Supervisión de eventos, rendimiento y estado

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Supervisión de eventos, rendimiento y estado . . . 1
Supervise el rendimiento del clúster con System Manager . . . 1
Supervise y gestione el rendimiento de los clústeres mediante la CLI . . . 12
Supervise el rendimiento del clúster con Unified Manager . . . 50
Supervise el rendimiento del clúster con Cloud Insights . . . 50
Registro de auditoría . . . 51
AutoSupport . . . 57
Supervisión del estado . . . 86
Análisis del sistema de archivos . . . 100
Configuración de EMS . . . 115

Supervisión de eventos, rendimiento y estado

Supervise el rendimiento del clúster con System Manager

Supervise el rendimiento del clúster mediante System Manager

Los temas de esta sección muestran cómo gestionar el estado y el rendimiento de los clústeres con System Manager en ONTAP 9.7 y versiones posteriores.

Para supervisar el rendimiento del clúster, consulte información sobre el sistema en la consola de System Manager. La consola muestra información sobre alertas y notificaciones importantes, la eficiencia y capacidad de los niveles de almacenamiento y volúmenes, los nodos disponibles en un clúster, el estado de los nodos de un par de alta disponibilidad, las aplicaciones y objetos más activos, y las métricas de rendimiento de un clúster o un nodo.

El panel permite determinar la siguiente información:

- **Salud**: ¿Qué tan saludable es el clúster?
- **Capacidad**: ¿Qué capacidad está disponible en el cluster?
- **Rendimiento**: ¿Hasta qué punto está funcionando el clúster en función de la latencia, IOPS y rendimiento?
- **Red**: ¿Cómo se configura la red con hosts y objetos de almacenamiento, como puertos, interfaces y equipos virtuales de almacenamiento?

En la información general de estado y capacidad, puede hacer clic en → para ver información adicional y realizar tareas.

En la información general sobre rendimiento, puede ver las métricas en función de la hora, el día, la semana, el mes o el año.

En la información general sobre la red, se muestra el número de cada objeto de la red (por ejemplo, "8 puertos NVMe/FC"). Puede hacer clic en los números para ver los detalles de cada objeto de red.

Vea el rendimiento en la consola de clústeres

Utilice la consola para tomar decisiones informadas sobre las cargas de trabajo que puede añadir o mover. También puede observar los tiempos de uso máximos para planificar posibles cambios.

Los valores de rendimiento se actualizan cada 3 segundos y el gráfico de rendimiento se actualiza cada 15 segundos.

Pasos

1. Haga clic en **Panel**.
2. En **rendimiento**, seleccione el intervalo.

Identifique volúmenes activos y otros objetos

Acelere el rendimiento de su clúster identificando los volúmenes a los que se accede con

frecuencia (volúmenes activos) y los datos (objetos activos).

> A partir de ONTAP 9.10.1, puede usar la función Seguimiento de actividades de Análisis del sistema de archivos para supervisar los objetos activos de un volumen.

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Filtre las columnas IOPS, latencia y rendimiento para ver los volúmenes y los datos a los que se accede con frecuencia.

Modifique la calidad de servicio

A partir de ONTAP 9,8, cuando aprovisiona almacenamiento, Calidad de servicio (QoS) está activado de forma predeterminada. Puede deshabilitar la calidad de servicio o elegir una política de calidad de servicio personalizada durante el proceso de aprovisionamiento. También puede modificar la calidad de servicio después de aprovisionar el almacenamiento.

Pasos

1. En System Manager, seleccione **Almacenamiento** y luego **Volúmenes**.
2. Junto al volumen para el que desea modificar la calidad de servicio, seleccione ⋮ Luego **Editar**.

Control de riesgos

A partir de ONTAP 9.10.0, puede usar System Manager para supervisar los riesgos notificados por el asesor digital de Active IQ. A partir de ONTAP 9.10.1, puede usar System Manager para reconocer también los riesgos.

El asesor digital de Active IQ de NetApp informa sobre las oportunidades de reducir el riesgo y mejorar el rendimiento y la eficiencia de su entorno de almacenamiento. System Manager le permite obtener información sobre los riesgos registrados por Active IQ y recibir información procesable que le ayuda a administrar el almacenamiento y lograr una mayor disponibilidad, una seguridad mejorada y un mejor rendimiento del almacenamiento.

Enlace a su cuenta de Active IQ

Para recibir información sobre riesgos de Active IQ, primero debe enlazar con la cuenta de Active IQ de System Manager.

Pasos

1. En System Manager, haga clic en **clúster > Configuración**.
2. En **Registro de Active IQ**, haga clic en **Registro**.
3. Introduzca sus credenciales para Active IQ.
4. Una vez autenticadas las credenciales, haga clic en **Confirmar para vincular Active IQ con System Manager**.

Ver el número de riesgos

A partir de ONTAP 9.10.0, puede ver desde la consola de System Manager la cantidad de riesgos notificados por Active IQ.

Antes de empezar

Debe establecer una conexión desde System Manager con la cuenta de Active IQ. Consulte Enlace a su cuenta de Active IQ.

Pasos

1. En System Manager, haga clic en **Panel**.
2. En la sección **Salud**, vea el número de riesgos reportados.

> Puede ver información más detallada sobre cada riesgo haciendo clic en el mensaje que muestra el número de riesgos. Consulte Consulte detalles de riesgos.

Consulte detalles de riesgos

A partir de ONTAP 9.10.0, puede ver desde System Manager cómo se clasifican los riesgos notificados por Active IQ en las áreas de impacto. También puede ver información detallada sobre cada riesgo notificado, su impacto potencial en el sistema y las acciones correctivas que puede tomar.

Antes de empezar

Debe establecer una conexión desde System Manager con la cuenta de Active IQ. Consulte Enlace a su cuenta de Active IQ.

Pasos

1. Haga clic en **Eventos > todos los eventos**.
2. En la sección **Descripción general**, en **Sugerencias** de Active IQ, vea el número de riesgos en cada categoría de área de impacto. Las categorías de riesgo incluyen:
   - Rendimiento y eficiencia
   - Disponibilidad y protección
   - Capacidad
   - Configuración
   - Seguridad
3. Haga clic en la ficha **Sugerencias** de Active IQ para ver información sobre cada riesgo, incluidos los siguientes:
   - Nivel de impacto en el sistema
   - Categoría del riesgo
   - Nodos afectados
   - Tipo de mitigación necesaria
   - Acciones correctivas que puede tomar

Reconocer riesgos

A partir de ONTAP 9.10.1, puede usar System Manager para reconocer cualquiera de los riesgos abiertos.

Pasos

1. En System Manager, muestre la lista de riesgos siguiendo el procedimiento en Consulte detalles de riesgos.
2. Haga clic en el nombre de riesgo de un riesgo abierto que desee reconocer.
3. Introduzca información en los siguientes campos:
   - Recordatorio (fecha)
   - Justificación
   - Comentarios
4. Haga clic en **acuse de recibo**.

> Tras reconocer un riesgo, el cambio tarda unos minutos en reflejarse en la lista de sugerencias de Active IQ.

No reconocer riesgos

A partir de ONTAP 9.10.1, puede usar System Manager para anular el reconocimiento de cualquier riesgo que anteriormente se hubiera reconocido.

Pasos

1. En System Manager, muestre la lista de riesgos siguiendo el procedimiento en Consulte detalles de riesgos.
2. Haga clic en el nombre de riesgo de un riesgo reconocido que desea no reconocer.
3. Introduzca información en los siguientes campos:
   - Justificación
   - Comentarios
4. Haga clic en **no confirmar**.

> Tras reconocer un riesgo, el cambio tarda unos minutos en reflejarse en la lista de sugerencias de Active IQ.

Información de System Manager

A partir de ONTAP 9.11.1, System Manager muestra *insights* que le ayudan a optimizar el rendimiento y la seguridad de su sistema.

> Para ver, personalizar y responder a los datos, consulte "Obtenga información interna para ayudarle a optimizar su sistema"

Información de la capacidad

System Manager puede mostrar la siguiente información en respuesta a las condiciones de capacidad de su sistema:

Insight	Gravedad	Condición	Soluciones

A los niveles locales les falta espacio	Solucione los riesgos	Uno o más niveles locales están llenos al 95% y crecen rápidamente. Es posible que las cargas de trabajo existentes no puedan crecer o, en casos extremos, las cargas de trabajo existentes pueden quedarse sin espacio y fallar.	**Revisión recomendada**: Realice una de las siguientes opciones. • Borre la cola de recuperación del volumen. • Habilite thin provisioning en volúmenes de thick provisioning para liberar el almacenamiento atrapado. • Mueva volúmenes a otro nivel local. • Elimine las copias Snapshot no necesarias. • Elimine los directorios o los archivos que no sean necesarios en los volúmenes. • Habilite Fabric Pool para organizar los datos en niveles en el cloud.
Las aplicaciones carecen de espacio	Necesita atención	Uno o más volúmenes están llenos a más del 95 %, pero no tienen habilitado el crecimiento automático.	**Recomendado**: Habilita el crecimiento automático hasta el 150% de la capacidad actual. **Otras opciones**: • Reclame espacio eliminando copias Snapshot. • Cambie el tamaño de los volúmenes. • Elimine directorios o archivos.
La capacidad del volumen FlexGroup se desequilibra	Optimizar el almacenamiento	El tamaño de los volúmenes constituyentes de uno o más volúmenes FlexGroup creció de forma desigual con el tiempo, lo que conduce a un desequilibrio en el uso de la capacidad. Si los volúmenes constituyentes se completan, se podrían producir errores de escritura.	**Recomendado**: Reequilibre los volúmenes de FlexGroup.

Los equipos virtuales de almacenamiento se están quedando sin capacidad	Optimizar el almacenamiento	Una o varias máquinas virtuales de almacenamiento se encuentran cerca de su capacidad máxima. No podrá aprovisionar más espacio para volúmenes nuevos o existentes si las máquinas virtuales de almacenamiento alcanzan la capacidad máxima.	**Recomendado**: Si es posible, aumente el límite de capacidad máxima de la VM de almacenamiento.

Información sobre seguridad

System Manager puede mostrar la siguiente información en respuesta a condiciones que podrían poner en peligro la seguridad de sus datos o del sistema.

Insight	Gravedad	Condición	Soluciones
Los volúmenes siguen en modo de aprendizaje anti-ransomware	Necesita atención	Uno o más volúmenes han estado en el modo de aprendizaje antiransomware durante 90 días.	**Recomendado**: Habilita el modo activo anti-ransomware para esos volúmenes.
La eliminación automática de copias de Snapshot se habilita en los volúmenes	Necesita atención	La eliminación automática de Snapshot se habilita en uno o más volúmenes.	**Recomendado**: Desactiva la eliminación automática de copias snapshot. De lo contrario, podría no ser posible llevar a cabo la recuperación de datos de estos volúmenes.
Los volúmenes no tienen políticas de Snapshot	Necesita atención	Uno o más volúmenes no tienen una política de Snapshot adecuada anexada a ellos.	**Recomendado**: Adjunte una política de Snapshot a volúmenes que no tengan uno. De lo contrario, podría no ser posible llevar a cabo la recuperación de datos de estos volúmenes.

FPolicy nativo no configurado	Mejor práctica	La política nativa de FPolicy no está configurada en una o más máquinas virtuales de almacenamiento NAS.	**Recomendado**: **IMPORTANTE**: Bloquear extensiones puede dar lugar a resultados inesperados. A partir de 9.11.1, podrá habilitar FPolicy nativo para máquinas virtuales de almacenamiento, que bloquea más de 3000 extensiones de archivos que se sabe que se utilizan para ataques de ransomware. "Configurar FPolicy nativa" En equipos virtuales de almacenamiento NAS para controlar las extensiones de archivos que permiten o no escribirse en volúmenes del entorno.
Telnet está activado	Mejor práctica	Se debe utilizar Secure Shell (SSH) para un acceso remoto seguro.	**Recomendado**: Desactiva Telnet y usa SSH para un acceso remoto seguro.
Hay muy pocos servidores NTP configurados	Mejor práctica	El número de servidores configurados para NTP es inferior a 3.	**Recomendado**: Asocie al menos tres servidores NTP con el cluster. De lo contrario, se pueden producir problemas con la sincronización de la hora del clúster.
Shell remoto (RSH) está activado	Mejor práctica	Se debe utilizar Secure Shell (SSH) para un acceso remoto seguro.	**Recomendado**: Desactiva RSH y usa SSH para un acceso remoto seguro.
El banner de inicio de sesión no está configurado	Mejor práctica	Los mensajes de inicio de sesión no están configurados para el clúster, para la máquina virtual de almacenamiento o para ambos.	**Recomendado**: Configure los banners de inicio de sesión para el clúster y la VM de almacenamiento y habilite su uso.
AutoSupport está utilizando un protocolo no seguro	Mejor práctica	AutoSupport no está configurado para comunicarse a través de HTTPS.	**Recomendado**: Se recomienda encarecidamente utilizar HTTPS como protocolo de transporte predeterminado para enviar mensajes AutoSupport al soporte técnico.
El usuario administrador predeterminado no está bloqueado	Mejor práctica	Nadie ha iniciado sesión con una cuenta administrativa predeterminada (admin o diag), y estas cuentas no están bloqueadas.	**Recomendado**: Bloquea las cuentas administrativas predeterminadas cuando no se estén utilizando.

Secure Shell (SSH) utiliza cifrados no seguros	Mejor práctica	La configuración actual utiliza cifrados de CBC no seguros.	**Recomendado**: Solo debe permitir cifrados seguros en su servidor web para proteger la comunicación segura con sus visitantes. Elimine los cifrados que tengan nombres que contengan “cbc”, como “ais128-cbc”, “AES192-cbc”, “AES256-cbc” y “3DES-cbc”.
El cumplimiento de la normativa global FIPS 140-2 está desactivado	Mejor práctica	El cumplimiento de la normativa global FIPS 140-2 está deshabilitado en el clúster.	**Recomendado**: Por razones de seguridad, debe habilitar la criptografía conforme a FIPS 140-2 global para garantizar que ONTAP pueda comunicarse de forma segura con clientes externos o clientes de servidor.
No se supervisan los volúmenes de ataques de ransomware	Necesita atención	El anti-ransomware está deshabilitado en uno o más volúmenes.	**Recomendado**: Habilitar anti-ransomware en los volúmenes. De lo contrario, es posible que no note cuándo los volúmenes se están amenazando o bajo ataque.
Las máquinas virtuales de almacenamiento no están configuradas para el ransomware	Mejor práctica	Una o varias máquinas virtuales de almacenamiento no están configuradas para la protección contra el ransomware.	**Recomendado**: Habilitar anti-ransomware en las VM de almacenamiento. De lo contrario, es posible que no se dé cuenta de cuándo las máquinas virtuales de almacenamiento se ven amenazadas o sufren un ataque.

Información de configuración

System Manager puede mostrar la siguiente información en respuesta a las dudas acerca de la configuración del sistema.

Insight	Gravedad	Condición	Soluciones
El clúster no está configurado para notificaciones	Mejor práctica	Correo electrónico, WebHooks o un host de capturas de SNMP no están configurados para permitirle recibir notificaciones acerca de problemas con el clúster.	**Recomendado**: Configurar notificaciones para el cluster.

El clúster no está configurado para las actualizaciones automáticas.	Mejor práctica	El clúster no se ha configurado para recibir actualizaciones automáticas del paquete de cualificación de disco más reciente, el firmware de disco, el firmware de la bandeja y los archivos de firmware SP/BMC cuando estén disponibles.	**Recomendado**: Habilita esta función.
El firmware del clúster no está actualizado	Mejor práctica	Su sistema no dispone de la última actualización del firmware, lo que podría tener mejoras, parches de seguridad o nuevas funciones que ayuden a proteger el clúster para lograr un mejor rendimiento.	**Recomendado**: Actualizar el firmware de ONTAP.

Obtenga información interna para ayudarle a optimizar su sistema

Con System Manager, puede ver información que le ayudará a optimizar su sistema.

Acerca de esta tarea

A partir de ONTAP 9.11.0, puede ver información de System Manager que le ayuda a optimizar el cumplimiento de normativas de seguridad y capacidad de su sistema.

A partir de ONTAP 9.11.1, puede ver información adicional que le ayuda a optimizar la capacidad, el cumplimiento de normativas de seguridad y la configuración del sistema.

Las extensiones de bloqueo pueden dar lugar a resultados inesperados. A partir de ONTAP 9.11.1, puedes habilitar FPolicy nativa para VM de almacenamiento usando System Manager. Puede recibir un mensaje de System Manager Insight que le recomienda "Configurar FPolicy nativa" Para una máquina virtual de almacenamiento.

Con el modo nativo de FPolicy, puede permitir o rechazar extensiones de archivo específicas. System Manager recomienda más de 3000 extensiones de archivos no permitidas que se hayan usado en ataques anteriores de ransomware. Algunas de estas extensiones pueden ser utilizadas por archivos legítimos en su entorno y bloquearlas puede dar lugar a problemas inesperados.

Por lo tanto, se recomienda encarecidamente que modifique la lista de extensiones para satisfacer las necesidades de su entorno. Consulte "Cómo quitar una extensión de archivo de una configuración nativa de FPolicy creada por System Manager con System Manager para volver a crear la política".

Para obtener más información sobre las FPolicy nativas, consulte "Tipos de configuración de FPolicy".

Basándose en las prácticas recomendadas, esta información se muestra en una página desde la cual puede iniciar acciones inmediatas para optimizar su sistema. Para obtener más información sobre cada detalle, consulte "Información de System Manager".

Vea información sobre optimización

Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.

   La página **Insights** muestra grupos de perspectivas. Cada grupo de perspectivas puede contener una o más información. Se muestran los siguientes grupos:

   - Necesita su atención
   - Solucione los riesgos
   - Optimice su almacenamiento

2. (Opcional) filtre las estadísticas que se muestran haciendo clic en estos botones en la esquina superior derecha de la página:

   - Muestra información relacionada con la seguridad.
   - Muestra la información relacionada con la capacidad.
   - Muestra la información relacionada con la configuración.
   - All Muestra todas las estadísticas.

Responda a la información para optimizar su sistema

En System Manager, puede responder a información descontada, explorando distintas formas de solucionar los problemas o iniciando el proceso para solucionarlos.

Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.
2. Pase el ratón sobre una información para mostrar los botones que se utilizan para llevar a cabo las siguientes acciones:
   - **Descartar**: Quita la visión de la vista. Para «'desconocer'» la información, consulte [customize-settings-insights].
   - **Explore**: Descubra varias formas de solucionar el problema mencionado en la visión. Este botón sólo aparece si hay más de un método de corrección.
   - **Fix**: Iniciar el proceso de solucionar el problema mencionado en la perspectiva. Se le pedirá que confirme si desea realizar la acción necesaria para aplicar la corrección.

> Algunas de estas acciones se pueden iniciar desde otras páginas en System Manager, pero la página **Insights** le ayuda a optimizar sus tareas diarias al permitirle iniciar esta acción desde esta página única.

Personalice la configuración para obtener información

Puede personalizar las conclusiones sobre las que se le notificará en System Manager.

Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.
2. En la esquina superior derecha de la página, haga clic en ⋮, Luego seleccione **Configuración**.
3. En la página **Configuración**, asegúrese de que hay una Marca en las casillas de verificación situadas junto a las estadísticas sobre las que desea recibir notificación. Si ha rechazado previamente una información, puede descartarla asegurándose de que la casilla de verificación está en su lugar.
4. Haga clic en **Guardar**.

Exporte las estadísticas como un archivo PDF

Puede exportar todos los datos aplicables como un archivo PDF.

Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.
2. En la esquina superior derecha de la página, haga clic en ⋮, Luego seleccione **Exportar**.

Configurar FPolicy nativa

A partir de ONTAP 9.11.1, cuando recibe un informe del administrador del sistema que sugiere implementar FPolicy nativa, puede configurarla en sus máquinas virtuales y volúmenes de almacenamiento.

Antes de empezar

Al acceder a System Manager Insights, en **Aplicar prácticas recomendadas**, es posible que reciba un mensaje que indique que FPolicy nativo no está configurado.

Para obtener más información sobre los tipos de configuración FPolicy, consulte "Tipos de configuración de FPolicy".

Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.
2. En **Aplicar las mejores prácticas**, localice **La FPolicy nativa no está configurada**.
3. Lea el siguiente mensaje antes de tomar medidas:

> **Las extensiones de bloqueo pueden dar lugar a resultados inesperados.** A partir de ONTAP 9.11.1, puedes habilitar FPolicy nativa para VM de almacenamiento usando System Manager.
> Con el modo nativo de FPolicy, puede permitir o rechazar extensiones de archivo específicas. System Manager recomienda más de 3000 extensiones de archivos no permitidas que se hayan usado en ataques anteriores de ransomware. Algunas de estas extensiones pueden ser utilizadas por archivos legítimos en su entorno y bloquearlas puede dar lugar a problemas inesperados.
>
> Por lo tanto, se recomienda encarecidamente que modifique la lista de extensiones para satisfacer las necesidades de su entorno. Consulte "Cómo quitar una extensión de archivo de una configuración nativa de FPolicy creada por System Manager con System Manager para volver a crear la política".

4. Haga clic en **Fix**.
5. Seleccione las máquinas virtuales de almacenamiento a las que desea aplicar la FPolicy nativa.
6. Para cada máquina virtual de almacenamiento, seleccione los volúmenes que recibirán la FPolicy nativa.
7. Haga clic en **Configurar**.

Supervise y gestione el rendimiento de los clústeres mediante la CLI

Información general sobre la gestión y el control del rendimiento

Puede configurar tareas básicas de supervisión y gestión del rendimiento, e identificar y resolver problemas comunes de rendimiento.

Puede utilizar estos procedimientos para supervisar y gestionar el rendimiento del clúster si se aplican las siguientes suposiciones a su situación:

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.
- Si desea mostrar el estado y las alertas del sistema, supervisar el rendimiento del clúster y realizar análisis de las causas subyacentes utilizando Active IQ Unified Manager (antes Unified Manager de OnCommand), además de la interfaz de línea de comandos de ONTAP.
- Se utiliza la interfaz de línea de comandos de ONTAP para configurar la calidad de servicio (QoS) de almacenamiento.

  La calidad de servicio también está disponible en System Manager, NSLM, WFA, VSC (complemento de VMware) y API.

- Desea instalar Unified Manager mediante un dispositivo virtual, en lugar de una instalación basada en Linux o Windows.
- Está dispuesto a utilizar una configuración estática en lugar de DHCP para instalar el software.
- Puede acceder a los comandos de ONTAP en el nivel de privilegios avanzados.

- Es un administrador de clústeres con el rol "admin".

Información relacionada

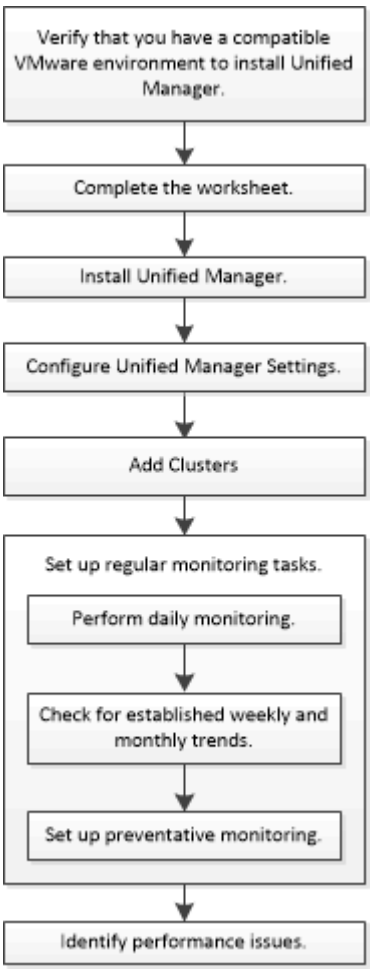
Si estas suposiciones no son correctas para su situación, debería consultar los recursos siguientes:

- "Instalación de Active IQ Unified Manager 9.8"
- "Administración del sistema"

Supervisión del rendimiento

Información general sobre el flujo de trabajo de supervisión y mantenimiento del rendimiento

La supervisión y el mantenimiento del rendimiento de los clústeres implica instalar el software Active IQ Unified Manager, configurar tareas de supervisión básicas, identificar problemas de rendimiento y realizar ajustes según sea necesario.



Comprobar que su entorno VMware es compatible

Para instalar Active IQ Unified Manager correctamente, debe comprobar que el entorno de VMware cumple con los requisitos necesarios.

Pasos

1. Compruebe que su infraestructura VMware cumple los requisitos de tamaño para la instalación de Unified

Manager.

2. Vaya a la "Matriz de interoperabilidad" para verificar que tiene una combinación compatible de los siguientes componentes:
   - Versión de ONTAP
   - Versión del sistema operativo ESXi
   - La versión de VMware vCenter Server
   - Versión de VMware Tools
   - Tipo y versión del navegador

   La "Matriz de interoperabilidad" Enumera las configuraciones admitidas para Unified Manager.

3. Haga clic en el nombre de la configuración seleccionada.

   Los detalles de esa configuración se muestran en la ventana Detalles de configuración.

4. Revise la información en las siguientes pestañas:
   - Notas

     Enumera las alertas e información importantes que son específicas de su configuración.

   - Políticas y directrices

     Proporciona directrices generales para todas las configuraciones.

Hoja de cálculo de Active IQ Unified Manager

Antes de instalar, configurar y conectar Active IQ Unified Manager, debe tener disponible información específica acerca de su entorno. Puede registrar la información en la hoja de cálculo.

Información de instalación de Unified Manager

Máquina virtual en la que se ha puesto en marcha el software	Su valor
Dirección IP del servidor ESXi	
Nombre de dominio completo del host	
Dirección IP del host	
Máscara de red	
Dirección IP de la pasarela	
Dirección DNS principal	

Dirección DNS secundaria	
Buscar dominios	
Nombre de usuario de mantenimiento	
Contraseña de usuario de mantenimiento	

Información de configuración de Unified Manager

Ajuste	Su valor
Dirección de correo electrónico del usuario de mantenimiento	
Servidor NTP	
Nombre de host o dirección IP del servidor SMTP	
Nombre de usuario SMTP	
Contraseña SMTP	
Puerto predeterminado SMTP	25 (valor predeterminado)
Correo electrónico desde el cual se envían notificaciones de alerta	
Nombre distintivo de enlace LDAP	
Contraseña de enlace LDAP	
Nombre del administrador de Active Directory	
Contraseña de Active Directory	
Nombre distintivo de la base del servidor de autenticación	
Nombre de host o dirección IP del servidor de autenticación	

Información del clúster

Capture la siguiente información para cada clúster en Unified Manager.

Clúster 1 de N	Su valor
El nombre de host o la dirección IP de administración del clúster	
Nombre de usuario del administrador ONTAP Debe haber asignado el rol de administrador.	
Contraseña del administrador de ONTAP	
Protocolo (HTTP o HTTPS)	

Información relacionada

"Autenticación de administrador y RBAC"

Instale Active IQ Unified Manager

Descargue e implemente Active IQ Unified Manager

Para instalar el software, debe descargar el archivo de instalación de dispositivos virtuales (va) y, a continuación, usar un cliente de VMware vSphere para implementar el archivo en un servidor ESXi de VMware. El va está disponible en un archivo OVA.

Pasos

1. Vaya a la página **Descarga de software del sitio de soporte de NetApp** y localice Active IQ Unified Manager.

   https://mysupport.netapp.com/products/index.html

2. Seleccione **VMware vSphere** en el menú desplegable **Select Platform** y haga clic en **Go!**
3. Guarde el archivo «'OVA» en una ubicación local o de red a la que pueda acceder VMware vSphere Client.
4. En VMware vSphere Client, haga clic en **Archivo** > **implementar plantilla OVF**.
5. Localice el archivo «'OVA'» y utilice el asistente para implementar el dispositivo virtual en el servidor ESXi.

   Puede utilizar la ficha **Propiedades** del asistente para introducir la información de configuración estática.

6. Encienda la máquina virtual.
7. Haga clic en la ficha **Consola** para ver el proceso de inicio inicial.
8. Siga el prompt para instalar VMware Tools en la VM.
9. Configure la zona horaria.
10. Introduzca un nombre de usuario y una contraseña de mantenimiento.
11. Vaya a la URL que muestra la consola de VM.

Configure los ajustes iniciales de Active IQ Unified Manager

El cuadro de diálogo Active IQ Unified Manager Initial Setup aparece cuando se accede por primera vez a la interfaz de usuario web, que permite configurar algunos ajustes iniciales y añadir clústeres.

Pasos

1. Acepte la configuración predeterminada de AutoSupport habilitada.
2. Introduzca los detalles del servidor NTP, la dirección de correo electrónico del usuario de mantenimiento, el nombre de host del servidor SMTP y las opciones SMTP adicionales y, a continuación, haga clic en **Guardar**.

Después de terminar

Una vez finalizada la configuración inicial, se muestra la página Cluster Data Sources, donde puede agregar los detalles del clúster.

Especifique los clústeres que se van a supervisar

Debe añadir un clúster a un servidor Active IQ Unified Manager para supervisar el clúster, ver el estado de detección del clúster y supervisar su rendimiento.

Lo que necesitará

- Debe tener la siguiente información:
  - El nombre de host o la dirección IP de administración del clúster

    El nombre de host es el nombre de dominio completo (FQDN) o el nombre corto que Unified Manager utiliza para conectarse con el clúster. Este 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.

  - Nombre de usuario y contraseña del administrador de ONTAP
  - Tipo de protocolo (HTTP o HTTPS) que se puede configurar en el clúster y el número de puerto del clúster
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- El administrador de ONTAP debe tener los roles de administrador ONAPI y SSH.
- El FQDN de Unified Manager debe poder hacer ping ONTAP.

  Puede verificarlo con el comando ONTAP `ping -node` *`node_name`* `-destination` *`Unified_Manager_FQDN`*.

Acerca de esta tarea

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

Pasos

1. Haga clic en **Configuración** > **fuentes de datos de clúster**.

2. En la página Clusters, 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 (IPv4 o IPv6) del clúster, el nombre de usuario, la contraseña, el protocolo para la comunicación y el número de puerto.

   De manera predeterminada, se selecciona el protocolo HTTPS.

   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 que finaliza el próximo ciclo de supervisión.
4. Haga clic en **Agregar**.
5. Si selecciona HTTPS, realice los siguientes pasos:

   a. En el cuadro de diálogo **autorizar host**, haga clic en **Ver certificado** para ver la información del certificado sobre el clúster.

   b. Haga clic en **Sí**.

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

   Si el certificado ha caducado, no puede añadir el clúster. Debe renovar el certificado SSL y, a continuación, añadir el clúster.
6. **Opcional**: Ver el estado de detección del clúster:

   a. Revise el estado de detección del clúster desde la página **Configuración del clúster**.

   El clúster se añade a la base de datos de Unified Manager después del intervalo de supervisión predeterminado de aproximadamente 15 minutos.

Configurar tareas básicas de supervisión

Realizar una supervisión diaria

Puede realizar una supervisión diaria para garantizar que no tenga ningún problema de rendimiento inmediato que requiera atención.

Pasos

1. Desde la interfaz de usuario de Active IQ Unified Manager, vaya a la página **Inventario de eventos** para ver todos los eventos actuales y obsoletos.
2. En la opción **Ver**, seleccione `Active Performance Events` y determinar qué acción se requiere.

Utilice tendencias de rendimiento semanales y mensuales para identificar problemas de rendimiento

La identificación de las tendencias de rendimiento puede ayudarle a identificar si el clúster se está utilizando en exceso o está infrautilizado mediante el análisis de latencia de volumen. Puede seguir pasos similares para identificar cuellos de botella en la CPU, la red u otros sistemas.

Pasos

1. Localice el volumen que sospecha está infrautilizado o en exceso.
2. En la ficha **Detalles de volumen**, haga clic en **30 d** para mostrar los datos históricos.
3. En el menú desplegable "Break down data by", seleccione **latencia** y, a continuación, haga clic en **Enviar**.
4. Anule la selección de **agregado** en el gráfico de comparación de componentes del clúster y, a continuación, compare la latencia del clúster con el gráfico de latencia del volumen.
5. Seleccione **agregado** y anule la selección de todos los demás componentes del gráfico de comparación de componentes del clúster y, a continuación, compare la latencia de agregado con el gráfico de latencia de volumen.
6. Compare el gráfico de latencia de lecturas/escrituras con el gráfico de latencia de volúmenes.
7. Determine si las cargas de aplicaciones cliente han causado una contención de carga de trabajo y reequilibrio de cargas de trabajo según sea necesario.
8. Determine si el agregado está sobrecargado y causa contención y reequilibre las cargas de trabajo según sea necesario.

Utilice umbrales de rendimiento para generar notificaciones de eventos

Los eventos son notificaciones que el Active IQ Unified Manager genera automáticamente cuando se produce una condición predefinida o cuando un valor de contador de rendimiento cruza un umbral. Los eventos le ayudan a identificar problemas de rendimiento en los clústeres que se supervisan. Es posible configurar alertas para que envíen notificaciones por correo electrónico automáticamente cuando se produzcan eventos de ciertos tipos de gravedad.

Definir umbrales de rendimiento

Se pueden establecer umbrales de rendimiento para supervisar problemas de rendimiento críticos. Los umbrales definidos por el usuario activan una notificación de sucesos críticos o de advertencia cuando el sistema se acerca o supera el umbral definido.

Pasos

1. Cree los umbrales de sucesos críticos y de advertencia:
   a. Seleccione **Configuración** > **umbrales de rendimiento**.
   b. Haga clic en **Crear**.
   c. Seleccione el tipo de objeto y especifique un nombre y una descripción de la política.
   d. Seleccione la condición del contador de objetos y especifique los valores de límite que definen los eventos de advertencia y críticos.
   e. Seleccione la duración del tiempo durante el que deben incumplir los valores límite para que se envíe un evento y, a continuación, haga clic en **Guardar**.
2. Asigne la política de umbral al objeto de almacenamiento.
   a. Vaya a la página Inventory para el mismo tipo de objeto de clúster que seleccionó anteriormente y seleccione **Performance** en la opción View.
   b. Seleccione el objeto al que desea asignar la directiva de umbral y, a continuación, haga clic en **asignar directiva de umbral**.

c. Seleccione la directiva que creó anteriormente y, a continuación, haga clic en **asignar directiva**.

Ejemplo

Puede establecer umbrales definidos por el usuario para aprender acerca de problemas de rendimiento críticos. Por ejemplo, si tiene un servidor Microsoft Exchange Server y sabe que falla si la latencia del volumen supera los 20 milisegundos, puede establecer un umbral de advertencia de 12 milisegundos y un umbral crítico de 15 milisegundos. Con este ajuste de umbral, se pueden recibir notificaciones cuando la latencia del volumen supere el límite.

Añadir alertas

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

Lo que necesitará

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

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 contiene "abc" y excluye todos los volúmenes cuyo nombre contiene "xyz".
- Eventos: Incluye todos los eventos críticos de salud
- Acciones: Incluye "sample@domain.com", una secuencia de comandos "Test" y el usuario debe 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**.

Configure los ajustes de alerta

Es posible especificar qué eventos de Active IQ Unified Manager desencadenan las alertas, los destinatarios de correo electrónico para esas alertas y la frecuencia de las alertas.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Acerca de esta tarea

Puede configurar ajustes de alerta únicos para los siguientes tipos de eventos de rendimiento:

- Eventos críticos desencadenados por infracciones de umbrales definidos por el usuario
- Eventos de advertencia provocados por infracciones de umbrales definidos por el usuario, umbrales definidos por el sistema o umbrales dinámicos

De manera predeterminada, las alertas por correo electrónico se envían a los usuarios administradores de Unified Manager para todos los eventos nuevos. Es posible que se envíen alertas por correo electrónico a otros usuarios con la adición de las direcciones de correo electrónico de esos usuarios.

> Para deshabilitar el envío de alertas para determinados tipos de eventos, debe desactivar todas las casillas de comprobación de una categoría de eventos. Esta acción no detiene que los eventos aparezcan en la interfaz de usuario.

Pasos

1. En el panel de navegación izquierdo, seleccione **Administración de almacenamiento** > **Configuración de alertas**.

   Aparecerá la página Configuración de alertas.

2. Haga clic en **Agregar** y configure los valores adecuados para cada uno de los tipos de evento.

   Para que se envíen alertas de correo electrónico a varios usuarios, introduzca una coma entre cada dirección de correo electrónico.

3. Haga clic en **Guardar**.

Identifique problemas de rendimiento en Active IQ Unified Manager

Si se produce un evento de rendimiento, puede localizar el origen del problema en Active IQ Unified Manager y utilizar otras herramientas para solucionarlo. Es posible que reciba una notificación por correo electrónico sobre un evento o que se lo notifique durante su supervisión diaria.

Pasos

1. Haga clic en el enlace de la notificación por correo electrónico, que le llevará directamente al objeto de

almacenamiento que tiene un evento de rendimiento.

Si…	Realice lo siguiente…
Recibir una notificación por correo electrónico de un evento	Haga clic en el enlace para ir directamente a la página de detalles del evento.
Observe el evento mientras analiza la página Event Inventory	Seleccione el evento para ir directamente a la página de detalles del evento.

2. Si el evento ha superado un umbral definido por el sistema, siga las acciones sugeridas en la interfaz de usuario para solucionar el problema.
3. Si el evento ha superado un umbral definido por el usuario, analice el evento para determinar si necesita realizar alguna acción.
4. Si el problema persiste, compruebe los siguientes ajustes:
   - Configuración de protocolo en el sistema de almacenamiento
   - Ajustes de red en cualquier switch Ethernet o estructural
   - Ajustes de red en el sistema de almacenamiento
   - Distribución de discos y métricas agregadas en el sistema de almacenamiento
5. Si el problema persiste, póngase en contacto con el soporte técnico para obtener ayuda.

Utilice el asesor digital de Active IQ para ver el rendimiento del sistema

En cualquier sistema ONTAP que envíe telemetría AutoSupport a NetApp, puede ver una gran cantidad de datos sobre rendimiento y capacidad. Active IQ muestra el rendimiento del sistema durante un período más largo de lo que se puede ver en System Manager.

Puede ver gráficos de la utilización de CPU, latencia, IOPS, IOPS por protocolo y rendimiento de la red. También puede descargar estos datos en formato .csv para analizarlos en otras herramientas.

Además de estos datos de rendimiento, Active IQ puede mostrarle eficiencia de almacenamiento por carga de trabajo y comparar esa eficiencia con la eficiencia esperada para ese tipo de carga de trabajo. Puede ver las tendencias de capacidad y calcular una estimación de la cantidad de almacenamiento adicional que puede necesitar añadir en un periodo de tiempo determinado.

- La eficiencia del almacenamiento está disponible a nivel del cliente, clúster y nodo en el lado izquierdo del panel principal.
- El rendimiento está disponible en el nivel del clúster y del nodo en el lado izquierdo del panel principal.

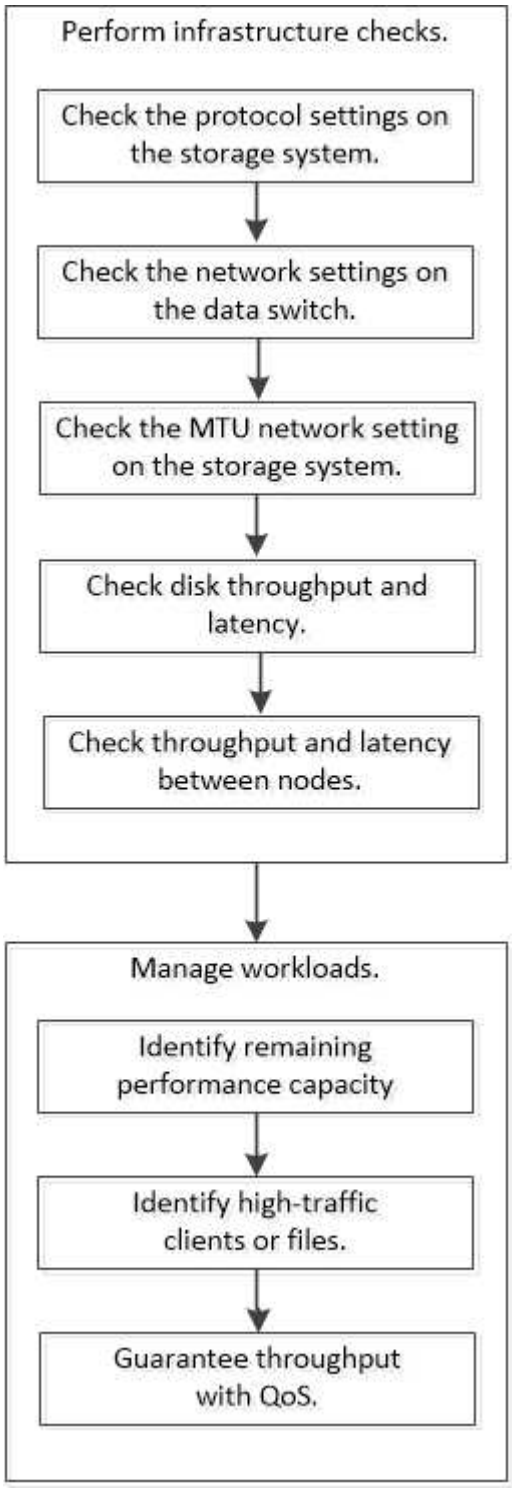
Información relacionada

- "Documentación del asesor digital de Active IQ"
- "Lista de reproducción de vídeo del asesor digital Active IQ"
- "Portal web de Active IQ"

Gestione los problemas de rendimiento

Flujo de trabajo de gestión del rendimiento

Una vez identificado un problema de rendimiento, puede llevar a cabo algunas comprobaciones de diagnóstico básicas de la infraestructura para descartar errores evidentes de configuración. Si esas personas no identifican el problema, puede empezar a examinar problemas de gestión de la carga de trabajo.



Realizar comprobaciones básicas de la infraestructura

Compruebe la configuración del protocolo en el sistema de almacenamiento

Compruebe el tamaño máximo de transferencia de TCP de NFS

Para NFS, puede comprobar si el tamaño máximo de transferencia TCP para lecturas y escrituras puede estar provocando un problema de rendimiento. Si cree que el tamaño ralentiza el rendimiento, puede aumentarlo.

Lo que necesitará

- Para realizar esta tarea, debe tener privilegios de administrador de clúster.
- Para esta tarea, debe utilizar comandos de nivel de privilegio avanzado.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Compruebe el tamaño máximo de transferencia TCP:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

3. Si el tamaño máximo de transferencia del TCP es demasiado pequeño, aumente el tamaño:

   ```
   vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
   ```

4. Volver al nivel de privilegio administrativo:

   ```
   set -privilege admin
   ```

Ejemplo

En el ejemplo siguiente se cambia el tamaño máximo de transferencia TCP de `SVM1` a 1048576:

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

Compruebe el tamaño de lectura/escritura del TCP de iSCSI

Para iSCSI, es posible comprobar el tamaño de lectura/escritura de TCP para determinar si la configuración de tamaño está creando un problema de rendimiento. Si el tamaño es el origen de un problema, puede corregirlo.

Lo que necesitará

Para esta tarea, se requieren comandos de nivel de privilegio avanzado.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Compruebe la configuración del tamaño de la ventana TCP:

   `vserver iscsi show -vserv,er vserver_name -instance`

3. Modifique la configuración del tamaño de la ventana TCP:

   `vserver iscsi modify -vserver vserver_name -tcp-window-size integer`

4. Devolver al privilegio administrativo:

   `set -privilege admin`

Ejemplo

En el ejemplo siguiente se cambia el tamaño de la ventana TCP de `SVM1` a 131,400 bytes:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

Controlar los valores multiplexados CIFS

Si el rendimiento lento de la red CIFS provoca un problema de rendimiento, puede modificar los ajustes multiplexados para mejorarlos y corregirlos.

Pasos

1. Controlar el reglaje multiplexado CIFS:

   `vserver cifs options show -vserver –vserver_name -instance`

2. Modificar el reglaje multiplexado CIFS:

   `vserver cifs options modify –vserver –vserver_name –max-mpx integer`

Ejemplo

En el ejemplo siguiente se modifica el recuento máximo de los multiplexados `SVM1` a 255:

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

Compruebe la velocidad del puerto del adaptador de FC

La velocidad del puerto de destino del adaptador debe coincidir con la velocidad del dispositivo al que se conecta, para optimizar el rendimiento. Si el puerto está definido en autonegociación, puede tardar más en reconectar después de una toma de control y devolución u otra interrupción.

Lo que necesitará

Todos los LIF que utilizan este adaptador como puerto de inicio deben estar desconectados.

Pasos

1. Desconectar el adaptador:

   ```
   network fcp adapter modify -node nodename -adapter adapter -state down
   ```

2. Compruebe la velocidad máxima del adaptador de puerto:

   ```
   fcp adapter show -instance
   ```

3. Cambie la velocidad del puerto, si es necesario:

   ```
   network fcp adapter modify -node nodename -adapter adapter -speed
   {1|2|4|8|10|16|auto}
   ```

4. Conectar el adaptador:

   ```
   network fcp adapter modify -node nodename -adapter adapter -state up
   ```

5. Conectar todas las LIF del adaptador:

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
   -status-admin up
   ```

Ejemplo

En el ejemplo siguiente se cambia la velocidad del puerto del adaptador `0d` encendido `node1` Hasta 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

Compruebe la configuración de red en los switches de datos

Aunque debe mantener la misma configuración MTU en los clientes, los servidores y los sistemas de almacenamiento (es decir, los extremos de red), los dispositivos de red intermedios como las NIC y los switches deben configurarse con sus valores máximos de MTU para garantizar que el rendimiento no se vea afectado.

Para obtener el mejor rendimiento, todos los componentes de la red deben ser capaces de reenviar tramas gigantes (IP de 9000 bytes, 9022 bytes incluyendo Ethernet). Los switches de datos deben establecerse en al menos 9022 bytes, pero es posible un valor típico de 9216 en la mayoría de los switches.

Procedimiento

En el caso de los switches de datos, compruebe que el tamaño de MTU esté establecido en 9022 o superior.

Para obtener más información, consulte la documentación del proveedor de switches.

Compruebe la configuración de red MTU en el sistema de almacenamiento

Puede cambiar la configuración de red en el sistema de almacenamiento si no son los mismos que en el cliente o en otros extremos de red. Mientras que la configuración de MTU de red de gestión se establece en 1500, el tamaño de MTU de red de datos debe ser de 9000.

Acerca de esta tarea

Todos los puertos dentro de un dominio de retransmisión tienen el mismo tamaño de MTU, a excepción del puerto e0M que gestiona el tráfico de gestión. Si el puerto forma parte de un dominio de retransmisión, use el `broadcast-domain modify` Comando para cambiar la MTU de todos los puertos dentro del dominio de retransmisión modificado.

Tenga en cuenta que los dispositivos de red intermedios, como NIC y switches de datos, se pueden establecer con tamaños de MTU superiores a los extremos de red. Para obtener más información, consulte "Compruebe la configuración de red en los switches de datos".

Pasos

1. Compruebe la configuración de puerto MTU en el sistema de almacenamiento:

   ```
   network port show -instance
   ```

2. Cambie la MTU en el dominio de retransmisión que utilizan los puertos:

   ```
   network port broadcast-domain modify -ipspace ipspace -broadcast-domain
   broadcast_domain -mtu new _mtu
   ```

Ejemplo

En el ejemplo siguiente se cambia la configuración de puerto MTU a 9000:

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

Comprobar el rendimiento del disco y la latencia

Puede comprobar las métricas de rendimiento de disco y latencia para los nodos del clúster para ayudarle a resolver problemas.

Acerca de esta tarea

Para esta tarea, se requieren comandos de nivel de privilegio avanzado.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Compruebe las métricas de rendimiento y latencia del disco:

   ```
   statistics disk show -sort-key latency
   ```

Ejemplo

En el siguiente ejemplo se muestran los totales de cada operación de lectura o escritura de usuario para `node2` encendido `cluster1`:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                    Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

Compruebe el rendimiento y la latencia entre los nodos

Puede utilizar el `network test-path` comando para identificar cuellos de botella de red o para precalificar las rutas de red entre los nodos. Se puede ejecutar el comando entre nodos de interconexión de clústeres o nodos dentro del clúster.

Lo que necesitará

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Para esta tarea, se requieren comandos de nivel de privilegio avanzado.
- En el caso de una ruta de interconexión de clústeres, los clústeres de origen y destino deben tener una relación entre iguales.

Acerca de esta tarea

En ocasiones, es posible que el rendimiento de red entre nodos no cumpla las expectativas de la configuración de la ruta. Por ejemplo, una tasa de transmisión de 1 Gbps para el tipo de transferencias de datos grandes que se ven en operaciones de replicación de SnapMirror no sería coherente con un enlace de 10 GbE entre los clústeres de origen y destino.

Puede utilizar el `network test-path` comando para medir el rendimiento y la latencia entre nodos. Se puede ejecutar el comando entre nodos de interconexión de clústeres o nodos dentro del clúster.

> La prueba satura la ruta de red con los datos, de modo que debe ejecutar el comando cuando el sistema no está ocupado y cuando el tráfico de red entre nodos no es excesivo. El tiempo de prueba se agota al cabo de diez segundos. El comando se puede ejecutar solo entre nodos de ONTAP 9.

La `session-type` Option identifica el tipo de operación que se ejecuta en la ruta de red, por ejemplo, "AsyncMirrorRemote" para la replicación de SnapMirror en un destino remoto. El tipo determina la cantidad de datos utilizados en la prueba. En la siguiente tabla se definen los tipos de sesión:

Tipo de sesión	Descripción

AsyncMirrorlocal	Configuración que utiliza SnapMirror entre nodos del mismo clúster
AsyncMirrorRemote	Configuración que utiliza SnapMirror entre nodos de diferentes clústeres (tipo predeterminado)
RemoteDataTransfer	La configuración que utiliza ONTAP para acceder de forma remota a datos entre nodos del mismo clúster (por ejemplo, una solicitud NFS a un nodo de un archivo almacenado en un volumen en un nodo diferente)

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Mida el rendimiento y la latencia entre nodos:

   ```
   network test-path -source-node source_nodename |local -destination-cluster
   destination_clustername -destination-node destination_nodename -session-type
   Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
   ```

   El nodo de origen debe estar en el clúster local. El nodo de destino puede estar en el clúster local o en un clúster con una relación entre iguales. Valor "local" para `-source-node` especifica el nodo en el que está ejecutando el comando.

   El siguiente comando mide el rendimiento y la latencia de las operaciones de replicación del tipo SnapMirror entre `node1` en el clúster local y. `node3` encendido `cluster2`:

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   Min latency in ms:  61.14
   Max latency in ms:  3056.86
   ```

3. Devolver al privilegio administrativo:

   ```
   set -privilege admin
   ```

Después de terminar

Si el rendimiento no cumple las expectativas de configuración de la ruta, debe comprobar las estadísticas de rendimiento del nodo, utilizar las herramientas disponibles para aislar el problema en la red, comprobar la

configuración del switch, etc.

Gestionar cargas de trabajo

Identifique la capacidad de rendimiento restante

La capacidad de rendimiento, o *margen adicional*, mide la cantidad de trabajo que se puede realizar en un nodo o en un agregado antes de que el rendimiento de las cargas de trabajo del recurso comience a verse afectado por la latencia. Saber que la capacidad de rendimiento disponible en el clúster le ayuda a aprovisionar y equilibrar las cargas de trabajo.

Lo que necesitará

Para esta tarea, se requieren comandos de nivel de privilegio avanzado.

Acerca de esta tarea

Puede usar los siguientes valores para el `-object` opción de recopilar y mostrar estadísticas de margen adicional:

- Para CPU, `resource_headroom_cpu`.
- Para agregados, `resource_headroom_aggr`.

También puede completar esta tarea mediante System Manager y Active IQ Unified Manager.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Inicie la recopilación de estadísticas de margen en tiempo real:

   ```
   statistics start -object resource_headroom_cpu|aggr
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

3. Mostrar información de estadísticas de margen adicional en tiempo real:

   ```
   statistics show -object resource_headroom_cpu|aggr
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

4. Devolver al privilegio administrativo:

   ```
   set -privilege admin
   ```

Ejemplo

En el siguiente ejemplo, se muestran las estadísticas de margen adicional medio por hora para los nodos del clúster.

Puede calcular la capacidad de rendimiento disponible para un nodo restando el `current_utilization` en el contador de `optimal_point_utilization` contador. En este ejemplo, la capacidad de utilización para

`CPU_sti2520-213` Es de -14% (72%-86%), lo que sugiere que la CPU ha sido sobreutilizada de media durante la última hora.

Podría haber especificado `ewma_daily`, `ewma_weekly`, o. `ewma_monthly` obtener la misma información promediada en períodos de tiempo más largos.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                current_utilization                               86
                  optimal_point_ops                             2573
               optimal_point_latency                            3589
            optimal_point_utilization                             72
     optimal_point_confidence_factor                               1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                current_utilization                                 0
                  optimal_point_ops                                 0
               optimal_point_latency                                0
            optimal_point_utilization                              71
     optimal_point_confidence_factor                               1
2 entries were displayed.
```

Identifique los ficheros o clientes de alto tráfico

Puede utilizar la tecnología ONTAP Active Objects para identificar clientes o archivos que son responsables de una cantidad desproporcionadamente grande del tráfico del clúster. Cuando haya identificado estos archivos o clientes «principales», podrá reequilibrar las cargas de trabajo del clúster o realizar otros pasos para resolver el problema.

Lo que necesitará

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Vea los principales clientes que acceden al clúster:

   `statistics top client show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   El siguiente comando muestra los principales clientes que acceden `cluster1`:

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                              *Total
        Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

2. Vea los archivos principales a los que se accede en el clúster:

   `statistics top file show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   El siguiente comando muestra los principales archivos en los que se puede acceder `cluster1`:

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

Garantice el rendimiento con calidad de servicio

Garantice el rendimiento con información general de calidad de servicio

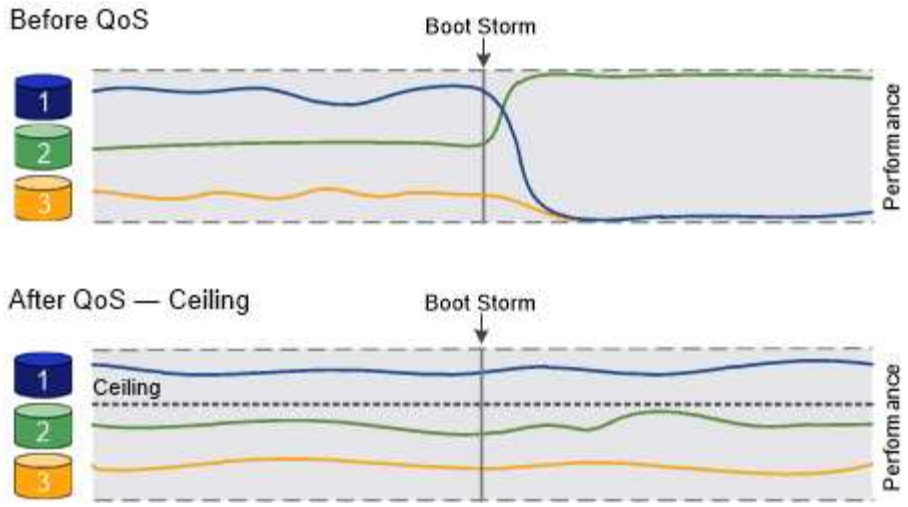
Puede utilizar calidad de servicio del almacenamiento para garantizar que el rendimiento de las cargas de trabajo críticas no se vea degradado por cargas de trabajo de la competencia. Puede establecer un rendimiento *plaft* en una carga de trabajo en competencia para limitar su impacto en los recursos del sistema o establecer un rendimiento *floor* para una carga de trabajo crítica, garantizando que cumple los objetivos de rendimiento mínimos, sin importar la demanda de otras cargas de trabajo de la competencia. Puede incluso fijar un techo y un suelo para la misma carga de trabajo.

Acerca de los techos de rendimiento (QoS máx.)

Un techo de rendimiento limita el rendimiento de una carga de trabajo a un número máximo de IOPS o Mbps, o IOPS y Mbps. En la siguiente figura, el máximo rendimiento de la carga de trabajo 2 garantiza que no "intimida" las cargas de trabajo 1 y 3.

Un *policy group* define el techo de rendimiento de una o más cargas de trabajo. Una carga de trabajo representa las operaciones de I/o para un objeto *Storage:* un volumen, un archivo, un qtree o una LUN o todos los volúmenes, archivos, qtrees o LUN de una SVM. Puede especificar el techo al crear el grupo de políticas, o bien se puede esperar hasta después de supervisar las cargas de trabajo para especificarlo.

> El rendimiento en las cargas de trabajo puede superar el límite máximo especificado hasta en un 10 %, especialmente si una carga de trabajo experimenta cambios rápidos en el rendimiento. El techo podría ser superado en hasta un 50% para manejar las ráfagas. Las ráfagas se producen en nodos únicos cuando los tokens se acumulan hasta un 150 %



Acerca de los pisos de rendimiento (calidad de servicio mínima)

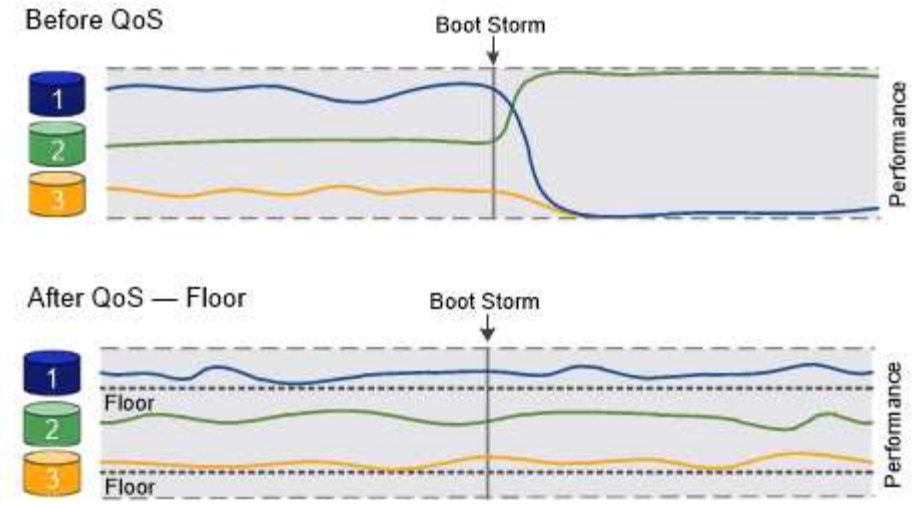
Un nivel de rendimiento garantiza que el rendimiento de una carga de trabajo no caiga por debajo del número mínimo de IOPS o MBps, ni de IOPS y MBps. En la siguiente figura, los pisos de rendimiento de la carga de trabajo 1 y la carga de trabajo 3 garantizan que cumplen los objetivos de rendimiento mínimos, sin importar la demanda por carga de trabajo 2.

> Tal y como sugieren los ejemplos, un límite máximo de rendimiento limita el rendimiento directamente. Un entorno de rendimiento limita el rendimiento de forma indirecta, al dar prioridad a las cargas de trabajo para las que se ha establecido un piso.

Puede especificar la planta al crear el grupo de políticas, o bien esperar hasta que supervise las cargas de trabajo para especificarlas.

A partir de ONTAP 9.13.1, se pueden establecer pisos de rendimiento en el ámbito de SVM con [adaptive-qos-templates]. En versiones de ONTAP anteriores a 9.13.1, no puede aplicarse a una SVM un grupo de políticas que define un piso de rendimiento.

> En las versiones anteriores a ONTAP 9.7, se garantizan pisos de rendimiento cuando hay suficiente capacidad de rendimiento disponible.
>
> En ONTAP 9.7 y versiones posteriores, se puede garantizar el uso de suelos de rendimiento incluso cuando la capacidad de rendimiento no sea suficiente. Este nuevo comportamiento del suelo se llama pisos v2. Para cumplir las garantías, el segundo plano puede generar una mayor latencia en las cargas de trabajo sin tener que pasar por una planta de rendimiento o en el trabajo que supere la configuración inicial. Floors v2 se aplica tanto a QoS como a QoS adaptativo.
>
> La opción de habilitar/deshabilitar el nuevo comportamiento de los pisos v2 está disponible en ONTAP 9.7P6 y posteriores. Una carga de trabajo puede quedar por debajo del piso especificado durante operaciones cruciales como `volume move trigger-cutover`. Incluso cuando haya suficiente capacidad disponible y no se realicen operaciones críticas, el rendimiento de una carga de trabajo puede quedar por debajo del nivel especificado hasta un 5 %. Si se sobreaprovisiona la tasa de suelos y no hay capacidad de rendimiento, es posible que algunas cargas de trabajo se encuentren por debajo de la superficie especificada.



Acerca de los grupos de políticas de calidad de servicio compartidos y no compartidos

A partir de ONTAP 9.4, puede usar un grupo de políticas *no compartido* QoS para especificar que el techo o el piso de rendimiento definidos se apliquen a la carga de trabajo de cada miembro de manera individual. El comportamiento de los grupos de directivas *shared* depende del tipo de directiva:

- Para los techos de rendimiento, el rendimiento total de las cargas de trabajo asignadas al grupo de políticas compartidas no puede exceder el techo especificado.
- En los pisos de rendimiento, el grupo de políticas compartidas puede aplicarse únicamente a una única carga de trabajo.

Acerca de la calidad de servicio adaptativa

Por lo general, el valor del grupo de políticas que asigna a un objeto de almacenamiento es fijo. Es necesario cambiar el valor de forma manual cuando cambia el tamaño del objeto de almacenamiento. Por ejemplo, un aumento de la cantidad de espacio utilizado en un volumen requiere, por lo general, un aumento correspondiente en el techo de rendimiento especificado para el volumen.

Adaptive QoS escala automáticamente el valor del grupo de políticas al tamaño de la carga de trabajo, y mantiene la ratio de IOPS en TB|GB a medida que cambia el tamaño de la carga de trabajo. Esto es una ventaja importante si gestiona cientos o miles de cargas de trabajo en una puesta en marcha grande.

Normalmente, la calidad de servicio adaptativa se puede utilizar para ajustar los techos de rendimiento, pero también para gestionar el uso de pisos de rendimiento (cuando aumenta el tamaño de la carga de trabajo). El tamaño de la carga de trabajo se expresa como el espacio asignado para el objeto de almacenamiento o el espacio utilizado por el objeto de almacenamiento.

> El espacio usado está disponible para pisos de rendimiento en ONTAP 9.5 y versiones posteriores. No se admite para pisos de rendimiento en ONTAP 9.4 y versiones anteriores.

- Una política de *espacio* mantiene la ratio de IOPS/TB|GB según el tamaño nominal del objeto de almacenamiento. Si la relación es de 100 IOPS/GB, un volumen de 150 GB tendrá un techo de rendimiento de 15,000 IOPS mientras el volumen siga siendo de ese tamaño. Si el tamaño del volumen cambia a 300 GB, la calidad de servicio adaptativa ajusta el techo de rendimiento a 30,000 IOPS.
- Una política de *space* utilizada (predeterminada) mantiene la relación IOPS/TB|GB según la cantidad de datos reales almacenados antes de las eficiencias de almacenamiento. Si la relación es de 100 IOPS/GB, un volumen de 150 GB que tiene 100 GB de datos almacenados tendría un límite máximo de rendimiento de 10,000 IOPS. A medida que cambia la cantidad de espacio usado, la calidad de servicio adaptativa

ajusta el techo de rendimiento en función de la ratio.

A partir de ONTAP 9.5, es posible especificar un tamaño de bloque de I/o para su aplicación que permite expresar un límite de rendimiento tanto en IOPS como en Mbps. El límite de Mbps se calcula a partir del tamaño de bloque multiplicado por el límite de IOPS. Por ejemplo, un tamaño de bloque de I/o de 32 KB para un límite de IOPS de 6144 IOPS/TB proporciona un límite de Mbps de 192 MBps.

Puede esperar el siguiente comportamiento tanto para techos de rendimiento como para pisos:

- Cuando una carga de trabajo se asigna a un grupo de políticas de calidad de servicio adaptativa, el techo o el piso se actualizan de inmediato.
- Cuando se cambia el tamaño de una carga de trabajo de un grupo de políticas de calidad de servicio adaptativa, el techo o el piso se actualizan en aproximadamente cinco minutos.

El rendimiento debe aumentar al menos en 10 000 IOPS antes de que se produzca la actualización.

Los grupos de políticas de calidad de servicio adaptativos siempre no son compartidos: El techo o el piso de rendimiento definidos se aplican a la carga de trabajo de cada miembro de forma individual.

A partir de ONTAP 9,6, los pisos de rendimiento son compatibles con ONTAP Select Premium con SSD.

Plantilla de grupo de políticas adaptativas

A partir de ONTAP 9.13.1, puede establecer una plantilla de calidad de servicio adaptativa en una SVM. Las plantillas de grupos de políticas adaptativas permiten establecer pisos y techos de rendimiento para todos los volúmenes de una SVM.

Las plantillas de grupos de políticas adaptativas solo pueden establecerse después de crear la SVM. Utilice la `vserver modify` con el `-qos-adaptive-policy-group-template` parámetro para establecer la política.

Cuando establece una plantilla de grupo de políticas adaptativas, los volúmenes creados o migrados después de configurar la política heredan automáticamente la política. Los volúmenes que existan en la SVM no se ven afectados al asignar la plantilla de políticas. Si deshabilita la política en la SVM, todos los volúmenes posteriores migrados o creados en la SVM no recibirán la política. La desactivación de la plantilla de grupo de políticas adaptativas no afecta a los volúmenes que han heredado la plantilla de políticas, ya que conservan la plantilla de políticas.

Para obtener más información, consulte Defina una plantilla de grupo de políticas adaptativas.

Apoyo general

En la siguiente tabla se muestran las diferencias en compatibilidad con los techos de rendimiento, pisos de rendimiento y calidad de servicio adaptativa.

Recurso o característica	Techo de rendimiento	Piso de rendimiento	Piso de salida v2	Calidad de servicio adaptativa
Versión de ONTAP 9	Todo	9,2 y posterior	9,7 y posterior	9,3 y posterior

Recurso o característica	Techo de rendimiento	Piso de rendimiento	Piso de salida v2	Calidad de servicio adaptativa
Plataformas	Todo	• AFF • C190 * • ONTAP Select premium con SSD *	• AFF • C190 • ONTAP Select premium con SSD	Todo
Protocolos	Todo	Todo	Todo	Todo
FabricPool	Sí	Sí, si la política de organización en niveles está establecida en "ninguna" y no hay bloques en el cloud.	Sí, si la política de organización en niveles está establecida en "ninguna" y no hay bloques en el cloud.	No
SnapMirror síncrono	Sí	No	No	Sí

La compatibilidad con C190 y ONTAP Select comenzó con la versión 9,6 de ONTAP.

Cargas de trabajo compatibles con techos de rendimiento

En la siguiente tabla se muestra compatibilidad con cargas de trabajo para techos de rendimiento con la versión ONTAP 9. No se admiten los volúmenes raíz, los reflejos con uso compartido de carga y los reflejos de protección de datos.

Soporte de carga de trabajo: Techo	ONTAP 9,0	ONTAP 9,1	ONTAP 9,2	ONTAP 9,3	ONTAP 9,4 - 9,7	ONTAP 9,8 y versiones posteriores
Volumen	sí	sí	sí	sí	sí	sí
Archivo	sí	sí	sí	sí	sí	sí
LUN	sí	sí	sí	sí	sí	sí
SVM	sí	sí	sí	sí	sí	sí
Volumen FlexGroup	no	no	no	sí	sí	sí
qtrees*	no	no	no	no	no	sí

Soporte de carga de trabajo: Techo	ONTAP 9,0	ONTAP 9,1	ONTAP 9,2	ONTAP 9,3	ONTAP 9,4 - 9,7	ONTAP 9,8 y versiones posteriores
Varias cargas de trabajo por grupo de políticas	sí	sí	sí	sí	sí	sí
Grupos de políticas no compartidos	no	no	no	no	sí	sí

A partir de ONTAP 9,8, el acceso NFS es compatible con qtrees en volúmenes FlexVol y FlexGroup con NFS habilitado. A partir de ONTAP 9.9.1, también se admite el acceso SMB en qtrees de volúmenes FlexVol y FlexGroup con SMB habilitado.

Cargas de trabajo admitidas para el nivel de rendimiento

En la siguiente tabla se muestra la compatibilidad con cargas de trabajo para pisos de rendimiento en la versión de ONTAP 9. No se admiten los volúmenes raíz, los reflejos con uso compartido de carga y los reflejos de protección de datos.

Soporte de cargas de trabajo: Suelo	ONTAP 9,2	ONTAP 9,3	ONTAP 9,4 - 9,7	ONTAP 9,8 - 9.13.0	ONTAP 9.13.1 y versiones posteriores
Volumen	sí	sí	sí	sí	sí
Archivo	no	sí	sí	sí	sí
LUN	sí	sí	sí	sí	sí
SVM	no	no	no	no	sí
Volumen FlexGroup	no	no	sí	sí	sí
qtrees *	no	no	no	sí	sí
Varias cargas de trabajo por grupo de políticas	no	no	sí	sí	sí
Grupos de políticas no compartidos	no	no	sí	sí	sí

*A partir de ONTAP 9,8, el acceso NFS es compatible con qtrees en volúmenes FlexVol y FlexGroup con NFS habilitado. A partir de ONTAP 9.9.1, también se admite el acceso SMB en qtrees de volúmenes FlexVol y FlexGroup con SMB habilitado.

Cargas de trabajo compatibles para calidad de servicio adaptable

En la siguiente tabla se muestra la compatibilidad con las cargas de trabajo para la calidad de servicio adaptativa según la versión de ONTAP 9. No se admiten los volúmenes raíz, los reflejos con uso compartido de carga y los reflejos de protección de datos.

Compatibilidad con cargas de trabajo: Calidad de servicio adaptable	ONTAP 9,3	ONTAP 9,4 - 9.13.0	ONTAP 9.13.1 y versiones posteriores
Volumen	sí	sí	sí
Archivo	no	sí	sí
LUN	no	sí	sí
SVM	no	no	sí
Volumen FlexGroup	no	sí	sí
Varias cargas de trabajo por grupo de políticas	sí	sí	sí
Grupos de políticas no compartidos	sí	sí	sí

El número máximo de cargas de trabajo y grupos de políticas

En la siguiente tabla se muestra el número máximo de cargas de trabajo y grupos de políticas en la versión de ONTAP 9.

Compatibilidad con cargas de trabajo	ONTAP 9,3 y anteriores	ONTAP 9,4 y versiones posteriores
Cargas de trabajo máximas por clúster	12.000	40.000
Número máximo de cargas de trabajo por nodo	12.000	40.000
Número máximo de grupos de políticas	12.000	12.000

Habilite o deshabilite pisos de salida v2

Puede habilitar o deshabilitar las plantas de procesamiento v2 en AFF. El valor predeterminado es Enabled. Con el suelo v2 habilitado, se pueden cumplir los pisos de rendimiento cuando se utilizan en gran medida las controladoras a expensas de una mayor latencia en otras cargas de trabajo. Floors v2 se aplica tanto a QoS como a Adaptive QoS.

Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Escriba uno de los siguientes comandos:

Si desea…	Utilizar este comando:
Desactivar pisos v2	`qos settings throughput-floors-v2 -enable false`
Habilitar pisos v2	`qos settings throughput-floors-v2 -enable true`

> Para deshabilitar los pisos de procesamiento v2 en un clúster de MetroCluster, debe ejecutar la
>
> `qos settings throughput-floors-v2 -enable false`
>
> comando en los clústeres de origen y destino.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

Flujo de trabajo de calidad de servicio del almacenamiento

Si ya conoce los requisitos de rendimiento de las cargas de trabajo que desea gestionar con calidad de servicio, puede especificar el límite de rendimiento al crear el grupo de políticas. De lo contrario, puede esperar hasta que supervise las cargas de trabajo para especificar el límite.

Establezca el límite máximo de rendimiento con calidad de servicio

Puede utilizar el `max-throughput` Campo para un grupo de políticas a fin de definir un techo de rendimiento para las cargas de trabajo de objetos de almacenamiento (QoS máx.). Puede aplicar el grupo de políticas cuando crea o modifica el objeto de almacenamiento.

Lo que necesitará

- Para crear un grupo de políticas, debe ser un administrador de clústeres.
- Para aplicar un grupo de políticas a una SVM, debe ser un administrador de clústeres.

Acerca de esta tarea

- A partir de ONTAP 9.4, puede usar un grupo de políticas *no compartido* QoS para especificar que el techo de rendimiento definido se aplique a la carga de trabajo de cada miembro de forma individual. De lo contrario, el grupo de políticas es *shared:* el rendimiento total de las cargas de trabajo asignadas al grupo de políticas no puede superar el límite máximo especificado.

  Configurado `-is-shared=false` para la `qos policy-group create` comando para especificar un

grupo de políticas no compartido.

- Puede especificar el límite de rendimiento para el límite máximo en IOPS, MB/s o IOPS, MB/s. Si especifica tanto IOPS como MB/s, se aplicará el límite alcanzado primero.

> Si establece un techo y un piso para la misma carga de trabajo, puede especificar el límite de rendimiento para el techo solo en IOPS.

- Un objeto de almacenamiento sujeto a un límite de calidad de servicio debe ser contenido por la SVM a la que pertenece el grupo de políticas. Pueden pertenecer varios grupos de políticas a la misma SVM.
- No puede asignar un objeto de almacenamiento a un grupo de políticas si su objeto que contiene o sus objetos secundarios pertenecen al grupo de políticas.
- Es una práctica recomendada de la calidad de servicio aplicar un grupo de políticas al mismo tipo de objetos de almacenamiento.

Pasos

1. Cree un grupo de políticas:

   `qos policy-group create -policy-group` *`policy_group`* `-vserver` *`SVM`* `-max -throughput` *`number_of_iops`*`|Mb/S|iops,Mb/S -is-shared true|false`

   Para obtener una sintaxis de comando completa, consulte la página man. Puede utilizar el `qos policy-group modify` comando para ajustar los techos de rendimiento.

   El siguiente comando crea el grupo de políticas compartidas `pg-vs1` Con un rendimiento máximo de 5,000 IOPS:

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   El siguiente comando crea el grupo de políticas no compartido `pg-vs3` Con un rendimiento máximo de 100 000 IOPS y 400 Kb/s:

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   El siguiente comando crea el grupo de políticas no compartido `pg-vs4` sin límite de rendimiento:

   ```
   cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
   -is-shared false
   ```

2. Aplique un grupo de políticas a una SVM, un archivo, un volumen o una LUN:

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   Para obtener una sintaxis de comando completa, consulte las páginas man. Puede utilizar el *`storage_object`* `modify` comando para aplicar un grupo de políticas diferente al objeto de

almacenamiento.

El siguiente comando aplica un grupo de políticas `pg-vs1` A SVM `vs1`:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

Los siguientes comandos aplican grupo de políticas `pg-app` a los volúmenes `app1` y.. `app2`:

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

3. Supervise el rendimiento del grupo de políticas:

   `qos statistics performance show`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Supervise el rendimiento desde el clúster. No utilice una herramienta en el host para supervisar el rendimiento.

   El siguiente comando muestra el rendimiento del grupo de políticas:

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. Supervisar el rendimiento de la carga de trabajo:

   `qos statistics workload performance show`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Supervise el rendimiento desde el clúster. No utilice una herramienta en el host para supervisar el rendimiento.

   El siguiente comando muestra el rendimiento de la carga de trabajo:

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app1-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

Puede utilizar el `qos statistics workload latency show` Comando para ver estadísticas detalladas de latencia de las cargas de trabajo de calidad de servicio.

Fije un piso de rendimiento con calidad de servicio

Puede utilizar el `min-throughput` Campo para un grupo de políticas a fin de definir un piso de rendimiento para las cargas de trabajo de objetos de almacenamiento (QoS mín.). Puede aplicar el grupo de políticas cuando crea o modifica el objeto de almacenamiento. A partir de ONTAP 9.8, puede especificar el nivel mínimo de rendimiento en IOPS o Mbps, o IOPS y Mbps.

Antes de empezar

- Debe ejecutar ONTAP 9,2 o una versión posterior. Los pisos de alto rendimiento están disponibles a partir de ONTAP 9.2.
- Para crear un grupo de políticas, debe ser un administrador de clústeres.
- A partir de ONTAP 9.13.1, puede aplicar pisos de rendimiento a nivel de la SVM mediante un plantilla de grupo de políticas adaptativas. No puede establecer una plantilla de grupo de políticas adaptativas en una SVM con un grupo de políticas de calidad de servicio.

Acerca de esta tarea

- A partir de ONTAP 9.4, puede usar un grupo de políticas *no compartido* QoS para especificar que la planta de rendimiento definida se aplique a cada carga de trabajo miembro de forma individual. Esta es la única condición en la que un grupo de políticas para una planta de rendimiento se puede aplicar a varias cargas de trabajo.

  Configurado `-is-shared=false` para la `qos policy-group create` comando para especificar un grupo de políticas no compartido.

- El rendimiento de una carga de trabajo puede caer por debajo de la superficie especificada si no hay suficiente capacidad de rendimiento (margen adicional) en el nodo o el agregado.
- Un objeto de almacenamiento sujeto a un límite de calidad de servicio debe ser contenido por la SVM a la que pertenece el grupo de políticas. Pueden pertenecer varios grupos de políticas a la misma SVM.
- Es una práctica recomendada de la calidad de servicio aplicar un grupo de políticas al mismo tipo de objetos de almacenamiento.
- Un grupo de políticas que define un piso de rendimiento no se puede aplicar a una SVM.

Pasos

1. Compruebe que la capacidad de rendimiento sea adecuada en el nodo o el agregado, como se describe en "Identificar la capacidad de rendimiento restante".
2. Cree un grupo de políticas:

   `qos policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-min -throughput` *`qos_target`* `-is-shared true|false`

   Para obtener una sintaxis de comando completa, consulte la página man de la versión ONTAP. Puede utilizar el `qos policy-group modify` comando para ajustar los pisos de rendimiento.

   El siguiente comando crea el grupo de políticas compartidas `pg-vs2` Con un rendimiento mínimo de 1,000 IOPS:

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   El siguiente comando crea el grupo de políticas no compartido `pg-vs4` sin límite de rendimiento:

   ```
   cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
   -is-shared false
   ```

3. Aplique un grupo de políticas a un volumen o una LUN:

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   Para obtener una sintaxis de comando completa, consulte las páginas man. Puede utilizar el `_storage_object_modify` comando para aplicar un grupo de políticas diferente al objeto de almacenamiento.

   El siguiente comando aplica un grupo de políticas `pg-app2` al volumen `app2`:

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
   -qos-policy-group pg-app2
   ```

4. Supervise el rendimiento del grupo de políticas:

   `qos statistics performance show`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Supervise el rendimiento desde el clúster. No utilice una herramienta en el host para supervisar el rendimiento.

   El siguiente comando muestra el rendimiento del grupo de políticas:

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

5. Supervisar el rendimiento de la carga de trabajo:

   `qos statistics workload performance show`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Supervise el rendimiento desde el clúster. No utilice una herramienta en el host para supervisar el rendimiento.

   El siguiente comando muestra el rendimiento de la carga de trabajo:

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

   > Puede utilizar el `qos statistics workload latency show` Comando para ver estadísticas detalladas de latencia de las cargas de trabajo de calidad de servicio.

Utilice grupos de políticas de calidad de servicio adaptativos

Puede usar un grupo de políticas *Adaptive QoS* para escalar automáticamente un techo o un tamaño de piso a volumen y mantener la ratio de IOPS en TB|GB a medida que cambie el tamaño del volumen. Esto es una ventaja importante si gestiona cientos o miles de cargas de trabajo en una puesta en marcha grande.

Antes de empezar

- Debe ejecutar ONTAP 9,3 o una versión posterior. Los grupos de políticas de calidad de servicio adaptativa están disponibles a partir de ONTAP 9.3.
- Para crear un grupo de políticas, debe ser un administrador de clústeres.

Acerca de esta tarea

Un objeto de almacenamiento puede ser miembro de un grupo de políticas adaptables o de un grupo de

políticas no adaptativas, pero no ambos. La SVM del objeto de almacenamiento y la política deben ser iguales. El objeto de almacenamiento debe estar en línea.

Los grupos de políticas de calidad de servicio adaptativos siempre no son compartidos: El techo o el piso de rendimiento definidos se aplican a la carga de trabajo de cada miembro de forma individual.

La relación de límites de rendimiento con el tamaño de objeto de almacenamiento se determina por la interacción de los siguientes campos:

- `expected-iops` Es el mínimo esperado de IOPS por TB|GB asignado.

> `expected-iops` Sólo se garantiza en plataformas AFF. `expected-iops` FabricPool solo tiene garantía si la política de organización en niveles está establecida en "none" y no hay bloques en el cloud. `expected-iops` Está garantizado para volúmenes que no estén en una relación de SnapMirror síncrono.

- `peak-iops` Es la cantidad máxima de IOPS posible por TB|GB asignado o usada.
- `expected-iops-allocation` especifica si el espacio asignado (predeterminado) o el espacio utilizado se usa para el iops esperado.

> `expected-iops-allocation` Está disponible en ONTAP 9.5 y versiones posteriores. No es compatible con ONTAP 9.4 y versiones anteriores.

- `peak-iops-allocation` especifica si se utiliza el espacio asignado o el espacio utilizado (el valor predeterminado) para `peak-iops`.
- `absolute-min-iops` Es el número mínimo absoluto de IOPS. Puede utilizar este campo con objetos de almacenamiento muy pequeños. Anula ambos `peak-iops` y/o. `expected-iops` cuando `absolute-min-iops` es mayor que el calculado `expected-iops`.

  Por ejemplo, si ha establecido `expected-iops` Para 1,000 IOPS/TB, y el tamaño del volumen es inferior a 1 GB, calculado `expected-iops` Será un IOP fraccionario. El calculado `peak-iops` será una fracción aún menor. Puede evitar esto mediante la configuración `absolute-min-iops` a un valor realista.

- `block-size` Especifica el tamaño de bloque de I/o de la aplicación. El valor predeterminado es 32K. Los valores válidos son 8K, 16K, 32K, 64K, CUALQUIERA. CUALQUIER significa que no se aplica el tamaño de los bloques.

Existen tres grupos de políticas de calidad de servicio adaptativas predeterminados disponibles, como se muestra en la siguiente tabla. Puede aplicar estos grupos de políticas directamente a un volumen.

Grupo de políticas predeterminado	Tasa prevista de IOPS/TB	Pico de IOPS/TB	IOPS mín. Absoluto
`extreme`	6.144	12.288	1000

`performance`	2.048	4.096	500
`value`	128	512	75

No puede asignar un objeto de almacenamiento a un grupo de políticas si su objeto que contiene o sus objetos secundarios pertenecen a un grupo de políticas. En la siguiente tabla se enumeran las restricciones.

Si asigna…	**No puede asignar…**
SVM a un grupo de políticas	Todos los objetos de almacenamiento que contiene la SVM a un grupo de políticas
Del volumen a un grupo de políticas	El volumen que contiene la SVM o cualquier LUN secundario a un grupo de políticas
LUN a un grupo de políticas	El volumen o la SVM que contiene el LUN a un grupo de políticas
Archivo a un grupo de políticas	El volumen o la SVM del archivo a un grupo de políticas

Pasos

1. Cree un grupo de políticas de calidad de servicio adaptativo:

   `qos adaptive-policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-expected-iops` *`number_of_iops`*`/TB|GB -peak-iops` *`number_of_iops`*`/TB|GB -expected -iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-space -absolute-min-iops` *`number_of_iops`* `-block-size 8K|16K|32K|64K|ANY`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > `-expected-iops-allocation` y.. `-block-size` Está disponible en ONTAP 9.5 y versiones posteriores. Estas opciones no son compatibles con ONTAP 9.4 y versiones anteriores.

   El siguiente comando crea un grupo de políticas de calidad de servicio adaptativo `adpg-app1` con `-expected-iops` Establecido en 300 IOPS/TB, `-peak-iops` Establecido en 1,000 IOPS/TB, `-peak -iops-allocation` establezca en `used-space`, y. `-absolute-min-iops` Establecido en 50 IOPS:

   ```
   cluster1::> qos adaptive-policy-group create -policy group adpg-app1
   -vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
   -allocation used-space -absolute-min-iops 50iops
   ```

2. Aplique un grupo de políticas de calidad de servicio adaptable a un volumen:

   `volume create -vserver SVM -volume` *`volume`* `-aggregate` *`aggregate`* `-size` *`number_of`* `TB|GB -qos-adaptive-policy-group` *`policy_group`*

Para obtener una sintaxis de comando completa, consulte las páginas man.

El siguiente comando aplica el grupo de políticas de calidad de servicio adaptativa `adpg-app1` al volumen `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

Los siguientes comandos aplican el grupo de políticas de calidad de servicio adaptativo predeterminado `extreme` al nuevo volumen `app4` y al volumen existente `app5`. El techo de rendimiento definido para el grupo de políticas se aplica a los volúmenes `app4` y.. `app5` individualmente:

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

Defina una plantilla de grupo de políticas adaptativas

A partir de ONTAP 9.13.1, puede aplicar pisos y techos de rendimiento en el nivel de SVM mediante una plantilla de grupo de políticas adaptativas.

Acerca de esta tarea

- La plantilla de grupo de políticas adaptativas es una política predeterminada `apg1`. La política se puede modificar en cualquier momento. Solo se puede establecer con la interfaz de línea de comandos o la API DE REST DE ONTAP y solo se puede aplicar a las SVM existentes.
- La plantilla de grupo de políticas adaptativas solo afecta a los volúmenes creados en la SVM o migrados a ella después de establecer la política. Los volúmenes existentes en la SVM conservan su estado existente.

  Si deshabilita la plantilla de grupo de políticas adaptativas, los volúmenes de la SVM conservarán las políticas existentes. Solo los volúmenes que se creen posteriormente en la SVM o se migren a ella se verán afectados por la desactivación.

- No puede establecer una plantilla de grupo de políticas adaptativas en una SVM con un grupo de políticas de calidad de servicio.
- Las plantillas de grupos de políticas adaptativas están diseñadas para las plataformas AFF. Se puede definir una plantilla de grupo de políticas adaptativas en otras plataformas, pero es posible que la política no aplique un rendimiento mínimo. Del mismo modo, puede añadir una plantilla de grupo de políticas adaptable a una SVM en un agregado de FabricPool o en un agregado que no admita un rendimiento mínimo, pero el nivel de rendimiento no se aplicará.
- Si la SVM está en una configuración de MetroCluster o una relación de SnapMirror, la plantilla de grupo de políticas adaptativas se aplicará en la SVM reflejada.

Pasos

1. Modifique la SVM para aplicar la plantilla de grupo de políticas adaptativas:
   `vserver modify -qos-adaptive-policy-group-template apg1`
2. Confirme que se ha establecido la política:
   `vserver show -fields qos-adaptive-policy-group`

Supervise el rendimiento del clúster con Unified Manager

Con Active IQ Unified Manager, puede maximizar la disponibilidad y mantener el control de su infraestructura de almacenamiento AFF y FAS de NetApp para disfrutar de una mayor escalabilidad, compatibilidad, rendimiento y seguridad.

Active IQ Unified Manager supervisa de forma continua el estado del sistema y envía alertas, para que su organización pueda liberar recursos del personal DE TECNOLOGÍA. Puede ver al instante el estado de su almacenamiento desde un único panel y abordar rápidamente problemas mediante acciones recomendadas.

La gestión de datos se simplifica porque puede detectar, supervisar y recibir notificaciones para gestionar el almacenamiento de forma proactiva y resolver los problemas con rapidez. La eficiencia de administración ha mejorado porque puede supervisar petabytes de datos desde una única consola y gestionar sus datos a escala.

Con Active IQ Unified Manager, puede mantener el ritmo de las fluctuaciones en las demandas del negocio y optimizar el rendimiento mediante datos del rendimiento y análisis avanzados. Las funciones de generación de informes permiten acceder a informes estándar o crear informes operativos personalizados que satisfagan las necesidades específicas de su empresa.

Enlaces relacionados:

- "Obtenga más información acerca de Active IQ Unified Manager"
- "Comienza a usar Active IQ Unified Manager para VMware"
- "Comience con Active IQ Unified Manager para Linus"
- "Comience a usar Active IQ Unified Manager para Windows"

Supervise el rendimiento del clúster con Cloud Insights

Cloud Insights de NetApp es una herramienta de supervisión que le ofrece visibilidad de toda su infraestructura. Con Cloud Insights, puede supervisar, solucionar problemas y optimizar todos los recursos, incluidos los clouds públicos y los centros de datos privados.

Cloud Insights se presenta en dos ediciones

La edición básica de Cloud Insights está diseñada específicamente para supervisar y optimizar sus activos de Data Fabric de NetApp. Proporciona análisis avanzados para las conexiones entre todos los recursos de NetApp, incluidos HCI y All Flash FAS (AFF) en el entorno de forma gratuita.

Cloud Insights Standard Edition no solo se centra en componentes de infraestructura habilitados para Data Fabric de NetApp, sino también en entornos de varios proveedores y clouds. Con sus capacidades enriquecidas, usted puede acceder al apoyo para más de 100 servicios y recursos.

En el mundo actual, donde los recursos están en juego desde los centros de datos locales hasta varios clouds públicos, es fundamental tener una imagen completa desde la propia aplicación hasta el disco de back-end de la cabina de almacenamiento. El soporte adicional para la supervisión de aplicaciones (como Kafka, MongoDB y Nginx) le proporciona la información y el conocimiento que necesita para operar al nivel óptimo de utilización, así como con el búfer de riesgo perfecto.

Ambas ediciones (Basic y Standard) pueden integrarse con Active IQ Unified Manager de NetApp. Los clientes que usan Active IQ Unified Manager pueden ver la información de unión dentro de la interfaz de usuario de Cloud Insights. Las notificaciones publicadas en Active IQ Unified Manager no se pasan por alto y pueden correlacionarse con eventos en Cloud Insights. En otras palabras, obtienes lo mejor de ambos mundos.

Supervisión, solución de problemas y optimización de todos los recursos

Cloud Insights le ayuda a reducir significativamente el tiempo necesario para resolver problemas y evitar que afecten a los usuarios finales. También le ayuda a reducir los costes de infraestructura del cloud. Su exposición a las amenazas internas se reduce al proteger sus datos con una inteligencia práctica.

Cloud Insights le ofrece visibilidad de toda su infraestructura híbrida en un mismo lugar, desde el cloud público hasta su centro de datos. Puede crear instantáneamente paneles relevantes que se puedan personalizar según sus necesidades específicas. También puedes crear alertas específicas y condicionales que sean específicas y relevantes para las necesidades de tu organización.

La detección avanzada de anomalías le ayuda a corregir problemas de forma proactiva antes de que surjan. Puede ver automáticamente la contención y degradación de los recursos para restaurar rápidamente las cargas de trabajo afectadas. La solución de problemas va más rápido con la jerarquía automatizada de relaciones entre los distintos componentes de la pila.

Puede identificar los recursos no utilizados o abandonados en todo su entorno, lo que le ayudará a descubrir oportunidades para dimensionar adecuadamente la infraestructura y optimizar el gasto completo.

Cloud Insights visualiza la topología de su sistema para entender su arquitectura de Kubernetes. Puede supervisar el estado de los clústeres de Kubernetes, incluidos qué nodos tienen problemas y ampliar cuando observe un problema.

Cloud Insights le ayuda a proteger los datos de la organización frente a un uso inadecuado por parte de usuarios malintencionados o en riesgo mediante el aprendizaje automático avanzado y la detección de anomalías que le proporciona inteligencia procesable sobre amenazas internas.

Cloud Insights le ayuda a visualizar métricas de Kubernetes para que pueda comprender por completo las relaciones entre los pods, los nodos y los clústeres. Podrá evaluar el estado de un clúster o un módulo de trabajo, así como la carga que está procesando actualmente, lo que le permite tomar el control del clúster K8S y controlar tanto el estado como el coste de la implementación.

Enlaces relacionados

- "Obtenga más información acerca de Cloud Insights"
- "Comience a usar Cloud Insights"

Registro de auditoría

Cómo implementa ONTAP el registro de auditoría

Las actividades de gestión registradas en el registro de auditoría se incluyen en los

informes estándar de AutoSupport y determinadas actividades de registro se incluyen en los mensajes de EMS. También puede reenviar el registro de auditoría a los destinos que especifique y mostrar los archivos de registro de auditoría mediante la CLI o un explorador web.

A partir de ONTAP 9.11.1, es posible mostrar contenido del registro de auditoría mediante System Manager.

A partir de ONTAP 9.12.1, ONTAP proporciona alertas de manipulación para los registros de auditoría. ONTAP ejecuta un trabajo diario en segundo plano para comprobar si hay manipulación de archivos audit.log y envía una alerta de EMS si encuentra algún archivo de registro que se haya modificado o alterado.

ONTAP registra las actividades de gestión que se realizan en el clúster; por ejemplo, qué solicitud se emitió, el usuario que activó la solicitud, el método de acceso del usuario y la hora de la solicitud.

Las actividades de gestión pueden ser uno de los siguientes tipos:

- SET Requests, que suelen aplicarse a comandos o operaciones que no son de visualización
  - Estas solicitudes se emiten cuando se ejecuta un `create`, `modify`, o. `delete` por ejemplo.
  - Las solicitudes SET se registran de forma predeterminada.
- OBTENGA solicitudes, que recuperan información y la muestran en la interfaz de gestión
  - Estas solicitudes se emiten cuando se ejecuta un `show` por ejemplo.
  - LAS solicitudes GET no se registran de forma predeterminada, pero puede controlar si GET Requests enviadas desde la CLI de ONTAP (`-cliget`), de la API de ONTAP (`-ontapiget`), o desde la API DE REST (`-httpget`) se registran en el archivo.

ONTAP actividades de gestión de registros en el `/mroot/etc/log/mlog/audit.log` archivo de un nodo. Los comandos de los tres shell para los comandos de la CLI -el clustershell, el nodeshell y el shell del sistema no interactivo (los comandos de shell del sistema interactivos no se registran)- así como los comandos de la API se registran aquí. Los registros de auditoría incluyen marcas de tiempo para mostrar si todos los nodos de un clúster están sincronizados con la hora.

La `audit.log` El archivo es enviado por la herramienta AutoSupport a los destinatarios especificados. También es posible reenviar el contenido de manera segura a destinos externos que especifique; por ejemplo, un servidor de Splunk o syslog.

La `audit.log` el archivo se gira diariamente. La rotación también ocurre cuando alcanza los 100 MB de tamaño y se conservan las 48 copias anteriores (con un máximo de 49 archivos). Cuando el archivo de auditoría realiza su rotación diaria, no se genera ningún mensaje EMS. Si el archivo de auditoría gira porque se supera el límite de tamaño de archivo, se genera un mensaje EMS.

Cambios en el registro de auditoría en ONTAP 9

A partir de ONTAP 9, el `command-history.log` el archivo se sustituye por `audit.log`, y la `mgwd.log` el archivo ya no contiene información de auditoría. Si actualiza a ONTAP 9, debe revisar cualquier script o herramienta que haga referencia a los archivos heredados y su contenido.

Después de actualizar a ONTAP 9, existente `command-history.log` los archivos se conservan. Se rotan (eliminan) como nuevas `audit.log` los archivos se giran en (crean).

Herramientas y scripts que comprueban `command-history.log` es posible que el archivo continúe funcionando, porque un vínculo de software de `command-history.log` para `audit.log` se crea al actualizar. Sin embargo, herramientas y scripts que comprueban `mgwd.log` el archivo fallará porque ese archivo ya no contiene información de auditoría.

Además, los registros de auditoría de ONTAP 9 y versiones posteriores ya no incluyen las siguientes entradas porque no se consideran útiles y provocan una actividad de registro innecesaria:

- Comandos internos ejecutados por ONTAP (es decir, donde username=root)
- Alias de comandos (por separado del comando al que apuntan)

A partir de ONTAP 9, puede transmitir los registros de auditoría de manera segura a destinos externos mediante los protocolos TCP y TLS.

Mostrar el contenido del registro de auditoría

Puede mostrar el contenido del clúster `/mroot/etc/log/mlog/audit.log` Archivos mediante la interfaz de línea de comandos de ONTAP, System Manager o un explorador web.

Las entradas del archivo de registro del clúster incluyen lo siguiente:

Tiempo

Marca de hora de entrada del registro.

Cliente más

La aplicación utilizada para conectarse al clúster. Ejemplos de valores posibles son `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, y.. `service-processor`.

Usuario

El nombre de usuario del usuario remoto.

Estado

El estado actual de la solicitud de auditoría, que podría ser `success`, `pending`, o. `error`.

Mensaje

Un campo opcional que puede contener errores o información adicional acerca del estado de un comando.

ID de sesión

El ID de sesión en el que se recibe la solicitud. A cada SSH *Session* se le asigna un ID de sesión, mientras que a cada HTTP, ONAPI o SNMP *Request* se le asigna un ID de sesión único.

Máquina virtual de almacenamiento

La SVM a través de la cual se conectó el usuario.

Ámbito

Pantallas `svm` Cuando la solicitud se encuentra en una máquina virtual de almacenamiento de datos; de lo contrario, se muestra `cluster`.

ID del comando

El ID de cada comando recibido en una sesión de CLI. Esto permite correlacionar una solicitud y una respuesta. LAS solicitudes ZAPI, HTTP y SNMP no tienen ID de comandos.

Puede mostrar las entradas del registro del clúster desde la interfaz de línea de comandos de ONTAP, desde un explorador web y a partir de ONTAP 9.11.1, desde System Manager.

System Manager

- Para visualizar el inventario, seleccione **Eventos y trabajos > registros de auditoría**.
  Cada columna tiene controles para filtrar, ordenar, buscar, mostrar y categorías de inventario. Los detalles del inventario se pueden descargar como un libro de Excel.
- Para establecer filtros, haga clic en el botón **Filtro** en la parte superior derecha y, a continuación, seleccione los campos deseados.
  También puede ver todos los comandos ejecutados en la sesión en la que se produjo un fallo haciendo clic en el enlace Identificador de Sesión.

CLI

Para mostrar las entradas de auditoría combinadas de varios nodos en el clúster, introduzca:
`security audit log show [parameters]`

Puede utilizar el `security audit log show` comando para mostrar las entradas de auditoría de nodos individuales o fusionadas desde varios nodos en el clúster. También puede mostrar el contenido de `/mroot/etc/log/mlog` directorio en un solo nodo mediante un navegador web.
Consulte la página man para obtener más información.

Navegador Web

Puede mostrar el contenido de `/mroot/etc/log/mlog` directorio en un solo nodo mediante un navegador web. "Obtenga información acerca de cómo acceder a los archivos log, de volcado principal y MIB de un nodo mediante un explorador web".

Gestione la configuración DE SOLICITUDES DE RECEPCIÓN de auditoría

Mientras QUE LAS solicitudes SET se registran de forma predeterminada, LAS solicitudes GET no lo son. Sin embargo, puede controlar si SE envían solicitudes desde HTML de ONTAP (`-httpget`), la CLI de ONTAP (`-cliget`), o desde las API de ONTAP (`-ontapiget`) se registran en el archivo.

Es posible modificar la configuración de registro de auditoría desde la interfaz de línea de comandos de ONTAP, y a partir de ONTAP 9.11.1, desde System Manager.

System Manager

1. Seleccione **Eventos y trabajos > registros de auditoría**.
2. Haga clic en ⚙ en la esquina superior derecha, elija las solicitudes que desea agregar o quitar.

CLI

- Para especificar que las solicitudes GET de la CLI o las API de ONTAP se deben registrar en el registro de auditoría (el archivo audit.log), además de las solicitudes predeterminadas, introduzca: `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Para mostrar los ajustes actuales, introduzca: `security audit show`

Consulte las páginas de manual para obtener más información.

Permite gestionar destinos de registro de auditoría

Es posible reenviar el registro de auditoría a un máximo de 10 destinos. Por ejemplo, es posible reenviar el registro a un servidor de Splunk o syslog para que realice tareas de supervisión, análisis o backup.

Acerca de esta tarea

Para configurar el reenvío, debe proporcionar la dirección IP del host de syslog o Splunk, su número de puerto, un protocolo de transmisión y la facilidad de syslog que se usarán para los registros reenviados. "Obtenga información sobre las instalaciones de syslog".

Puede seleccionar uno de los siguientes valores de transmisión:

UDP no cifrado

Protocolo de datagramas de usuario sin seguridad (predeterminado)

TCP sin cifrar

Protocolo de control de la transmisión sin seguridad

Cifrado TCP

Protocolo de control de transmisión con seguridad de la capa de transporte (TLS)
Una opción **Verificar servidor** está disponible cuando se selecciona el protocolo cifrado TCP.

Es posible reenviar registros de auditoría desde la interfaz de línea de comandos de ONTAP y a partir de ONTAP 9.11.1, desde System Manager.

System Manager

- Para visualizar los destinos de registro de auditoría, seleccione **clúster > Configuración**.
  Se muestra un recuento de destinos de registro en el mosaico **Gestión de notificaciones**. Haga clic en ⋮ para mostrar los detalles.
- Para agregar, modificar o eliminar destinos de registro de auditoría, seleccione **Eventos y trabajos > registros de auditoría** y, a continuación, haga clic en **Administrar destinos de auditoría** en la parte superior derecha de la pantalla.
  Haga clic en + Add o haga clic en ⋮ En la columna **Dirección de host** para editar o eliminar entradas.

CLI

1. Para cada destino al que se desea reenviar el registro de auditoría, especifique la dirección IP o el nombre de host de destino y todas las opciones de seguridad.

   ```
   cluster1::> cluster log-forwarding create -destination
   192.168.123.96
   -port 514 -facility user

   cluster1::> cluster log-forwarding create -destination
   192.168.123.98
   -port 514 -protocol tcp-encrypted -facility user
   ```

   - Si la `cluster log-forwarding create` el comando no puede hacer ping al host de destino para verificar la conectividad; se produce un error en el comando. Aunque no se recomienda, utilice la `-force` parámetro con el comando omite la verificación de conectividad.
   - Al ajustar la `-verify-server` parámetro a. `true`, la identidad del destino de reenvío de registros se verifica mediante la validación de su certificado. Puede establecer el valor en `true` sólo cuando seleccione la `tcp-encrypted` valor en la `-protocol` campo.
2. Compruebe que los registros de destino son correctos mediante el `cluster log-forwarding show` comando.

   ```
   cluster1::> cluster log-forwarding show

                                                   Verify Syslog
   Destination Host          Port   Protocol        Server Facility
   ------------------------- ------ --------        ------ --------
   192.168.123.96            514    udp-unencrypted false  user
   192.168.123.98            514    tcp-encrypted   true   user
   2 entries were displayed.
   ```

Consulte las páginas de manual para obtener más información.

AutoSupport

Gestione la configuración de AutoSupport con System Manager

Puede usar System Manager para gestionar la configuración de su cuenta de AutoSupport.

Puede realizar los siguientes procedimientos:

Ver la configuración de AutoSupport

Puede usar System Manager para ver la configuración de su cuenta de AutoSupport.

Pasos

1. En System Manager, haga clic en **clúster > Configuración**.

   En la sección **AutoSupport**, se muestra la siguiente información:

   - Estado
   - Protocolo de transporte
   - Servidor proxy
   - Dirección de correo electrónico del remitente
2. En la sección **AutoSupport**, selecciona ⋮, A continuación, seleccione **Más opciones**.

   Se muestra información adicional acerca de la configuración de la conexión AutoSupport y del correo electrónico. Además, se muestra el historial de transferencia de mensajes.

Generar y enviar datos de AutoSupport

En System Manager, puede iniciar la generación de mensajes de AutoSupport y elegir el nodo o los nodos del clúster que se recopilan los datos.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, selecciona ⋮, A continuación, seleccione **Generar y Enviar**.
3. Introduzca un asunto.
4. Seleccione la casilla de verificación en **Recopilar datos de** para especificar los nodos de los cuales recopilar los datos.

Pruebe la conexión a AutoSupport

En System Manager, es posible enviar un mensaje de prueba para verificar la conexión a AutoSupport.

Pasos

1. En System Manager, haga clic en **clúster > Configuración**.
2. En la sección **AutoSupport**, selecciona ⋮, A continuación, seleccione **Test Connectivity**.
3. Introduzca un asunto para el mensaje.

Habilite o deshabilite AutoSupport

AutoSupport ofrece ventajas empresariales demostradas a los clientes de NetApp, incluida la identificación proactiva de posibles problemas de configuración y la resolución acelerada de los casos de soporte. AutoSupport está activado de forma predeterminada en los sistemas nuevos. Si es necesario, puede usar System Manager para deshabilitar la capacidad de AutoSupport de supervisar el estado del sistema de almacenamiento y enviar mensajes de notificación. Es posible habilitar AutoSupport de nuevo después de que se haya deshabilitado.

Acerca de esta tarea

Antes de deshabilitar AutoSupport, tiene que tener en cuenta que está desactivando el sistema de llamada a casa de NetApp y perderá los siguientes beneficios:

- **Monitoreo de salud**: AutoSupport supervisa el estado de su sistema de almacenamiento y envía notificaciones al soporte técnico y a su organización de soporte interno.
- **Automatización**: AutoSupport automatiza la presentación de informes de casos de soporte. La mayoría de los casos de soporte se abren automáticamente antes de que los clientes se den cuenta de que hay un problema.
- **Resolución más rápida**: Los sistemas que envían datos AutoSupport tienen sus casos de soporte resueltos en la mitad del tiempo en comparación con los casos de los sistemas que no envían datos AutoSupport.
- * Actualizaciones más rápidas *: AutoSupport impulsa los flujos de trabajo de autoservicio de los clientes, como actualizaciones de versiones, complementos, renovaciones y automatización de actualizaciones de firmware en System Manager.
- **Más funciones**: Ciertas funciones de otras herramientas solo funcionan cuando AutoSupport está habilitado, por ejemplo, algunos flujos de trabajo en BlueXP.

Pasos

1. Seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, selecciona ⋮, A continuación, seleccione **Desactivar**.
3. Si desea volver a activar AutoSupport, en la sección **AutoSupport**, seleccione ⋮, A continuación, seleccione **Activar**.

Suprimir la generación de casos de soporte

A partir de ONTAP 9.10.1, se puede utilizar System Manager para enviar una solicitud a AutoSupport con el fin de suprimir la generación de casos de soporte.

Acerca de esta tarea

Para suprimir la generación de casos de soporte, especifique los nodos y el número de horas para las que desea que se produzca la supresión.

La supresión de casos de soporte puede ser especialmente útil si no desea que AutoSupport cree casos automatizados mientras realiza el mantenimiento en los sistemas.

Pasos

1. Seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, selecciona ⋮, A continuación, seleccione **Suprimir Soporte Case Generation**.
3. Introduzca el número de horas que desea que se produzca la supresión.

4. Seleccione los nodos para los que desea que se produzca la supresión.

Reanudar la generación de casos de soporte

A partir de ONTAP 9.10.1, es posible usar System Manager para reanudar la generación de casos de soporte desde AutoSupport si se ha suprimido.

Pasos

1. Seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, selecciona ⋮, A continuación, seleccione **Reanudar Support Case Generation**.
3. Seleccione los nodos para los que desea que se reanude la generación.

Editar configuración de AutoSupport

Puede usar System Manager para modificar la configuración de conexión y correo electrónico de la cuenta de AutoSupport.

Pasos

1. Seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, selecciona ⋮, A continuación, seleccione **Más opciones**.
3. En la sección **Conexiones** o en la sección **Correo electrónico**, selecciona Edit para modificar la configuración de cualquiera de las secciones.

Gestione AutoSupport con la interfaz de línea de comandos

Información general sobre Manage AutoSupport

AutoSupport es un mecanismo que supervisa de forma proactiva el estado del sistema y envía automáticamente mensajes al soporte técnico de NetApp, su organización de soporte interno y un partner de soporte. Aunque los mensajes de AutoSupport al soporte técnico se habilitan de forma predeterminada, debe establecer las opciones correctas y disponer de un host de correo válido para que se envíen mensajes a la organización de soporte interna.

Solo el administrador de clúster puede realizar la gestión de AutoSupport. El administrador de máquinas virtuales de almacenamiento (SVM) no tiene acceso a AutoSupport.

De forma predeterminada, AutoSupport se habilita al configurar el sistema de almacenamiento por primera vez. AutoSupport comienza a enviar mensajes al soporte técnico 24 horas después de habilitar AutoSupport. Se puede reducir el período de 24 horas mediante la actualización o la reversión del sistema, la modificación de la configuración de AutoSupport o el cambio de la hora del sistema para que sea algo distinto de un período de 24 horas.

> Es posible deshabilitar AutoSupport en cualquier momento, pero debe dejarla habilitada. Habilitar AutoSupport puede ayudar significativamente a acelerar la detección y resolución de problemas cuando se producen fallos en el sistema de almacenamiento. De forma predeterminada, el sistema recopila información de AutoSupport y la almacena localmente, incluso si deshabilita AutoSupport.

Para obtener más información sobre AutoSupport, consulte el sitio de soporte de NetApp.

Información relacionada

- "Soporte de NetApp"
- "Obtenga más información acerca de los comandos de la AutoSupport en la CLI de ONTAP"

Utilice el asesor digital AutoSupport y Active IQ

El componente AutoSupport de ONTAP recopila telemetría y la envía para su análisis. El asesor digital de Active IQ analiza los datos de AutoSupport y ofrece optimización y atención proactivas. Utilizando la inteligencia artificial, Active IQ puede identificar problemas potenciales y ayudarle a resolverlos antes de que afecten a su negocio.

Active IQ le permite optimizar su infraestructura de datos en el cloud híbrido global mediante la entrega de análisis predictivos aplicables y soporte proactivo a través de un portal basado en cloud y una aplicación para dispositivos móviles. En Active IQ, todos los clientes de NetApp con un contrato activo de SupportEdge disponen de información y recomendaciones basadas en los datos (las funciones varían según el producto y el nivel de soporte).

Estas son algunas cosas que puede hacer con Active IQ:

- Planificación de actualizaciones. Active IQ identifica los problemas en su entorno que se pueden resolver actualizando a una versión más reciente de ONTAP y el componente Upgrade Advisor le ayuda a planificar una actualización correcta.
- Ver el bienestar del sistema. Su consola de Active IQ informa de cualquier problema con el bienestar y le ayuda a corregir estos problemas. Supervise la capacidad del sistema para asegurarse de que nunca se queda sin espacio de almacenamiento. Vea los casos de soporte de su sistema.
- Gestión del rendimiento. Active IQ muestra el rendimiento del sistema durante un período más largo de lo que se puede ver en System Manager. Identifique problemas de configuración y del sistema que afectan a su rendimiento.
- Optimice la eficiencia. Consulte los criterios de medición de la eficiencia del almacenamiento e identifique formas de almacenar más datos en menos espacio.
- Ver el inventario y la configuración. Active IQ muestra información completa sobre la configuración de inventario y software y hardware. Vea cuándo caducan los contratos de servicio y renueve su soporte para asegurarse de que sigue siendo compatible.

Información relacionada

"Documentación de NetApp: Asesor digital de Active IQ"

"Inicie Active IQ"

"Servicios de SupportEdge"

Cuándo y dónde se envían los mensajes de AutoSupport

AutoSupport envía mensajes a diferentes destinatarios, en función del tipo de mensaje. Saber cuándo y dónde envía AutoSupport los mensajes puede ayudarle a comprender los mensajes que recibe por correo electrónico o visualizarlos en el sitio web de Active IQ (antes conocido como My AutoSupport).

A menos que se especifique lo contrario, la configuración de las tablas siguientes son parámetros de `system node autosupport modify` comando.

Mensajes activados por eventos

Cuando se producen eventos en el sistema que requieren una acción correctiva, AutoSupport envía automáticamente un mensaje activado por el evento.

Cuando se envía el mensaje	Dónde se envía el mensaje
AutoSupport responde a un evento desencadenante en EMS	Direcciones especificadas en `-to` y.. `-noteto`. (Solo se envían los eventos críticos que afectan al servicio). Direcciones especificadas en `-partner-address` El soporte técnico, si `-support` se establece en `enable`

Mensajes programados

AutoSupport envía automáticamente varios mensajes con una programación normal.

Cuando se envía el mensaje	Dónde se envía el mensaje
Daily (de forma predeterminada, enviado entre las 12:00 a.m. y la 1:00 a.m. como mensaje de registro)	Direcciones especificadas en `-partner-address` El soporte técnico, si `-support` se establece en `enable`
Daily (de forma predeterminada, enviado entre las 12:00 a.m. y la 1:00 a.m. como mensaje de rendimiento), si el `-perf` el parámetro se establece en `true`	Direcciones especificadas en -Partner-address' El soporte técnico, si `-support` se establece en `enable`
Semanal (de forma predeterminada, enviado el domingo entre las 12:00 a.m. y la 1:00 a. m.)	Direcciones especificadas en `-partner-address` El soporte técnico, si `-support` se establece en `enable`

Mensajes activados manualmente

Puede iniciar o reenviar manualmente un mensaje de AutoSupport.

Cuando se envía el mensaje	Dónde se envía el mensaje
Puede iniciar manualmente un mensaje mediante el `system node autosupport invoke` comando	Si se especifica un URI mediante el `-uri` en la `system node autosupport invoke` Comando, el mensaje se envía a ese URI. Si `-uri` se omite, el mensaje se envía a las direcciones especificadas en `-to` y.. `-partner -address`. El mensaje también se envía al soporte técnico si `-support` se establece en `enable`.
Puede iniciar manualmente un mensaje mediante el `system node autosupport invoke-core-upload` comando	Si se especifica un URI mediante el `-uri` en la `system node autosupport invoke-core-upload` Comando, el mensaje se envía a ese URI y el archivo de volcado principal se carga en el URI. Si `-uri` se omite en la `system node autosupport invoke-core-upload` comando, el mensaje se envía al soporte técnico y el archivo de volcado principal se carga en el sitio de soporte técnico. Ambos escenarios lo requieren `-support` se establece en `enable` y.. `-transport` se establece en `https` o. `http`. Debido al gran tamaño de los archivos de volcado principales, el mensaje no se envía a las direcciones especificadas en la `-to` y.. `-partner-addresses` parámetros.
Puede iniciar manualmente un mensaje mediante el `system node autosupport invoke-performance-archive` comando	Si se especifica un URI mediante el `-uri` en la `system node autosupport invoke-performance-archive` Comando, el mensaje se envía a ese URI y el archivo de archivado de rendimiento se carga en el URI. Si `-uri` se omite en la `system node autosupport invoke-performance-archive`, el mensaje se envía al soporte técnico y el archivo de rendimiento se carga en el sitio de soporte técnico. Ambos escenarios lo requieren `-support` se establece en `enable` y.. `-transport` se establece en `https` o. `http`. Debido al gran tamaño de los archivos de archivo de rendimiento, el mensaje no se envía a las direcciones especificadas en la `-to` y.. `-partner-addresses` parámetros.

Cuando se envía el mensaje	Dónde se envía el mensaje
Reenvíe manualmente un mensaje anterior mediante el `system node autosupport history retransmit` comando	Únicamente del URI que especifique en la `-uri` parámetro de `system node autosupport history retransmit` comando

Mensajes activados por el soporte técnico

El soporte técnico puede solicitar mensajes de AutoSupport con la función AutoSupport OnDemand.

Cuando se envía el mensaje	Dónde se envía el mensaje
Cuando AutoSupport obtiene instrucciones de entrega para generar nuevos mensajes de AutoSupport	Direcciones especificadas en `-partner-address` El soporte técnico, si `-support` se establece en `enable` y.. `-transport` se establece en `https`
Cuando AutoSupport obtiene instrucciones de entrega para reenviar mensajes anteriores de AutoSupport	El soporte técnico, si `-support` se establece en `enable` y.. `-transport` se establece en `https`
Cuando AutoSupport obtiene instrucciones de entrega para generar nuevos mensajes de AutoSupport que cargan archivos de volcado principales o de archivo de rendimiento	El soporte técnico, si `-support` se establece en `enable` y.. `-transport` se establece en `https`. El volcado principal o el archivo de archivado de rendimiento se cargan en el sitio de soporte técnico.

Cómo crea AutoSupport y envía los mensajes activados por un evento

AutoSupport crea mensajes de AutoSupport activados por un evento cuando EMS procesa un evento de activación. Un mensaje AutoSupport activado para el evento alerta a los destinatarios sobre problemas que requieren acción correctiva y solo contiene información relevante para el problema. Puede personalizar el contenido que desea incluir y quién recibe los mensajes.

AutoSupport utiliza el siguiente proceso para crear y enviar mensajes de AutoSupport activados por un evento:

1. Cuando EMS procesa un evento de activación, EMS envía una solicitud a AutoSupport.

   Un evento trigger es un evento de EMS con un destino de AutoSupport y un nombre que comienza por `callhome.` prefijo.

2. AutoSupport crea un mensaje de AutoSupport activado por eventos.

   AutoSupport recopila información básica y de solución de problemas de subsistemas asociados con el desencadenador para crear un mensaje que incluya únicamente información relevante para el evento desencadenador.

   Un conjunto predeterminado de subsistemas está asociado con cada desencadenador. Sin embargo, puede optar por asociar subsistemas adicionales a un desencadenador mediante el `system node`

`autosupport trigger modify` comando.

3. AutoSupport envía el mensaje AutoSupport activado por el evento a los destinatarios definidos por el `system node autosupport modify` con el `-to`, `-noteto`, `-partner-address`, y. `-support` parámetros.

   Puede habilitar y deshabilitar la entrega de mensajes de AutoSupport para activadores específicos mediante el `system node autosupport trigger modify` con el `-to` y.. `-noteto` parámetros.

Ejemplo de datos enviados para un evento específico

La `storage shelf PSU failed` El evento EMS activa un mensaje que contiene datos básicos de la obligatoria, Archivos de registro, almacenamiento, RAID, ha, Los subsistemas de plataforma y red y los datos de solución de problemas de los subsistemas de almacenamiento, Archivos de registro y obligatorios.

Decide que desea incluir datos sobre NFS en cualquier mensaje de AutoSupport que se envíe como respuesta a un futuro `storage shelf PSU failed` evento. Introduzca el siguiente comando para habilitar los datos a nivel de solución de problemas para NFS en el `callhome.shlf.ps.fault` evento:

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Observe que el `callhome.` el prefijo se descarta de `callhome.shlf.ps.fault` evento cuando utilice `system node autosupport trigger` Comandos o cuando los eventos de AutoSupport y EMS se hagan referencia en la CLI.

Tipos de mensajes de AutoSupport y su contenido

Los mensajes AutoSupport contienen información de estado acerca de los subsistemas compatibles. Saber qué contienen los mensajes de AutoSupport puede ayudarle a interpretar o a responder a los mensajes que reciba por correo electrónico o que aparecen en el sitio Web de Active IQ (anteriormente denominado My AutoSupport).

Tipo de mensaje	Tipo de datos que contiene el mensaje
Activado por evento	Archivos que contienen datos contextuales sobre el subsistema específico en el que se produjo el evento
Todos los días	Archivos de registro
Rendimiento	Datos de rendimiento muestreados durante las 24 horas anteriores
Semanal	Datos de configuración y estado

Tipo de mensaje	Tipo de datos que contiene el mensaje
Activado por la `system node autosupport invoke` comando	Depende del valor especificado en la `-type` parámetro: • `test` envía un mensaje activado por el usuario con algunos datos básicos. Este mensaje también activa una respuesta de correo electrónico automática del soporte técnico a cualquier dirección de correo electrónico especificada mediante el `-to` Para confirmar que se están recibiendo mensajes de AutoSupport. • `performance` envía datos de rendimiento. • `all` envía un mensaje activado por el usuario con un conjunto completo de datos similar al mensaje semanal, incluidos los datos de resolución de problemas de cada subsistema. El soporte técnico normalmente solicita este mensaje.
Activado por la `system node autosupport invoke-core-upload` comando	Archivos de volcado principales para un nodo
Activado por la `system node autosupport invoke-performance-archive` comando	Archivos de archivado de rendimiento durante un periodo de tiempo específico
Activado por AutoSupport OnDemand	AutoSupport OnDemand puede solicitar mensajes nuevos o pasados: • Los mensajes nuevos, dependiendo del tipo de colección AutoSupport, pueden ser `test`, `all`, o. `performance`. • Los mensajes anteriores dependen del tipo de mensaje que se vuelva a enviar. AutoSupport OnDemand puede solicitar nuevos mensajes que cargan los siguientes archivos en el sitio de soporte de NetApp en "mysupport.netapp.com": • Volcado de memoria • Archivado del rendimiento

Qué son los subsistemas AutoSupport

Cada subsistema proporciona información básica y de solución de problemas que

AutoSupport utiliza para sus mensajes. Cada subsistema también está asociado con eventos desencadenadores que permiten a AutoSupport recopilar de subsistemas únicamente información relevante para el evento desencadenante.

AutoSupport recopila contenido sensible al contexto. Puede ver información acerca de los subsistemas y los eventos desencadenadores mediante el `system node autosupport trigger show` comando.

Tamaño y tiempo de AutoSupport

AutoSupport recopila información organizada por subsistemas y aplica un presupuesto de tamaño y tiempo sobre el contenido de cada subsistema. A medida que crecen los sistemas de almacenamiento, los presupuestos de AutoSupport proporcionan control sobre la carga útil de AutoSupport, que, a su vez, proporciona una entrega escalable de datos de AutoSupport.

AutoSupport deja de recopilar información y acorta el contenido de AutoSupport si el contenido del subsistema supera su tamaño o presupuesto para tiempo. Si el contenido no se puede truncar fácilmente (por ejemplo, archivos binarios), AutoSupport omite el contenido.

Solo debe modificar el tamaño y el presupuesto de tiempo predeterminados si el soporte de NetApp le solicita que lo haga. También puede revisar el tamaño predeterminado y los presupuestos de tiempo de los subsistemas mediante el `autosupport manifest show` comando.

Archivos enviados en mensajes AutoSupport activados por eventos

Los mensajes AutoSupport activados por eventos sólo contienen información básica y de solución de problemas de subsistemas asociados al evento que provocó que AutoSupport genere el mensaje. Los datos específicos ayudan a los partners de soporte y soporte de NetApp a solucionar el problema.

AutoSupport utiliza los siguientes criterios para controlar el contenido de los mensajes de AutoSupport activados por un evento:

- Qué subsistemas están incluidos

  Los datos se agrupan en subsistemas, incluidos subsistemas comunes, como los archivos de registro y subsistemas específicos, como RAID. Cada evento activa un mensaje que sólo contiene los datos de subsistemas específicos.

- El nivel de detalle de cada subsistema incluido

  Los datos de cada subsistema incluido se proporcionan a nivel básico o de resolución de problemas.

Puede ver todos los eventos posibles y determinar qué subsistemas se incluyen en los mensajes acerca de cada evento mediante el `system node autosupport trigger show` con el `-instance` parámetro.

Además de los subsistemas incluidos de forma predeterminada para cada evento, puede agregar subsistemas adicionales en un nivel básico o de solución de problemas mediante el `system node autosupport trigger modify` comando.

Archivos de registro enviados en mensajes de AutoSupport

Los mensajes de AutoSupport pueden contener varios archivos de registro clave que permiten al personal de soporte técnico revisar la actividad reciente del sistema.

Todos los tipos de mensajes de AutoSupport pueden incluir los siguientes archivos de registro cuando el subsistema de archivos de registro está habilitado:

Archivo de registro	Cantidad de datos incluidos del archivo
• Archivos de registro de `/mroot/etc/log/mlog/` directorio • El archivo de registro DE MENSAJES	Solo se han añadido líneas nuevas a los registros desde el último mensaje de AutoSupport hasta un máximo especificado. Esto garantiza que los mensajes AutoSupport tengan datos únicos, relevantes, no superpuestos. (Los archivos de registro de los partners son la excepción; para los partners, se incluyen los datos máximos permitidos).
• Archivos de registro de `/mroot/etc/log/shelflog/` directorio • Archivos de registro de `/mroot/etc/log/acp/` directorio • Datos de registro del sistema de gestión de eventos (EMS)	Las líneas de datos más recientes hasta un máximo especificado.

El contenido de los mensajes de AutoSupport puede cambiar entre las versiones de ONTAP.

Archivos enviados en mensajes semanales de AutoSupport

Los mensajes semanales de AutoSupport contienen datos adicionales de configuración y estado que son útiles para realizar el seguimiento de los cambios que se producen en el sistema a lo largo del tiempo.

La siguiente información se envía en mensajes semanales de AutoSupport:

- Información básica sobre cada subsistema
- Contenido de seleccionado `/mroot/etc` archivos de directorio
- Archivos de registro
- Resultado de comandos que proporcionan información del sistema
- Información adicional, incluida la información de la base de datos replicada (RDB), las estadísticas de servicio, etc.

De qué manera AutoSupport OnDemand obtiene instrucciones de entrega del soporte técnico

AutoSupport OnDemand se comunica periódicamente con el soporte técnico para obtener instrucciones de entrega para enviar, reenviar y rechazar mensajes de AutoSupport, así como para cargar archivos de gran tamaño en el sitio de soporte de

NetApp. AutoSupport OnDemand permite enviar mensajes de AutoSupport bajo demanda en lugar de esperar a que se ejecute el trabajo de AutoSupport semanal.

OnDemand de AutoSupport consta de los siguientes componentes:

- Cliente OnDemand de AutoSupport que se ejecuta en cada nodo
- Servicio OnDemand de AutoSupport que reside en el soporte técnico

El cliente OnDemand de AutoSupport sondea periódicamente el servicio AutoSupport OnDemand para obtener instrucciones de entrega del soporte técnico. Por ejemplo, el soporte técnico puede utilizar el servicio AutoSupport OnDemand para solicitar que se genere un nuevo mensaje de AutoSupport. Cuando el cliente AutoSupport OnDemand sondea el servicio AutoSupport OnDemand, el cliente obtiene las instrucciones de entrega y envía el nuevo mensaje de AutoSupport bajo demanda según corresponda.

AutoSupport OnDemand está habilitado de forma predeterminada. Sin embargo, AutoSupport OnDemand utiliza algunos ajustes de AutoSupport para continuar comunicándose con el soporte técnico. AutoSupport OnDemand se comunica automáticamente con el soporte técnico cuando se cumplen los siguientes requisitos:

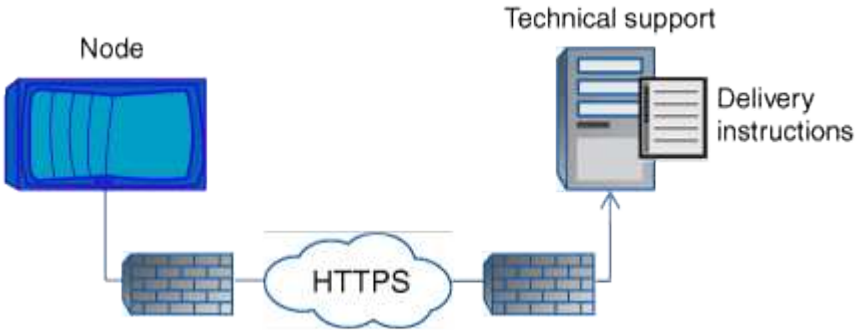
- AutoSupport está habilitado.
- AutoSupport está configurado para enviar mensajes al soporte técnico.
- AutoSupport se configura para utilizar el protocolo de transporte HTTPS.

El cliente AutoSupport OnDemand envía solicitudes HTTPS a la misma ubicación de soporte técnico a la que se envían los mensajes de AutoSupport. El cliente AutoSupport OnDemand no acepta conexiones entrantes.

> AutoSupport OnDemand utiliza la cuenta de usuario «'AutoSupport'» para comunicarse con la asistencia técnica. ONTAP le impide eliminar esta cuenta.

Si desea deshabilitar AutoSupport OnDemand, pero mantener AutoSupport habilitado, utilice el comando: Link:https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters[`system node autosupport modify -ondemand-state disable`].

En la siguiente ilustración, se muestra cómo AutoSupport OnDemand envía las solicitudes HTTPS al soporte técnico para obtener instrucciones de entrega.



Las instrucciones de entrega pueden incluir solicitudes para que AutoSupport haga lo siguiente:

- Generar nuevos mensajes de AutoSupport.

  El soporte técnico puede solicitar nuevos mensajes de AutoSupport como ayuda para la clasificación de problemas.

- Genere nuevos mensajes de AutoSupport que cargan archivos de volcado principales o archivos de archivado de rendimiento en el sitio de soporte de NetApp.

  El soporte técnico puede solicitar un volcado de memoria o archivos de archivado de rendimiento que ayuden a clasificar los problemas.

- Retransmita mensajes de AutoSupport generados previamente.

  Esta solicitud se produce automáticamente si no se ha recibido un mensaje debido a un fallo de entrega.

- Deshabilite la entrega de mensajes de AutoSupport para eventos de activación específicos.

  El soporte técnico puede deshabilitar la entrega de datos que no se utiliza.

Estructura de los mensajes AutoSupport enviados por correo electrónico

Cuando se envía un mensaje AutoSupport por correo electrónico, el mensaje tiene un asunto estándar, un cuerpo breve y un archivo adjunto grande en formato de archivo 7z que contiene los datos.

> Si AutoSupport está configurado para ocultar datos privados, cierta información, como el nombre de host, se omite o se oculta en el encabezado, el asunto, el cuerpo y los datos adjuntos.

Asunto

La línea de asunto de los mensajes enviados por el mecanismo AutoSupport contiene una cadena de texto que identifica el motivo de la notificación. El formato de la línea del asunto es el siguiente:

Notificación DE grupo HA de *System_Name* (*Message*) *Severity*

- *System_Name* es el nombre de host o el ID del sistema, según la configuración de AutoSupport

Cuerpo

El cuerpo del mensaje de AutoSupport contiene la siguiente información:

- Fecha y Marca de hora del mensaje
- Versión de ONTAP en el nodo que generó el mensaje
- El ID del sistema, el número de serie y el nombre de host del nodo que generó el mensaje
- Número de secuencia de AutoSupport
- Nombre y ubicación del contacto SNMP, si se especifica
- El ID del sistema y el nombre de host del partner de alta disponibilidad

Archivos adjuntos

La información clave de un mensaje de AutoSupport contiene archivos comprimidos en un archivo 7z llamado `body.7z` y adjunto al mensaje.

Los archivos contenidos en el archivo adjunto son específicos del tipo de mensaje AutoSupport.

Tipos de gravedad de AutoSupport

Los mensajes de AutoSupport tienen tipos de gravedad que le ayudan a entender el propósito de cada mensaje, por ejemplo, para llamar la atención inmediata a un problema de emergencia, o sólo para proporcionar información.

Los mensajes tienen una de las siguientes gravedades:

- **Alerta**: Los mensajes de alerta indican que podría producirse un evento de nivel superior si no realiza alguna acción.

  Debe realizar una acción contra los mensajes de alerta en un plazo de 24 horas.

- **Emergencia**: Los mensajes de emergencia se muestran cuando se produce una interrupción.

  Usted debe tomar una acción contra los mensajes de emergencia inmediatamente.

- **Error**: Las condiciones de error indican lo que podría suceder si ignora.
- **Aviso**: Condición normal pero significativa.
- **Info**: El mensaje informativo proporciona detalles sobre el problema, que usted puede ignorar.
- **Depurar**: Los mensajes de nivel de depuración proporcionan instrucciones que debe realizar.

Si su organización de soporte interno recibe mensajes de AutoSupport por correo electrónico, la gravedad aparecerá en la línea del asunto del mensaje de correo electrónico.

Requisitos para usar AutoSupport

Debe utilizar HTTPS con TLSv1,2 o SMTP seguro para la entrega de mensajes de AutoSupport a fin de proporcionar la mejor seguridad y admitir todas las funciones de AutoSupport más recientes. Se rechazarán los mensajes de AutoSupport entregados con cualquier otro protocolo.

Protocolos compatibles

Todos estos protocolos se ejecutan en IPv4 o IPv6, según la familia de direcciones a la que se resuelve el nombre.

Protocolo y puerto	Descripción
HTTPS en el puerto 443	Este es el protocolo predeterminado. Debe utilizarlo siempre que sea posible. Este protocolo es compatible con AutoSupport OnDemand y la carga de archivos de gran tamaño. El certificado del servidor remoto se valida con el certificado raíz, a menos que se deshabilite la validación. La entrega utiliza una solicitud PUT HTTPS. Con PUT, si la solicitud falla durante la transmisión, la solicitud se reinicia donde se detuvo. Si el servidor que recibe la solicitud no admite PUT, la entrega utiliza una solicitud POST HTTPS.
HTTP en el puerto 80	Este protocolo es el más preferido que SMTP. Este protocolo admite cargas de archivos de gran tamaño, pero no AutoSupport OnDemand. La entrega utiliza una solicitud PUT HTTPS. Con PUT, si la solicitud falla durante la transmisión, la solicitud se reinicia donde se detuvo. Si el servidor que recibe la solicitud no admite PUT, la entrega utiliza una solicitud POST HTTPS.
SMTP en el puerto 25 u otro puerto	Solo debe utilizar este protocolo si la conexión de red no permite HTTPS. El valor predeterminado del puerto es 25, pero puede configurar AutoSupport para que utilice un puerto diferente. Tenga en cuenta las siguientes limitaciones al utilizar SMTP: • No se admiten las cargas de archivos de gran tamaño bajo demanda de AutoSupport. • Los datos no están cifrados. SMTP envía datos en texto sin cifrar, haciendo que el texto en el mensaje de AutoSupport sea fácil de interceptar y leer. • Se pueden introducir limitaciones en la longitud del mensaje y la longitud de la línea.

Si configura AutoSupport con direcciones de correo electrónico específicas para su organización de soporte interno o una organización de partner de soporte, esos mensajes siempre los envía SMTP.

Por ejemplo, si utiliza el protocolo recomendado para enviar mensajes al soporte técnico y también desea enviar mensajes a la organización de soporte interno, los mensajes se transportarán mediante HTTPS y SMTP, respectivamente.

AutoSupport limita el tamaño máximo de archivo para cada protocolo. La configuración predeterminada para las transferencias HTTP y HTTPS es 25 MB. El valor predeterminado para las transferencias SMTP es 5 MB. Si el tamaño del mensaje de AutoSupport supera el límite configurado, AutoSupport entregará la mayor parte posible del mensaje. Se puede editar el tamaño máximo modificando la configuración de AutoSupport. Consulte `system node autosupport modify` manual para más información.

> AutoSupport anula automáticamente el límite de tamaño máximo de archivo de los protocolos HTTPS y HTTP cuando se generan y envían mensajes de AutoSupport que cargan archivos de volcado principales o de archivo de rendimiento al sitio de soporte de NetApp o un URI especificado. La anulación automática sólo se aplica cuando se cargan archivos mediante el `system node autosupport invoke-core-upload` o la `system node autosupport invoke-performance-archive` comandos.

Requisitos de configuración

Dependiendo de la configuración de red, el protocolo HTTPS puede requerir una configuración adicional de una URL de proxy. Si HTTPS envía mensajes de AutoSupport al soporte técnico y tiene un proxy, debe identificar la URL de ese proxy. Si el proxy utiliza un puerto distinto del predeterminado, que es 3128, puede especificar el puerto para ese proxy. También puede especificar un nombre de usuario y una contraseña para la autenticación del proxy.

Si utiliza SMTP para enviar mensajes de AutoSupport a la organización de soporte interno o al soporte técnico, debe configurar un servidor de correo externo. El sistema de almacenamiento no funciona como un servidor de correo; requiere un servidor de correo externo en su sitio para enviar correo. El servidor de correo debe ser un host que escucha en el puerto SMTP (25) u otro puerto, y debe estar configurado para enviar y recibir codificación MIME (Extensiones multipropósito de correo Internet) de 8 bits. Los hosts de correo de ejemplo incluyen un host UNIX que ejecuta un servidor SMTP como el programa sendmail y un servidor Windows que ejecuta el servidor Microsoft Exchange. Puede tener uno o más hosts de correo.

Configure AutoSupport

Puede controlar si la información de AutoSupport se envía al soporte técnico y a la organización de soporte interna, y luego probar que la configuración es correcta.

Acerca de esta tarea

En ONTAP 9.5 y versiones posteriores, es posible habilitar AutoSupport y modificar su configuración en todos los nodos del clúster de forma simultánea. Cuando un nuevo nodo se une al clúster, el nodo hereda automáticamente la configuración del clúster de AutoSupport. No es necesario actualizar la configuración en cada nodo por separado.

> A partir de ONTAP 9.5, el ámbito de la `system node autosupport modify` el comando se encuentra en todo el clúster. La configuración de AutoSupport se modifica en todos los nodos del clúster, incluso cuando el `-node` se especifica la opción. La opción se omite, pero se conserva para la compatibilidad con versiones anteriores de la CLI.
>
> En ONTAP 9,4 y versiones anteriores, el alcance del `system node autosupport modify` el comando es específico del nodo. La configuración de AutoSupport debe modificarse en cada nodo del clúster.

De manera predeterminada, AutoSupport se habilita en cada nodo para enviar mensajes al soporte técnico mediante el protocolo de transporte HTTPS.

Debe utilizar HTTPS con TLSv1,2 o SMTP seguro para la entrega de mensajes de AutoSupport a fin de proporcionar la mejor seguridad y admitir todas las funciones de AutoSupport más recientes.

Pasos

1. Asegúrese de que AutoSupport esté habilitado:

```
system node autosupport modify -state enable
```

2. Si desea que el soporte técnico reciba mensajes de AutoSupport, utilice el comando siguiente:

```
system node autosupport modify -support enable
```

   Debe habilitar esta opción si desea habilitar AutoSupport para trabajar con AutoSupport OnDemand o si desea cargar archivos grandes, como archivos de volcado de memoria y de archivo de rendimiento, al soporte técnico o una URL específica.

3. Si el soporte técnico está habilitado para recibir mensajes de AutoSupport, especifique el protocolo de transporte que debe utilizar para los mensajes.

   Es posible elegir entre las siguientes opciones:

Si desea…	A continuación, configure los siguientes parámetros del `system node autosupport modify` comando…
Utilizar el protocolo HTTPS predeterminado	a. Configurado `-transport` para `https`. b. Si utiliza un proxy, establezca `-proxy-url` A la dirección URL de su proxy. Esta configuración admite la comunicación con AutoSupport OnDemand y la carga de archivos de gran tamaño.
Utilice SMTP	Configurado `-transport` para `smtp`. Esta configuración no admite AutoSupport OnDemand ni la carga de archivos de gran tamaño.

4. Si desea que su organización de soporte interno o un partner de soporte reciban mensajes de AutoSupport, realice las siguientes acciones:

   a. Identifique a los destinatarios de su organización estableciendo los siguientes parámetros de `system node autosupport modify` comando:

Configurar este parámetro…	A esto…

`-to`	Hasta cinco direcciones de correo electrónico individuales separadas por comas o listas de distribución en su organización de soporte interno que recibirán mensajes clave de AutoSupport
`-noteto`	Hasta cinco direcciones de correo electrónico individuales separadas por comas o listas de distribución en su organización de soporte interno que recibirán una versión abreviada de los mensajes clave de AutoSupport diseñados para teléfonos móviles y otros dispositivos móviles
`-partner-address`	Hasta cinco direcciones de correo electrónico individuales separadas por comas o listas de distribución en su organización de partners de soporte que recibirán todos los mensajes de AutoSupport

b. Compruebe que las direcciones se han configurado correctamente enumerando los destinos mediante el `system node autosupport destinations show` comando.

5. Si va a enviar mensajes a su organización de soporte interno o ha elegido el transporte SMTP para mensajes al soporte técnico, configure SMTP estableciendo los siguientes parámetros de `system node autosupport modify` comando:

   - Configurado `-mail-hosts` en uno o más hosts de correo, separados por comas.

     Puede establecer un máximo de cinco.

   Puede configurar un valor de puerto para cada host de correo especificando dos puntos y un número de puerto después del nombre de host de correo: Por ejemplo, `mymailhost.example.com:5678`, donde 5678 es el puerto del host de correo.

   - Configurado `-from` A la dirección de correo electrónico que envía el mensaje AutoSupport.

6. Configure DNS.
7. Opcionalmente, agregue opciones de comando si desea cambiar ajustes específicos:

Si desea hacer esto…	A continuación, configure los siguientes parámetros del `system node autosupport modify` comando…
Oculte datos privados eliminando, enmascarando o codificando datos confidenciales en los mensajes	Configurado `-remove-private-data` para `true`. Si cambia de `false` para `true`, Se eliminan todos los archivos de historial de AutoSupport y todos los archivos asociados.
Detenga el envío de datos de rendimiento en mensajes periódicos de AutoSupport	Configurado `-perf` para `false`.

8. Compruebe la configuración general mediante el `system node autosupport show` con el `-node`

parámetro.

9. Verifique el funcionamiento de la AutoSupport mediante el `system node autosupport check show` comando.

   Si se informa de algún problema, utilice `system node autosupport check show-details` comando para ver más información.

10. Comprobar que se envían y reciben mensajes de AutoSupport:

    a. Utilice la `system node autosupport invoke` con el `-type` parámetro establecido en `test`.

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. Confirme que NetApp recibe sus mensajes de AutoSupport:

    el historial de AutoSupport del nodo del sistema muestra -node local

    El estado del último mensaje AutoSupport saliente debería cambiar a `sent-successful` para todos los destinos de protocolo adecuados.

    a. De manera opcional, si el mensaje de AutoSupport se envía a la organización de soporte interna o a su partner de soporte, consulte el correo electrónico de cualquier dirección que haya configurado para el `-to`, `-noteto`, o. `-partner-address` parámetros de `system node autosupport modify` comando.

Cargar archivos de volcado principales

Cuando se guarda un archivo de volcado principal, se genera un mensaje de evento. Si el servicio AutoSupport está habilitado y configurado para enviar mensajes al soporte de NetApp, se transmite un mensaje AutoSupport y se le envía un mensaje de correo electrónico de confirmación automatizado.

Lo que necesitará

- Debe haber configurado AutoSupport con las siguientes opciones:
  - AutoSupport está habilitado en el nodo.
  - AutoSupport está configurado para enviar mensajes al soporte técnico.
  - AutoSupport está configurado para utilizar el protocolo de transporte HTTP o HTTPS.

    El protocolo de transporte SMTP no se admite cuando se envían mensajes que incluyen archivos de gran tamaño, como archivos de volcado principales.

Acerca de esta tarea

También se puede cargar el archivo de volcado principal a través del servicio AutoSupport mediante HTTPS con el `system node autosupport invoke-core-upload` Si lo solicita el soporte de NetApp.

"Cómo cargar un archivo en NetApp"

Pasos

1. Vea los archivos de volcado principales de un nodo mediante el `system node coredump show`

comando.

En el siguiente ejemplo, se muestran los archivos de volcado principales para el nodo local:

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
--------- ------------------------------------------- -----
-----------------
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Genere un mensaje de AutoSupport y cargue un archivo de volcado principal con la `system node autosupport invoke-core-upload` comando.

   En el siguiente ejemplo, se genera un mensaje de AutoSupport y se envía a la ubicación predeterminada, es decir, al soporte técnico, y el archivo de volcado principal se carga en la ubicación predeterminada, que es el sitio de soporte de NetApp:

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

   En el ejemplo siguiente, se genera un mensaje de AutoSupport que se envía a la ubicación especificada en el URI y el archivo de volcado principal se carga en el URI:

```
cluster1::> system node autosupport invoke-core-upload -uri
https//files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

Cargue archivos de archivado de rendimiento

Puede generar y enviar un mensaje de AutoSupport que contenga un archivo de rendimiento. De forma predeterminada, el soporte técnico de NetApp recibe el mensaje AutoSupport y el archivo de rendimiento se carga en el sitio de soporte de NetApp. Puede especificar un destino alternativo para el mensaje y cargarlo.

Lo que necesitará

- Debe haber configurado AutoSupport con las siguientes opciones:
  - AutoSupport está habilitado en el nodo.
  - AutoSupport está configurado para enviar mensajes al soporte técnico.
  - AutoSupport está configurado para utilizar el protocolo de transporte HTTP o HTTPS.

    El protocolo de transporte SMTP no se admite cuando se envían mensajes que incluyen archivos de gran tamaño, como archivos de archivado de rendimiento.

Acerca de esta tarea

Debe especificar una fecha de inicio para los datos de archivo de rendimiento que desea cargar. La mayoría de los sistemas de almacenamiento conservan los archivos de rendimiento durante dos semanas, lo que permite especificar una fecha de inicio hasta hace dos semanas. Por ejemplo, si hoy es el 15 de enero, puede especificar una fecha de inicio del 2 de enero.

Paso

1. Genere un mensaje de AutoSupport y cargue el archivo de archivado de rendimiento mediante la `system node autosupport invoke-performance-archive` comando.

   En el siguiente ejemplo, se añaden 4 horas de archivos de archivado de rendimiento desde el 12 de enero de 2015 a un mensaje de AutoSupport y se cargan en la ubicación predeterminada, que es el sitio de soporte de NetApp:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   En el siguiente ejemplo, se agregan 4 horas de archivos de rendimiento desde el 12 de enero de 2015 a un mensaje de AutoSupport y se cargan en la ubicación especificada por el URI:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

Obtener descripciones de mensajes de AutoSupport

Las descripciones de los mensajes de AutoSupport que recibe están disponibles a través del traductor de syslog de ONTAP.

Pasos

1. Vaya a la "Traductor de syslog".
2. En el campo **Versión**, introduzca la versión de ONTAP que está utilizando. En el campo **cadena de búsqueda**, introduzca "callhome". Seleccione **Traducir**.
3. Syslog Translator mostrará alfabéticamente todos los eventos que coincidan con la cadena de mensaje introducida.

Comandos para gestionar AutoSupport

Utilice la `system node autosupport` Comandos para cambiar o ver la configuración de AutoSupport, mostrar información acerca de mensajes anteriores de AutoSupport y enviar, reenviar o cancelar un mensaje de AutoSupport.

Configure AutoSupport

Si desea…	Se usa este comando…
Controle si se envían mensajes de AutoSupport	`system node autosupport modify` con la `-state` parámetro
Controlar si se envían mensajes de AutoSupport al soporte técnico	`system node autosupport modify` con la `-support` parámetro
Configure AutoSupport o modifique la configuración de AutoSupport	`system node autosupport modify`
Habilite y deshabilite los mensajes de AutoSupport a su organización de soporte interno para eventos de activación individuales y especifique informes de subsistema adicionales que se incluirán en los mensajes enviados en respuesta a eventos de activación individuales	`system node autosupport trigger modify`

Muestra información acerca de la configuración de AutoSupport

Si desea…	Se usa este comando…
Mostrar la configuración de AutoSupport	`system node autosupport show` con la `-node` parámetro
Vea un resumen de todas las direcciones y direcciones URL que reciben mensajes de AutoSupport	`system node autosupport destinations show`
Mostrar los mensajes de AutoSupport que se envían a su organización de soporte interno para eventos de activación individuales	`system node autosupport trigger show`
Mostrar el estado de la configuración de AutoSupport, así como la entrega a varios destinos	`system node autosupport check show`
Mostrar el estado detallado de la configuración de AutoSupport, así como la entrega a varios destinos	`system node autosupport check show-details`

Muestra información acerca de los mensajes anteriores de AutoSupport

Si desea…	Se usa este comando…
Muestra información acerca de uno o más de los 50 mensajes de AutoSupport más recientes	`system node autosupport history show`

Si desea…	Se usa este comando…
Muestra información sobre los mensajes de AutoSupport recientes generados para cargar archivos de volcado principal o de archivado de rendimiento en el sitio de soporte técnico o un URI especificado	`system node autosupport history show-upload-details`
Vea la información de los mensajes de AutoSupport, incluidos el nombre y el tamaño de cada archivo recopilado para el mensaje, junto con cualquier error	`system node autosupport manifest show`

Enviar, reenviar o cancelar mensajes de AutoSupport

Si desea…	Se usa este comando…
Retransmitir un mensaje AutoSupport almacenado localmente, identificado por su número de secuencia AutoSupport Si retransmite un mensaje de AutoSupport y si la compatibilidad ya recibió ese mensaje, el sistema de soporte no creará una incidencia duplicada. Si, por otro lado, el soporte no recibió ese mensaje, entonces el sistema AutoSupport analizará el mensaje y creará un caso, si es necesario.	`system node autosupport history retransmit`
Generar y enviar un mensaje de AutoSupport, por ejemplo, con fines de pruebas	`system node autosupport invoke` Utilice la `-force` Parámetro para enviar un mensaje incluso si AutoSupport está deshabilitado. Utilice la `-uri` parámetro para enviar el mensaje al destino que especifique en lugar del destino configurado.
Cancelar un mensaje de AutoSupport	`system node autosupport history cancel`

Información relacionada

"Comandos de ONTAP 9"

La información incluida en el manifiesto AutoSupport

El manifiesto AutoSupport ofrece una vista detallada de los archivos recopilados para cada mensaje de AutoSupport. El manifiesto AutoSupport también incluye información sobre los errores de recopilación cuando AutoSupport no puede recopilar los archivos

que necesita.

El manifiesto de AutoSupport incluye la siguiente información:

- Número de secuencia del mensaje AutoSupport
- Qué archivos incluye AutoSupport en el mensaje AutoSupport
- Tamaño de cada archivo, en bytes
- Estado de la colección de manifiesto AutoSupport
- Descripción del error, si AutoSupport no pudo recopilar uno o varios archivos

Puede ver el manifiesto AutoSupport mediante la `system node autosupport manifest show` comando.

El manifiesto AutoSupport se incluye con todos los mensajes de AutoSupport y se presenta en formato XML, lo que significa que puede utilizar un visor XML genérico para leerlo o verlo utilizando el portal Active IQ (anteriormente conocido como My AutoSupport).

Supresión de casos AutoSupport durante las ventanas de mantenimiento programadas

La supresión de casos de AutoSupport permite impedir que se creen casos innecesarios mediante mensajes de AutoSupport que se activan durante las ventanas de mantenimiento programadas.

Para suprimir casos de AutoSupport, debe invocar manualmente un mensaje de AutoSupport con una cadena de texto con formato especial: `MAINT=xh`. `x` es la duración del plazo de mantenimiento en unidades de horas.

Información relacionada

"Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"

Solucionar problemas de AutoSupport cuando no se reciben mensajes

Si el sistema no envía el mensaje de AutoSupport, puede determinar si esto es porque AutoSupport no puede generar el mensaje o no puede entregar el mensaje.

Pasos

1. Compruebe el estado de entrega de los mensajes mediante el `system node autosupport history show` comando.
2. Lea el estado.

Este estado	Medios
inicializando	Se está iniciando el proceso de recopilación. Si este estado es temporal, todo está bien. Sin embargo, si este estado persiste, hay un problema.
error de recopilación	AutoSupport no puede crear el contenido de AutoSupport en el directorio de spool. Para ver qué está intentando recopilar AutoSupport, introduzca el `system node autosupport history show -detail` comando.

Este estado	Medios
recogida en curso	AutoSupport está recopilando contenido de AutoSupport. Para ver la recopilación de AutoSupport, introduzca la `system node autosupport manifest show` comando.
en cola	Los mensajes de AutoSupport se ponen en cola para su entrega, pero aún no se han entregado.
transmitiendo	AutoSupport proporciona mensajes actualmente.
enviado correctamente	AutoSupport ha entregado el mensaje correctamente. Para averiguar dónde ha entregado el mensaje AutoSupport, introduzca el `system node autosupport history show -delivery` comando.
ignorar	AutoSupport no tiene destinos para el mensaje. Para ver los detalles de la entrega, introduzca la `system node autosupport history show -delivery` comando.
volver a poner en cola	AutoSupport intentó entregar mensajes, pero el intento falló. Como resultado, AutoSupport volvió a colocar los mensajes en la cola de entrega para otro intento. Para ver el error, introduzca el `system node autosupport history show` comando.
la transmisión ha fallado	AutoSupport no pudo entregar el mensaje el número especificado de veces y dejó de intentar entregar el mensaje. Para ver el error, introduzca el `system node autosupport history show` comando.
ondemand-ignore	El mensaje AutoSupport se procesó correctamente, pero el servicio OnDemand de AutoSupport decidió ignorarlo.

3. Ejecute una de las siguientes acciones:

Para este estado	Haga esto
error de inicialización o recopilación	Póngase en contacto con el soporte de NetApp, porque AutoSupport no puede generar el mensaje. Mencione el siguiente artículo de la base de conocimientos: "AutoSupport no puede proporcionar: Estado bloqueado en inicialización"
se ha producido un error al ignorar, volver a poner en cola o al transmitir	Compruebe que los destinos estén configurados correctamente para SMTP, HTTP o HTTPS porque AutoSupport no puede entregar el mensaje.

Solucione problemas de entrega de mensajes de AutoSupport a través de HTTP o HTTPS

Si el sistema no envía el mensaje AutoSupport esperado y utiliza HTTP o HTTPS, o la función de actualización automática no está funcionando, puede comprobar una serie de configuraciones para resolver el problema.

Lo que necesitará

Debe haber confirmado la conectividad de red básica y la búsqueda de DNS:

- El LIF de gestión de nodos debe estar activo para tener el estado operativo y administrativo.
- Debe poder hacer ping a un host en funcionamiento en la misma subred desde la LIF de gestión del clúster (no una LIF en ninguno de los nodos).
- Debe poder hacer ping a un host en funcionamiento fuera de la subred desde la LIF de administración de clústeres.
- Debe poder hacer ping a un host en funcionamiento fuera de la subred desde la LIF de administración de clústeres con el nombre del host (no la dirección IP).

Acerca de esta tarea

Estos pasos son para casos en los que se ha determinado que AutoSupport puede generar el mensaje, pero no puede entregarlo a través de HTTP o HTTPS.

Si encuentra errores o no puede completar un paso de este procedimiento, determine y resuelva el problema antes de continuar con el siguiente paso.

Pasos

1. Muestre el estado detallado del subsistema AutoSupport:

   ```
   system node autosupport check show-details
   ```

   Esto incluye verificar la conectividad a los destinos de AutoSupport, mediante el envío de mensajes de prueba y la provisión de una lista de los posibles errores en las opciones de configuración de AutoSupport.

2. Compruebe el estado de la LIF de gestión de nodos:

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   La `status-oper` y.. `status-admin` los campos deberán devolver «'up'».

3. Registre el nombre de la SVM, el nombre de la LIF y la dirección IP de la LIF para usarlos más adelante.
4. Asegúrese de que DNS esté habilitado y configurado correctamente:

   ```
   vserver services name-service dns show
   ```

5. Resuelva los errores devueltos por el mensaje de AutoSupport:

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   Para obtener ayuda sobre la solución de problemas de los errores devueltos, consulte "Guía de resolución de ONTAP AutoSupport (Transport HTTPS y HTTP)".

6. Confirme que el clúster puede acceder a los servidores que necesita y a Internet correctamente:

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

   > La dirección `support.netapp.com` en sí mismo no responde a ping/traceroute, pero la información por salto es valiosa.

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   Si alguna de estas rutas no funciona, pruebe la misma ruta desde un host en funcionamiento en la misma subred que el clúster, utilizando la utilidad «'traceroute' o «'tracert'» que se encuentra en la mayoría de los clientes de red de terceros. Esto le ayuda a determinar si el problema está en la configuración de red o en la configuración del clúster.

7. Si utiliza HTTPS para el protocolo de transporte AutoSupport, asegúrese de que el tráfico HTTPS pueda salir de la red:

   a. Configure un cliente web en la misma subred que la LIF de gestión de clústeres.

      Asegúrese de que todos los parámetros de configuración sean los mismos valores que para la configuración de AutoSupport, incluido el uso del mismo servidor proxy, nombre de usuario, contraseña y puerto.

   b. Acceso `https://support.netapp.com` con el cliente web.

      El acceso debe ser correcto. Si no es así, asegúrese de que todos los firewalls estén configurados correctamente para permitir el tráfico HTTPS y DNS, y de que el servidor proxy esté configurado correctamente. Para obtener más información sobre la configuración de la resolución de nombres estáticos para support.netapp.com, consulte el artículo de Knowledge base "Cómo se puede añadir una entrada DE HOST en ONTAP para la versión support.netapp.com?"

8. A partir de ONTAP 9.10.1, si ha activado la función de actualización automática, asegúrese de que dispone de conectividad HTTPS con las siguientes direcciones URL adicionales:

   - https://support-sg-emea.netapp.com
   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

Solucionar los problemas de entrega de mensajes de AutoSupport a través de SMTP

Si el sistema no puede entregar mensajes de AutoSupport a través de SMTP, puede comprobar una serie de opciones para resolver el problema.

Lo que necesitará

Debe haber confirmado la conectividad de red básica y la búsqueda de DNS:

- El LIF de gestión de nodos debe estar activo para tener el estado operativo y administrativo.
- Debe poder hacer ping a un host en funcionamiento en la misma subred desde la LIF de gestión del clúster (no una LIF en ninguno de los nodos).

- Debe poder hacer ping a un host en funcionamiento fuera de la subred desde la LIF de administración de clústeres.
- Debe poder hacer ping a un host en funcionamiento fuera de la subred desde la LIF de administración de clústeres con el nombre del host (no la dirección IP).

Acerca de esta tarea

Estos pasos son para casos en los que ha determinado que AutoSupport puede generar el mensaje, pero no puede entregarlo a través de SMTP.

Si encuentra errores o no puede completar un paso de este procedimiento, determine y resuelva el problema antes de continuar con el siguiente paso.

Todos los comandos se introducen en la interfaz de línea de comandos de ONTAP, a menos que se especifique lo contrario.

Pasos

1. Compruebe el estado de la LIF de gestión de nodos:

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   La `status-oper` y.. `status-admin` los campos deben regresar `up`.

2. Registre el nombre de la SVM, el nombre de la LIF y la dirección IP de la LIF para usarlos más adelante.
3. Asegúrese de que DNS esté habilitado y configurado correctamente:

   ```
   vserver services name-service dns show
   ```

4. Mostrar todos los servidores configurados para ser utilizados por AutoSupport:

   ```
   system node autosupport show -fields mail-hosts
   ```

   Registre todos los nombres de servidor mostrados.

5. Para cada servidor que se muestra en el paso anterior, y. `support.netapp.com`, Asegúrese de que el nodo puede acceder al servidor o a la URL:

   ```
   network traceroute -node local -destination server_name
   ```

   Si alguna de estas rutas no funciona, pruebe la misma ruta desde un host en funcionamiento en la misma subred que el clúster, utilizando la utilidad «'traceroute' o «'tracert'» que se encuentra en la mayoría de los clientes de red de terceros. Esto le ayuda a determinar si el problema está en la configuración de red o en la configuración del clúster.

6. Inicie sesión en el host designado como host de correo y asegúrese de que puede atender solicitudes SMTP:

   ```
   netstat -aAn|grep 25
   ```

   `25` Es el número de puerto SMTP del listener.

   Se muestra un mensaje similar al siguiente texto:

```
ff64878c tcp        0      0  *.25    *.*    LISTEN.
```

7. Desde otro host, abra una sesión Telnet con el puerto SMTP del host de correo:

   telnet *mailhost* 25

   Se muestra un mensaje similar al siguiente texto:

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. En el símbolo de telnet, asegúrese de que se puede transmitir un mensaje desde su host de correo:

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` es el nombre de dominio de la red.

   Si se devuelve un error que indica que se deniega la retransmisión, la retransmisión no está activada en el host de correo. Póngase en contacto con el administrador del sistema.

9. En el símbolo de telnet, envíe un mensaje de prueba:

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   > Asegúrese de introducir el último período (.) en una línea por sí misma. El período indica al host de correo que el mensaje ha finalizado.

   Si se devuelve un error, el host de correo no está configurado correctamente. Póngase en contacto con el administrador del sistema.

10. Desde la interfaz de línea de comandos de ONTAP, envíe un mensaje de prueba de AutoSupport a una dirección de correo electrónico de confianza a la que tenga acceso:

    system node autosupport invoke -node local -type test

11. Busque el número de secuencia del intento:

    system node autosupport history show -node local -destination smtp

    Busque el número de secuencia para su intento basado en la Marca de hora. Probablemente sea el intento más reciente.

12. Mostrar el error para el intento de mensaje de prueba:

    `system node autosupport history show -node local -seq-num seq_num -fields error`

    Si el error mostrado es `Login denied`, El servidor SMTP no acepta peticiones de envío desde la LIF de administración del clúster. Si no desea cambiar al uso de HTTPS como protocolo de transporte, póngase en contacto con el administrador de red del sitio para configurar las puertas de enlace SMTP para resolver este problema.

    Si esta prueba se realiza correctamente pero el mismo mensaje enviado a mailto:autosupport@netapp.com no lo hace, asegúrese de que la retransmisión SMTP está activada en todos los hosts de correo SMTP o utilice HTTPS como protocolo de transporte.

    Si incluso el mensaje a la cuenta de correo administrada localmente no se realiza correctamente, confirme que los servidores SMTP están configurados para reenviar archivos adjuntos con ambas características:

    - El sufijo "'7z'"
    - El tipo MIME "'Application/x-7x-Compressed'".

Solucione problemas del subsistema AutoSupport

La `system node check show` Los comandos se pueden utilizar para verificar y solucionar los problemas relacionados con la configuración y la entrega de AutoSupport.

Paso

1. Use los siguientes comandos para mostrar el estado del subsistema AutoSupport.

Se usa este comando…	Para hacer esto…
`system node autosupport check show`	Mostrar el estado general del subsistema AutoSupport, como el estado del destino HTTP o HTTPS de AutoSupport, destinos SMTP de AutoSupport, servidor AutoSupport OnDemand y la configuración de AutoSupport
`system node autosupport check show-details`	Mostrar el estado detallado del subsistema AutoSupport, como descripciones detalladas de errores y las acciones correctivas

Supervisión del estado

Supervise el estado de la información general del sistema

Los monitores de estado supervisan proactivamente ciertas condiciones críticas de su clúster y generan alertas si detectan una falla o un riesgo. Si hay alertas activas, el estado del sistema informa de un estado degradado para el clúster. Las alertas incluyen la información que necesita para responder a un estado del sistema degradado.

Si el estado es degradado, puede ver detalles del problema, incluidas la causa probable y las acciones de

recuperación recomendadas. Después de resolver el problema, el estado del sistema vuelve automáticamente a OK.

El estado del sistema refleja varios monitores de estado independientes. Un estado degradado en un monitor de estado individual provoca un estado degradado para el estado general del sistema.

Si quiere más información sobre cómo ONTAP admite los switches de clúster para supervisar el estado del sistema en el clúster, puede consultar el *Hardware Universe*.

"Los switches compatibles del Hardware Universe"

Para obtener información detallada sobre las causas de los mensajes de AutoSupport del monitor de estado del switch de clúster (CSHM) y las acciones necesarias para resolver estas alertas, consulte el artículo de la base de conocimientos.

"Mensaje de AutoSupport: Proceso del monitor de estado CSHM"

Cómo funciona la supervisión del estado

Los monitores de estado individuales tienen un conjunto de políticas que activan alertas cuando se dan ciertas condiciones. Comprender cómo funciona la supervisión del estado puede ayudarle a responder a problemas y controlar alertas futuras.

La supervisión del estado consta de los siguientes componentes:

- Monitores de salud individuales para subsistemas específicos, cada uno de los cuales tiene su propio estado de salud

  Por ejemplo, el subsistema de almacenamiento tiene un monitor de estado de conectividad de nodo.

- Un monitor de estado general del sistema que consolida el estado de los monitores de estado individuales

  Un estado degradado en cualquier subsistema único da como resultado un estado degradado para todo el sistema. Si ningún subsistema tiene alertas, el estado general del sistema es correcto.

Cada monitor de estado se compone de los siguientes elementos clave:

- Alertas que el monitor de estado puede generar potencialmente

  Cada alerta tiene una definición, que incluye detalles como la gravedad de la alerta y su causa probable.

- Políticas de estado que identifican cuándo se activa cada alerta

  Cada política de mantenimiento tiene una expresión de regla, que es la condición o cambio exactos que desencadena la alerta.

Un monitor de estado supervisa y valida continuamente los recursos en su subsistema para comprobar la condición o los cambios de estado. Cuando un cambio de condición o estado coincide con una expresión de regla de una política de estado, el monitor de estado genera una alerta. Una alerta hace que el estado del subsistema y su estado general del sistema se degraden.

Formas de responder a las alertas de estado del sistema

Cuando se produce una alerta de estado del sistema, puede reconocerla, obtener más información sobre él, reparar la condición subyacente y evitar que vuelva a producirse.

Cuando un monitor de estado genera una alerta, puede responder de cualquiera de las siguientes maneras:

- Obtenga información sobre la alerta, que incluye el recurso afectado, la gravedad de la alerta, la causa probable, el posible efecto y las acciones correctivas.
- Obtenga información detallada sobre la alerta, como el momento en que se planteó la alerta y si alguien más ya ha reconocido dicha alerta.
- Obtenga información relacionada con el estado del recurso o subsistema afectado, como una bandeja o un disco específicos.
- Reconozca la alerta para indicar que alguien está trabajando en el problema e identifíquese como el "acusador".
- Resuelva el problema siguiendo las acciones correctivas proporcionadas en la alerta, como la corrección de cableado para resolver un problema de conectividad.
- Elimine la alerta si el sistema no la borró automáticamente.
- Suprime una alerta para evitar que afecte al estado de un subsistema.

  La supresión es útil cuando se entiende un problema. Después de suprimir una alerta, todavía puede ocurrir, pero el estado del subsistema se muestra como "'ok-with-suppress"""". cuando se produce la alerta suprimida.

Personalización de alertas de estado del sistema

Puede controlar qué alertas genera un monitor de estado mediante la habilitación y la deshabilitación de las políticas de estado del sistema que definen cuándo se activan las alertas. Esto le permite personalizar el sistema de control del estado para su entorno concreto.

Puede obtener más información sobre el nombre de una política mediante la visualización de información detallada sobre una alerta generada o la visualización de definiciones de políticas para un monitor de estado, nodo o ID de alerta específicos.

Deshabilitar políticas de estado es diferente de suprimir alertas. Cuando se suprime una alerta, esta no afecta al estado del subsistema, pero aún puede aparecer la alerta.

Si deshabilita una política, la condición o el estado definidos en la expresión de regla de política ya no activan una alerta.

Ejemplo de una alerta que desea deshabilitar

Por ejemplo, supongamos que se produce una alerta que no le resulta útil. Utilice la `system health alert show -instance` Comando para obtener el ID de política de la alerta. El ID de política se utiliza en la `system health policy definition show` comando para ver información acerca de la política. Después de revisar la expresión de regla y otra información acerca de la directiva, decide deshabilitar la directiva. Utilice la `system health policy definition modify` comando para deshabilitar la política.

Cómo activan las alertas de estado los mensajes y eventos de AutoSupport

Las alertas de estado del sistema activan mensajes y eventos de AutoSupport en el sistema de gestión de eventos (EMS), lo que permite supervisar el estado del sistema mediante mensajes de AutoSupport y EMS, además de utilizar el sistema de supervisión de estado directamente.

El sistema envía un mensaje de AutoSupport dentro de los cinco minutos posteriores a una alerta. El mensaje AutoSupport incluye todas las alertas generadas desde el mensaje de AutoSupport anterior, a excepción de las alertas que duplican una alerta para el mismo recurso y la misma causa probable en la semana anterior.

Algunas alertas no activan mensajes de AutoSupport. Una alerta no activa un mensaje de AutoSupport si su política de estado deshabilita el envío de mensajes de AutoSupport. Por ejemplo, una directiva de estado podría deshabilitar los mensajes de AutoSupport de forma predeterminada porque AutoSupport ya genera un mensaje cuando se produce el problema. Puede configurar directivas para que no activen mensajes AutoSupport mediante el `system health policy definition modify` comando.

Puede ver una lista de todos los mensajes de AutoSupport activados por alertas enviados en la semana anterior mediante el `system health autosupport trigger history show` comando.

Las alertas también activan la generación de eventos en el EMS. Se genera un evento cada vez que se crea una alerta y se borra cada vez que se borra una alerta.

Monitores de estado del clúster disponibles

Existen varios monitores de estado que supervisan diferentes partes de un clúster. Los monitores de estado le ayudan a recuperarse de errores en sistemas ONTAP mediante la detección de eventos, el envío de alertas a usted y la eliminación de eventos según los borre.

Nombre del monitor de estado (identificador)	Nombre del subsistema (identificador)	Específico
Switch de clúster (switch de clúster)	Switch (Switch-Health)	Supervisa los switches de red de clúster y los switches de red de gestión para obtener temperatura, utilización, configuración de interfaces, redundancia (solo switches de red de clúster) y funcionamiento de suministro de alimentación y ventilador. El monitor de estado del switch del clúster se comunica con los switches a través de SNMP. SNMPv2c es el valor predeterminado. A partir de ONTAP 9.2, este monitor puede detectar y generar informes cuando se ha reiniciado un switch de clúster desde el último periodo de sondeo.
Estructura MetroCluster	Conmutador	Supervisa la topología de la estructura del back-end de la configuración de MetroCluster y detecta mala configuración como el cableado y la división en zonas incorrectas y los fallos de ISL.
MetroCluster Salud	Interconexión, RAID y almacenamiento	Supervisa los adaptadores FC-VI, los adaptadores del iniciador FC, los agregados y discos subyacentes y los puertos entre clústeres
Conectividad de nodo (conexión por nodo)	Operaciones no disruptivas de CIFS (CIFS-NDO)	Supervisa conexiones SMB para proporcionar operaciones no disruptivas a aplicaciones de Hyper-V.
Almacenamiento (conexión SAS)	Supervisa las bandejas, los discos y los adaptadores a nivel de nodo para obtener las rutas y conexiones adecuadas.	Sistema

Nombre del monitor de estado (identificador)	Nombre del subsistema (identificador)	Específico
no aplicable	Agrega información de otros monitores de estado.	Conectividad del sistema (conexión del sistema)

Reciba alertas de estado del sistema automáticamente

Puede ver manualmente las alertas de estado del sistema usando la `system health alert show` comando. Sin embargo, debe suscribirse a mensajes específicos de Event Management System (EMS) para recibir notificaciones automáticamente cuando un monitor de estado genera una alerta.

Acerca de esta tarea

En el siguiente procedimiento se muestra cómo configurar notificaciones para todos los mensajes hm.alert.levantados y todos los mensajes hm.alert.borrados.

Todos los mensajes hm.alert.levantados y todos los mensajes hm.alert.borrados incluyen una captura SNMP. Los nombres de las capturas SNMP son `HealthMonitorAlertRaised` y.. `HealthMonitorAlertCleared`. Para obtener información acerca de las capturas SNMP, consulte *Network Management Guide*.

Pasos

1. Utilice la `event destination create` Comando para definir el destino al que desea enviar mensajes de EMS.

   ```
   cluster1::> event destination create -name health_alerts -mail
   admin@example.com
   ```

2. Utilice la `event route add-destinations` comando para enrutar la `hm.alert.raised` y el `hm.alert.cleared` mensaje a un destino.

   ```
   cluster1::> event route add-destinations -messagename hm.alert*
   -destinations health_alerts
   ```

Información relacionada

"Gestión de redes"

Responda al estado degradado del sistema

Cuando el estado del sistema es degradado, puede mostrar alertas, leer acerca de la causa probable y acciones correctivas, mostrar información sobre el subsistema degradado y resolver el problema. También se muestran alertas suprimidas para que pueda modificarlas y ver si se han reconocido.

Acerca de esta tarea

Puede detectar que se generó una alerta mediante un mensaje de AutoSupport o un evento de EMS, o mediante el `system health` comandos.

Pasos

1. Utilice la `system health alert show` comando para ver las alertas que están afectando al estado del sistema.
2. Lea la causa probable, el posible efecto y las acciones correctivas de la alerta para determinar si puede resolver el problema o necesita más información.
3. Si necesita más información, utilice `system health alert show -instance` comando para ver información adicional disponible para la alerta.
4. Utilice la `system health alert modify` con el `-acknowledge` parámetro para indicar que está trabajando en una alerta específica.
5. Tome medidas correctivas para resolver el problema como se describe en `Corrective Actions` campo de la alerta.

   Las acciones correctivas pueden incluir reiniciar el sistema.

   Cuando se resuelve el problema, la alerta se borra automáticamente. Si el subsistema no tiene otras alertas, el estado del subsistema cambia a. `OK`. Si el estado de todos los subsistemas es correcto, el estado general del sistema cambia a. `OK`.

6. Utilice la `system health status show` comando para confirmar que el estado del sistema es `OK`.

   Si el estado del sistema no es `OK`, repetir este procedimiento.

Ejemplo de respuesta al estado degradado del sistema

Al revisar un ejemplo específico de estado del sistema degradado causado por una bandeja que carece de dos rutas a un nodo, puede ver lo que muestra la CLI cuando responde a una alerta.

Después de iniciar ONTAP, compruebe el estado del sistema y detecte que el estado es degradado:

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

Muestra las alertas para averiguar dónde está el problema y ver que la bandeja 2 no tiene dos rutas al nodo 1:

```
      cluster1::>system health alert show
               Node: node1
           Resource: Shelf ID 2
           Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

Se muestran detalles de la alerta para obtener más información, incluido el ID de alerta:

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
           Acknowledge: false
              Suppress: false
                Policy: DualPathToDiskShelf_Policy
          Acknowledger: -
            Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

Reconoce la alerta para indicar que está trabajando en ella.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

Fije el cableado entre la bandeja 2 y la nodo 1 y, a continuación, reinicie el sistema. Luego, vuelva a comprobar el estado del sistema y compruebe que el estado es `OK`:

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

Configurar la detección de switches de red de gestión y clústeres

El monitor de estado del switch de clúster intenta automáticamente detectar los switches de red de gestión y clúster mediante el protocolo de detección de Cisco (CDP). Debe configurar el monitor de estado si no puede detectar automáticamente un switch o si no desea usar CDP para la detección automática.

Acerca de esta tarea

La `system cluster-switch show` el comando enumera los switches que detectó el monitor de estado. Si no ve un switch que esperaba ver en esa lista, el monitor de estado no podrá detectarlo automáticamente.

Pasos

1. Si desea utilizar CDP para la detección automática, haga lo siguiente:

   a. Asegúrese de que el protocolo de descubrimiento de Cisco (CDP) está habilitado en los switches.

      Consulte la documentación de su switch para obtener instrucciones.

   b. Ejecute el siguiente comando en cada nodo del clúster para verificar si CDP está habilitado o deshabilitado:

      `run -node node_name -command options cdpd.enable`

      Si CDP está habilitado, vaya al paso d. Si CDP está desactivado, vaya al paso c.

   c. Ejecute el siguiente comando para habilitar CDP:

      `run -node node_name -command options cdpd.enable on`

   Espere cinco minutos antes de pasar al siguiente paso.

   a. Utilice la `system cluster-switch show` Para verificar si ONTAP ahora puede detectar automáticamente los switches.

2. Si el monitor de estado no puede detectar automáticamente un switch, use el `system cluster-switch create` comando para configurar la detección del switch:

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   Espere cinco minutos antes de pasar al siguiente paso.

3. Utilice la `system cluster-switch show` Comando para verificar que ONTAP puede detectar el switch

al que ha añadido información.

Después de terminar

Compruebe que el monitor de estado puede supervisar los switches.

Compruebe la supervisión de los switches de red de clúster y de gestión

El monitor de estado del switch de clúster intenta supervisar automáticamente los switches que detecta; sin embargo, es posible que la supervisión no se produzca de manera automática si los switches no se han configurado correctamente. Debe verificar que el monitor de estado esté correctamente configurado para supervisar los switches.

Pasos

1. Para identificar los switches que detectó el monitor de estado del switch del clúster, introduzca el siguiente comando:

   ONTAP 9,8 y versiones posteriores

   ```
   system switch ethernet show
   ```

   ONTAP 9,7 y anteriores

   ```
   system cluster-switch show
   ```

   Si la `Model` columna muestra el valor `OTHER`, Entonces ONTAP no puede supervisar el conmutador. ONTAP establece el valor en `OTHER` si un switch que detecta automáticamente no es compatible con la supervisión del estado.

   > Si un switch no se muestra en el resultado del comando, debe configurar la detección del switch.

2. Actualice al software de switch más reciente admitido y consulte el archivo de configuración (RCF) desde el sitio de soporte de NetApp.

   "Página de descargas de soporte de NetApp"

   La cadena de comunidad en el RCF del conmutador debe coincidir con la cadena de comunidad que el monitor de estado está configurado para utilizar. De forma predeterminada, el monitor de estado utiliza la cadena de comunidad `cshm1!`.

   > En este momento, el monitor de estado sólo admite SNMPv2.

   Si necesita cambiar información sobre un switch que supervisa el clúster, puede modificar la cadena de comunidad que utiliza el monitor de estado mediante el siguiente comando:

ONTAP 9,8 y versiones posteriores

```
system switch ethernet modify
```

ONTAP 9,7 y anteriores

```
system cluster-switch modify
```

3. Compruebe que el puerto de gestión del switch está conectado a la red de gestión.

   Esta conexión es necesaria para realizar consultas SNMP.

Comandos para supervisar el estado del sistema

Puede utilizar el `system health` comandos para mostrar información sobre el estado de los recursos del sistema, responder a las alertas y configurar alertas futuras. El uso de los comandos de la CLI le permite ver información en profundidad sobre la configuración del control del estado. Las páginas de manual de los comandos contienen más información.

Mostrar el estado del estado del sistema

Si desea…	Se usa este comando…
Muestre el estado del sistema, que refleja el estado general de cada monitor de estado	`system health status show`
Mostrar el estado de los subsistemas para los que está disponible la supervisión de estado	`system health subsystem show`

Mostrar el estado de conectividad de los nodos

Si desea…	Se usa este comando…
Muestra detalles acerca de la conectividad del nodo a la bandeja de almacenamiento, incluida la información de puertos, la velocidad del puerto de HBA, el rendimiento de I/o y la tasa de operaciones de I/o por segundo	`storage shelf show -connectivity` Utilice la `-instance` para mostrar información detallada de cada bandeja.
Muestra información sobre las unidades y los LUN de cabina, incluidos el espacio utilizable, los números de bandeja y bahía y el nombre del nodo propietario	`storage disk show` Utilice la `-instance` parámetro para mostrar información detallada acerca de cada unidad.

Si desea…	Se usa este comando…
Muestra información detallada sobre los puertos de las bandejas de almacenamiento, incluido el tipo de puerto, la velocidad y el estado	`storage port show` Utilice la `-instance` parámetro para mostrar información detallada sobre cada adaptador.

Gestionar la detección de switches de redes de gestión, almacenamiento y clúster

Si desea…	Utilice este comando. (ONTAP 9.8 y posterior)	Utilice este comando. (ONTAP 9.7 y anterior)
Muestre los switches que supervisa el clúster	`system switch ethernet show`	`system cluster-switch show`
Muestre los switches que el clúster supervisa actualmente, incluidos los switches que ha eliminado (que se muestran en la columna motivo del resultado del comando), y la información de configuración que necesita para el acceso de red a los switches de red de gestión y clúster. Este comando solo está disponible en el nivel de privilegios avanzado.	`system switch ethernet show-all`	`system cluster-switch show-all`
Configurar la detección de un switch no detectado	`system switch ethernet create`	`system cluster-switch create`
Modificar la información sobre un conmutador que supervisa el clúster (por ejemplo, nombre de dispositivo, dirección IP, versión SNMP y cadena de comunidad)	`system switch ethernet modify`	`system cluster-switch modify`
Desactive la supervisión de un interruptor	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
Desactive la detección y supervisión de un switch y elimine la información de configuración del switch	`system switch ethernet delete`	`system cluster-switch delete`

Si desea…	Utilice este comando. (ONTAP 9.8 y posterior)	Utilice este comando. (ONTAP 9.7 y anterior)
Eliminar permanentemente la información de configuración del conmutador almacenada en la base de datos (al hacerlo se vuelve a activar el descubrimiento automático del conmutador)	`system switch ethernet delete -force`	`system cluster-switch delete -force`
Active el registro automático para que se envíe con mensajes de AutoSupport.	`system switch ethernet log`	`system cluster-switch log`

Responda a alertas generadas

Si desea…	Se usa este comando…
Muestra información sobre las alertas generadas, como el recurso y el nodo donde se activó la alerta, y la gravedad y la causa probable de la alerta	`system health alert show`
Muestra información sobre cada alerta generada	`system health alert show -instance`
Indique que alguien está trabajando en una alerta	`system health alert modify`
Reconozca una alerta	`system health alert modify -acknowledge`
Suprimir una alerta posterior para que no afecte al estado de un subsistema	`system health alert modify -suppress`
Eliminar una alerta que no se borró automáticamente	`system health alert delete`
Muestra información sobre los mensajes de AutoSupport que se han activado en la última semana, por ejemplo, para determinar si una alerta ha activado un mensaje de AutoSupport	`system health autosupport trigger history show`

Configurar alertas futuras

Si desea…	Se usa este comando…
Habilite o deshabilite la política que controla si un estado de recurso específico genera una alerta específica	`system health policy definition modify`

Muestra información acerca de cómo se configura la supervisión del estado

Si desea…	Se usa este comando…
Muestra información acerca de los monitores de estado, como sus nodos, nombres, subsistemas y estado	`system health config show` Utilice la `-instance` parámetro para mostrar información detallada sobre cada monitor de estado.
Muestre información sobre las alertas que un monitor de estado puede generar potencialmente	`system health alert definition show` Utilice la `-instance` parámetro para mostrar información detallada sobre cada definición de alerta.
Muestra información sobre las políticas de control de estado, que determinan cuándo se generan las alertas	`system health policy definition show` Utilice la `-instance` parámetro para mostrar información detallada de cada política. Utilice otros parámetros para filtrar la lista de alertas, por ejemplo, el estado de la política (habilitada o no), el monitor de estado, las alertas, etc.

Muestra información del entorno

Los sensores le ayudan a supervisar los componentes medioambientales de su sistema. La información que puede mostrar acerca de los sensores medioambientales incluye sus advertencias de tipo, nombre, estado, valor y umbral.

Paso

1. Para mostrar la información de los sensores medioambientales, utilice `system node environment sensors show` comando.

Análisis del sistema de archivos

Descripción general de File System Analytics

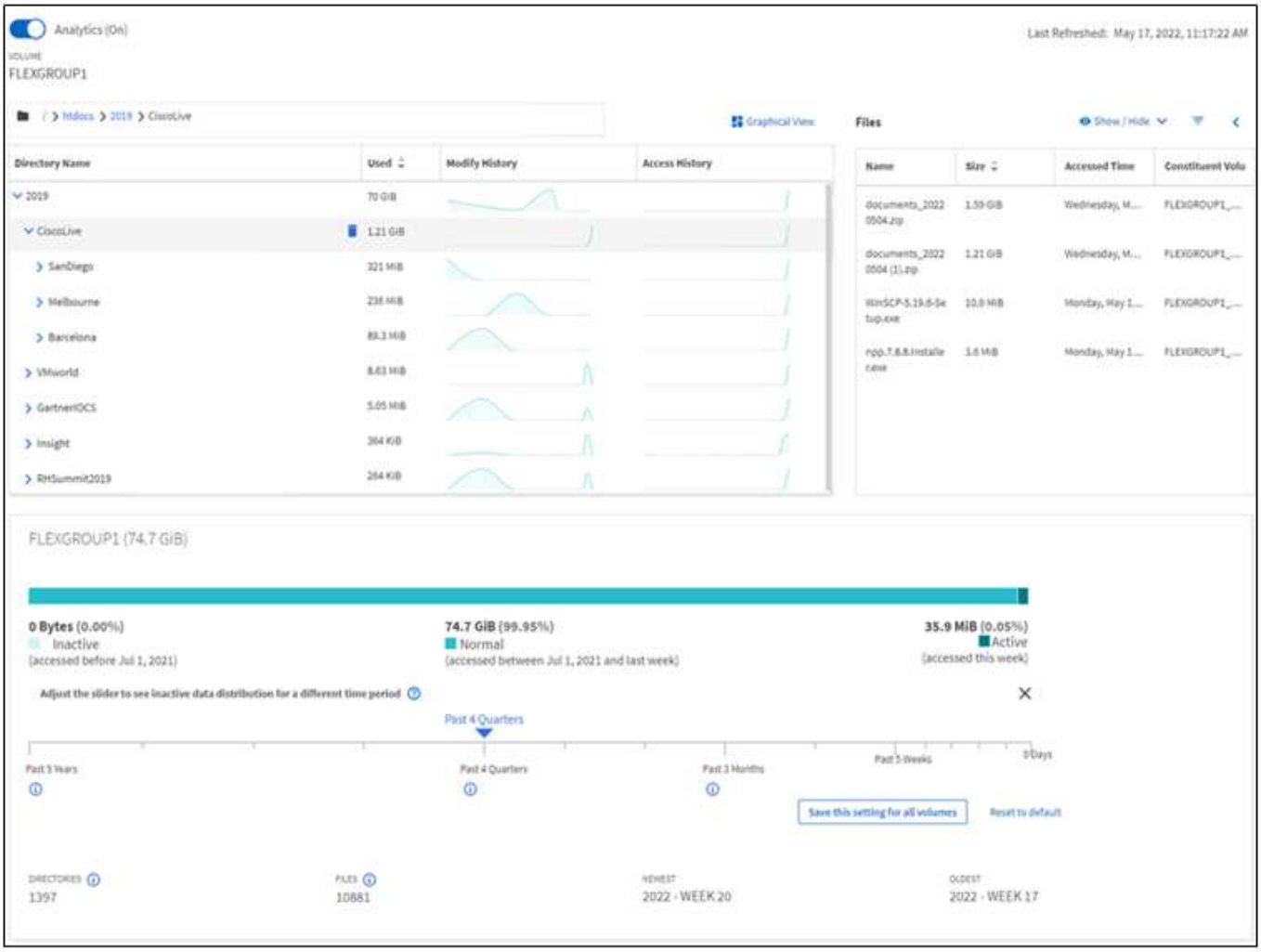
El análisis de sistemas de archivos (FSA, File System Analytics) se introdujo por primera vez en ONTAP 9.8 para ofrecer visibilidad en tiempo real de las tendencias de la capacidad de almacenamiento y el uso de ficheros dentro de los volúmenes de ONTAP FlexGroup o FlexVol. Esta funcionalidad nativa elimina la necesidad de herramientas externas y proporciona información clave sobre cómo se utiliza el almacenamiento y si existen oportunidades para optimizar el almacenamiento según las necesidades de su negocio.

Con FSA, usted tiene visibilidad en todos los niveles de la jerarquía de sistema de archivos de un volumen en NAS. Por ejemplo, puede obtener información sobre uso y capacidad en los niveles de máquina virtual de almacenamiento (SVM), volumen, directorio y archivo. Puede utilizar la FSA para responder preguntas como:

- ¿Qué está llenando el almacenamiento y tengo archivos de gran tamaño que puedo mover a otra ubicación de almacenamiento?
- ¿Cuáles son los volúmenes, directorios y archivos más activos? ¿Está optimizado el rendimiento de mi almacenamiento para las necesidades de mis usuarios?
- ¿Cuántos datos se han añadido el último mes?
- ¿Quiénes son los usuarios de almacenamiento más activos o menos activos?
- ¿Qué cantidad de datos inactivos o inactivos contiene mi almacenamiento primario? ¿Puedo mover los datos a un nivel de datos más bajo coste?
- ¿Los cambios previstos de calidad de servicio afectarán negativamente al acceso a archivos críticos y a los que se accede con frecuencia?

El análisis del sistema de archivos está integrado en System Manager de ONTAP. Las vistas de System Manager proporcionan:

- Visibilidad en tiempo real para una gestión y un funcionamiento de los datos efectivos
- Recopilación y agregación de datos en tiempo real
- Los tamaños y el número de subdirectorios y archivos, junto con los perfiles de rendimiento asociados
- Histogramas de edad de archivo para modificar e historial de acceso



Tipos de volúmenes admitidos

El análisis de sistemas de archivos está diseñado para proporcionar visibilidad en volúmenes con datos NAS activos, a excepción de las cachés de FlexCache y los volúmenes de destino de SnapMirror.

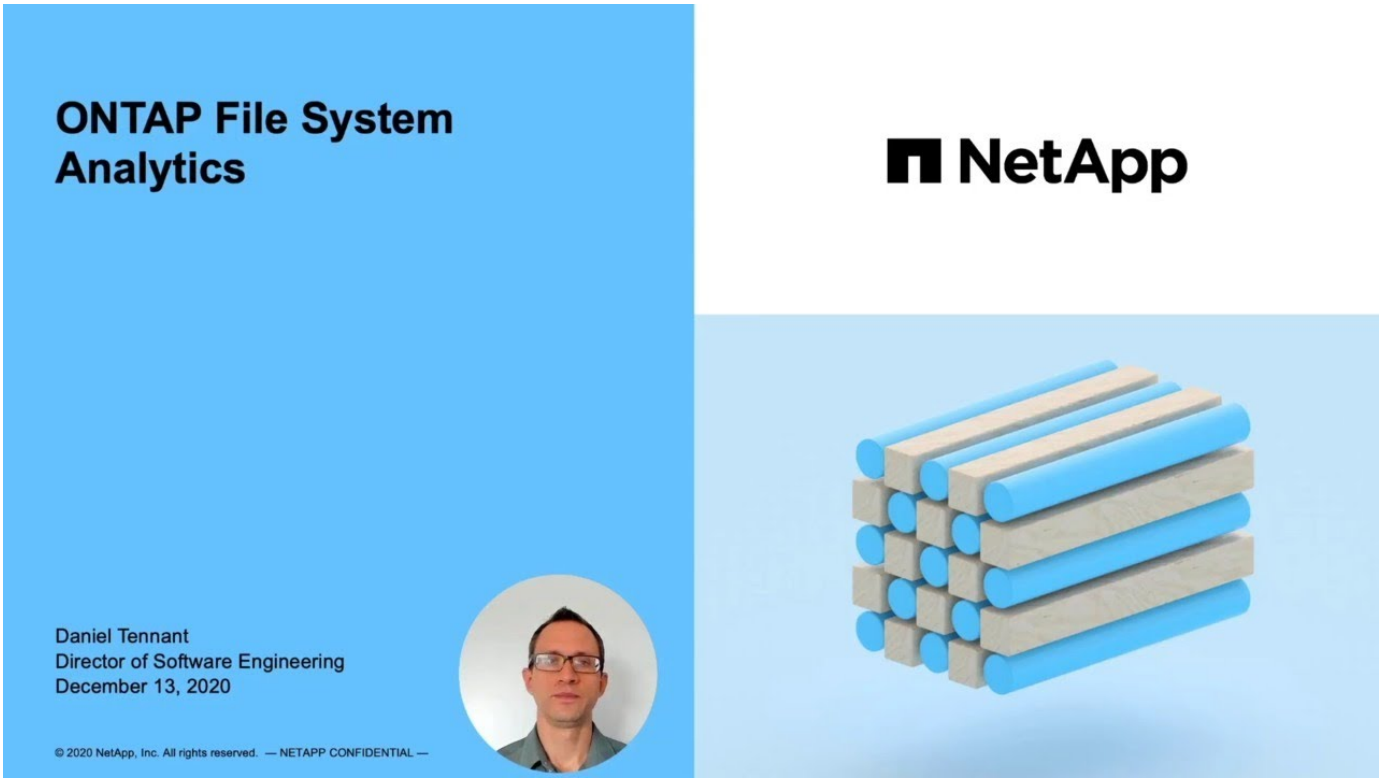
Disponibilidad de funciones de análisis de sistemas de archivos

Cada versión de ONTAP amplía el alcance del análisis de sistemas de archivos.

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9,8
Visualización en System Manager	✓	✓	✓	✓	✓	✓	✓
Análisis de capacidad	✓	✓	✓	✓	✓	✓	✓
Información de datos inactivos	✓	✓	✓	✓	✓	✓	✓
Compatibilidad con volúmenes que han realizado la transición desde Data ONTAP 7-Mode	✓	✓	✓	✓	✓	✓	

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9,8
Capacidad para personalizar el período inactivo en System Manager	✓	✓	✓	✓	✓	✓	
Seguimiento de actividad a nivel de volumen	✓	✓	✓	✓	✓		
Descargue los datos de seguimiento de actividad en CSV	✓	✓	✓	✓	✓		
Seguimiento de actividad a nivel de SVM	✓	✓	✓	✓			
Línea de tiempo	✓	✓	✓	✓			
Análisis del uso	✓	✓	✓				
Opción para activar el análisis del sistema de archivos de forma predeterminada	✓	✓					
Supervisión de progreso de exploración de inicialización	✓						

Obtenga más información sobre el análisis del sistema de archivos



Lecturas adicionales

- "TR 4687: Directrices de prácticas recomendadas para el análisis del sistema de archivos de ONTAP"
- "Base de conocimientos: Latencia alta o fluctuante tras activar el análisis del sistema de archivos ONTAP

de NetApp"

Active File System Analytics

Para recopilar y mostrar datos de uso, como los análisis de capacidad, es necesario habilitar File System Analytics en un volumen.

Acerca de esta tarea

- A partir de ONTAP 9.8, puede habilitar el análisis del sistema de archivos en un volumen nuevo o existente. Si actualiza un sistema a ONTAP 9.8 o posterior, asegúrese de que todos los procesos de actualización se han completado antes de habilitar el análisis del sistema de archivos.
- Según el tamaño y el contenido del volumen, la habilitación del análisis puede llevar tiempo mientras ONTAP procesa los datos existentes en el volumen. System Manager muestra el progreso y presenta datos de análisis cuando se completa. Si necesita información más precisa sobre el progreso de inicialización, puede utilizar el comando CLI de ONTAP `volume analytics show`.

  A partir de ONTAP 9.14.1, ONTAP proporciona seguimiento de progreso para la exploración de inicialización, además de notificaciones sobre eventos de limitación que afectan al progreso de la exploración.

  Para obtener más información relacionada con la secuencia de inicialización, consulte Consideraciones sobre la adquisición.

Pasos

Puede habilitar el análisis del sistema de archivos con el Administrador del sistema de ONTAP o la CLI.

System Manager

En ONTAP 9.8 y 9.9.1	A partir de ONTAP 9.10.1
1. Seleccione **almacenamiento > volúmenes**. 2. Seleccione el volumen deseado y, a continuación, seleccione **Explorer**. 3. Seleccione **Activar análisis** o **Desactivar análisis**.	1. Seleccione **almacenamiento > volúmenes**. 2. Seleccione el volumen deseado. En el menú volumen individual, seleccione **sistema de archivos > Explorador**. 3. Seleccione **Activar análisis** o **Desactivar análisis**.

CLI

Active File System Analytics con la CLI

1. Ejecute el siguiente comando:
   `volume analytics on -vserver` *`svm_name`* `-volume` *`volume_name`* `[-foreground {true|false}]`
   De forma predeterminada, el comando se ejecuta en primer plano; ONTAP muestra el progreso y presenta datos de análisis cuando se completa. Si necesita información más precisa, puede ejecutar el comando en segundo plano mediante la `-foreground false` y, a continuación, utilice la `volume analytics show` Comando para mostrar el progreso de inicialización en la CLI.
2. Después de habilitar correctamente el análisis del sistema de archivos, utilice System Manager o la API REST DE ONTAP para mostrar los datos analíticos.

Modificar la configuración predeterminada de análisis del sistema de archivos

A partir de ONTAP 9.13.1, se puede modificar la configuración de SVM o de los clústeres para habilitar el análisis del sistema de archivos de forma predeterminada en los volúmenes nuevos.

System Manager

Si utiliza System Manager, puede modificar la configuración de la máquina virtual de almacenamiento o del clúster para permitir los análisis de capacidad y el seguimiento de actividad durante la creación del volumen de forma predeterminada. La habilitación predeterminada solo se aplica a los volúmenes creados después de modificar la configuración, no a los volúmenes existentes.

Modificar la configuración de análisis del sistema de archivos en un clúster

1. En System Manager, vaya a **Configuración del clúster**.
2. En **Configuración del clúster**, revise la pestaña Configuración del sistema de archivos. Para modificar la configuración, seleccione la ⚙ .
3. En el campo **Seguimiento de actividad**, introduzca los nombres de las SVM para habilitar Seguimiento de actividad de forma predeterminada. Si deja el campo vacío, el seguimiento de actividad quedará deshabilitado en todas las SVM.

   Desactive la casilla **Activar en nuevas máquinas virtuales de almacenamiento** para desactivar el Seguimiento de actividad de forma predeterminada en las nuevas máquinas virtuales de almacenamiento.

4. En el campo **Analytics**, introduzca los nombres de las máquinas virtuales de almacenamiento para las que desea habilitar la analítica de capacidad de forma predeterminada. Si deja el campo vacío, los análisis de capacidad quedarán deshabilitados en todas las SVM.

   Desactive la casilla **Enable on new storage VMs** para desactivar los análisis de capacidad de forma predeterminada en las nuevas máquinas virtuales de almacenamiento.

5. Selecciona **Guardar**.

Modificar la configuración de análisis del sistema de archivos en una SVM

1. Seleccione la SVM que desea modificar, a continuación **Configuración de la máquina virtual de almacenamiento**.
2. En la tarjeta **File System Analytics**, utilice los botones para activar o desactivar el Seguimiento de actividad y el análisis de capacidad para todos los volúmenes nuevos en la máquina virtual de almacenamiento.

CLI

Puede configurar la máquina virtual de almacenamiento para habilitar el análisis del sistema de archivos de forma predeterminada en los nuevos volúmenes mediante la interfaz de línea de comandos de ONTAP.

Habilite File System Analytics de forma predeterminada en una SVM

1. Modifique la SVM para habilitar los análisis de capacidad y el seguimiento de actividad de forma predeterminada en todos los volúmenes recién creados:
   `vserver modify -vserver` *`svm_name`* `-auto-enable-activity-tracking true -auto -enable-analytics true`

Ver la actividad del sistema de archivos

Después de habilitar File System Analytics (FSA), puede ver el contenido del directorio raíz de un volumen seleccionado ordenado por el espacio utilizado en cada subárbol.

Seleccione cualquier objeto del sistema de archivos para examinar el sistema de archivos y mostrar información detallada sobre cada objeto de un directorio. La información sobre los directorios también se puede visualizar gráficamente. Con el paso del tiempo, se muestran los datos históricos de cada subárbol. El espacio utilizado no se ordena si hay más de 3000 directorios.

Explorador

La pantalla File System Analytics **Explorer** consta de tres áreas:

- Vista en árbol de directorios y subdirectorios; lista ampliable que muestra el nombre, el tamaño, el historial de modificación y el historial de acceso.
- Archivos; muestra el nombre, tamaño y tiempo de acceso del objeto seleccionado en la lista de directorios.
- Comparación de datos activos e inactivos para el objeto seleccionado en la lista de directorios.

  A partir de ONTAP 9.9.1, se puede personalizar el rango que se informará. El valor predeterminado es un año. En función de estas personalizaciones, puede tomar medidas correctivas, como mover volúmenes y modificar la política de organización en niveles.

La hora de acceso se muestra de forma predeterminada. Sin embargo, si el valor predeterminado del volumen se ha modificado desde la CLI (mediante el establecimiento del `-atime-update` opción a. `false` con la `volume modify`), entonces sólo se muestra la última hora modificada. Por ejemplo:

- La vista de árbol no mostrará el **historial de acceso**.
- La vista de archivos se modificará.
- La vista de datos activa/inactiva se basará en el tiempo modificado (`mtime`).

Mediante estas pantallas, puede examinar lo siguiente:

- Las ubicaciones de los sistemas de archivos consumen más espacio
- Información detallada sobre un árbol de directorios, incluido el recuento de archivos y subdirectorios dentro de directorios y subdirectorios
- Ubicaciones del sistema de archivos que contienen datos antiguos (por ejemplo, arboles, temp o log)

Tenga en cuenta lo siguiente al interpretar la salida FSA:

- La FSA muestra dónde y cuándo están en uso sus datos, no cuántos datos se están procesando. Por ejemplo, un gran consumo de espacio por parte de los archivos modificados o a los que se ha accedido recientemente no indica necesariamente que haya cargas elevadas de procesamiento del sistema.
- La forma en que la pestaña **Explorador de volúmenes** calcula el consumo de espacio para FSA podría ser diferente de otras herramientas. En particular, podría haber diferencias significativas en comparación con el consumo informado en **Resumen de volumen** si el volumen tiene las funciones de eficiencia del almacenamiento activadas. Esto se debe a que la pestaña **Explorador de volúmenes** no incluye el ahorro de eficiencia.
- Debido a las limitaciones de espacio en la visualización de directorios, no es posible ver una profundidad de directorio superior a 8 niveles en *List View*. Para ver los directorios con más de 8 niveles de

profundidad, debe cambiar a *Graphical View*, localizar el directorio deseado y, a continuación, volver a *List View*. Esto permitirá espacio adicional en la pantalla.

Pasos

1. Vea el contenido del directorio raíz de un volumen seleccionado:

En ONTAP 9.8 y 9.9.1	A partir de ONTAP 9.10.1
Haga clic en **almacenamiento > volúmenes**, seleccione el volumen deseado y, a continuación, haga clic en **Explorador**.	Seleccione **almacenamiento > volúmenes**, seleccione el volumen deseado. En el menú volumen individual, seleccione **sistema de archivos > Explorador**.

Activar seguimiento de actividad

A partir de ONTAP 9.10.1, el análisis del sistema de archivos incluye una función de seguimiento de actividades que le permite identificar objetos activos y descargar los datos como un archivo CSV. A partir de ONTAP 9.11.1, el seguimiento de la actividad se amplía al ámbito de SVM. A partir de ONTAP 9.11.1, el Administrador del sistema incluye una línea de tiempo para el seguimiento de actividades, lo que le permite buscar hasta cinco minutos de datos de seguimiento de actividades.

El seguimiento de actividad permite la supervisión en cuatro categorías:

- Directorios
- Archivos
- Clientes
- Usuarios

En cada categoría supervisada, el seguimiento de actividad mostrará IOPS de lectura, IOPS de escritura, rendimiento de lectura y rendimiento de escritura. Consultas sobre la actualización de seguimiento de actividad cada 10 a 15 segundos relacionadas con puntos calientes vistos en el sistema durante el intervalo de cinco segundos anterior.

La información de seguimiento de la actividad es aproximada, y la precisión de los datos depende de la distribución del tráfico de I/o entrante.

Al ver el seguimiento de actividad en System Manager a nivel de volumen, sólo se actualizará activamente el menú del volumen expandido. Si la vista de cualquier volumen se contrae, no se actualizará hasta que se expanda la visualización del volumen. Puede detener las actualizaciones con el botón **Pausa Actualizar**. Los datos de actividad se pueden descargar en formato CSV que mostrará todos los datos de un momento específico capturados para el volumen seleccionado.

Con la función de línea de tiempo disponible a partir de ONTAP 9.11.1, puede conservar un registro de la actividad de punto de acceso en un volumen o SVM, actualizando de forma continua aproximadamente cada cinco segundos y conservando los cinco minutos anteriores de datos. Los datos de la escala de tiempo sólo se conservan para los campos que son áreas visibles de la página. Si contrae una categoría de seguimiento o se desplaza para que la escala de tiempo esté fuera de la vista, la escala de tiempo dejará de recopilar datos. De forma predeterminada, las líneas de tiempo están desactivadas y se desactivarán automáticamente cuando salga de la ficha actividad.

Activar seguimiento de actividad para un único volumen

Puede habilitar el seguimiento de actividad con ONTAP System Manager o la interfaz de línea de comandos.

Acerca de esta tarea

Si utiliza RBAC con la API REST de ONTAP o System Manager, deberá crear roles personalizados para gestionar el acceso al seguimiento de actividades. Consulte Control de acceso basado en roles para este proceso.

System Manager

Pasos

1. Seleccione **almacenamiento > volúmenes**. Seleccione el volumen deseado. En el menú volumen individual, seleccione sistema de archivos y, a continuación, seleccione la ficha actividad.
2. Asegúrese de que **Activity Tracking** está activado para ver informes individuales en los directorios principales, archivos, clientes y usuarios.
3. Para analizar los datos a mayor profundidad sin actualizaciones, seleccione **Pausa Actualizar**. También puede descargar los datos para tener un registro CSV del informe.

CLI

Pasos

1. Activar seguimiento de actividad:

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. Compruebe si el estado Seguimiento de actividad de un volumen está activado o desactivado con el comando:

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. Una vez habilitada, use el administrador del sistema de ONTAP o la API REST de ONTAP para mostrar los datos de seguimiento de actividad.

Habilite el seguimiento de actividad para varios volúmenes

Puede habilitar el seguimiento de actividades para varios volúmenes con System Manager o la interfaz de línea de comandos.

Acerca de esta tarea

Si utiliza RBAC con la API REST de ONTAP o System Manager, deberá crear roles personalizados para gestionar el acceso al seguimiento de actividades. Consulte Control de acceso basado en roles para este proceso.

System Manager

Habilite para volúmenes específicos

1. Seleccione **almacenamiento > volúmenes**. Seleccione el volumen deseado. En el menú volumen individual, seleccione sistema de archivos y, a continuación, seleccione la ficha actividad.
2. Seleccione los volúmenes en los que desea habilitar el seguimiento de actividad. En la parte superior de la lista de volúmenes, seleccione el botón **más opciones**. Seleccione **Activar seguimiento de actividad**.
3. Para ver el seguimiento de actividad en el nivel de SVM, seleccione la SVM específica que desea ver en **almacenamiento > volúmenes**. Vaya a la pestaña sistema de archivos y luego a Activity y verá datos de los volúmenes que tienen activado Activity Tracking.

Habilitar para todos los volúmenes

1. Seleccione **almacenamiento > volúmenes**. Seleccione una SVM del menú.
2. Vaya a la ficha **sistema de archivos**, seleccione la ficha **más** para activar el seguimiento de actividad en todos los volúmenes de la SVM.

CLI

A partir de ONTAP 9.13.1, puede habilitar el seguimiento de actividades para varios volúmenes mediante la interfaz de línea de comandos de ONTAP.

Pasos

1. Activar seguimiento de actividad:

   ```
   volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
   ```

   Uso `*` Para habilitar el seguimiento de actividad para todos los volúmenes en la máquina virtual de almacenamiento especificada.

   Uso `!` Seguido de los nombres de volúmenes para habilitar el seguimiento de actividad para todos los volúmenes en la SVM, excepto los volúmenes con nombre.

2. Confirme que la operación se ha realizado correctamente:

   ```
   volume show -fields activity-tracking-state
   ```

3. Una vez habilitada, use el administrador del sistema de ONTAP o la API REST de ONTAP para mostrar los datos de seguimiento de actividad.

Habilite la analítica de uso

A partir de ONTAP 9.12.1, puede habilitar el análisis de uso para ver qué directorios de un volumen están utilizando la mayor cantidad de espacio. Puede ver el número total de directorios de un volumen o el número total de archivos de un volumen. Los informes están limitados a los 25 directorios que utilizan la mayor parte del espacio.

Los análisis de directorios grandes se actualizan cada 15 minutos. Puede supervisar el refrescamiento más reciente comprobando la última marca de tiempo refrescada en la parte superior de la página. También puede hacer clic en el botón Descargar para descargar datos en un libro de Excel. La operación de descarga se ejecuta en segundo plano y presenta la información más reciente del volumen seleccionado. Si el análisis

vuelve sin ningún resultado, asegúrese de que el volumen está en línea. Eventos como SnapRestore harán que el Análisis del sistema de archivos reconstruya su lista de directorios grandes.

Pasos

1. Seleccione **almacenamiento > volúmenes**. Seleccione el volumen deseado.
2. En el menú volumen individual, seleccione **sistema de archivos**. A continuación, seleccione la ficha **uso**.
3. Cambie el conmutador **Analytics** para activar el análisis de uso.
4. System Manager mostrará un gráfico de barras que identifica los directorios con el tamaño más grande en orden descendente.

> ONTAP puede mostrar datos parciales o ningún dato mientras se recopila la lista de directorios principales. El progreso de la exploración puede encontrarse en la pestaña **uso** que se muestra durante la exploración.

Para obtener más información sobre un directorio específico, puede hacerlo ver la actividad en un sistema de archivos.

Adopte medidas correctivas basadas en análisis

A partir de ONTAP 9.9.1, puede tomar medidas correctivas basadas en los datos actuales y los resultados deseados directamente desde las pantallas de análisis del sistema de archivos.

Eliminar directorios y archivos

En la pantalla del explorador, puede seleccionar directorios o archivos individuales que desea eliminar. Los directorios se eliminan con la funcionalidad de eliminación rápida de directorios de baja latencia. (FAST Directory delete también está disponible a partir de ONTAP 9.9.1 sin análisis activados).

Pasos

1. Haga clic en **almacenamiento > volúmenes** y, a continuación, en **Explorador**.

   Al pasar el ratón sobre un archivo o carpeta, aparece la opción para eliminar. Sólo puede eliminar un objeto cada vez.

> Cuando se eliminan directorios y archivos, los nuevos valores de capacidad de almacenamiento no se muestran inmediatamente.

Asignación de costes de medios en niveles de almacenamiento para comparar los costes de las ubicaciones de almacenamiento de datos inactivas

El coste del medio es un valor que usted asigna en función de su evaluación de los costes de almacenamiento, que se representan como la moneda por GB que elija. Cuando se establece, System Manager usa el costo de medios asignado para proyectar el ahorro estimado cuando se mueven volúmenes.

El coste de los medios establecido no es persistente; sólo se puede establecer para una única sesión de explorador.

Pasos

1. Haga clic en **Almacenamiento > Niveles** y, a continuación, haga clic en **Establecer coste de medios** en

los mosaicos de nivel local (agregado) deseados.

Asegúrese de seleccionar los niveles activo e inactivo para permitir la comparación.

2. Introduzca un tipo de moneda y un importe.

   Al introducir o cambiar el coste del material, el cambio se realiza en todos los tipos de material.

Mueva volúmenes para reducir los costes de almacenamiento

Según los análisis mostrados y las comparaciones de costes en medios, puede trasladar volúmenes a un almacenamiento menos costoso en niveles locales.

Solo se puede comparar y mover un volumen cada vez.

Pasos

1. Después de habilitar la visualización de costo de medios, haga clic en **almacenamiento > niveles** y, a continuación, haga clic en **volúmenes**.
2. Para comparar las opciones de destino de un volumen, haga clic en ⋮ Para el volumen, haga clic en **mover**.
3. En la pantalla **Seleccionar nivel local de destino**, seleccione niveles de destino para mostrar la diferencia de coste estimada.
4. Después de comparar las opciones, seleccione el nivel deseado y haga clic en **mover**.

Control de acceso basado en roles con Análisis del sistema de archivos

A partir de ONTAP 9.12.1, ONTAP incluye un rol predefinido denominado control de acceso basado en roles (RBAC) `admin-no-fsa`. La `admin-no-fsa` el rol concede privilegios a nivel de administrador, pero impide que el usuario realice operaciones relacionadas con `files` Extremo (es decir, análisis del sistema de archivos) en la interfaz de línea de comandos de ONTAP, la API DE REST y System Manager.

Para obtener más información sobre `admin-no-fsa` función, consulte Roles predefinidos para administradores de clúster.

Si utiliza una versión de ONTAP publicada antes de ONTAP 9.12.1, tendrá que crear un rol dedicado para controlar el acceso al análisis del sistema de archivos. En las versiones de ONTAP anteriores a ONTAP 9.12.1, debe configurar los permisos de RBAC a través de la interfaz de línea de comandos de ONTAP o la API DE REST de ONTAP.

System Manager

A partir de ONTAP 9.12.1, puede configurar permisos de RBAC para análisis de sistemas de archivos con System Manager.

Pasos

1. Seleccione **Cluster > Settings**. En **Seguridad**, vaya a **usuarios y roles** y seleccione →.
2. En **roles**, seleccione + Add .
3. Escriba un nombre para el rol. En atributos de función, configure el acceso o las restricciones para la función de usuario proporcionando el adecuado "Extremos de API". Consulte la tabla siguiente para ver las rutas principales y las rutas secundarias para configurar restricciones o acceso al análisis del sistema de archivos.

Restricción	Ruta primaria	Ruta secundaria
Seguimiento de actividad en volúmenes	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Seguimiento de actividad en las SVM	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Todas las operaciones de análisis del sistema de archivos	`/api/storage/volumes`	`/:uuid/files`

   Puede utilizar `/*/` En lugar de un UUID para establecer la política para todos los volúmenes o SVM en el extremo.

   Elija los privilegios de acceso para cada extremo.

4. Seleccione **Guardar**.
5. Para asignar el rol a un usuario o a un usuario, consulte Control del acceso de administradores.

CLI

Si utiliza una versión de ONTAP publicada antes de ONTAP 9.12.1, utilice la interfaz de línea de comandos de ONTAP para crear un rol personalizado.

Pasos

1. Cree una función predeterminada para tener acceso a todas las funciones.

   Esto debe hacerse antes de crear la función restrictiva para asegurarse de que la función sólo se limita en el seguimiento de actividad:

   ```
   security login role create -cmddirname DEFAULT -access all -role
   storageAdmin
   ```

2. Cree el rol restrictivo:

   ```
   security login role create -cmddirname "volume file show-disk-usage"
   -access none -role storageAdmin
   ```

3. Autorice a los roles para acceder a los servicios web de la SVM:

   - `rest` Para llamadas a la API DE REST
   - `security` para protección mediante contraseña
   - `sysmgr` Para acceder a System Manager

     ```
     vserver services web access create -vserver svm-name -name_ -name rest
     -role storageAdmin
     ```

     ```
     vserver services web access create -vserver svm-name -name security
     -role storageAdmin
     ```

   ```
   vserver services web access create -vserver svm-name -name sysmgr -role
   storageAdmin
   ```

4. Cree un usuario.

   Debe emitir un comando CREATE distinto para cada aplicación que desee aplicar al usuario. Llamar crea varias veces en el mismo usuario simplemente aplica todas las aplicaciones a ese usuario y no crea un nuevo usuario cada vez. La `http` El parámetro del tipo de aplicación se aplica a la API REST de ONTAP y System Manager.

   ```
   security login create -user-or-group-name storageUser -authentication
   -method password -application http -role storageAdmin
   ```

5. Ahora, con las credenciales de usuario nuevas, puede iniciar sesión en System Manager o usar la API DE REST de ONTAP para acceder a los datos de análisis de sistemas de archivos.

Más información

- Roles predefinidos para administradores de clúster
- Controle el acceso de administradores con System Manager
- "Obtenga más información acerca de los roles de RBAC y la API DE REST de ONTAP"

Consideraciones para el análisis del sistema de archivos

Debe conocer ciertos límites de uso e impactos de rendimiento potenciales asociados

con la implementación de los análisis del sistema de archivos.

Relaciones protegidas por SVM

Si ha habilitado File System Analytics en los volúmenes que contienen SVM se encuentran en una relación de protección, los datos de análisis no se replican en la SVM de destino. Si la SVM de origen debe volver a sincronizarse en una operación de recuperación, debe volver a habilitar manualmente los análisis de los volúmenes deseados una vez que se recupera.

Consideraciones de rendimiento

En algunos casos, la activación del análisis del sistema de archivos podría afectar negativamente al rendimiento durante la recopilación inicial de metadatos. Esto se suele ver en sistemas con un aprovechamiento máximo. Para evitar habilitar análisis en dichos sistemas, puede utilizar las herramientas de supervisión del rendimiento de System Manager de ONTAP.

Si experimenta un aumento significativo en la latencia, consulte el artículo de la base de conocimientos "Una latencia elevada o fluctuante después de activar el análisis del sistema de archivos ONTAP de NetApp".

Consideraciones sobre la adquisición

Cuando se habilita el análisis de capacidad, ONTAP realiza un análisis de inicialización para los análisis de capacidad. El análisis accede a los metadatos de todos los archivos de los volúmenes para los que están habilitados los análisis de capacidad. No se leen datos de archivos durante el análisis. A partir de ONTAP 9.14.1, puede realizar un seguimiento del progreso del análisis con la API REST, en la pestaña **Explorer** del Administrador del sistema o con el `volume analytics show` Comando de la CLI. Si hay un evento de limitación, ONTAP proporciona una notificación.

Una vez que se completa el análisis, File System Analytics se actualiza continuamente en tiempo real a medida que el sistema de archivos cambia sin necesidad de volver a ejecutar el análisis.

El tiempo necesario para la exploración es proporcional al número de directorios y archivos del volumen. Como el análisis recoge metadatos, el tamaño del archivo no afecta el tiempo de análisis.

Para obtener más información sobre la secuencia de inicialización, consulte "TR-4867: Directrices de prácticas recomendadas para análisis de sistemas de archivos".

Mejores prácticas

Debe iniciar el análisis en los volúmenes que no comparten agregados. Puede ver qué agregados alojan actualmente los volúmenes con el comando:

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

Mientras se ejecuta el análisis, los volúmenes siguen sirviendo al tráfico de cliente. Se recomienda iniciar la exploración durante los períodos en los que se anticipa un tráfico de cliente más bajo.

Si aumenta el tráfico del cliente, consumirá recursos del sistema y el análisis tardará más tiempo.

A partir de ONTAP 9.12.1, se puede pausar la recogida de datos en System Manager y con la CLI de ONTAP.

- Si utiliza la CLI de ONTAP:
  - Puede pausar la recopilación de datos con el comando: `volume analytics initialization pause -vserver svm_name -volume volume_name`

- Una vez que el tráfico del cliente se ha ralentizado, puede reanudar la recopilación de datos con el comando: `volume analytics initialization resume -vserver svm_name -volume volume_name`

- Si está utilizando System Manager, en la vista **Explorer** del menú de volumen, utilice los botones **Pausar la recopilación de datos** y **Reanudar la recopilación de datos** para administrar el escaneo.

Configuración de EMS

Información general de la configuración de EMS

Puede configurar ONTAP 9 para que envíe importantes notificaciones de eventos de EMS (Event Management System) directamente a una dirección de correo electrónico, un servidor de syslog, un host de capturas de protocolo simple de red de gestión (SNMP) o una aplicación webhook para que se le informe de inmediato de los problemas del sistema que requieren atención urgente.

Dado que las notificaciones de eventos importantes no están habilitadas de forma predeterminada, debe configurar EMS para que envíe notificaciones a una dirección de correo electrónico, a un servidor de syslog, a un host de capturas de SNMP o a una aplicación webhook.

Revise las versiones específicas de cada versión de "Referencia de ONTAP 9 EMS".

Si la asignación de eventos de EMS utiliza conjuntos de comandos ONTAP obsoletos (como el destino de eventos o la ruta de eventos), se recomienda actualizar la asignación. "Aprenda a actualizar el mapa de EMS desde comandos de ONTAP obsoletos".

Configure las notificaciones de eventos de EMS y los filtros con System Manager

Puede usar System Manager para configurar cómo el sistema de gestión de eventos (EMS) envía notificaciones de eventos de modo que se puedan notificar de los problemas del sistema que requieren su atención.

Versión de ONTAP	Con System Manager, podrá…
ONTAP 9.12.1 y versiones posteriores	Especifique el protocolo TLS (Seguridad de la capa de transporte) cuando envíe eventos a servidores de syslog remotos.
ONTAP 9.10.1 y posteriores	Configurar las direcciones de correo electrónico, los servidores de syslog y las aplicaciones de webhook, así como los hosts de capturas SNMP.
ONTAP 9.7 a 9.10.0	Configurar solo los hosts de capturas de SNMP. Es posible configurar otro destino de EMS con la interfaz de línea de comandos de ONTAP. Consulte "Información general de la configuración de EMS".

Puede realizar los siguientes procedimientos:

- [add-ems-destination]
- [create-ems-filter]

- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]
- [delete-ems-filter]

Información relacionada

- "Referencia de EMS de ONTAP"
- "Uso de la interfaz de línea de comandos para configurar los hosts de capturas de SNMP para recibir notificaciones de eventos"

Añada un destino de notificación de eventos de EMS

Puede usar System Manager para especificar dónde desea enviar mensajes de EMS.

A partir de ONTAP 9.12.1, los eventos EMS se pueden enviar a un puerto designado en un servidor de syslog remoto a través del protocolo de seguridad de la capa de transporte (TLS). Para obtener más detalles, consulte `event notification destination create` página de manual.

Pasos

1. Haga clic en **clúster > Configuración**.
2. En la sección **Administración de notificaciones**, haga clic en ⋮, A continuación, haga clic en **Ver destinos de evento**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Destinos de eventos**.
4. Haga clic en + Add .
5. Especifique un nombre, un tipo de destino EMS y filtros.

   Si es necesario, puede agregar un filtro nuevo. Haga clic en **Agregar un nuevo filtro de sucesos**.

6. Según el tipo de destino de EMS seleccionado, especifique lo siguiente:

Para configurar…	Especificar o seleccionar…
Host de capturas de SNMP	• Nombre de TrapHost
Correo electrónico (A partir de 9.10.1)	• Dirección de correo electrónico de destino • Servidor de correo • Dirección de correo electrónico del remitente

Servidor de syslog (A partir de 9.10.1)	• Nombre de host o dirección IP del servidor • Puerto de syslog (9.12.1 y posterior) • Transporte de syslog (a partir de 9.12.1) Al seleccionar **cifrado TCP** se activa el protocolo de seguridad de la capa de transporte (TLS). Si no se introduce ningún valor para **puerto Syslog**, se utiliza un valor predeterminado basado en la selección **Transporte Syslog**.
Webhook (A partir de 9.10.1)	• URL de Webhook • Autenticación de cliente (seleccione esta opción para especificar un certificado de cliente)

Cree un nuevo filtro de notificación de eventos EMS

A partir de ONTAP 9.10.1, es posible usar System Manager para definir nuevos filtros personalizados que especifiquen las reglas para el manejo de las notificaciones de EMS.

Pasos

1. Haga clic en **clúster > Configuración**.
2. En la sección **Administración de notificaciones**, haga clic en ⋮, A continuación, haga clic en **Ver destinos de eventos**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Filtros de sucesos**.
4. Haga clic en + Add .
5. Especifique un nombre y seleccione si desea copiar reglas de un filtro de eventos existente o agregar nuevas reglas.
6. En función de su elección, realice los siguientes pasos:

Si elige….	A continuación, realice estos pasos…
Copiar reglas del filtro de sucesos existente	1. Seleccione un filtro de sucesos existente. 2. Modifique las reglas existentes. 3. Si es necesario, agregue otras reglas haciendo clic en + Add .
Añadir nuevas reglas	Especifique el tipo, patrón de nombre, gravedad y tipo de captura SNMP para cada nueva regla.

Edite un destino de notificación de eventos de EMS

A partir de ONTAP 9.10.1, puede utilizar System Manager para cambiar la información del destino de notificaciones de eventos.

Pasos

1. Haga clic en **clúster > Configuración**.

2. En la sección **Administración de notificaciones**, haga clic en ⋮, A continuación, haga clic en **Ver destinos de evento**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Destinos de eventos**.
4. Junto al nombre del destino del evento, haga clic en ⋮, A continuación, haga clic en **Editar**.
5. Modifique la información del destino del evento y, a continuación, haga clic en **Guardar**.

Edite un filtro de notificación de eventos EMS

A partir de ONTAP 9.10.1, es posible usar System Manager para modificar los filtros personalizados y cambiar la forma en que se manejan las notificaciones de eventos.

> No puede modificar filtros definidos por el sistema.

Pasos

1. Haga clic en **clúster > Configuración**.
2. En la sección **Administración de notificaciones**, haga clic en ⋮, A continuación, haga clic en **Ver destinos de eventos**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Filtros de sucesos**.
4. Junto al nombre del filtro de eventos, haga clic en ⋮, A continuación, haga clic en **Editar**.
5. Modifique la información del filtro de sucesos y haga clic en **Guardar**.

Elimine un destino de notificación de eventos de EMS

A partir de ONTAP 9.10.1, es posible usar System Manager para eliminar un destino de notificación de eventos de EMS.

> No puede eliminar destinos SNMP.

Pasos

1. Haga clic en **clúster > Configuración**.
2. En la sección **Administración de notificaciones**, haga clic en ⋮, A continuación, haga clic en **Ver destinos de eventos**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Destinos de eventos**.
4. Junto al nombre del destino del evento, haga clic en ⋮, Luego haga clic en **Eliminar**.

Elimine un filtro de notificación de eventos EMS

A partir de ONTAP 9.10.1, se puede usar System Manager para eliminar filtros personalizados.

> No puede eliminar filtros definidos por el sistema.

Pasos

1. Haga clic en **clúster > Configuración**.
2. En la sección **Administración de notificaciones**, haga clic en ⋮, A continuación, haga clic en **Ver destinos de eventos**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Filtros de sucesos**.

4. Junto al nombre del filtro de eventos, haga clic en ⋮, A continuación, haga clic en **Eliminar**.

Configure las notificaciones de eventos de EMS con la CLI

Flujo de trabajo de configuración de EMS

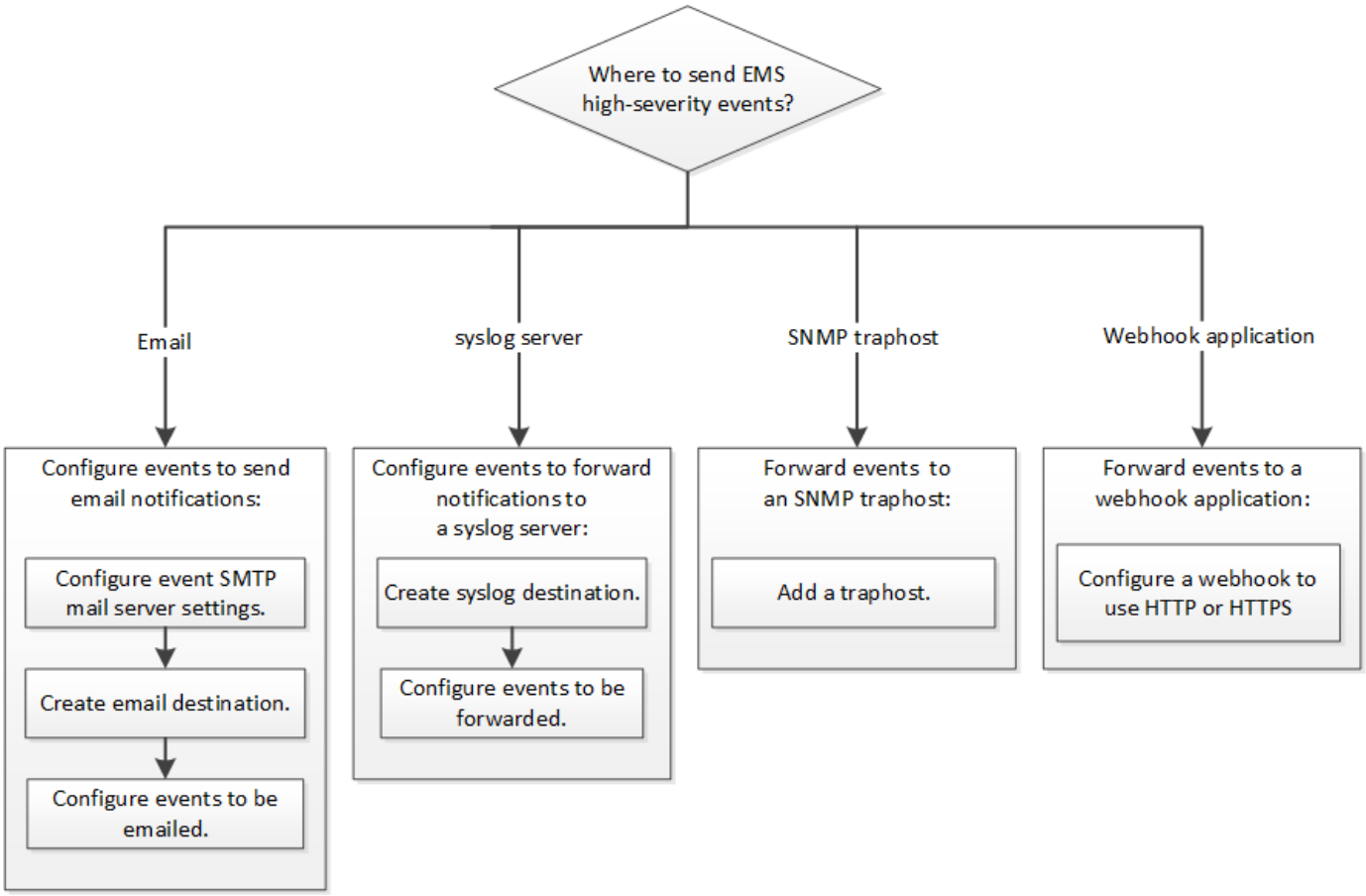
Debe configurar las notificaciones de eventos de EMS importantes para que se envíen como correo electrónico, se reenvíen a un servidor de syslog, se reenvíen a un host de capturas de SNMP o se reenvíen a una aplicación de webhook. Esto le ayuda a evitar interrupciones en el sistema tomando medidas correctivas de forma puntual.

Acerca de esta tarea

Si el entorno ya contiene un servidor de syslog para añadir los eventos registrados de otros sistemas, como servidores y aplicaciones, resulta más fácil utilizar el mismo servidor de syslog para enviar las notificaciones de eventos importantes de sistemas de almacenamiento.

Si el entorno no contiene ningún servidor de syslog, resulta más fácil usar un correo electrónico para enviar las notificaciones de eventos importantes.

Si ya ha reenviado notificaciones de eventos a un host de capturas de SNMP, es posible que desee supervisar dicho host de capturas para buscar eventos importantes.



Opciones

- Configure EMS para que envíe notificaciones de eventos.

Si desea que…	Consulte…
EMS envíe notificaciones de eventos importantes a una dirección de correo electrónico	Configure eventos de EMS importantes para que envíen notificaciones por correo electrónico
EMS reenvíe notificaciones de eventos importantes a un servidor de syslog	Configure eventos de EMS importantes para reenviar notificaciones a un servidor de syslog
EMS reenvíe notificaciones de eventos a un host de capturas de SNMP	Configure los hosts de capturas de SNMP para recibir notificaciones de eventos
Si desea que EMS reenvíe notificaciones de eventos a una aplicación webhook	Configure eventos EMS importantes para reenviar notificaciones a una aplicación webhook

Configure eventos de EMS importantes para que envíen notificaciones por correo electrónico

Para recibir notificaciones por correo electrónico acerca de los eventos más importantes, debe configurar EMS para que envíe mensajes por correo electrónico de los eventos que representan actividades importantes.

Lo que necesitará

El DNS debe haberse configurado en el clúster para resolver las direcciones de correo electrónico.

Acerca de esta tarea

Puede realizar esta tarea en cualquier momento que el clúster esté en ejecución. Para ello, introduzca los comandos en la línea de comandos de ONTAP.

Pasos

1. Configure las opciones del servidor de correo SMTP de eventos:

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

2. Cree un destino de correo electrónico para las notificaciones de eventos:

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

3. Configure los eventos importantes para que envíen notificaciones por correo electrónico:

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

Configuración de eventos de EMS importantes para reenviar notificaciones a un servidor de syslog

Para registrar las notificaciones de los eventos más graves en un servidor de syslog, debe configurar EMS para reenviar las notificaciones de los eventos que representan actividades importantes.

Lo que necesitará

El DNS debe haberse configurado en el clúster para resolver el nombre del servidor de syslog.

Acerca de esta tarea

Si el entorno no contiene un servidor de syslog para las notificaciones de eventos, primero debe crear uno. Si el entorno ya contiene un servidor de syslog para registrar eventos de otros sistemas, se recomienda usarlo para las notificaciones de eventos importantes.

Puede realizar esta tarea en cualquier momento que el clúster esté en ejecución. Para ello, introduzca los comandos en la CLI de ONTAP.

A partir de ONTAP 9.12.1, los eventos EMS se pueden enviar a un puerto designado en un servidor de syslog remoto a través del protocolo de seguridad de la capa de transporte (TLS). Hay dos nuevos parámetros disponibles:

`tcp-encrypted`

Cuando `tcp-encrypted` se especifica para la `syslog-transport`, ONTAP verifica la identidad del host de destino validando su certificado. El valor predeterminado es `udp-unencrypted`.

`syslog-port`

El valor predeterminado `syslog-port` el parámetro depende del valor del `syslog-transport` parámetro. Si `syslog-transport` se establece en `tcp-encrypted`, `syslog-port` tiene el valor predeterminado 6514.

Para obtener más detalles, consulte `event notification destination create` página de manual.

Pasos

1. Cree un destino de servidor de syslog para los eventos importantes:

   `event notification destination create -name` *`syslog-ems`* `-syslog` *`syslog-server-address`* `-syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   A partir de ONTAP 9.12.1, se pueden especificar los siguientes valores para `syslog-transport`:

   - `udp-unencrypted` - Protocolo de datagramas de usuario sin seguridad
   - `tcp-unencrypted` - Protocolo de control de la transmisión sin seguridad
   - `tcp-encrypted` - Protocolo de control de la transmisión con seguridad de la capa de transporte (TLS)

   El protocolo predeterminado es `udp-unencrypted`.

2. Configure los eventos importantes de manera que reenvíen notificaciones al servidor de syslog:

   `event notification create -filter-name` *`important-events`* `-destinations` *`syslog-ems`*

Configure los hosts de capturas de SNMP para recibir notificaciones de eventos

Para recibir notificaciones de eventos en un host de capturas de SNMP, debe configurar un host de capturas.

Lo que necesitará

- Se debe habilitar SNMP y las capturas de SNMP en el clúster.

  SNMP y las capturas de SNMP se habilitan de forma predeterminada.

- El DNS debe haberse configurado en el clúster para resolver los nombres de host de capturas.

Acerca de esta tarea

Si no tiene un host de capturas de SNMP configurado para recibir notificaciones de eventos (capturas de SNMP), debe añadir uno.

Puede realizar esta tarea en cualquier momento que el clúster esté en ejecución. Para ello, introduzca los comandos en la línea de comandos de ONTAP.

Paso

1. Si su entorno no tiene un host de capturas de SNMP configurado para recibir notificaciones de eventos, añada uno:

   ```
   system snmp traphost add -peer-address snmp_traphost_name
   ```

   Todas las notificaciones de eventos que SNMP admite de forma predeterminada se reenvían al host de capturas de SNMP.

Configure eventos EMS importantes para reenviar notificaciones a una aplicación webhook

Puede configurar ONTAP para reenviar notificaciones de eventos importantes a una aplicación webhook. Los pasos de configuración necesarios dependen del nivel de seguridad que elija.

Prepare la configuración del reenvío de eventos EMS

Hay varios conceptos y requisitos que debe tener en cuenta antes de configurar ONTAP para reenviar notificaciones de eventos a una aplicación webhook.

Aplicación Webhook

Necesita una aplicación de webhook capaz de recibir las notificaciones de eventos de ONTAP. Un webhook es una rutina de devolución de llamada definida por el usuario que amplía la capacidad de la aplicación remota o el servidor donde se ejecuta. El cliente llama o activa a los enlaces web (en este caso ONTAP) enviando una solicitud HTTP a la dirección URL de destino. Específicamente, ONTAP envía una solicitud HTTP POST al servidor que aloja la aplicación webhook junto con los detalles de notificación de eventos formateados en XML.

Opciones de seguridad

Hay varias opciones de seguridad disponibles en función de cómo se utilice el protocolo de seguridad de la capa de transporte (TLS). La opción que elija determina la configuración de ONTAP que requiere.

TLS es un protocolo criptográfico que se utiliza ampliamente en Internet. Proporciona privacidad, así como integridad de datos y autenticación mediante uno o varios certificados de clave pública. Los certificados son emitidos por autoridades de certificados de confianza.

HTTP

Es posible utilizar HTTP para transportar las notificaciones de eventos. Con esta configuración, la conexión no es segura. Las identidades del cliente ONTAP y de la aplicación webhook no se verifican. Además, el tráfico de red no está cifrado ni protegido. Consulte "Configure un destino de webhook para utilizar HTTP" para obtener detalles de la configuración.

HTTPS

Para mayor seguridad, puede instalar un certificado en el servidor que aloja la rutina de webhook. ONTAP utiliza el protocolo HTTPS para verificar la identidad del servidor de aplicaciones webhook, así como de ambas partes, para garantizar la privacidad e integridad del tráfico de red. Consulte "Configure un destino de webhook para utilizar HTTPS" para obtener detalles de la configuración.

HTTPS con autenticación mutua

Puede mejorar aún más la seguridad HTTPS mediante la instalación de un certificado de cliente en el sistema ONTAP que emite las solicitudes webbook. Además ONTAP de verificar la identidad del servidor de aplicaciones webhook y proteger el tráfico de red, la aplicación webhook verifica la identidad del cliente ONTAP. Esta autenticación de par bidireccional se conoce como *Mutual TLS*. Consulte "Configure un destino de webhook para utilizar HTTPS con autenticación mutua" para obtener detalles de la configuración.

Información relacionada

- "Protocolo de seguridad de la capa de transporte (TLS) versión 1.3"

Configure un destino de webhook para utilizar HTTP

Puede configurar ONTAP para reenviar notificaciones de eventos a una aplicación webhook mediante HTTP. Esta es la opción menos segura pero la más sencilla de configurar.

Pasos

1. Cree un nuevo destino `restapi-ems` para recibir los eventos:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   En el comando anterior, debe utilizar el esquema **HTTP** para el destino.

2. Cree una notificación que vincule el `important-events` filtre con la `restapi-ems` destino:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Configure un destino de webhook para utilizar HTTPS

Puede configurar ONTAP para reenviar notificaciones de eventos a una aplicación de webhook mediante HTTPS. ONTAP utiliza el certificado de servidor para confirmar la identidad de la aplicación webhook y proteger el tráfico de red.

Antes de empezar

- Genere una clave privada y un certificado para el servidor de aplicaciones de webhook
- Tenga el certificado raíz disponible para instalar en ONTAP

Pasos

1. Instale la clave privada y los certificados del servidor adecuados en el servidor que aloja la aplicación webhook. Los pasos de configuración específicos dependen del servidor.
2. Instale el certificado raíz de servidor en ONTAP:

   ```
   security certificate install -type server-ca
   ```

   El comando solicitará el certificado.

3. Cree el `restapi-ems` destino para recibir los eventos:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   En el comando anterior, debe usar el esquema **HTTPS** para el destino.

4. Cree la notificación que vincula el `important-events` filtrar con el nuevo `restapi-ems` destino:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Configure un destino de webhook para utilizar HTTPS con autenticación mutua

Puede configurar ONTAP para reenviar notificaciones de eventos a una aplicación de webhook mediante HTTPS con autenticación mutua. Con esta configuración hay dos certificados. ONTAP utiliza el certificado de servidor para confirmar la identidad de la aplicación webhook y proteger el tráfico de red. Además, la aplicación que aloja el webhook utiliza el certificado de cliente para confirmar la identidad del cliente ONTAP.

Antes de empezar

Debe hacer lo siguiente antes de configurar ONTAP:

- Genere una clave privada y un certificado para el servidor de aplicaciones de webhook
- Tenga el certificado raíz disponible para instalar en ONTAP
- Genere una clave privada y un certificado para el cliente ONTAP

Pasos

1. Realice los dos primeros pasos de la tarea "Configure un destino de webhook para utilizar HTTPS" Instalar el certificado de servidor para que ONTAP pueda verificar la identidad del servidor.
2. Instale los certificados raíz e intermedios adecuados en la aplicación webhook para validar el certificado de cliente.
3. Instale el certificado de cliente en ONTAP:

   ```
   security certificate install -type client
   ```

   El comando solicitará la clave privada y el certificado.

4. Cree el `restapi-ems` destino para recibir los eventos:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application> -certificate-authority <issuer of the client
   certificate> -certificate-serial <serial of the client certificate>
   ```

En el comando anterior, debe utilizar el esquema **HTTPS** para el destino.

5. Cree la notificación que vincula el `important-events` filtrar con el nuevo `restapi-ems` destino:

   ```
   event notification create -filter-name important-events -destinations restapi-ems
   ```

Actualizar asignación de eventos de EMS obsoleta

Modelos de asignación de eventos EMS

Antes de ONTAP 9.0, los eventos de EMS solo podían asignarse a destinos de eventos en función de la correspondencia entre el patrón de nombres de eventos. Los conjuntos de comandos de la ONTAP (`event destination`, `event route`) Que usan este modelo siguen estando disponibles en las últimas versiones de ONTAP, pero han sido obsoletas empezando por ONTAP 9.0.

A partir de ONTAP 9.0, la práctica recomendada para la asignación de destinos de eventos EMS de ONTAP es utilizar el modelo de filtro de eventos más escalable en el que la coincidencia de patrones se realiza en varios campos, mediante la `event filter`, `event notification`, y. `event notification destination` conjuntos de comandos.

Si la asignación de EMS se configura con los comandos obsoletos, debe actualizar la asignación para utilizar los `event filter`, `event notification`, y. `event notification destination` conjuntos de comandos.

Hay dos tipos de destinos de eventos:

1. **Destinos generados por el sistema**: Hay cinco destinos de eventos generados por el sistema (creados de forma predeterminada)
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     Algunos de los destinos generados por el sistema tienen un propósito especial. Por ejemplo, el destino asup enruta los eventos callhome.* al módulo AutoSupport de ONTAP para generar mensajes AutoSupport.

2. **Destinos creados por el usuario**: Se crean manualmente mediante el `event destination create` comando.

```
cluster-1::event*> destination show
                                                                    Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
traphost         -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

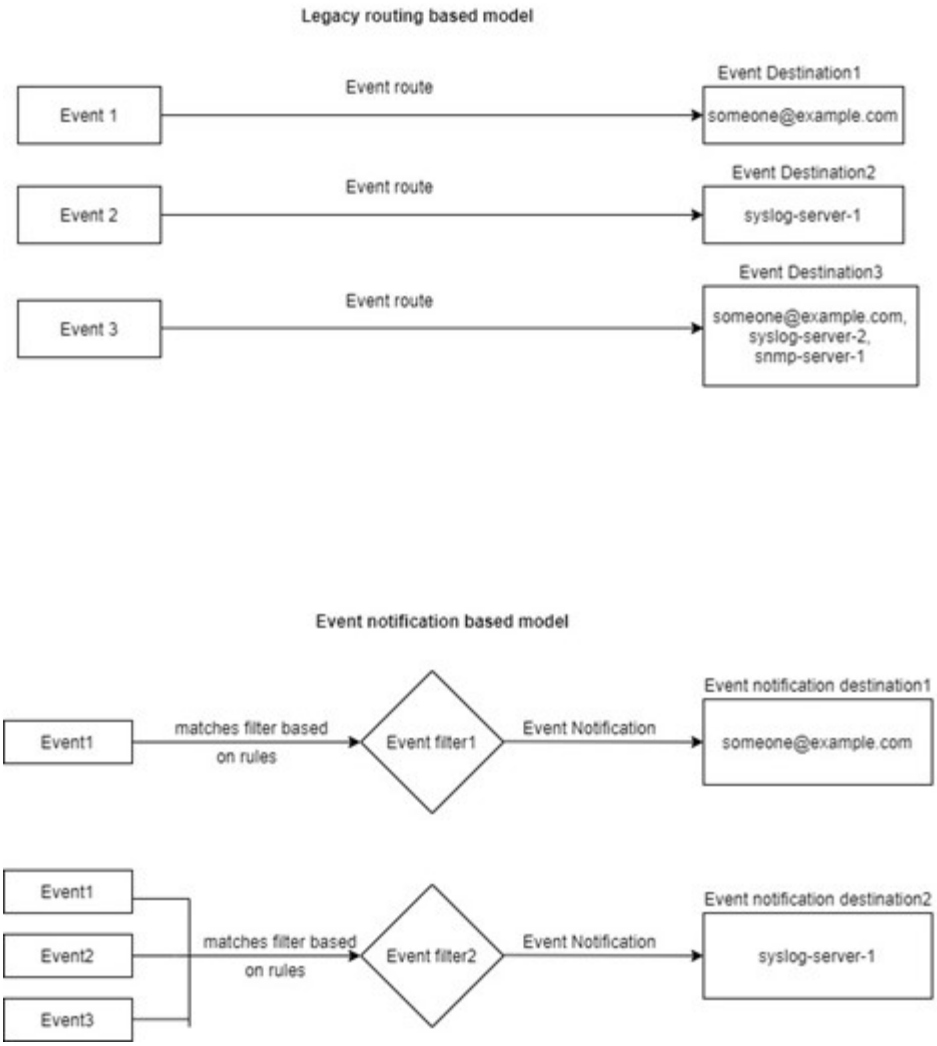
En el modelo obsoleto, los eventos EMS se asignan individualmente a un destino mediante el `event route add-destinations` comando.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                    Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
--------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

El nuevo mecanismo de notificaciones de eventos de EMS más escalable se basa en filtros de eventos y destinos de notificaciones de eventos. Consulte el siguiente artículo de la base de conocimientos para obtener información detallada sobre el nuevo mecanismo de notificación de eventos:

- "Descripción general del sistema de gestión de eventos para ONTAP 9"



Actualice la asignación de eventos de EMS desde comandos ONTAP obsoletos

Si la asignación de eventos de EMS se configura actualmente con los conjuntos de comandos ONTAP obsoletos (`event destination`, `event route`), debe seguir este procedimiento para actualizar la asignación para utilizar `event filter`, `event notification`, y. `event notification destination` conjuntos de comandos.

Pasos

1. Enumere todos los destinos de eventos del sistema mediante `event destination show` comando.

```
cluster-1::event*> destination show

Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

2. Para cada destino, enumere los eventos que se están asignando con el `event route show -destinations <destination name>` comando.

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

3. Cree una correspondiente `event filter` lo que incluye todos estos subconjuntos de eventos.
Por ejemplo, si desea incluir solo el `raid.aggr.*` sucesos, utilice un comodín para el `message-name` parámetro al crear el filtro. También puede crear filtros para eventos individuales.

> Es posible crear hasta 50 filtros de eventos.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. Cree un `event notification destination` para cada uno de los `event destination` Extremos (es decir, SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  ---------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. Cree una notificación de eventos asignando el filtro de eventos al destino de notificación de eventos.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                     Destinations
---- ------------------------------  -----------------
1    default-trap-events             snmp-traphost
2    asup_events                     dest1
2 entries were displayed.
```

6. Repita los pasos 1-5 para cada uno `event destination` eso tiene una `event route` asignación.

Los eventos enrutados a destinos de SNMP se deben asignar a `snmp-traphost` destino de notificaciones de eventos. El destino del host de capturas de SNMP utiliza el host de capturas de SNMP configurado del sistema.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

                Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```