 9"](#)

Certificados de cliente: Utilizados para la autenticación. Se requiere un certificado válido para añadir un clúster. No puede agregar un clúster a Unified Manager con un certificado caducado y si el

certificado de cliente ya ha caducado, debe volver a regenerarlo antes de agregar el clúster. Sin embargo, si este certificado caduca en un clúster que ya se ha añadido y está siendo utilizado por Unified Manager, la mensajería de EMS sigue funcionando con el certificado caducado. No es necesario regenerar el certificado de cliente.



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.

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**.

Notas:

- Si la dirección de origen está precargada con la dirección «'ActiveIQUnifiedManager@localhost.com'», debe cambiarla a una dirección de correo electrónico real y activa para asegurarse de que todas las notificaciones de correo electrónico se envían correctamente.
- Si no se puede resolver el nombre de host del servidor SMTP, puede especificar la dirección IP (IPv4 o IPv6) del servidor SMTP en lugar del nombre de host.

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	<ul style="list-style-type: none">• Nombre del administrador del servidor de autenticación en uno de los siguientes formatos:<ul style="list-style-type: none">◦ domainname \username◦ username@domainname◦ Bind Distinguished Name (Usando la notación LDAP adecuada)• Contraseña de administrador• Nombre completo base (con la notación LDAP adecuada)

Para tipo de autenticación...	Introduzca la siguiente información...
Abra LDAP	<ul style="list-style-type: none"> • Enlazar nombre distintivo (en la notación LDAP correspondiente) • Enlazar contraseña • Nombre distintivo de base

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

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

1. Añada servidores de autenticación y pruebe la autenticación.
2. Haga clic en **Guardar**.

Deshabilitar grupos anidados de la autenticación remota

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

Antes de empezar

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

Acerca de esta tarea

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

Pasos

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

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 comuniquen 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	<ol style="list-style-type: none">1. Seleccione la opción utilizar conexión segura.2. En el área servidores de autenticación, haga clic en Agregar.3. En el cuadro de diálogo Add Authentication Server, introduzca el nombre o la dirección IP de autenticación (IPv4 o IPv6) del servidor.4. En el cuadro de diálogo autorizar host, haga clic en Ver certificado.5. En el cuadro de diálogo Ver certificado, compruebe la información del certificado y, a continuación, haga clic en Cerrar.6. En el cuadro de diálogo autorizar host, haga clic en Sí. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"><p>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.</p></div>

Si desea...	Realice lo siguiente...
Deshabilitarla	<ol style="list-style-type: none"> 1. Desactive la opción utilizar conexión segura. 2. En el área servidores de autenticación, haga clic en Agregar. 3. En el cuadro de diálogo Add Authentication Server, especifique el nombre de host o la dirección IP (IPv4 o IPv6) del servidor y los detalles del puerto. 4. Haga clic en Agregar.

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

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

Prueba de la configuración de los servidores de autenticación

Puede validar la configuración de los servidores de autenticación para garantizar que el servidor de gestión pueda comunicarse con ellos. Puede validar la configuración buscando un usuario remoto o un grupo remoto desde los servidores de autenticación y autenticándolos 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 autenticarlos.
- 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 **<<All Volumes whose name contains 'abc'>>** en el área Recursos disponibles y muévalos al área Recursos seleccionados.
 - c. Haga clic en **excluir** e introduzca `xyz` En el campo **Nombre contiene** y, a continuación, haga clic en **Agregar**.
3. Haga clic en **Eventos** y seleccione **críticos** en el campo gravedad del evento.
4. Seleccione **todos los eventos críticos** en el área Eventos coincidentes y muévalos al área Eventos seleccionados.
5. Haga clic en **acciones** e introduzca `sample@domain.com` En el campo Alerta a estos usuarios.
6. Seleccione **Recordar cada 15 minutos** para notificar al usuario cada 15 minutos.

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

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

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	wافل.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
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

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
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 encerró	qos.monitor.memory.mutiled	Nodo	Error
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

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
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.cifsMaxSessPerUserConn	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
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

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
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	wافل.vol.autoSize.fail	Volumen	Error
Se ha completado el tamaño automático de volúmenes de WAFL	wافل.vol.autoSize.done	Volumen	Información
Tiempo de espera de operación de archivo DE READDIR de WAFL	wافل.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 y recibir alertas de la suscripción a eventos EMS de ONTAP en 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:

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

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

Otros requisitos de configuración

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

Habilitación de la autenticación SAML

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

Antes de empezar

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

Acerca de esta tarea

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

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

los comandos de Unified Manager o las ZAPI.



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

Pasos

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

Se mostrarán los campos necesarios para configurar la conexión IDP.

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

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

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

Ahora es posible configurar el servidor IDP con esta información.

5. Haga clic en **Guardar**.

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

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

Resultados

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

Después de terminar

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



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

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

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

Antes de empezar

Debe tener la función Administrador de aplicaciones.

Acerca de esta tarea

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

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


Pasos

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

Aparece el cuadro de diálogo Regenerate HTTPS Certificate.

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

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

Si desea...	Realice lo siguiente...
<p>Genere el certificado con diferentes valores</p>	<p>Haga clic en la opción Actualizar atributos de certificado actuales.</p> <p>Los campos Nombre común y nombres alternativos utilizarán los valores del certificado existente si no introduce nuevos valores. El "Nombre común" debe ajustarse al FQDN del host. Los demás campos no requieren valores, pero puede introducir valores, por ejemplo, PARA EL CORREO ELECTRÓNICO, LA EMPRESA, EL DEPARTAMENTO, Ciudad, provincia y país si desea que esos valores se rellenen en el certificado. También puede seleccionar EL TAMAÑO de CLAVE disponible (el algoritmo de clave es "RSA"). Y PERÍODO DE VALIDEZ.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p> Los valores permitidos para el tamaño de clave son 2048, 3072 y. 4096.</p> <p>Los períodos de validez son como mínimo de 1 día a un máximo de 36500 días.</p> <p>Aunque se permita un período de validez de 36500 días, se recomienda que utilice un período de validez de no más de 397 días o 13 meses. Como si selecciona un periodo de validez de más de 397 días y piensa exportar una CSR para este certificado y conseguir que la firme una CA bien conocida, la validez del certificado firmado que la CA le devolvió se reducirá a 397 días.</p> <p>Puede seleccionar la casilla de verificación "excluir la información de identificación local \ (por ejemplo, localhost)" si desea quitar la información de identificación local del campo nombres alternativos del certificado. Cuando se selecciona esta casilla de verificación, sólo se utiliza lo que se introduce en el campo nombres alternativos. Cuando se deja en blanco, el certificado resultante no tendrá ningún campo nombres alternativos.</p> </div>

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. Regenera 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
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 deslizador hacia la izquierda.
Gestión del almacenamiento basada en normativas	En el panel Administración de almacenamiento basada en directivas , mueva el botón deslizador hacia la derecha.

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.