Utilice la monitorización SNMP

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Utilice la monitorización SNMP

Utilice la monitorización SNMP

Si desea supervisar StorageGRID mediante el Protocolo simple de administración de red (SNMP), debe configurar el agente SNMP que se incluye con StorageGRID.

- "Configurar el agente SNMP"
- "Actualizar el agente SNMP"

Capacidades

Cada nodo StorageGRID ejecuta un agente SNMP, o demonio, que proporciona una MIB. La MIB de StorageGRID contiene definiciones de tablas y notificaciones para alertas. La MIB también contiene información de descripción del sistema, como la plataforma y el número de modelo de cada nodo. Cada nodo StorageGRID también admite un subconjunto de objetos MIB-II.

Ver"Acceder a archivos MIB" Si desea descargar los archivos MIB en los nodos de su red.

Inicialmente, SNMP está deshabilitado en todos los nodos. Cuando configura el agente SNMP, todos los nodos StorageGRID reciben la misma configuración.

El agente SNMP de StorageGRID admite las tres versiones del protocolo SNMP. Proporciona acceso MIB de solo lectura para consultas y puede enviar dos tipos de notificaciones basadas en eventos a un sistema de administración:

Trampas

Las trampas son notificaciones enviadas por el agente SNMP que no requieren reconocimiento por parte del sistema de administración. Las trampas sirven para notificar al sistema de administración que algo ha sucedido dentro de StorageGRID, como por ejemplo la activación de una alerta.

Las trampas son compatibles con las tres versiones de SNMP.

Informa

Los informes son similares a las trampas, pero requieren el reconocimiento del sistema de gestión. Si el agente SNMP no recibe un acuse de recibo dentro de un período de tiempo determinado, vuelve a enviar el informe hasta que recibe un acuse de recibo o se alcanza el valor máximo de reintentos.

Los informes son compatibles con SNMPv2c y SNMPv3.

Las notificaciones de trampa e información se envían en los siguientes casos:

- Se activa una alerta predeterminada o personalizada en cualquier nivel de gravedad. Para suprimir las notificaciones SNMP de una alerta, debe"configurar un silencio" para la alerta. Las notificaciones de alerta son enviadas por el"Nodo de administración del remitente preferido" .

  Cada alerta se asigna a uno de tres tipos de trampa según el nivel de gravedad de la alerta: activeMinorAlert, activeMajorAlert y activeCriticalAlert. Para obtener una lista de las alertas que pueden activar estas trampas, consulte la"Referencia de alertas" .

Compatibilidad con versiones SNMP

La tabla proporciona un resumen de alto nivel de lo que se admite para cada versión de SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Consultas (GET y GETNEXT)	Consultas MIB de solo lectura	Consultas MIB de solo lectura	Consultas MIB de solo lectura
Autenticación de consultas	Cadena comunitaria	Cadena comunitaria	Modelo de seguridad basado en el usuario (USM)
Notificaciones (TRAMPA e INFORME)	Solo trampas	Atrapa e informa	Atrapa e informa
Autenticación de notificaciones	Comunidad de trampa predeterminada o una cadena de comunidad personalizada para cada destino de trampa	Comunidad de trampa predeterminada o una cadena de comunidad personalizada para cada destino de trampa	Usuario USM para cada destino de trampa

Limitaciones

- StorageGRID admite acceso MIB de solo lectura. No se admite el acceso de lectura y escritura.
- Todos los nodos de la red reciben la misma configuración.
- SNMPv3: StorageGRID no admite el modo de soporte de transporte (TSM).
- SNMPv3: el único protocolo de autenticación admitido es SHA (HMAC-SHA-96).
- SNMPv3: el único protocolo de privacidad admitido es AES.

Configurar el agente SNMP

Puede configurar el agente SNMP de StorageGRID para utilizar un sistema de administración SNMP de terceros para acceso y notificaciones de MIB de solo lectura.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso root" .

Acerca de esta tarea

El agente SNMP de StorageGRID admite SNMPv1, SNMPv2c y SNMPv3. Puede configurar el agente para una o más versiones. Para SNMPv3, solo se admite la autenticación del modelo de seguridad de usuario (USM).

Todos los nodos de la red utilizan la misma configuración SNMP.

Especificar la configuración básica

Como primer paso, habilite el agente SMNP de StorageGRID y proporcione información básica.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Monitoreo** > **Agente SNMP**.

   Aparece la página del agente SNMP.

2. Para habilitar el agente SNMP en todos los nodos de la red, seleccione la casilla de verificación **Habilitar SNMP**.
3. Introduzca la siguiente información en la sección Configuración básica.

Campo	Descripción
Contacto del sistema	Opcional. El contacto principal del sistema StorageGRID , que se devuelve en los mensajes SNMP como sysContact. El contacto del sistema normalmente es una dirección de correo electrónico. Este valor se aplica a todos los nodos del sistema StorageGRID . **Contacto del sistema** puede tener un máximo de 255 caracteres.
Ubicación del sistema	Opcional. La ubicación del sistema StorageGRID , que se devuelve en los mensajes SNMP como sysLocation. La ubicación del sistema puede ser cualquier información que sea útil para identificar dónde se encuentra su sistema StorageGRID . Por ejemplo, puede utilizar la dirección de una instalación. Este valor se aplica a todos los nodos del sistema StorageGRID . **Ubicación del sistema** puede tener un máximo de 255 caracteres.
Habilitar notificaciones del agente SNMP	• Si se selecciona, el agente SNMP de StorageGRID envía notificaciones de captura e información. • Si no se selecciona, el agente SNMP admite acceso MIB de solo lectura, pero no envía ninguna notificación SNMP.
Habilitar trampas de autenticación	Si se selecciona, el agente SNMP de StorageGRID envía trampas de autenticación si recibe mensajes de protocolo autenticados incorrectamente.

Introduzca cadenas de la comunidad

Si utiliza SNMPv1 o SNMPv2c, complete la sección Cadenas de comunidad.

Cuando el sistema de administración consulta la MIB de StorageGRID , envía una cadena de comunidad. Si la cadena de comunidad coincide con uno de los valores especificados aquí, el agente SNMP envía una respuesta al sistema de administración.

Pasos

1. Para **Comunidad de solo lectura**, ingrese opcionalmente una cadena de comunidad para permitir el acceso MIB de solo lectura en direcciones de agente IPv4 e IPv6.

   Para garantizar la seguridad de su sistema StorageGRID , no utilice "público" como cadena de comunidad. Si deja este campo en blanco, el agente SNMP utiliza la ID de red de su sistema StorageGRID como cadena de comunidad.

   Cada cadena de comunidad puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

2. Seleccione **Agregar otra cadena de comunidad** para agregar cadenas adicionales.

   Se permiten hasta cinco cuerdas.

Crear destinos de trampa

Utilice la pestaña Destinos de trampa en la sección Otras configuraciones para definir uno o más destinos para las notificaciones de trampa o información de StorageGRID . Cuando habilita el agente SNMP y selecciona **Guardar**, StorageGRID envía notificaciones a cada destino definido cuando se activan alertas. También se envían notificaciones estándar para las entidades MIB-II compatibles (por ejemplo, ifDown y coldStart).

Pasos

1. Para el campo **Comunidad de trampa predeterminada**, ingrese opcionalmente la cadena de comunidad predeterminada que desea utilizar para los destinos de trampa SNMPv1 o SNMPv2.

   Según sea necesario, puede proporcionar una cadena de comunidad diferente ("personalizada") cuando defina un destino de trampa específico.

   La comunidad de trampa predeterminada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

2. Para agregar un destino de trampa, seleccione **Crear**.
3. Seleccione qué versión de SNMP se utilizará para este destino de trampa.
4. Complete el formulario Crear destino de trampa para la versión que seleccionó.

SNMPv1

Si seleccionó SNMPv1 como versión, complete estos campos.

Campo	Descripción
Tipo	Debe ser una trampa para SNMPv1.
Host	Una dirección IPv4 o IPv6 o un nombre de dominio completo (FQDN) para recibir la trampa.
Puerto	Utilice 162, que es el puerto estándar para trampas SNMP, a menos que deba utilizar otro valor.
Protocolo	Utilice UDP, que es el protocolo de trampa SNMP estándar, a menos que necesite utilizar TCP.
Cadena comunitaria	Utilice la comunidad de trampa predeterminada, si se especificó una, o ingrese una cadena de comunidad personalizada para este destino de trampa. La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

SNMPv2c

Si seleccionó SNMPv2c como versión, complete estos campos.

Campo	Descripción
Tipo	Si el destino se utilizará para trampas o informes.
Host	Una dirección IPv4 o IPv6 o FQDN para recibir la trampa.
Puerto	Utilice 162, que es el puerto estándar para trampas SNMP a menos que deba utilizar otro valor.
Protocolo	Utilice UDP, que es el protocolo de trampa SNMP estándar, a menos que necesite utilizar TCP.
Cadena comunitaria	Utilice la comunidad de trampa predeterminada, si se especificó una, o ingrese una cadena de comunidad personalizada para este destino de trampa. La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

SNMPv3

Si seleccionó SNMPv3 como versión, complete estos campos.

Campo	Descripción
Tipo	Si el destino se utilizará para trampas o informes.
Host	Una dirección IPv4 o IPv6 o FQDN para recibir la trampa.
Puerto	Utilice 162, que es el puerto estándar para trampas SNMP a menos que deba utilizar otro valor.
Protocolo	Utilice UDP, que es el protocolo de trampa SNMP estándar, a menos que necesite utilizar TCP.
Usuario de USM	El usuario USM que se utilizará para la autenticación. • Si seleccionó **Trampa**, solo se mostrarán los usuarios de USM sin identificaciones de motor autorizadas. • Si seleccionó **Informar**, solo se mostrarán los usuarios de USM con ID de motor autorizados. • Si no se muestran usuarios: i. Crea y guarda el destino de la trampa. ii. Ir aCrear usuarios de USM y crear el usuario. iii. Regrese a la pestaña Destinos de trampa, seleccione el destino guardado de la tabla y seleccione **Editar**. iv. Seleccione el usuario.

5. Seleccione **Crear**.

   Se crea el destino de la trampa y se agrega a la tabla.

Crear direcciones de agentes

Opcionalmente, utilice la pestaña Direcciones del agente en la sección Otras configuraciones para especificar una o más "direcciones de escucha". Estas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas.

Si no configura una dirección de agente, la dirección de escucha predeterminada es el puerto UDP 161 en todas las redes StorageGRID .

Pasos

1. Seleccione **Crear**.
2. Introduzca la siguiente información.

Campo	Descripción
Protocolo de Internet	Si esta dirección utilizará IPv4 o IPv6. De forma predeterminada, SNMP utiliza IPv4.
Protocolo de transporte	Si esta dirección utilizará UDP o TCP. De forma predeterminada, SNMP utiliza UDP.
Red StorageGRID	En qué red StorageGRID escuchará el agente. • Redes de cuadrícula, administración y cliente: el agente SNMP escuchará consultas en las tres redes. • Red de cuadrícula • Red de administración • Red de clientes **Nota**: Si utiliza la red del cliente para datos no seguros y crea una dirección de agente para la red del cliente, tenga en cuenta que el tráfico SNMP también será inseguro.
Puerto	Opcionalmente, el número de puerto en el que debe escuchar el agente SNMP. El puerto UDP predeterminado para un agente SNMP es 161, pero puede ingresar cualquier número de puerto no utilizado. **Nota**: Cuando guarda el agente SNMP, StorageGRID abre automáticamente los puertos de dirección del agente en el firewall interno. Debe asegurarse de que todos los firewalls externos permitan el acceso a estos puertos.

3. Seleccione **Crear**.

   Se crea la dirección del agente y se agrega a la tabla.

Crear usuarios USM

Si está utilizando SNMPv3, utilice la pestaña Usuarios USM en la sección Otras configuraciones para definir los usuarios USM que están autorizados a consultar la MIB o a recibir trampas e informes.

> Los destinos *inform* de SNMPv3 deben tener usuarios con ID de motor. El destino *trap* de SNMPv3 no puede tener usuarios con ID de motor.

Estos pasos no se aplican si solo utiliza SNMPv1 o SNMPv2c.

Pasos

1. Seleccione **Crear**.

2. Introduzca la siguiente información.

Campo	Descripción
Nombre de usuario	Un nombre único para este usuario de USM. Los nombres de usuario pueden tener un máximo de 32 caracteres y no pueden contener espacios en blanco. El nombre de usuario no se puede cambiar una vez creado el usuario.
Acceso MIB de solo lectura	Si se selecciona, este usuario debe tener acceso de solo lectura a la MIB.
Identificación de motor autorizada	Si este usuario se utilizará en un destino de información, el ID del motor autorizado para este usuario. Ingrese de 10 a 64 caracteres hexadecimales (de 5 a 32 bytes) sin espacios. Este valor es necesario para los usuarios de USM que se seleccionarán en los destinos de trampa para los informes. Este valor no está permitido para los usuarios de USM que se seleccionarán en destinos de trampas. **Nota**: Este campo no se muestra si seleccionó **Acceso MIB de solo lectura** porque los usuarios de USM que tienen acceso MIB de solo lectura no pueden tener ID de motor.
Nivel de seguridad	El nivel de seguridad para el usuario USM: • **authPriv**: Este usuario se comunica con autenticación y privacidad (cifrado). Debe especificar un protocolo de autenticación y una contraseña y un protocolo de privacidad y una contraseña. • **authNoPriv**: Este usuario se comunica con autenticación y sin privacidad (sin cifrado). Debe especificar un protocolo de autenticación y una contraseña.
Protocolo de autenticación	Siempre configúrelo en SHA, que es el único protocolo compatible (HMAC-SHA-96).
Password	La contraseña que este usuario utilizará para la autenticación.
Protocolo de privacidad	Solo se muestra si seleccionó **authPriv** y siempre se configura en AES, que es el único protocolo de privacidad compatible.
Password	Sólo se muestra si seleccionó **authPriv**. La contraseña que este usuario utilizará para su privacidad.

3. Seleccione **Crear**.

   Se crea el usuario USM y se agrega a la tabla.

4. Cuando haya completado la configuración del agente SNMP, seleccione **Guardar**.

   La nueva configuración del agente SNMP se vuelve activa.

Actualizar el agente SNMP

Puede deshabilitar las notificaciones SNMP, actualizar cadenas de comunidad o agregar o eliminar direcciones de agentes, usuarios USM y destinos de trampa.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso root" .

Acerca de esta tarea

Ver"Configurar el agente SNMP" para obtener detalles sobre cada campo en la página del agente SNMP. Debes seleccionar **Guardar** en la parte inferior de la página para confirmar cualquier cambio que realices en cada pestaña.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Monitoreo** > **Agente SNMP**.

   Aparece la página del agente SNMP.

2. Para deshabilitar el agente SNMP en todos los nodos de la red, desmarque la casilla **Habilitar SNMP** y seleccione **Guardar**.

   Si vuelve a habilitar el agente SNMP, se conservarán todas las configuraciones de SNMP anteriores.

3. Opcionalmente, actualice la información en la sección Configuración básica:
   a. Según sea necesario, actualice el **Contacto del sistema** y la **Ubicación del sistema**.
   b. De manera opcional, seleccione o desmarque la casilla de verificación **Habilitar notificaciones del agente SNMP** para controlar si el agente SNMP de StorageGRID envía notificaciones de captura e información.

      Cuando esta casilla de verificación no está marcada, el agente SNMP admite acceso MIB de solo lectura, pero no envía notificaciones SNMP.

   c. De manera opcional, seleccione o desmarque la casilla de verificación **Habilitar trampas de autenticación** para controlar si el agente SNMP de StorageGRID envía trampas de autenticación cuando recibe mensajes de protocolo autenticados incorrectamente.
4. Si usa SNMPv1 o SNMPv2c, opcionalmente actualice o agregue una **Comunidad de solo lectura** en la sección Cadenas de la comunidad.
5. Para actualizar los destinos de trampa, seleccione la pestaña Destinos de trampa en la sección Otras configuraciones.

   Utilice esta pestaña para definir uno o más destinos para las notificaciones de captura o información de StorageGRID . Cuando habilita el agente SNMP y selecciona **Guardar**, StorageGRID envía notificaciones a cada destino definido cuando se activan alertas. También se envían notificaciones estándar para las entidades MIB-II compatibles (por ejemplo, ifDown y coldStart).

   Para obtener detalles sobre qué ingresar, consulte"Crear destinos de trampa" .

- Opcionalmente, actualice o elimine la comunidad de trampas predeterminada.

  Si elimina la comunidad de trampa predeterminada, primero debe asegurarse de que todos los destinos de trampa existentes utilicen una cadena de comunidad personalizada.

- Para agregar un destino de trampa, seleccione **Crear**.
- Para editar un destino de trampa, seleccione el botón de opción y seleccione **Editar**.
- Para eliminar un destino de trampa, seleccione el botón de opción y seleccione **Eliminar**.
- Para confirmar los cambios, seleccione **Guardar** en la parte inferior de la página.

6. Para actualizar las direcciones del agente, seleccione la pestaña Direcciones del agente en la sección Otras configuraciones.

   Utilice esta pestaña para especificar una o más "direcciones de escucha". Estas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas.

   Para obtener detalles sobre qué ingresar, consulte"Crear direcciones de agentes" .

   - Para agregar una dirección de agente, seleccione **Crear**.
   - Para editar la dirección de un agente, seleccione el botón de opción y seleccione **Editar**.
   - Para eliminar una dirección de agente, seleccione el botón de opción y seleccione **Eliminar**.
   - Para confirmar los cambios, seleccione **Guardar** en la parte inferior de la página.

7. Para actualizar los usuarios de USM, seleccione la pestaña Usuarios de USM en la sección Otras configuraciones.

   Utilice esta pestaña para definir los usuarios de USM que están autorizados a consultar la MIB o a recibir trampas e informes.

   Para obtener detalles sobre qué ingresar, consulte"Crear usuarios de USM" .

   - Para agregar un usuario USM, seleccione **Crear**.
   - Para editar un usuario USM, seleccione el botón de opción y seleccione **Editar**.

     No se puede cambiar el nombre de usuario de un usuario USM existente. Si necesita cambiar un nombre de usuario, debe eliminar el usuario y crear uno nuevo.

     > Si agrega o elimina el ID de motor autorizado de un usuario y ese usuario está actualmente seleccionado para un destino, debe editar o eliminar el destino. De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

   - Para eliminar un usuario de USM, seleccione el botón de opción y seleccione **Eliminar**.

     > Si el usuario que eliminó está actualmente seleccionado para un destino de trampa, debe editar o eliminar el destino. De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

   - Para confirmar los cambios, seleccione **Guardar** en la parte inferior de la página.

8. Cuando haya actualizado la configuración del agente SNMP, seleccione **Guardar**.

Acceder a archivos MIB

Los archivos MIB contienen definiciones e información sobre las propiedades de los recursos y servicios administrados para los nodos de su red. Puede acceder a los archivos MIB que definen los objetos y las notificaciones para StorageGRID. Estos archivos pueden ser útiles para monitorear su red.

Ver"Utilice la monitorización SNMP" para obtener más información sobre los archivos SNMP y MIB.

Acceder a archivos MIB

Siga estos pasos para acceder a los archivos MIB.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Monitoreo** > **Agente SNMP**.
2. En la página del agente SNMP, seleccione el archivo que desea descargar:
   - **NETAPP-STORAGEGRID-MIB.txt**: Define la tabla de alertas y las notificaciones (trampas) accesibles en todos los nodos de administración.
   - **ES-NETAPP-06-MIB.mib**: Define objetos y notificaciones para dispositivos basados en E-Series.
   - **MIB_1_10.zip**: Define objetos y notificaciones para dispositivos con una interfaz BMC .

   También puede acceder a los archivos MIB en la siguiente ubicación en cualquier nodo StorageGRID : `/usr/share/snmp/mibs`

3. Para extraer los OID de StorageGRID del archivo MIB:

   a. Obtenga el OID de la raíz del MIB de StorageGRID :

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Resultado: `.1.3.6.1.4.1.789.28669` (`28669` es siempre el OID para StorageGRID)

   a. Busque el OID de StorageGRID en todo el árbol (usando `paste` para unir líneas):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

El `snmptranslate` El comando tiene muchas opciones que son útiles para explorar la MIB. Este comando está disponible en cualquier nodo StorageGRID .

Contenido del archivo MIB

Todos los objetos están bajo el OID StorageGRID .

Nombre del objeto	Identificador de objeto (OID)	Descripción
		El módulo MIB para entidades NetApp StorageGRID .

Objetos MIB

Nombre del objeto	Identificador de objeto (OID)	Descripción
recuento de alertas activas		El número de alertas activas en activeAlertTable.
tabla de alerta activa		Una tabla de alertas activas en StorageGRID.
ID de alerta activa		El ID de la alerta. Único en el conjunto actual de alertas activas.
nombreAlertaActiva		El nombre de la alerta.
instancia de alerta activa		El nombre de la entidad que generó la alerta, normalmente el nombre del nodo.
activeAlertSeverity		La gravedad de la alerta.
hora de inicio de alerta activa		La fecha y hora en que se activó la alerta.

Tipos de notificaciones (trampas)

Todas las notificaciones incluyen las siguientes variables como varbinds:

- ID de alerta activa
- nombreAlertaActiva
- instancia de alerta activa
- activeAlertSeverity
- hora de inicio de alerta activa

Tipo de notificación	Identificador de objeto (OID)	Descripción
alerta menor activa		Una alerta con gravedad menor
alerta mayor activa		Una alerta con mayor gravedad
alerta crítica activa		Una alerta con gravedad crítica