Usar supervisión de SNMP

StorageGRID 11.8

NetApp
March 19, 2024

Tabla de contenidos

Usar supervisión de SNMP

Utilice la monitorización SNMP: Descripción general

Si desea supervisar StorageGRID mediante el protocolo simple de gestión de redes (SNMP), debe configurar el agente SNMP que se incluye con StorageGRID.

- "Configure el agente SNMP"
- "Actualice el agente SNMP"

Funcionalidades

Cada nodo StorageGRID ejecuta un agente SNMP, o demonio, que proporciona una MIB. El MIB de StorageGRID contiene definiciones de tablas y notificaciones para alertas y alarmas. El 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.

Consulte "Acceda a los archivos MIB" Si desea descargar los archivos MIB en los nodos de grid.

Inicialmente, SNMP está deshabilitado en todos los nodos. Al configurar 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 condicionadas por eventos a un sistema de gestión:

Trampas

Las trampas son notificaciones enviadas por el agente SNMP que no requieren reconocimiento por parte del sistema de gestión. Los traps sirven para notificar al sistema de gestión que algo ha sucedido dentro de StorageGRID, por ejemplo, que se activa una alerta.

Las tres versiones de SNMP admiten capturas.

Informa

Las informes son similares a las capturas, pero requieren el reconocimiento del sistema de gestión. Si el agente SNMP no recibe una confirmación dentro de un cierto período de tiempo, vuelve a enviar la información hasta que se reciba una confirmación o se haya alcanzado el valor máximo de reintento.

Las informa son compatibles con SNMPv2c y SNMPv3.

Las notificaciones Trap e INFORM se envían en los siguientes casos:

- Una alerta predeterminada o personalizada se activa en cualquier nivel de gravedad. Para suprimir las notificaciones SNMP correspondientes a una alerta, debe "configurar un silencio" para la alerta. Las notificaciones de alerta se envían mediante la "Nodo de administración de remitente preferido".

  Cada alerta se asigna a uno de los tres tipos de trampa según el nivel de gravedad de la alerta: ActiveMinorAlert, activeMajorAlert y activeCriticalAlert. Para ver una lista de las alertas que pueden activar estos retos, consulte la "Referencia de alertas".

- Seguro "alarmas (sistema heredado)" se disparan en niveles de gravedad especificados o superiores.

> Las notificaciones SNMP no se envían para cada alarma o cada gravedad de alarma.

Compatibilidad con versiones de SNMP

La tabla proporciona un resumen a grandes rasgos de lo que se admite para cada versión de SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Consultas	Consultas MIB de solo lectura	Consultas MIB de solo lectura	Consultas MIB de solo lectura
Consulta de autenticación	Cadena de comunidad	Cadena de comunidad	Usuario del modelo de seguridad basado en el usuario (USM)
Notificaciones	Sólo capturas	Atrapa e informa	Atrapa e informa
Autenticación de notificaciones	Comunidad de capturas predeterminada o una cadena de comunidad personalizada para cada destino de capturas	Comunidad de capturas predeterminada o una cadena de comunidad personalizada para cada destino de capturas	Usuario USM en cada destino de captura

Limitaciones

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

Configure el agente SNMP

Es posible configurar el agente SNMP de StorageGRID para que use un sistema de gestión SNMP de terceros para el acceso a MIB de solo lectura y las notificaciones.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

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 con modelos de seguridad de usuario (USM).

Todos los nodos del grid utilizan la misma configuración SNMP.

Especifique la configuración básica

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

Pasos

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

   Aparece la página del agente SNMP.

2. Para habilitar el agente SNMP en todos los nodos de la cuadrícula, seleccione la casilla de verificación **Activar 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 mensajes de SNMP como sysContact. El contacto del sistema suele ser una dirección de correo electrónico. Este valor se aplica a todos los nodos del sistema StorageGRID. **El contacto del sistema** puede tener un máximo de 255 caracteres.
Ubicación del sistema	Opcional. La ubicación del sistema StorageGRID, que se devuelve en mensajes de SNMP como sysLocation. La ubicación del sistema puede ser cualquier información útil para identificar dónde se encuentra el sistema StorageGRID. Por ejemplo, puede utilizar la dirección de una instalación. Este valor se aplica a todos los nodos del sistema StorageGRID. **La ubicación del sistema** puede tener un máximo de 255 caracteres.
Activar notificaciones de agente SNMP	• Si se selecciona, el agente SNMP de StorageGRID envía notificaciones de captura e información. • Si no se selecciona, el agente SNMP admite el acceso MIB de solo lectura, pero no envía ninguna notificación SNMP.
Habilite las capturas de autenticación	Si se selecciona, el agente SNMP de StorageGRID envía capturas de autenticación si recibe mensajes de protocolo autenticados incorrectamente.

Introduzca las cadenas de comunidad

Si usa SNMPv1 o SNMPv2c, complete la sección Community Strings.

Cuando el sistema de gestión consulta el 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**, opcionalmente, introduzca una cadena de comunidad para permitir el acceso MIB de solo lectura en las direcciones de agente IPv4 y IPv6.

Para garantizar la seguridad de su sistema StorageGRID, no utilice «public» como cadena de comunidad. Si deja este campo vacío, el agente SNMP utiliza el identificador de grid del sistema StorageGRID como la 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 cadenas.

Crear destinos de capturas

Use la pestaña Destinos de captura en la sección Otras configuraciones para definir uno o más destinos para las notificaciones de captura StorageGRID o Inform. 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 admitidas (por ejemplo, ifdown y coldStart).

Pasos

1. Para el campo **default trap community**, opcionalmente, introduzca la cadena de comunidad predeterminada que desea utilizar para destinos de captura SNMPv1 o SNMPv2.

   Según sea necesario, puede proporcionar una cadena de comunidad diferente (personalizada) al definir un destino de captura específico.

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

2. Para agregar un destino de captura, selecciona **Crear**.
3. Seleccione la versión de SNMP que se utilizará para este destino de capturas.
4. Complete el formulario Crear destino de captura para la versión seleccionada.

SNMPv1

Si seleccionó SNMPv1 como versión, complete estos campos.

Campo	Descripción
Tipo	Debe ser Trampa para SNMPv1.
Host	Una dirección IPv4 o IPv6, o un nombre de dominio completo (FQDN) para recibir la captura.
Puerto	Utilice 162, que es el puerto estándar para capturas de SNMP a menos que tenga que usar otro valor.
Protocolo	Utilice UDP, que es el protocolo de captura SNMP estándar a menos que necesite utilizar TCP.
Cadena de comunidad	Use la comunidad de capturas predeterminada, si se especificó una o introduzca una cadena de comunidad personalizada para este destino de captura. 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 un FQDN para recibir la captura.
Puerto	Utilice 162, que es el puerto estándar para capturas de SNMP a menos que se deba usar otro valor.
Protocolo	Utilice UDP, que es el protocolo de captura SNMP estándar a menos que necesite utilizar TCP.
Cadena de comunidad	Use la comunidad de capturas predeterminada, si se especificó una o introduzca una cadena de comunidad personalizada para este destino de captura. 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 un FQDN para recibir la captura.
Puerto	Utilice 162, que es el puerto estándar para capturas de SNMP a menos que se deba usar otro valor.
Protocolo	Utilice UDP, que es el protocolo de captura SNMP estándar a menos que necesite utilizar TCP.
Usuario USM	El usuario USM que se usará para la autenticación. • Si ha seleccionado **Trap**, sólo se mostrarán los usuarios USM sin identificación de motor autorizada. • Si ha seleccionado **INFORM**, sólo se mostrarán los usuarios USM con ID de motor autoritativos. • Si no se muestran usuarios: i. Cree y guarde el destino de captura. ii. Vaya a. Crear usuarios USM y crear el usuario. iii. Vuelva a la pestaña Destinos de solapamiento, seleccione el destino guardado de la tabla y seleccione **Editar**. iv. Seleccione el usuario.

5. Seleccione **Crear**.

   El destino de captura se crea y se añade a la tabla.

Crear direcciones de agente

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

Si no configura una dirección de agente, la dirección de recepción 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 usará IPv4 o IPv6. De forma predeterminada, SNMP utiliza IPv4.
Protocolo de transporte	Si esta dirección usará UDP o TCP. De forma predeterminada, SNMP utiliza UDP.
Red StorageGRID	En qué red StorageGRID escuchará el agente. • Redes Grid, Admin y Client: El agente SNMP escuchará las consultas en las tres redes. • Red Grid • Red de administración • Red cliente **Nota**: Si utiliza la Red de clientes para datos inseguros y crea una dirección de agente para la Red de clientes, tenga en cuenta que el tráfico SNMP también será inseguro.
Puerto	Opcionalmente, el número de puerto en el que debe recibir el agente SNMP. El puerto UDP predeterminado para un agente SNMP es 161, pero puede introducir cualquier número de puerto no utilizado. **Nota**: Al guardar el agente SNMP, StorageGRID abre automáticamente los puertos de dirección del agente en el firewall interno. Debe asegurarse de que cualquier firewall externo permita el acceso a estos puertos.

3. Seleccione **Crear**.

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

Crear usuarios USM

Si utiliza SNMPv3, use la pestaña Usuarios USM en la sección Otras configuraciones para definir los usuarios de USM que están autorizados a consultar la MIB o recibir capturas e informar.

> SNMPv3 *Inform* Los destinos 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 usas SNMPv1 o SNMPv2c.

Pasos

1. Seleccione **Crear**.

2. Introduzca la siguiente información.

Campo	Descripción
Nombre de usuario	Nombre único para este usuario 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 después de crear el usuario.
Acceso a la MIB de solo lectura	Si se selecciona, este usuario debe tener acceso de solo lectura a la MIB.
ID de motor autorizado	Si este usuario se va a utilizar en un destino de informe, el ID de motor autorizado para este usuario. Introduzca de 10 a 64 caracteres hexadecimales (de 5 a 32 bytes) sin espacios. Este valor es obligatorio para los usuarios de USM que se seleccionarán en destinos de captura para los informes. Este valor no está permitido para los usuarios de USM que se seleccionarán en destinos de captura para capturas. **Nota**: Este campo no se muestra si seleccionaste **Acceso MIB de solo lectura** porque los usuarios USM que tienen acceso MIB de solo lectura no pueden tener ID de motor.
Nivel de seguridad	Nivel de seguridad del usuario USM: • **Authpriv**: Este usuario se comunica con autenticación y privacidad (cifrado). Debe especificar un protocolo y una contraseña de autenticación, y un protocolo y una contraseña de privacidad. • **AuthNoprivilegios**: Este usuario se comunica con autenticación y sin privacidad (sin cifrado). Debe especificar un protocolo de autenticación y una contraseña.
Protocolo de autenticación	Siempre configurado en SHA, que es el único protocolo compatible (HMAC-SHA-96).
Contraseña	Contraseña que utilizará este usuario para la autenticación.
Protocolo de privacidad	Solo se muestra si seleccionó **AUTHPRIV** y siempre se establece en AES, que es el único protocolo de privacidad compatible.
Contraseña	Solo se muestra si seleccionaste **AUTHPRIV**. La contraseña que este usuario utilizará para la privacidad.

3. Seleccione **Crear**.

   El usuario USM se crea y se añade a la tabla.

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

   La nueva configuración del agente SNMP se activa.

Actualice el agente SNMP

Es posible deshabilitar notificaciones SNMP, actualizar cadenas de comunidad, o añadir o quitar direcciones de agentes, usuarios de USM y destinos de capturas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Acerca de esta tarea

Consulte "Configure el agente SNMP" Para obtener detalles sobre cada campo en la página del agente SNMP. Debe seleccionar **Guardar** en la parte inferior de la página para confirmar los cambios que realice en cada pestaña.

Pasos

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

   Aparece la página del agente SNMP.

2. Para desactivar el agente SNMP en todos los nodos de la cuadrícula, desactive la casilla de verificación **Habilitar SNMP** y seleccione **Guardar**.

   Si vuelve a habilitar el agente SNMP, se conservan todos los ajustes de configuración anteriores de SNMP.

3. Si lo desea, actualice la información en la sección Configuración básica:
   a. Según sea necesario, actualice el **Contacto del sistema** y **Ubicación del sistema**.
   b. Opcionalmente, seleccione o desactive la casilla de verificación **Activar notificaciones de agente SNMP** para controlar si el agente SNMP de StorageGRID envía notificaciones de trap e informen.

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

   c. Opcionalmente, seleccione o desactive la casilla de verificación **Habilitar capturas de autenticación** para controlar si el agente SNMP de StorageGRID envía capturas 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 de cadenas de comunidad.
5. Para actualizar los destinos de capturas, seleccione la pestaña Destinos de captura en la sección Otras configuraciones.

   Utilice esta pestaña para definir uno o más destinos para las notificaciones de captura StorageGRID o Inform. 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 admitidas (por ejemplo, ifdown y coldStart).

   Para obtener información detallada sobre qué introducir, consulte "Cree destinos de capturas".

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

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

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

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

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

   Para obtener información detallada sobre qué introducir, consulte "Crear direcciones de agente".

   - Para agregar una dirección de agente, seleccione **Crear**.
   - Para editar una dirección de 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, selecciona **Guardar** en la parte inferior de la página.

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

   Use esta pestaña para definir los usuarios USM que están autorizados a consultar el MIB o a recibir capturas e informes.

   Para obtener información detallada sobre qué introducir, consulte "Crear usuarios USM".

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

     No se puede cambiar el nombre de usuario de 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 seleccionado actualmente 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 USM, seleccione el botón de opción y seleccione **Eliminar**.

     > Si el usuario que eliminó está seleccionado actualmente para un destino de captura, 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, selecciona **Guardar** en la parte inferior de la página.

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

Acceda a los archivos MIB

Los archivos MIB contienen definiciones e información sobre las propiedades de los recursos y servicios gestionados para los nodos en el grid. Es posible acceder a los archivos MIB que definen los objetos y las notificaciones para StorageGRID. Estos archivos pueden ser útiles para supervisar la cuadrícula.

Consulte "Usar supervisión de SNMP" Para obtener más información acerca de los archivos SNMP y MIB.

Acceda a los archivos MIB

Siga estos pasos para acceder a los archivos MIB.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Supervisión** > **Agente SNMP**.
2. En la página del agente SNMP, seleccione el archivo que desee descargar:
   - **NETAPP-STORAGEGRID-MIB.txt**: Define la tabla de alertas y las notificaciones (traps) a las que se puede acceder 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 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 de la MIB de StorageGRID:

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

   Resultado: `.1.3.6.1.4.1.789.28669` (`28669` Es siempre el OID de StorageGRID)

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

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

> La `snmptranslate` Command 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 de StorageGRID.

Nombre del objeto	ID Objeto (OID)	Descripción
iso.org.dod.internet. empresas privadas. netapp.storagegrid		Módulo MIB para entidades de NetApp StorageGRID.

Objetos MIB

Nombre del objeto	ID Objeto (OID)	Descripción
Active AlertCount	**1,3.6,1.4,1.** 789.28669.1.3	El número de alertas activas en activeAlertTable.
Active AlertTable	**1,3.6,1.4,1.** 789.28669.1.4	Una tabla de alertas activas en StorageGRID.
Active AlertId	**1,3.6,1.4,1.** 789.28669.1.4.1.1	El ID de la alerta. Solo es único en el conjunto actual de alertas activas.
Active AlertName	**1,3.6,1.4,1.** 789.28669.1.4.1.2	El nombre de la alerta.
Active AlertInstance	**1,3.6,1.4,1.** 789.28669.1.4.1.3	El nombre de la entidad que generó la alerta, generalmente el nombre del nodo.
Active AlertSeverity	**1,3.6,1.4,1.** 789.28669.1.4.1.4	La gravedad de la alerta.
Active AlertStartTime	**1,3.6,1.4,1.** 789.28669.1.4.1.5	La fecha y la hora en la que se activó la alerta.

Tipos de notificación (retos)

Todas las notificaciones incluyen las siguientes variables como varbinds:

- Active AlertId
- Active AlertName
- Active AlertInstance
- Active AlertSeverity
- Active AlertStartTime

Tipo de notificación	ID Objeto (OID)	Descripción
ActiveMinorAlert	**1,3.6,1.4,1.** 789.28669.0.6	Una alerta de gravedad menor
Active MajorAlert	**1,3.6,1.4,1.** 789.28669.0.7	Una alerta de gravedad importante
ActiveCriticalAlert	**1,3.6,1.4,1.** 789.28669.0.8	Una alerta con gravedad crítica

Información de copyright

Información de la marca comercial