Preguntas frecuentes sobre ESA: ¿AsyncOS soporta el monitoreo SNMP?

Contenido

Introducción

Este documento describe qué trampas del protocolo simple de administración de red (SNMP) son admitidas por AsyncOS.

¿AsyncOS soporta el monitoreo SNMP?

El sistema operativo Cisco AsyncOS admite la supervisión del estado del sistema a través de SNMP. AsyncOS admite SNMPv1, v2 y v3.

Esto incluye la Base de información de administración empresarial (MIB) de Cisco, ASYNCOS-MAIL-MIB. ASYNCOS-MAIL-MIB ayuda a los administradores a monitorear mejor el estado del sistema. Además, esta versión implementa un subconjunto de sólo lectura de MIB-II según se define en los RFC 1213 y 1907. (Para obtener más información sobre SNMP, vea RFC 1065, 1066 y 1067.)

Tenga en cuenta lo siguiente:

- SNMP está desactivado de forma predeterminada.
- Las operaciones SNMP SET (configuración) no se implementan.
- El uso de SNMPv3 con autenticación de contraseña y cifrado DES es obligatorio para habilitar este servicio. (Para obtener más información sobre SNMPv3, vea RFC 2571-2575.) Se requiere que establezca una frase de paso SNMPv3 de al menos ocho caracteres para habilitar el monitoreo de estado del sistema SNMP. La primera vez que ingrese una frase de paso SNMPv3, debe volver a introducirla para confirmarla. El comando **snmpconfig** *recuerda* esta frase la próxima vez que ejecute el comando.
- El nombre de usuario SNMPv3 es: v3get.
  ```
  > snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport mail.example.com
  ```
- Si sólo utiliza SNMPv1 o SNMPv2, debe establecer una cadena de comunidad. La cadena de comunidad no es pública de forma predeterminada.
- Para SNMPv1 y SNMPv2, debe especificar una red desde la que se acepten las solicitudes GET SNMP.

- Para utilizar las trampas, un administrador SNMP (no incluido en AsyncOS) debe estar en ejecución y su dirección IP debe ingresarse como destino de trampa. (Puede utilizar un nombre de host, pero si lo hace, las trampas sólo funcionarán si DNS funciona.)

Utilice el comando **snmpconfig** para configurar el estado del sistema SNMP para el dispositivo. Después de elegir y configurar los valores para una interfaz, el dispositivo responde a las solicitudes GET SNMPv3. Estas solicitudes de la versión 3 deben incluir una contraseña que coincida. De forma predeterminada, se rechazan las solicitudes de la versión 1 y 2. Si se activa, las solicitudes de la versión 1 y 2 deben tener una cadena de comunidad coincidente.

Cisco Systems proporciona una MIB *empresarial* así como un archivo de Estructura de Información de Administración (SMI):

- ASYNCOS-MAIL-MIB.txt: descripción compatible con SNMPv2 de la MIB de empresa para los dispositivos Cisco.
- IRONPORT-SMI.txt: define la función de ASYNCOS-MAIL-MIB en los productos administrados SNMP de IronPort.

Ambos archivos MIB se pueden encontrar desde la página Soporte de Productos de Cisco Email Security Appliance.

> **Sugerencia**: Algunos clientes podrían necesitar compilar ambos archivos en un solo archivo ".my", por ejemplo para admitir HP OpenView. Una herramienta para lograrlo está disponible en www.mg-soft.com.

Consulte el capítulo **Administración y Monitoreo a través de la CLI** de la **Guía del Usuario de Correo Electrónico** para obtener detalles completos sobre el monitoreo SNMP.

Información Relacionada

- Guías de usuario final de Cisco Email Security Appliance
- Soporte Técnico y Documentación - Cisco Systems