Gestionar alertas SNMP

SANtricity 11.7

NetApp
February 12, 2024

Tabla de contenidos

Gestionar alertas SNMP

Configurar las alertas SNMP

Para configurar alertas del protocolo simple de gestión de redes (SNMP) se debe identificar al menos un servidor en el que el monitor de eventos de la cabina de almacenamiento pueda enviar capturas SNMP. La configuración requiere un nombre de comunidad o nombre de usuario y una dirección IP para el servidor.

Antes de empezar

- Debe configurarse un servidor de red con una aplicación de servicio SNMP. Es necesario tener la dirección de red de este servidor (ya sea una dirección IPv4 o IPv6), de manera que el monitor de eventos pueda enviar mensajes de captura a esa dirección. Es posible usar más de un servidor (se permiten hasta 10 servidores).
- El archivo de base de datos de información de gestión (MIB) se copió y compiló en el servidor con la aplicación de servicio SNMP. Este archivo MIB define los datos que se están supervisando y gestionando.

  Si no tiene el archivo MIB, puede obtenerlo en el sitio de soporte de NetApp:

  - Vaya a. "Soporte de NetApp".
  - Haga clic en la ficha **Descargas** y seleccione **Descargas**.
  - Haga clic en **E-Series SANtricity OS Controller Software**.
  - Seleccione **Descargar la última versión**.
  - Inicie sesión.
  - Acepte la declaración de precaución y el acuerdo de licencia.
  - Desplácese hacia abajo hasta que vea el archivo MIB para el tipo de controladora y haga clic en el enlace para descargar el archivo.

Acerca de esta tarea

En esta tarea, se describe cómo identificar el servidor SNMP para el destino de capturas y, a continuación, poner a prueba la configuración.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   En la primera configuración, la pestaña SNMP muestra "Configure Communities/Users".

3. Seleccione **Configurar comunidades/usuarios**.

   Se abre el cuadro de diálogo Seleccionar versión de SNMP.

4. Seleccione la versión SNMP para las alertas, ya sea **SNMPv2c** o **SNMPv3**.

   En función de lo que seleccione, se abrirá el cuadro de diálogo Configurar comunidades o el cuadro de diálogo Configurar usuarios SNMPv3.

5. Siga las instrucciones adecuadas para SNMPv2c (comunidades) o SNMPv3 (usuarios):

- **SNMPv2c (comunidades)** — en el diálogo Configurar comunidades, introduzca una o más cadenas de comunidad para los servidores de red. Un nombre de comunidad es una cadena que identifica un conjunto conocido de estaciones de gestión y que normalmente lo crea un administrador de red. Está compuesto solo por caracteres ASCII que se pueden imprimir. Puede añadir hasta 256 comunidades. Cuando haya terminado, haga clic en **Guardar**.
- **SNMPv3 (usuarios)** — en el cuadro de diálogo Configurar usuarios de SNMPv3, haga clic en **Agregar** e introduzca la siguiente información:
  - **Nombre de usuario** — Introduzca un nombre para identificar al usuario, que puede tener hasta 31 caracteres.
  - **ID del motor** — Seleccione el ID del motor, que se utiliza para generar claves de autenticación y cifrado para los mensajes, y debe ser único en el dominio administrativo. En la mayoría de los casos, debe seleccionar **local**. Si tiene una configuración no estándar, seleccione **personalizado**; aparece otro campo en el que debe introducir el ID de motor autorizado como una cadena hexadecimal, con un número par de caracteres de entre 10 y 32 caracteres de longitud.
  - **Credenciales de autenticación** — Seleccione un protocolo de autenticación que garantice la identidad de los usuarios. A continuación, introduzca una contraseña de autenticación, que es obligatoria cuando se defina el protocolo de autenticación o se modifique. La contraseña debe tener entre 8 y 128 caracteres.
  - **Credenciales de privacidad** — Seleccione un protocolo de privacidad que se utiliza para cifrar el contenido de los mensajes. A continuación, introduzca una contraseña de privacidad, que es necesaria cuando se establece o cambia el protocolo de privacidad. La contraseña debe tener entre 8 y 128 caracteres. Cuando haya terminado, haga clic en **Agregar** y, a continuación, haga clic en **Cerrar**.

6. En la página Alertas con la ficha SNMP seleccionada, haga clic en **Añadir destinos de captura**.

   Se abre el cuadro de diálogo Añadir destinos de captura.

7. Introduzca uno o más destinos de captura, seleccione sus nombres de comunidad o de usuario asociados y, a continuación, haga clic en **Agregar**.
   - **Destino de captura** — Introduzca una dirección IPv4 o IPv6 del servidor que ejecuta un servicio SNMP.
   - **Nombre de comunidad o Nombre de usuario** — en el menú desplegable, seleccione el nombre de comunidad (SNMPv2c) o el nombre de usuario (SNMPv3) para este destino de captura. (Si ha definido sólo uno, el nombre ya aparecerá en este campo.)
   - **Enviar captura de fallo de autenticación** — Seleccione esta opción (la casilla de verificación) si desea alertar al destino de la captura cada vez que se rechace una solicitud SNMP debido a un nombre de comunidad o de usuario no reconocido. Después de hacer clic en **Agregar**, los destinos de captura y los nombres asociados aparecen en la ficha **SNMP** de la página **Alertas**.
8. Para asegurarse de que una captura es válida, seleccione un destino de captura de la tabla y, a continuación, haga clic en **probar destino de captura** para enviar una captura de prueba a la dirección configurada.

Resultados

El monitor de eventos envía capturas SNMP a los servidores cada vez que ocurre un evento que genera alertas.

Añadir destinos de capturas para alertas SNMP

Es posible añadir hasta 10 servidores para enviar capturas SNMP.

Antes de empezar

- El servidor de red que desea añadir debe estar configurado con una aplicación de servicio SNMP. Es necesario tener la dirección de red de este servidor (ya sea una dirección IPv4 o IPv6), de manera que el monitor de eventos pueda enviar mensajes de captura a esa dirección. Es posible usar más de un servidor (se permiten hasta 10 servidores).
- El archivo de base de datos de información de gestión (MIB) se copió y compiló en el servidor con la aplicación de servicio SNMP. Este archivo MIB define los datos que se están supervisando y gestionando.

  Si no tiene el archivo MIB, puede obtenerlo en el sitio de soporte de NetApp:

  - Vaya a. "Soporte de NetApp".
  - Haga clic en **Descargas** y, a continuación, seleccione **Descargas**.
  - Haga clic en **E-Series SANtricity OS Controller Software**.
  - Seleccione **Descargar la última versión**.
  - Inicie sesión.
  - Acepte la declaración de precaución y el acuerdo de licencia.
  - Desplácese hacia abajo hasta que vea el archivo MIB para el tipo de controladora y haga clic en el enlace para descargar el archivo.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas definidos actualmente se muestran en la tabla.

3. Seleccione **Agregar destinos de captura**.

   Se abre el cuadro de diálogo Añadir destinos de captura.

4. Introduzca uno o más destinos de captura, seleccione sus nombres de comunidad o de usuario asociados y, a continuación, haga clic en **Agregar**.
   - **Destino de captura** — Introduzca una dirección IPv4 o IPv6 del servidor que ejecuta un servicio SNMP.
   - **Nombre de comunidad o Nombre de usuario** — en el menú desplegable, seleccione el nombre de comunidad (SNMPv2c) o el nombre de usuario (SNMPv3) para este destino de captura. (Si ha definido sólo uno, el nombre ya aparecerá en este campo.)
   - **Enviar captura de fallo de autenticación** — Seleccione esta opción (la casilla de verificación) si desea alertar al destino de la captura cada vez que se rechace una solicitud SNMP debido a un nombre de comunidad o de usuario no reconocido. Después de hacer clic en **Agregar**, los destinos de captura y los nombres de comunidad o de usuario asociados aparecen en la tabla.
5. Para asegurarse de que una captura es válida, seleccione un destino de captura de la tabla y, a continuación, haga clic en **probar destino de captura** para enviar una captura de prueba a la dirección configurada.

Resultados

El monitor de eventos envía capturas SNMP a los servidores cada vez que ocurre un evento que genera alertas.

Configure las variables MIB de SNMP

En el caso de las alertas SNMP, tiene la opción de configurar las variables de la base de datos de información de gestión (MIB) que se muestran en las excepciones SNMP. Estas variables pueden mostrar el nombre de la cabina de almacenamiento, su ubicación y una persona de contacto.

Antes de empezar

El archivo MIB debe copiarse y compilarse en el servidor con la aplicación de servicio SNMP.

Si no tiene un archivo MIB, puede obtenerlo del siguiente modo:

- Vaya a. "Soporte de NetApp".
- Haga clic en **Descargas** y, a continuación, seleccione **Descargas**.
- Haga clic en **E-Series SANtricity OS Controller Software**.
- Seleccione **Descargar la última versión**.
- Inicie sesión.
- Acepte la declaración de precaución y el acuerdo de licencia.
- Desplácese hacia abajo hasta que vea el archivo MIB para el tipo de controladora y haga clic en el enlace para descargar el archivo.

Acerca de esta tarea

En esta tarea, se describe cómo definir variables MIB para excepciones SNMP. Estas variables pueden mostrar los siguientes valores, en respuesta a los mensajes GetRequests de SNMP:

- `sysName` (nombre para la cabina de almacenamiento)
- `sysLocation` (ubicación de la cabina de almacenamiento)
- `sysContact` (nombre de un administrador)

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.
3. Seleccione **Configurar variables MIB de SNMP**.

   Se muestra el cuadro de diálogo Configurar variables MIB de SNMP.

4. Introduzca uno o más de los siguientes valores y, a continuación, haga clic en **Guardar**.
   - **Nombre** — el valor de la variable MIB `sysName`. Por ejemplo, introduzca un nombre para la cabina de almacenamiento.
   - **Ubicación** — el valor de la variable MIB `sysLocation`. Por ejemplo, introduzca la ubicación de la cabina de almacenamiento.
   - **Contacto** — el valor de la variable MIB `sysContact`. Por ejemplo, introduzca un administrador que sea responsable de la cabina de almacenamiento.

Resultados

Estos valores se muestran en los mensajes de captura SNMP en las alertas de la cabina de almacenamiento.

Editar comunidades para capturas SNMPv2c

Puede editar nombres de comunidad para capturas SNMPv2c.

Antes de empezar

Se debe crear un nombre de comunidad.

Pasos

1. Seleccione MENU:Setting[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas y los nombres de comunidad aparecen en la tabla.

3. Seleccione **Configurar comunidades**.
4. Introduzca el nuevo nombre de comunidad y haga clic en **Guardar**. Los nombres de comunidades deben consistir únicamente en caracteres ASCII imprimibles.

Resultados

La pestaña SNMP de la página Alertas muestra el nombre actualizado de la comunidad.

Edite la configuración de usuario de las capturas SNMPv3

Puede editar definiciones de usuario para solapamientos SNMPv3.

Antes de empezar

Se debe crear un usuario para la captura SNMPv3.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas y los nombres de usuario aparecen en la tabla.

3. Para editar una definición de usuario, seleccione el usuario en la tabla y, a continuación, haga clic en **Configurar usuarios**.
4. En el cuadro de diálogo, haga clic en **Ver/editar configuración**.
5. Edite la siguiente información:
   - **Nombre de usuario** — cambie el nombre que identifica al usuario, que puede tener hasta 31 caracteres.
   - **ID del motor** — Seleccione el ID del motor, que se utiliza para generar claves de autenticación y cifrado para los mensajes, y debe ser único en el dominio administrativo. En la mayoría de los casos, debe seleccionar **local**. Si tiene una configuración no estándar, seleccione **personalizado**; aparece otro campo en el que debe introducir el ID de motor autorizado como una cadena hexadecimal, con un número par de caracteres de entre 10 y 32 caracteres de longitud.
   - **Credenciales de autenticación** — Seleccione un protocolo de autenticación que garantice la identidad de los usuarios. A continuación, introduzca una contraseña de autenticación, que es obligatoria cuando se defina el protocolo de autenticación o se modifique. La contraseña debe tener entre 8 y 128 caracteres.

- **Credenciales de privacidad** — Seleccione un protocolo de privacidad que se utiliza para cifrar el contenido de los mensajes. A continuación, introduzca una contraseña de privacidad, que es necesaria cuando se establece o cambia el protocolo de privacidad. La contraseña debe tener entre 8 y 128 caracteres.

Resultados

La pestaña SNMP de la página Alertas muestra la configuración actualizada.

Añada comunidades para las trampas SNMPv2c

Puede agregar hasta 256 nombres de comunidad para las trampas SNMPv2c.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas y los nombres de comunidad aparecen en la tabla.

3. Seleccione **Configurar comunidades**.

   Se abre el cuadro de diálogo Configurar comunidades.

4. Seleccione **Añadir otra comunidad**.
5. Introduzca el nuevo nombre de comunidad y haga clic en **Guardar**.

Resultados

El nuevo nombre de la comunidad se muestra en la pestaña SNMP de la página Alertas.

Agregue usuarios para capturas SNMPv3

Puede agregar hasta 256 usuarios para capturas SNMPv3.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas y los nombres de usuario aparecen en la tabla.

3. Seleccione **Configurar usuarios**.

   Se abre el cuadro de diálogo Configurar usuarios de SNMPv3.

4. Seleccione **Agregar**.
5. Introduzca la siguiente información y, a continuación, haga clic en **Agregar**.
   - **Nombre de usuario** — Introduzca un nombre para identificar al usuario, que puede tener hasta 31 caracteres.
   - **ID del motor** — Seleccione el ID del motor, que se utiliza para generar claves de autenticación y cifrado para los mensajes, y debe ser único en el dominio administrativo. En la mayoría de los casos, debe seleccionar **local**. Si tiene una configuración no estándar, seleccione **personalizado**; aparece otro campo en el que debe introducir el ID de motor autorizado como una cadena hexadecimal, con un

número par de caracteres de entre 10 y 32 caracteres de longitud.

- **Credenciales de autenticación** — Seleccione un protocolo de autenticación que garantice la identidad de los usuarios. A continuación, introduzca una contraseña de autenticación, que es obligatoria cuando se defina el protocolo de autenticación o se modifique. La contraseña debe tener entre 8 y 128 caracteres.
- **Credenciales de privacidad** — Seleccione un protocolo de privacidad que se utiliza para cifrar el contenido de los mensajes. A continuación, introduzca una contraseña de privacidad, que es necesaria cuando se establece o cambia el protocolo de privacidad. La contraseña debe tener entre 8 y 128 caracteres.

Quitar comunidades de las trampas SNMPv2c

Puede eliminar un nombre de comunidad de las trampas SNMPv2c.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de captura y los nombres de comunidad aparecen en la página **Alertas**.

3. Seleccione **Configurar comunidades**.

   Se abre el cuadro de diálogo Configurar comunidades.

4. Seleccione el nombre de comunidad que desea eliminar y, a continuación, haga clic en el icono **Quitar** (X) situado en el extremo derecho.

   Si existen destinos de captura asociados con este nombre de comunidad, el cuadro de diálogo Confirmar eliminación de comunidad muestra las direcciones de los destinos de captura afectados.

5. Confirme la operación y haga clic en **Quitar**.

Resultados

El nombre de comunidad y el destino de captura asociado se eliminan de la página Alertas.

Eliminar usuarios para solapamientos SNMPv3

Puede eliminar un usuario para capturas SNMPv3.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los nombres de usuario y los destinos de captura se muestran en la página Alertas.

3. Seleccione **Configurar usuarios**.

   Se abre el cuadro de diálogo Configurar usuarios de SNMPv3.

4. Seleccione el nombre de usuario que desea eliminar y, a continuación, haga clic en **Eliminar**.

5. Confirme la operación y haga clic en **Eliminar**.

Resultados

El nombre de usuario y el destino de captura asociado se eliminan de la página Alertas.

Eliminar destinos de capturas

Es posible eliminar una dirección de destino de captura para que el monitor de eventos de la cabina de almacenamiento ya no envíe capturas SNMP a esa dirección.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Las direcciones de los destinos de captura se muestran en la tabla.

3. Seleccione un destino de captura y, a continuación, haga clic en **Eliminar** en la esquina superior derecha de la página.
4. Confirme la operación y haga clic en **Eliminar**.

   La dirección de destino ya no aparece en la página Alertas.

Resultados

El destino de captura eliminado ya no recibe capturas SNMP del monitor de eventos de la cabina de almacenamiento.