Supervisión de Cisco ESA con SNMP

Introducción

Este documento describe cómo monitorear Cisco Secure Email Gateway usando SNMP, incluida la estructura MIB, el uso de OID y las consultas prácticas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico del protocolo SNMP
- Acceso al dispositivo Cisco ESA
- Familiaridad con la línea de comandos de Linux
- Cisco ESA con el servicio SNMP habilitado
- Cliente SNMP instalado (como herramientas Net-SNMP)
- Archivos MIB de IronPort disponibles y cargados
- Cadena de comunidad o credenciales SNMP v3

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Email Gateway (ESA)
- Cliente Linux con herramientas Net-SNMP
- Archivos MIB: IRONPORT-SMI.txt, ASYNCOS-MAIL-MIB.txt

Configurar SNMP

La configuración SNMP en ESA se realiza a través de CLI. Para habilitar SNMP en Cisco ESA, acceda a CLI y ejecute snmpconfig.

La configuración predeterminada incluye:

- Habilitación del servicio SNMP
- Elección de la interfaz de gestión y el puerto (normalmente 161)
- Habilitación de SNMPv3 (seguridad predeterminada: authPriv con SHA y AES)
- Configuración de frases de contraseña de autenticación y privacidad
- Habilitación de SNMPv1/v2c, especificando la cadena de comunidad (por ejemplo, ironport)
- Definición de redes IPv4 permitidas para solicitudes SNMP
- Configuración de la versión de trampa SNMP y la dirección IP de destino de trampa
- Establecer la ubicación del sistema y la información de contacto

Después de habilitar SNMP, puede ver un resumen similar a este:

```
esa1.ironport.com> snmpconfig

Current SNMP settings:
Listening on interface "Management"



      port 161.
SNMP v3: Enabled. Security level: authPriv
Authentication Protocol: SHA
Encryption Protocol: AES
SNMP v1/v2: Enabled, accepting requests from subnet



      , .
SNMP v1/v2 Community String: ironport
Trap version: V3
Trap target:



Location: esxi data center
System Contact: ciscoros soc
```

Una vez que SNMP está habilitado y configurado, el dispositivo está listo para aceptar consultas SNMP de las IP de origen permitidas.

Configuración y Consulta de Cliente SNMP en Linux

Para este ejemplo, se utilizó un servidor Debian. Tenga en cuenta que los pasos de instalación pueden variar en función del administrador de paquetes de distribución.

Instalar herramientas SNMP

```
sudo apt-get install snmp snmp-mibs-downloader
```

Verifique que snmpwalk binary esté instalado.

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk --version
NET-SNMP version: 5.9
```

Cargar archivos MIB

Coloque los archivos MIB de IronPort en la carpeta /usr/share/snmp/mibs.

```
root@debian-server:/usr/share/snmp/mibs# pwd
/usr/share/snmp/mibs
root@debian-server:/usr/share/snmp/mibs# ls
ASYNCOS-MAIL-MIB.txt  IRONPORT-SMI.txt        NET-SNMP-EXAMPLES-MIB.txt  NET-SNMP-PASS-MIB.txt  UCD-DEMO-MIB.txt    UCD-IPFWACC-MIB.txt
iana                  LM-SENSORS-MIB.txt      NET-SNMP-EXTEND-MIB.txt    NET-SNMP-TC.txt        UCD-DISKIO-MIB.txt  UCD-SNMP-MIB.txt
ietf                  NET-SNMP-AGENT-MIB.txt  NET-SNMP-MIB.txt           NET-SNMP-VACM-MIB.txt  UCD-DLMOD-MIB.txt
```

debian-server oids

Nota: Los archivos MIB se pueden encontrar en el artículo SNMP compartido al final de este documento.

Uso de un OID para Monitorear el Uso de la CPU

Este comando consulta al ESA su uso actual de la CPU. El OID apunta directamente a la métrica de CPU definida en la MIB. El resultado muestra un valor, como INTEGER: 37, que indica el uso de CPU del dispositivo en un 37%. Esto permite a los administradores supervisar el rendimiento de los dispositivos en tiempo real e intervenir si la utilización supera los límites aceptables.

```
snmpwalk -v2c -c ironport
```

```
.1.3.6.1.4.1.15497.1.1.1.2
```

El uso de OID en los comandos SNMP proporciona acceso directo a métricas específicas para una supervisión y resolución de problemas eficaces.

Habilitar nombres simbólicos

```
export MIBS=ALL
```

La configuración de export MIBS=ALL permite que las herramientas SNMP utilicen nombres legibles definidos en los archivos MIB en lugar de OID numéricos largos. Esto facilita la escritura, la comprensión y la resolución de problemas de las consultas, ya que se puede hacer referencia a objetos con nombres significativos como workQueueMessages en lugar de secuencias de números.

Ejecutar consultas SNMP

Utilice snmpwalk para consultar ESA para métricas clave. Las consultas SNMP le permiten recuperar en tiempo real datos de estado y rendimiento de su ESA de Cisco. Mediante el uso de nombres simbólicos, puede supervisar fácilmente objetos específicos como el estado de la cola, la caducidad de la licencia y la utilización del hardware sin necesidad de hacer referencia a OID numéricos complejos.

Mensajes de cola de trabajo

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport
```

```
      workQueueMessages
ASYNCOS-MAIL-MIB::workQueueMessages.0 = Gauge32: 0
```

Este resultado muestra que actualmente hay cero mensajes en la cola de trabajo de ESA. El valor representa el número en tiempo real de correos electrónicos que esperan ser procesados.

Utilización de la CPU

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport
```

Esto indica que la CPU de ESA está actualmente en un 37% de utilización. El valor le proporciona información sobre la carga de procesamiento del dispositivo en el momento en que se ejecutó la consulta.

Tabla de vencimiento de claves de licencia

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport


       keyExpirationTable
ASYNCOS-MAIL-MIB::keyExpirationIndex.1 = INTEGER: 1
ASYNCOS-MAIL-MIB::keyExpirationIndex.2 = INTEGER: 2
ASYNCOS-MAIL-MIB::keyExpirationIndex.3 = INTEGER: 3
ASYNCOS-MAIL-MIB::keyExpirationIndex.4 = INTEGER: 4
ASYNCOS-MAIL-MIB::keyExpirationIndex.5 = INTEGER: 5
ASYNCOS-MAIL-MIB::keyExpirationIndex.6 = INTEGER: 6
ASYNCOS-MAIL-MIB::keyExpirationIndex.7 = INTEGER: 7
ASYNCOS-MAIL-MIB::keyExpirationIndex.8 = INTEGER: 8
ASYNCOS-MAIL-MIB::keyDescription.1 = STRING: Bounce Verification
ASYNCOS-MAIL-MIB::keyDescription.2 = STRING: Data Loss Prevention
ASYNCOS-MAIL-MIB::keyDescription.3 = STRING: External Threat Feeds
ASYNCOS-MAIL-MIB::keyDescription.4 = STRING: Incoming Mail Handling
ASYNCOS-MAIL-MIB::keyDescription.5 = STRING: IronPort Anti-Spam
ASYNCOS-MAIL-MIB::keyDescription.6 = STRING: IronPort Email Encryption
ASYNCOS-MAIL-MIB::keyDescription.7 = STRING: Outbreak Filters
ASYNCOS-MAIL-MIB::keyDescription.8 = STRING: Sophos Anti-Virus
ASYNCOS-MAIL-MIB::keyIsPerpetual.1 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.2 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.3 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.4 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.5 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.6 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.7 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.8 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.1 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.2 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.3 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.4 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.5 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.6 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.7 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.8 = Gauge32: 0
```

- keyExpirationIndex.X: Cada índice representa una clave de característica única instalada en Cisco ESA.
- keyDescription.X: Proporciona el nombre o la descripción de cada clave de característica, como 'Verificación de rebote', 'Prevención de pérdida de datos', 'IronPort Anti-Spam' y 'Sophos Anti-Virus'.
- keyIsPerpetual.X: Indica si la licencia de cada función es perpetua. El valor true (1) indica que la licencia no caduca.
- keySecondsUntilExpire.X: Muestra cuántos segundos quedan hasta que caduque la licencia. El valor 0 confirma que la licencia es perpetua o que ya ha caducado.

ejemplo de licencia

Este resultado confirma las claves de característica actuales del dispositivo, sus descripciones y el estado de la licencia. Todas las licencias enumeradas son perpetuas, como se indica en keyIsPerpetual y keySecondsUntilExpire. Esta información ayuda a garantizar que las funciones de seguridad esenciales permanecen activas y válidas en Cisco ESA.

Diferencia entre OID numéricos y nombres simbólicos

OID numéricos:

- Son universales y siempre funcionan, incluso si los archivos MIB no están cargados en el sistema.
- Ejemplo: .1.3.6.1.4.1.15497.1.1.1.2.
- Son menos legibles y pueden ser difíciles de recordar.

Nombres simbólicos:

- Estos son nombres descriptivos definidos en los archivos MIB, como perCentCPUtilization.
- Hacen que los comandos sean más fáciles de escribir y comprender.
- Requieren que los archivos MIB se carguen correctamente y que se configure la variable de entorno MIBS.
- Ejemplo: snmpwalk -v2c -c ironport 10.31.124.165 perCentCPUtilization.

¿Es lo mismo?

Ambos métodos consultan la misma métrica y producen resultados idénticos, pero los nombres simbólicos son más prácticos y legibles por las personas, mientras que los OID numéricos son más

confiables en entornos donde los archivos MIB no pueden estar presentes o cargados.

Información Relacionada

- Monitoreo del Estado y Estado del Sistema Usando SNMP
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).