Sistema de administración de red: Informe oficial de Mejores Prácticas

Contenido

Introducción

El modelo de administración de red de la Organización internacional para la normalización (ISO) define cinco áreas funcionales de la administración de red. Este documento abarca todas las áreas funcionales. El objetivo general de este documento es ofrecer recomendaciones prácticas en cada área funcional para aumentar la efectividad total de las prácticas y herramientas de administración actuales. También proporciona pautas de diseño para la implementación futura de tecnologías y herramientas de administración de redes.

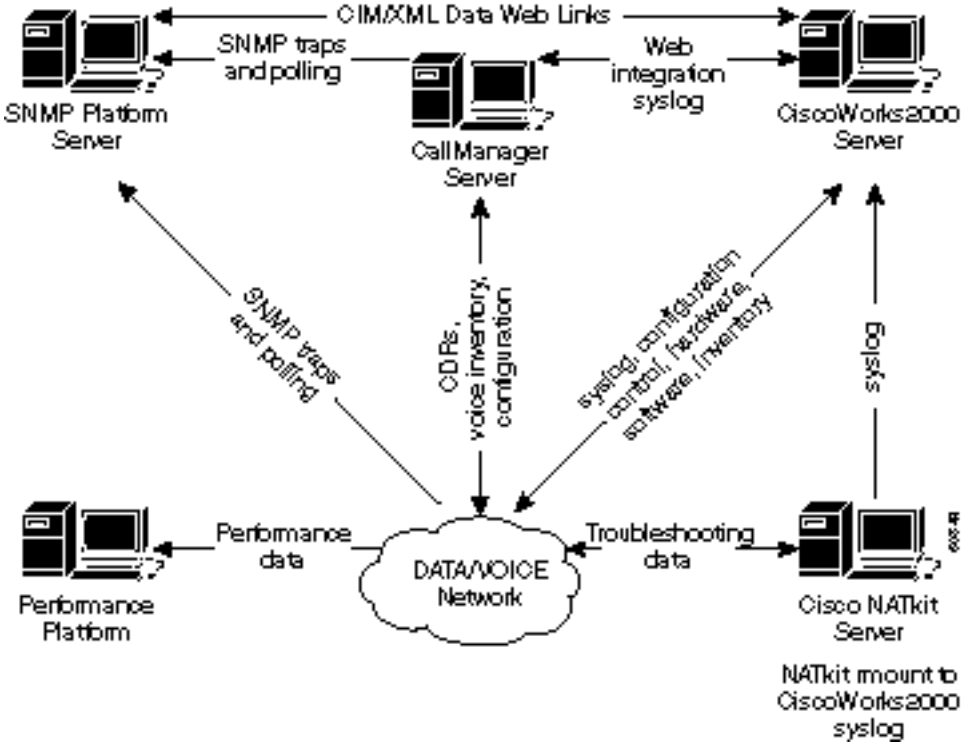
Administración de la red

A continuación, se enumeran las cinco áreas funcionales del modelo de administración de redes ISO.

- Administración de fallas: Detectar, aislar, notificar y corregir errores encontrados en la red.

- Administración de la configuración: Aspectos de configuración de los dispositivos de red, como la administración de archivos de configuración, la administración de inventario y la administración de software.
- Administración de rendimiento: Monitorear y medir varios aspectos del rendimiento para que el rendimiento general pueda mantenerse a un nivel aceptable.
- Administración de la seguridad: Proporcionar acceso a los dispositivos de red y a los recursos corporativos a las personas autorizadas.
- Administración de cuentas: Información de uso de los recursos de red.

El siguiente diagrama muestra una arquitectura de referencia que Cisco Systems considera como una solución mínima para la administración de una red de datos. Esta arquitectura incluye un servidor CallManager de Cisco para los que planean administrar el Protocolo de voz sobre IP (VoIP): El diagrama muestra cómo debe integrar el servidor del CallManager a la topología de NMS.



La arquitectura de administración de la red incluye lo siguiente:

- Plataforma del Protocolo de administración de red simple (SNMP) para la administración de fallas
- Plataforma de control del rendimiento para administración de rendimiento a largo plazo y análisis de tendencias.
- Servidor CiscoWorks2000 para la administración de configuración, la recolección de syslog y la administración del inventario de hardware y software

Algunas plataformas SNMP pueden compartir datos directamente con el servidor CiscoWorks2000 mediante los métodos de modelo de información común y de lenguaje de marcado extensible (CIM/XML). CIM es un modelo de datos común de un esquema implementación neutral para la descripción de la totalidad de la información de administración en un entorno de red/empresa. El CIM está formado por una especificación y un esquema. La especificación define los detalles para la integración con otros modelos de administración, como los MIB de SNMP o los archivos de información de administración del grupo de trabajo de administración de escritorio (MIF de DMTF), mientras que el esquema proporciona las descripciones de modelos reales.

XML es un lenguaje de marcado que se usa para representar datos estructurados en forma de texto. Un objetivo específico de XML era mantener la mayor parte del poder descriptivo de SGML y eliminar la mayor complejidad posible. En concepto, XML es similar a HTML pero mientras que HTML se utiliza para transmitir información gráfica acerca de un documento, XML se utiliza para representar datos estructurados en un documento.

Los clientes de servicios avanzados de Cisco también deberían incluir un servidor NATkit de Cisco para una supervisión proactiva y una solución de problemas adicionales. El servidor NATkit tiene un montaje de disco remoto (rmount) o acceso al Protocolo de transferencia de archivos (FTP) para los datos que se encuentran en el servidor CiscoWorks2000.

El capítulo Nociones básicas sobre administración de redes de la Descripción general de tecnología de conexión entre redes proporciona una visión general más detallada sobre las nociones básicas de administración de redes.

Administración de fallas'

El objetivo de la administración de fallas es detectar problemas de red, registrarlos, notificar a los usuarios de dichos problemas y (en la medida de lo posible) corregirlos automáticamente para mantener la red en funcionamiento eficazmente. Puesto que las fallas pueden causar tiempo de inactividad o degradación de la red inaceptable, la administración de las fallas es quizá uno de los elementos más implementados de la administración de redes ISO.

Plataformas de administración de redes

Una plataforma de administración de redes implementada en la empresa administra una infraestructura que consta de elementos de red de varios proveedores. La plataforma recibe y procesa eventos de los elementos de red en la red. Los eventos de los servidores y de otros recursos importantes también pueden ser reenviados a una plataforma de administración. Las siguientes funciones comúnmente disponibles se incluyen en una plataforma de administración estándar:

- Detección de redes
- Asignación de topología de los elementos de red
- Controlador de eventos
- Recolector y graficador de datos de rendimiento
- Explorador de datos de administración

Las plataformas de administración de red pueden verse como la consola principal para las operaciones de red en la detección de fallas en la infraestructura. La capacidad de detectar problemas rápidamente en cualquier red es fundamental. El personal de operaciones de redes puede basarse en un mapa gráfico de la red para visualizar los estados operativos de elementos críticos de la red, tales como routers y switches.

Las plataformas de gestión de redes, como HP OpenView, Computer Associates Unicenter y SUN Solstice, pueden llevar a cabo una búsqueda de dispositivos de red. Cada dispositivo de red está representado por un elemento gráfico en la consola de la plataforma de administración. Los diferentes colores en los elementos gráficos representan el estado de funcionamiento actual de los dispositivos de red. Los dispositivos de red se pueden configurar para enviar notificaciones, denominadas capturas de SNMP, a plataformas de administración de redes. Luego de recibir las notificaciones, el elemento gráfico que representa el dispositivo de red cambia de color en función de la gravedad de la notificación recibida. La notificación, normalmente denominada un evento, es

colocada en un archivo de registro. Es particularmente importante que la mayoría de los archivos de Base de información para administración (MIB) de Cisco se carguen en la plataforma SNMP para garantizar que las distintas alertas de los dispositivos de Cisco se interpreten correctamente.

Cisco publica los archivos de MIB para la administración de diferentes dispositivos de red. Los archivos MIB de Cisco están en el sitio web cisco.com e incluyen la siguiente información:

- Archivos MIB publicados en formato SNMPv1
- Archivos MIB publicados en formato SNMPv2
- Trampas de SNMP admitidas en dispositivos de Cisco
- OID para objetos de MIB de SNMP de Cisco actuales

Una serie de plataformas de administración de redes es capaz de administrar varios sitios distribuidos geográficamente. Esto se logra mediante el intercambio de datos de administración entre consolas de administración ubicadas en sitios remotos y con una estación de administración en el sitio principal. La principal ventaja de una arquitectura distribuida es que reduce el tráfico de administración, por lo que proporciona un uso más eficaz del ancho de banda. Una arquitectura distribuida también permite al personal administrar sus redes en forma local desde sitios remotos a través de sistemas.

Una mejora reciente introducida en las plataformas de administración consiste en la capacidad de administrar, de modo remoto, los elementos de la red mediante una interfaz web. Esta mejora elimina la necesidad de software de cliente especial en estaciones de usuario individual para acceder a una plataforma de administración.

Una empresa típica está compuesta de diferentes elementos de red. No obstante, cada dispositivo normalmente requiere sistemas de administración de elementos específicos del fabricante para administrar de manera eficaz los elementos de red. Por lo tanto, las estaciones de administración duplicadas podrían estar consultando elementos de red para la misma información. Los datos recolectados por diferentes sistemas son almacenados en bases de datos separadas, creando una administración general para los usuarios. Esta limitación ha impulsado a los proveedores de redes y software a adoptar estándares como Arquitectura de negociación de petición de objetos comunes (CORBA) y Fabricación integrada por computadora (CIM) para facilitar el intercambio de datos de administración entre las plataformas de administración y los sistemas de administración de elementos. Cuando los proveedores adoptan estándares para el desarrollo del sistema de administración, los usuarios pueden esperar interoperabilidad y ahorro de costos con relación a la implementación y a la administración de la infraestructura.

CORBA especifica un sistema que proporciona interoperabilidad entre objetos, en un entorno heterogéneo y distribuido, de un modo transparente para el programador. Su diseño se basa en el modelo de objetos del grupo de administración de objetos (OMG).

Infraestructura de solución de problemas

Los servidores de protocolo trivial de transferencia de archivos (TFTP) y de registro del sistema (syslog) son componentes fundamentales de una infraestructura de solución de problemas en las operaciones de red. El servidor TFTP se utiliza, fundamentalmente, para almacenar archivos de configuración e imágenes de software correspondientes a dispositivos de red. Los routers y los switches son capaces de enviar mensajes de registro de sistema a un servidor syslog. Los mensajes facilitan la función de resolución de problemas cuando éstos se detectan. Ocasionalmente, el personal de soporte de Cisco necesita los mensajes de syslog para realizar el análisis de la causa raíz.

La función de recolección de syslog distribuida de CiscoWorks2000 Resource Management Essentials (Essentials) permite el despliegue de varias estaciones de recolección UNIX o NT en sitios remotos para recolectar y filtrar mensajes. Los filtros pueden especificar cuáles serán los mensajes syslog que serán reenviados al servidor principal Essentials. Un beneficio importante de implementar la recopilación distribuida es la reducción de los mensajes reenviados a los principales servidores de syslog.

Detección de falla y notificación

El propósito del administrador de errores es detectar, aislar, notificar y corregir errores encontrados en la red. Los dispositivos de red pueden enviar alertas a las estaciones de administración cuando ocurre una falla en los sistemas. Un sistema de administración de fallas eficaz consta de varios subsistemas. La detección de fallas se realiza cuando los dispositivos envían mensajes de capturas de SNMP, sondeo de SNMP, umbrales de monitoreo remoto (RMON) y mensajes de syslog. Un sistema de administración alerta al usuario final cuando se informa una falla y se pueden tomar medidas correctivas.

Las capturas deben habilitarse de manera sistemática en los dispositivos de red. Las nuevas versiones del IOS de Cisco para routers y switches son compatibles con trampas adicionales. Es importante comprobar y actualizar el archivo de configuración para garantizar la decodificación correcta de las capturas. Una revisión periódica de las trampas configuradas con el equipo de Assured Network Service (ANS) de Cisco le asegurará de una manera eficaz detección de fallas en la red.

En la siguiente tabla, se enumeran las capturas de CISCO-STACK-MIB admitidas. Estas pueden utilizarse para supervisar las condiciones de falla en los switches de la red de área local (LAN) de Cisco Catalyst.

Trampa	Descripción
moduleUp	La entidad agente ha detectado que el **objeto moduleStatus en esta MIB ha pasado al estado correcto(2) para uno de sus módulos.**
moduleDown	La entidad agente ha detectado que el objeto moduleStatus en esta MIB ha hecho una transición fuera del estado ok(2) para uno de los módulos.
chassisAlarmOn	La entidad agente ha detectado que el objeto chassisTempAlarm, chassisMinorAlarm, o chassisMajorAlarm en este MIB ha hecho una transición al estado encendido (2). El objeto *chassisMajorAlarm indica la existencia de una de las siguientes condiciones:* • Cualquier falla de voltaje • Falla de ventilador y temperatura simultánea • Falla del suministro de energía del ciento por ciento (dos de dos o uno de uno) • Falla en la memoria de sólo lectura programable y borrable eléctricamente (EEPROM). • Falla de la memoria RAM no volátil

	(NVRAM) • Falla en la comunicación con MCP • Estado de NMP desconocido chassisMinorAlarm indica la existencia de una de las siguientes condiciones: • Alarma de temperatura • Falla de ventilador • Falla parcial del suministro de energía (una de dos) • Dos fuentes de alimentación de tipo incompatible
chassisAlarmOff	La entidad agente ha detectado que los objetos *chassisTempAlarm*, chassisMinorAlarm o *chassisMajorAlarm en esta MIB han pasado al estado* desconectado(1).

Las trampas de monitoreo de entorno (envmon) se definen en la trampa CISCO-ENVMON-MIB. La trampa envmon envía notificaciones de control del entorno específico de la empresa de Cisco cuando se excede un umbral de entorno. Cuando se utiliza envmon, puede activarse un tipo de trampa del entorno o pueden aceptarse todos los tipos de trampa del sistema de monitoreo del entorno. Si no se especifica una opción, se activan todos los tipos de entorno. Puede ser uno o más de los siguientes valores:

- Voltaje: ciscoEnvMonVoltageNotification se envía si el voltaje medido en un punto de prueba determinado está fuera del rango normal para el punto de prueba (por ejemplo, está en la etapa de advertencia, crítica o de apagado).
- Shutdown (apagado): ciscoEnvMonShutdownNotification se envía si el supervisor del entorno detecta que un punto de prueba está llegando a un estado crítico y está a punto de iniciar el apagado.
- Suministro: ciscoEnvMonRedundantSupplyNotification se envía si la fuente de alimentación redundante (en caso de que exista) falla.
- Ventilador: ciscoEnvMonFanNotification se envía si cualquiera de los ventiladores en el conjunto de ventiladores (en caso de que exista) falla.
- Temperatura: ciscoEnvMonTemperatureNotification se envía si la temperatura medida en un punto de prueba determinado está fuera del rango normal para el punto de prueba (por ejemplo, está en la etapa de advertencia, crítica o de apagado).

La detección de fallas y la supervisión de los elementos de la red pueden expandirse desde el nivel de los dispositivos hasta los niveles de protocolos e interfaces. Para un entorno de red, la supervisión de fallas puede incluir Virtual Local Area Network (VLAN), Asynchronous Transfer Mode (ATM), indicaciones de fallas en interfaces físicas, etc. La implementación de la administración de falla en el nivel de protocolo se puede llevar a cabo mediante un sistema de administración de elementos como CiscoWorks2000 Campus Manager. La aplicación TrafficDirector en Campus Manager se concentra en la administración del switch a través del uso de soporte de mini-RMON en switches Catalyst.

Ante una mayor cantidad de elementos de red y complejidad de los problemas de red, puede considerarse un sistema de administración de eventos que sea capaz de correlacionar diferentes eventos de red (syslog, trampa, archivos de registro). Esta arquitectura detrás de un sistema de administración de eventos se puede comparar con el sistema de Administrador de administradores (MOM). Un sistema de administración de eventos bien diseñado permite que el

personal del centro de operaciones de red (NOC) sea proactivo y eficaz para detectar y diagnosticar problemas de red. La supresión y priorización de eventos permiten que el personal de operaciones de red se concentre en eventos de red críticos, investigue varios sistemas de administración de eventos, como Cisco Info Center, y realice un análisis de factibilidad para analizar completamente las capacidades de esos sistemas. Para obtener más información, diríjase a Cisco info Center.

Supervisión y notificación de incidentes proactivos

La alarma y el evento RMON son dos grupos definidos dentro de la especificación RMON. Normalmente, una estación de administración realiza la consulta en los dispositivos de red a fin de determinar el estado o el valor de ciertas variables. Por ejemplo, una estación de administración consulta un router para hallar cuál es la utilización de la unidad central de procesamiento (CPU) y generar un evento cuando el valor llega a un umbral configurado. Este método desperdicia ancho de banda de red y también puede llegar a omitir el umbral, lo cual depende del intervalo de consulta.

Un dispositivo de red se configura con alarmas y eventos RMON, para controlar en sí mismo los aumentos y las caídas de umbrales. En un intervalo de tiempo predefinido, el dispositivo de red toma un ejemplo de una variable y la compara con los umbrales. Una notificación de SNMP se puede enviar a una estación de administración si el valor real supera o cae por debajo de los umbrales configurados. Los grupos de eventos y alarmas de RMON proporcionan un método proactivo para administrar los dispositivos de red críticos.

Cisco Systems recomienda implementar las alarmas y los eventos de RMON en dispositivos de red críticos. Las variables monitoreadas pueden incluir el uso de la CPU, las fallas en la memoria intermedia, las caídas de entrada/ salida o variables de tipos de números enteros. A partir de la versión de software Cisco IOS 11.1(1), todas las imágenes de router admiten los grupos de eventos y alarmas de RMON.

Para obtener información detallada acerca de la alarma RMON y la implementación de eventos, consulte la sección Alarma RMON e implementación de eventos.

Restricciones de memoria de RMON

El uso de memoria de RMON es constante en todas las plataformas de switches en relación con estadísticas, historiales, alarmas y eventos. RMON utiliza lo que se denomina depósito para almacenar historiales y estadísticas en el agente RMON (en este caso, el switch). El tamaño de la cubeta se define en la sonda RMON (dispositivo SwitchProbe) o en la aplicación RMON (herramienta TrafficDirector) y luego se envía al switch para configurarlo.

Se necesitan aproximadamente 450 K de espacio de código para admitir mini-RMON (por ejemplo, cuatro grupos RMON: estadísticas, historial, alarmas, y eventos). El requisito de memoria dinámica de RMON varía dado que depende de la configuración del tiempo de ejecución.

La siguiente tabla define la información sobre el uso de la memoria RMON de tiempo de ejecución para cada grupo mini-RMON.

Definición de grupo RMON	Espacio de DRAM utilizado	Notas

Estadísticas	140 bytes por puerto Ethernet/Fast Ethernet conmutado	Por puerto
Historial	3,6 K para depósitos de 50 *	Cada cubeta adicional utiliza 56 bytes.
Alarma y evento	2,6 K por alarma y sus correspondientes entradas de eventos	Por alarma por puerto

*RMON usa lo que se llama una cubeta para almacenar registros y estadísticas en el agente RMON (como un switch).

Alarma RMON e implementación de eventos

Al incorporar RMON como parte de la solución de administración de fallas, un usuario puede supervisar proactivamente la red antes de que ocurra un problema potencial. Por ejemplo, si la cantidad de paquetes de difusión recibidos aumenta de manera significativa, puede causar un aumento en la utilización de la CPU. Al implementar una alarma y un evento RMON, un usuario puede establecer un umbral para controlar la cantidad de paquetes de transmisión recibidos y alertar a la plataforma SNMP a través de una notificación de trampa SNMP si el umbral configurado es alcanzado. Las alarmas y los eventos RMON eliminan las consultas excesivas que normalmente realiza la plataforma SNMP para lograr el mismo objetivo.

Hay dos métodos disponibles para configurar la alarma y el evento de RMON:

- Interfaz de línea de comandos (CLI)
- SET DE SNMP

Los siguientes modelos de procedimiento muestran cómo establecer un umbral para supervisar la cantidad de paquetes de difusión recibidos en una interfaz. En estos procedimientos se utiliza el mismo contador que se muestra en el ejemplo del comando show interface al final de esta sección.

Ejemplo de interfaz de línea de comandos

Para implementar la alarma y evento RMON con una interfaz CLI, siga los pasos a continuación:

1. Busque el índice de interfaz asociado a Ethernet 0, recorriendo la MIB de ifTable.
```
interfaces.ifTable.ifEntry.ifDescr.1 = "Ethernet0"
interfaces.ifTable.ifEntry.ifDescr.2 = "Ethernet1"
interfaces.ifTable.ifEntry.ifDescr.3 = "FastEthernet0"
interfaces.ifTable.ifEntry.ifDescr.4 = "Fddi0"
```
2. Obtenga el OID relacionado con el campo CLI objeto de monitoreo. Para este ejemplo, el OID para las 'emisiones' es 1.3.6.1.2.1.2.2.1.12. Los OID de Cisco para variables MIB específicas están disponibles en el sitio Web cisco.com.
3. Determine los siguientes parámetros para configurar umbrales y eventos.umbrales descendentes y ascendentestipo de muestreo (absoluto o delta)intervalo de muestraacción cuando se alcanza el umbralA los efectos de este ejemplo, se configura un umbral para monitorear la cantidad de paquetes de difusión recibidos en Ethernet 0. Se generará una captura si la cantidad de paquetes de difusión recibida es superior a 500, entre muestras de

60 segundos. El umbral será reactivado cuando el número de difusiones de entrada no aumente entre las muestras tomadas.**Nota:** Para obtener información detallada sobre estos parámetros de comando, consulte la documentación de Cisco Connection Online (CCO) para ver los comandos de alarma y evento RMON para su versión específica de Cisco IOS.

4. Para especificar la trampa enviada (evento RMON) cuando se alcanza el umbral, ejecute los siguientes comandos CLI (Los comandos del IOS de Cisco se muestran en negrita):**rmon event 1, descripción de la trampa del gateway "High Broadcast on Ethernet 0" dueño ciscormon event 2 log description "normal broadcast received on ethernet 0" owner cisco**
5. Especifique los umbrales y parámetros relevantes (alarma RMON) utilizando los siguientes comandos CLI:**alarma rmon 1 ifEntry.12.1 60 delta umbral de límite superior 500 1falling-threshold 0 2 owner cisco**
6. Utilice SNMP para consultar estas tablar y verificar que las entradas de eventTable hayan sido realizadas en el dispositivo.

```
rmon.event.eventTable.eventEntry.eventIndex.1 = 1

rmon.event.eventTable.eventEntry.eventIndex.2 = 2

rmon.event.eventTable.eventEntry.eventDescription.1 =
"High Broadcast on Ethernet 0"

rmon.event.eventTable.eventEntry.eventDescription.2 =
"normal broadcast received on ethernet 0"

rmon.event.eventTable.eventEntry.eventType.1 = snmp-trap(3)

rmon.event.eventTable.eventEntry.eventType.2 = log(2)

rmon.event.eventTable.eventEntry.eventCommunity.1 = "gateway"

rmon.event.eventTable.eventEntry.eventCommunity.2 = ""

rmon.event.eventTable.eventEntry.eventLastTimeSent.1 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventLastTimeSent.2 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventOwner.1 = "cisco"

rmon.event.eventTable.eventEntry.eventOwner.2 = "cisco"

rmon.event.eventTable.eventEntry.eventStatus.1 = valid(1)

rmon.event.eventTable.eventEntry.eventStatus.2 = valid(1)
```

7. Utilice SNMP para consultar estas tablas y verificar que las entradas de alarmTable hayan sido establecidas.

```
rmon.alarm.alarmTable.alarmEntry.alarmIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmInterval.1 = 60

rmon.alarm.alarmTable.alarmEntry.alarmVariable.1 = OID:
interfaces.ifTable.ifEntry.ifInNUcastPkts.2

rmon.alarm.alarmTable.alarmEntry.alarmSampleType.1 = absoluteValue(1)

rmon.alarm.alarmTable.alarmEntry.alarmValue.1 = 170183

rmon.alarm.alarmTable.alarmEntry.alarmStartupAlarm.1 =
risingOrFallingAlarm(3)
```

```
rmon.alarm.alarmTable.alarmEntry.alarmRisingThreshold.1 = 500

rmon.alarm.alarmTable.alarmEntry.alarmFallingThreshold.1 = 0

rmon.alarm.alarmTable.alarmEntry.alarmRisingEventIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmFallingEventIndex.1 = 2

rmon.alarm.alarmTable.alarmEntry.alarmOwner.1 = "cisco"

rmon.alarm.alarmTable.alarmEntry.alarmStatus.1 = valid(1)
```

Ejemplo de la operación SNMP SET

Para implementar la alarma y el evento RMON con la operación de establecimiento de SNMP, siga estos pasos:

1. Especifique la captura enviada (evento RMON) cuando se alcance el umbral mediante las siguientes operaciones de SNMP SET:
```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.1
  octetstring "High Broadcast on Ethernet 0"
  eventDescription.1 : DISPLAY STRING- (ascii): High Broadcast on Ethernet 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.1
  integer 3 eventType.1 : INTEGER: SNMP-trap

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.4.1 octetstring "gateway"
  eventCommunity.1 : OCTET STRING- (ASCII): gateway

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.1
  octetstring "cisco" eventOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.1 integer 1
  eventStatus.1 : INTEGER: valid
```
2. Especifique los umbrales y los parámetros relevantes (alarma RMON) mediante las siguientes operaciones SNMP SET:
```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.2
  octetstring "normal broadcast received on ethernet 0"
  eventDescription.2 : DISPLAY STRING- (ASCII): normal broadcast
  received on ethernet 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.2 integer 2
  eventType.2 : INTEGER: log

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.2 octetstring "cisco"
  eventOwner.2 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.2 integer 1
  eventStatus.2 : INTEGER: valid
```
3. Consulte estas tablar para verificar que las entradas de eventTable hayan sido realizadas en el dispositivo.
```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.9.1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.2.1 integer 60
  alarmInterval.1 : INTEGER: 60

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.3.1
 objectidentifier .1.3.6.1.2.1.2.2.1.12.2
  alarmVariable.1 : OBJECT IDENTIFIER:
```

```
.iso.org.dod.internet.mgmt.mib2.interfaces.ifTable
  ifEntry.ifInNUcastPkts.2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.4.1 integer 2

alarmSampleType.1 : INTEGER: deltaValue

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.7.1 integer 500
  alarmRisingThreshold.1 : INTEGER: 500

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.8.1 integer 0
  alarmFallingThreshold.1 : INTEGER: 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.9.1 integer 1
  alarmRisingEventIndex.1 : INTEGER: 1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.10.1 integer 2
  alarmFallingEventIndex.1 : INTEGER: 2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.11.1 octetstring
"cisco"
  alarmOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.12.1 integer 1
  alarmStatus.1 : INTEGER: valid
```

4. Consulte estas tablas para verificar que las entradas de alarmTable hayan sido establecidas.
   ```
   % snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1
   ```

show interface

Este ejemplo es un resultado del comando **show interface.**

gateway> **show interface ethernet 0**

```
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0000.0c38.1669 (bia 0000.0c38.1669)
Description: NMS workstation LAN
Internet address is 172.16.97.132/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 27 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
21337627 packets input, 3263376846 bytes, 0 no buffer

Received 7731303 broadcasts , 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
17328035 packets output, 2824522759 bytes, 0 underruns
174 output errors, 44368 collisions, 4 interface resets
0 babbles, 0 late collision, 104772 deferred
174 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Administración de la Configuración

La meta de la administración de la configuración es supervisar la red y la información de configuración del sistema para que los efectos de varias versiones de elementos de hardware y software sobre la operación de la red puedan rastrearse y administrarse.

Normas de configuración

Con una cantidad cada vez mayor de dispositivos de red implementados, es fundamental poder identificar con precisión la ubicación de un dispositivo de red. Esta información de ubicación debería proveer una descripción detallada que tenga sentido para los que tengan tareas con recursos de envío cuando se produce un error en la red. Para acelerar una solución si ocurren problemas en la red, asegúrese de contar con información de contacto disponible de la persona o departamento responsable de los dispositivos. La información de contacto debería incluir el número de teléfono y el nombre de la persona o departamento.

Las convenciones para la asignación de nombres de los dispositivos de red, desde el nombre del dispositivo a la interfaz individual, deben planificarse e implementarse como parte del estándar de configuración. Una convención de nomenclatura bien definida le brinda al personal la capacidad de proporcionar información precisa a la hora de solucionar problemas de red. La convención de nomenclatura para los dispositivos puede utilizar la ubicación geográfica, el nombre del edificio, el piso, etc. Para la convención de denominación de interfaz, puede incluir el segmento al cual se conecta un puerto, el nombre del hub de conexión, etcétera. En interfaces seriales, debe incluir el ancho de banda real, el número de identificador de conexión de link de datos (DLCI) local (en caso de retransmisión de tramas), el destino y la Id. del circuito o la información suministrada por la portadora.

Administración del archivo de configuración

Cuando se agregan comandos nuevos de configuración a las necesidades de los dispositivos de red existentes, se debe verificar la integridad de los comandos antes de llevar a cabo la implementación. Un dispositivo de red configurado incorrectamente puede tener un efecto desastroso en el rendimiento y la conectividad de la red. La configuración y los parámetros de comando deben controlarse para evitar problemas de discordancia e incompatibilidad. Se recomienda planificar una revisión regular y exhaustiva de las configuraciones con los ingenieros de Cisco.

Un CiscoWorks2000 Essentials totalmente funcional permite realizar una copia de respaldo de los archivos de configuración en los routers y los switches Cisco Catalyst automáticamente. La característica de seguridad de Essentials se puede usar para realizar autenticación en los cambios de configuración. Está disponible un registro de auditoría de cambios para rastrear los cambios y el nombre de usuario de los individuos que los ejecutan. Para los cambios de configuración en varios dispositivos, hay dos opciones disponibles: el NetConfig basado en la web, en la versión actual de CiscoWorks2000 Essentials, o el script **cwconfig.** Los archivos de configuración se pueden descargar y cargar mediante CiscoWorks2000 Essentials con las plantillas predefinidas o definidas por el usuario.

Estas funciones pueden realizarse mediante las herramientas de administración de configuración en CiscoWorks2000 Essentials:

- Mueva loMueva los archivos de configuración del archivo de configuración Essentials a un dispositivo o a varios dispositivos.
- Extraiga la configuración del dispositivo al archivo Essentials.

- Extraer la configuración más reciente del archivo y escribirla en un archivo.
- Importe la configuración desde un archivo y aplíquela a los dispositivos
- Compare las últimas dos configuraciones en el archivo Essentials.
- Eliminar las configuraciones anteriores a una fecha especificada o una versión del archivo.
- Copiar la configuración de inicio a la configuración en ejecución

Inventory Management

La función de descubrimiento de la mayoría de las plataformas de administración de redes tiene como objetivo proporcionar un listado dinámico de los dispositivos encontrados en la red. Se deben utilizar motores de detección como los implementados en las plataformas de administración de redes.

Una base de datos de inventario proporciona información de configuración detallada sobre los dispositivos de red. La información frecuente incluye modelos de hardware, módulos instalados, imágenes de software, niveles de microcódigo, etc. Todos estos elementos de información son cruciales para completar tareas como el mantenimiento de software y hardware. El listado actualizado de los dispositivos de red generados por el proceso de detección puede usarse como una lista maestra para recolectar información del inventario por medio de SNMP o de la secuencia de comandos. Puede importarse una lista de dispositivos del CiscoWorks2000 Campus Manager a la base de datos del inventario del CiscoWorks2000 Essentials para obtener un inventario actualizado de los switches Catalyst de Cisco.

Administración de software

Una actualización exitosa de las imágenes del IOS de Cisco en los dispositivos de red requiere un análisis detallado de los requerimientos tales como memoria, ROM de inicio, nivel de microcódigo, etc. Los requisitos suelen estar documentados y disponibles en el sitio web de Cisco a modo de notas de la versión y guías de instalación. El proceso de actualización de un dispositivo de red que ejecuta el IOS de Cisco incluye descargar una imagen correcta desde un CCO, efectuar una copia de respaldo de la imagen actual, asegurarse de que todos los requisitos de hardware estén cubiertos, y luego descargar la nueva imagen en el dispositivo.

La ventana de actualización para completar el mantenimiento del dispositivo es muy limitada para algunas organizaciones. En un gran entorno de red con recursos limitados, podría ser necesario programar y automatizar las actualizaciones de software luego de las horas hábiles. Se puede completar el procedimiento mediante un lenguaje de secuenciación de comandos como Expect, o mediante una aplicación diseñada específicamente para realizar ese tipo de tareas.

Se debe realizar un seguimiento de los cambios en el software de los dispositivos de red, como las imágenes de Cisco IOS y las versiones de microcódigo, para facilitar la etapa de análisis cuando se requiere otro mantenimiento de software. Con un informe del historial de modificaciones fácilmente disponible, la persona que realiza la actualización puede minimizar el riesgo de cargar imágenes o microcódigos no compatibles en los dispositivos de red.

Administración de rendimiento

Contrato de nivel de servicio

Un acuerdo de nivel de servicio (SLA) es un acuerdo escrito entre el proveedor del servicio y sus

clientes sobre el nivel de rendimiento esperado de los servicios de red. El SLA consta de métricas acordadas entre el proveedor y sus clientes. Los valores configurados para las mediciones deben ser realistas, significativos y cuantificables para ambas partes.

Se pueden recopilar diferentes estadísticas de interfaz de los dispositivos de red para medir el nivel de rendimiento. Estas estadísticas pueden incluirse como métricas en el SLA. Las estadísticas, como las caídas de colas de entrada, las caídas de colas de salida y los paquetes ignorados, son útiles para diagnosticar problemas relacionados con el rendimiento.

A nivel de dispositivos, la medición del rendimiento pude incluir el uso de la CPU, la asignación del búfer (búfer grande y mediano, fallas y radio hit) y la asignación de la memoria. El rendimiento de ciertos protocolos de red está directamente relacionado con la disponibilidad de memoria intermedia en los dispositivos de red. La medición de las estadísticas de rendimiento a nivel del dispositivo son fundamentales para optimizar el rendimiento de los protocolos de alto nivel.

Los dispositivos de red, como los routers, admiten diversos protocolos de capa superior, como el grupo de trabajo de conmutación de enlace de datos (DLSW), el puente de ruta de origen remoto (RSRB), AppleTalk, etc. Pueden controlarse y recolectarse las estadísticas de rendimiento de las tecnologías de Wide Area Network (WAN) incluyendo Frame Relay, ATM, el Integrated Services Digital Network (ISDN) y otras.

Supervisión del rendimiento, medición e informes

Las diferentes mediciones del rendimiento en la interfaz, en el dispositivo o en los niveles de protocolo deberían recolectarse de forma regular utilizando SNMP. El motor del sondeo en un sistema de administración de red puede ser utilizado para fines de recolección de datos. La mayoría de los sistemas de administración de red son capaces de recolectar, almacenar y presentar los datos de sondeo.

Existen varias soluciones disponibles en el mercado para abordar las necesidades de administración de rendimiento para entornos empresariales. Estos sistemas son capaces de recolectar, almacenar y presentar datos de los dispositivos de red y los servidores. La interfaz basada en la web, en la mayoría de los productos, hace que los datos de rendimiento sean accesibles desde cualquier lugar de la empresa. Algunas de las soluciones de administración de rendimiento comúnmente implementadas son:

- InfoVista VistaView
- SAS IT Service Vision
- Trinagy TREND

Una evaluación de los productos antes mencionados determinará si cumplen con los requisitos de diferentes usuarios. Algunos proveedores admiten la integración con plataformas de administración de redes y de administración de sistemas. Por ejemplo, InfoVista es compatible con BMC Patrol Agent a fin de proporcionar estadísticas esenciales de rendimiento de servidores de aplicación. Cada producto posee un modelo de valuación diferente así como también capacidades diferentes con la oferta base. El soporte para funciones de administración de rendimiento para dispositivos Cisco como NetFlow, RMON y el Informante de hora del agente/respuesta para garantía de servicio del IOS de Cisco (RTR/SAA CSAA/RTR) está disponible en algunas soluciones. Recientemente, Concord agregó compatibilidad para switches WAN de Cisco que pueden utilizarse para reunir y visualizar datos de rendimiento.

La función CSAA/RTR Service Assurance Agent (SAA)/Response Time Reporter (RTR) [CSAA/RTR Agente de garantía de servicio (SAA)/Generador de informes de tiempo de respuesta

(RTR)] en Cisco IOS puede utilizarse para medir el tiempo de respuesta entre dispositivos IP. Un router de origen configurado con CSAA configured es capaz de medir el tiempo de respuesta hacia un dispositivo IP de destino, que puede ser un router o un dispositivo IP. El tiempo de respuesta puede medirse entre el origen y el destino o para cada salto a lo largo de trayecto. Las trampas SNMP pueden configurarse para alertar a las consolas de administración si el tiempo de respuesta excede los umbrales predefinidos.

Las actualizaciones recientes del IOS de Cisco extienden la capacidad del CSAA para medir lo siguiente:

- Rendimiento del servicio de Protocolo de transferencia de hipertexto (HTTP)Búsqueda del sistema de nombres de dominio (DNS)Conectar el protocolo de control de transmisión (TCP)Tiempo de transacción HTTP
- Varianza del retraso entre paquetes (fluctuación) del tráfico de Voz sobre IP (VoIP)
- Tiempo de respuesta entre los terminales para una calidad de servicio específica (QoS)Bits de tipo de servicio (ToS) IP
- Pérdida de paquetes mediante el uso de paquetes generados de CSAA

La configuración de la función de CSAA en los routers se puede realizar mediante la aplicación Cisco Internetwork Monitoring Performance (IPM). La función CSAA/RTR está incrustada en muchas pero no en todos los conjuntos de funciones del software Cisco IOS. Se debe instalar una versión del software Cisco IOS, que admita CSAA/RTR, en el dispositivo que utiliza IPM para recopilar estadísticas de rendimiento. Si desea ver un resumen de las versiones del IOS de Cisco que admiten CSAA/RTR/IPM, consulte el sitio Web Preguntas frecuentes acerca de IPM.

La información adicional relacionada con IPM incluye lo siguiente:

- Información general de IPM
- Agente de garantía del servicio

Análisis y ajuste del rendimiento

El tráfico de los usuarios ha aumentado considerablemente y ha generado una mayor demanda de recursos de red. Los administradores de red suelen tener una visión limitada de los tipos de tráfico que se ejecutan en la red. El perfil de tráfico de aplicación y de usuario proporciona una vista detallada del tráfico en la red. Dos tecnologías, sondas RMON y NetFlow proporcionan la capacidad de recopilar perfiles de tráfico.

RMON

Los estándares RMON están diseñados para implementarse en una arquitectura distribuida en la que los agentes (ya sea integrados o en sondas independientes) se comunican con una estación central (la consola de administración) mediante SNMP. La norma RFC 1757 RMON organiza las funciones de monitoreo en nueve grupos para poder utilizar las topologías Ethernet y agrega un décimo grupo en RFC 1513 para parámetros únicos de Token Ring. El monitoreo de enlaces Fast Ethernet se proporciona en el marco del estándar RFC 1757, y el monitoreo de anillo de la interfaz de datos distribuidos por fibra óptica (FDDI) se proporciona en el marco de los estándares RFC 1757 y RFC 1513.

La especificación emergente RMON para RFC 2021 lleva a las normas de supervisión remota más allá de la capa de control de acceso a medios (MAC) y hasta las capas de aplicación y de red. Esta configuración permite a los administradores analizar aplicaciones en red y resolver

problemas relacionados con ellas, como tráfico Web, NetWare, notas, correo electrónico, acceso a la base de datos, sistema de archivos de red (NFS), entre otros. Actualmente, los grupos de alarmas, estadísticas, historiales y de host/conversación de RMON pueden utilizarse para supervisar y realizar el mantenimiento de la disponibilidad de la red de manera proactiva en base al tráfico de la capa de aplicación, el tráfico más importante en la red. RMON2 permite que los administradores de redes continúen con la implementación de soluciones de monitoreo basado en estándares para admitir aplicaciones basadas en el servidor y de misión crítica.

En las siguientes tablas se enumeran las funciones de los grupos RMON.

Grupo RMON (RFC 1757)	Función
Estadísticas	Contadores para paquetes, octetos, difusiones, errores y ofertas en el segmento o el puerto.
Historial	Muestra y guarda periódicamente los contadores de grupos de estadística para la recuperación futura.
Hosts	Mantener estática en cada dispositivo del host en el segmento o el puerto.
Host Top N	Un informe de subconjuntos definido por el usuario del grupo Hosts, con la clasificación a cargo de un contador estadístico. Al devolver únicamente los resultados se minimiza el tráfico de administración.
Matriz de tráfico	Mantiene las estadísticas de conversaciones entre los hosts de la red.
Alarmas	Un umbral que pueda establecerse en las variables de RMON críticas para una administración proactiva.
Events	Genera trampas SNMP y entradas de registro cuando se excede un umbral del grupo de alarmas.
Captura de paquete	Administra los búferes de los paquetes capturados por el grupo de filtro para la carga en la consola de administración.
Token Ring	Estación de anillo: Estadísticas detalladas de estaciones individuales. Orden de la estación de anillo: Una lista ordenada de las estaciones que están actualmente en el anillo. Configuración de la estación de anillo: Configuración e inserción/eliminación por estación. Enrutamiento de origen: Estadísticas sobre el enrutamiento de origen, como el conteo de saltos, etc.

RMON2	Función
Directorio Protocol (Protocolo)	Protocolos para los que el agente monitorea y mantiene estadísticas.
Distribución del protocolo	Estadísticas de cada protocolo.
Host de capa de red	Estadísticas para cada dirección de capa de red en el segmento, anillo o puerto.
Matriz de capa de red	Estadísticas de tráfico para pares de las direcciones de capa de red.
Host de capa de aplicación	Estadísticas por protocolo de capa de aplicación para cada dirección de red.
Matriz de capa de Aplicación	Estadísticas de tráfico mediante el protocolo de capa de aplicación para pares de direcciones de capas de red.
Historial que puede ser definido por el usuario	Extiende el historial más allá de las estadísticas de la capa de enlace de RMON1 con el fin de incluir las estadísticas de RMON, RMON2, MIB-I o MIB-II.
Correspondencia de direcciones	Enlaces de direcciones de la capa de MAC a la red.
Grupo de configuración	Capacidades del agente y configuraciones.

Netflow

La característica Cisco NetFlow permite obtener estadísticas detalladas del flujo de tráfico a ser recolectadas a los fines de la planificación de la capacidad, la facturación y las funciones de resolución de problemas. Se puede configurar NetFlow en interfaces individuales, ofreciéndole información al tráfico que pasa a través de las interfaces. Los siguientes tipos de información son parte de las estadísticas de tráfico detalladas:

- Direcciones IP de origen y de destino
- Números de interfaz de entrada y salida
- Puerto de origen TCP/UPD y puertos de destino
- Cantidad de bytes y de paquetes en el flujo.
- Números del sistema autónomo de origen y destino
- Tipo de servicio (TOS) de IP

Los datos de NetFlow recolectados en los dispositivos de red se exportan a una máquina recolectora. El recolector realiza funciones como la reducción de la cantidad de datos (filtración y agregación), el almacenamiento jerárquico de datos y la administración del sistema de archivos. Cisco provee las aplicaciones NetFlow Collector y NetFlow Analyzer para reunir y analizar datos de routers y switches Cisco Catalyst. También existen herramientas shareware como cflowd que pueden recopilar registros del Protocolo de datagrama de usuario (UDP) de Cisco NetFlow.

Los datos NetFlow se transportan mediante el uso de los paquetes UDP en tres formatos diferentes:

- Versión 1: El formato original admitido en las versiones iniciales de NetFlow.
- Versión 5: Una mejora posterior que agregó información del sistema autónomo del protocolo BGP (Border Gateway Protocol) y números de secuencia de flujo.
- Versión 7: Una mejora aún más reciente que agregó soporte de switching de NetFlow para switches Cisco Catalyst de la serie 5000, junto con una tarjeta de función de NetFlow (NFFC).

Las versiones 2 a 4 y la versión 6 no se emitieron o no son admitidas por el FlowCollector En las tres versiones, el datagrama consiste en un encabezado y una o más grabaciones de flujo.

Si desea obtener más información, consulte el informe oficial sobre la Guía de soluciones de servicio .

La siguiente tabla describe las versiones del IOS de Cisco admitidas para recolectar información de NetFlow desde los routers y switches Catalyst.

Versión de software del IOS de Cisco	Plataforma(s) de hardware Cisco admitida(s)	Versión(es) exportada(s) de NetFlow admitida(s)
11.1 CA y 11.1 CC	7200, 7500 y RSP7000 de Cisco	V1 y V5
11.2 y 11.2 P	7200, 7500 y RSP7000 de Cisco	V1
11,2 P	Cisco Route Switch Module (RSM)	V1
11,3 y 11,3 T	7200, 7500 y RSP7000 de Cisco	V1
12.0	1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000 de Cisco y RSM	V1 y V5
12,0 T	1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8800 RPM, y BPX 8600 de Cisco	V1 y V5
12.0(3)T y posteriores	1600*, 1720, 2500**, 2600, 3600, 4500, 4700, AS5300*, AS5800, 7200, uBR7200, 7500, RSP7000,	V1, V5 y V8

	RSM, MGX8800 RPM y BPX 8650 de Cisco.	
12.0(6)S	Cisco 12000	V1, V5 y V8
—	Cisco Catalyst 5000 con tarjeta de función de NetFlow (NFFC) ***	V7

* La compatibilidad con NetFlow Export V1, V5 y V8 en las plataformas Cisco 1600 y 2500 está dirigida a la versión de software Cisco IOS 12.0(T). El soporte NetFlow para estas plataformas no está disponible en la versión estándar de Cisco IOS 12.0.

** El soporte para NetFlow V1, V5 y V8 en la plataforma AS5300 está diseñado para versión de software Cisco IOS 12.06(T).

*** La exportación de datos MLS y NetFlow es soportada por la versión 4.1(1) o posterior de la serie 5000 del software del motor supervisor de Catalyst.

Administración de seguridad:

El objetivo de la administración de la seguridad es controlar el acceso a los recursos de red de acuerdo con las pautas locales, de modo que la red no pueda ser saboteada (intencional o no intencionalmente). Un subsistema de administración de seguridad, por ejemplo, puede monitorear a los usuarios que ingresan a un recurso de la red, rechazando el acceso a aquellos que ingresan códigos de acceso inapropiados. La administración de la seguridad es un tema muy amplio. por lo tanto esta parte del documento únicamente cubre la seguridad relacionada con SNMP y con la seguridad de acceso a los dispositivos básicos.

La información detallada sobre seguridad avanzada incluye lo siguiente:

- Mejora de la seguridad en las redes IP
- OpenSystems

Una buena implementación de la administración de seguridad comienza con el establecimiento de políticas y procedimientos de seguridad razonables. Es importante crear un estándar de configuración mínimo de plataforma específica para todos los routers y switches que cumplen con las mejores prácticas de la industria relativas a seguridad y rendimiento.

Existen varios métodos para controlar el acceso en los routers de Cisco y los switches Catalyst. Algunos de estos métodos son:

- Listas de control de acceso (ACL)
- ID de usuario y contraseñas locales del dispositivo
- Sistema de control de acceso al controlador de acceso al terminal (TACACS)

TACACS es un protocolo de seguridad estándar del Grupo de Trabajo de Ingeniería de Internet (RFC 1492) que se ejecuta entre dispositivos cliente en una red y contra un servidor TACACS. TACACS es un mecanismo de autenticación que se utiliza para autenticar la identidad de un dispositivo en la búsqueda de un acceso remoto a una base de datos privilegiada. Las variaciones de TACACS incluyen TACACS +, la arquitectura AAA que separa las funciones de autenticación, autorización y auditoría.

Cisco usa TACACS+ para permitir un mejor control sobre quiénes pueden acceder al dispositivo de Cisco en modo privilegiado y no privilegiado. Se pueden configurar varios servidores TACACS + para la tolerancia de fallos. Con TACACS+ habilitado, el router y el switch solicita al usuario su nombre y contraseña. La autenticación puede configurarse para el control del inicio de sesión o para autenticar comandos individuales.

Autenticación

La autenticación es el proceso de identificación de usuarios, que incluye el cuadro de diálogo de inicio de sesión y contraseña, el desafío y respuesta y el soporte de mensajería. La autenticación es la manera en que se identifica al usuario antes de permitir el acceso al router o al switch. Existe una relación fundamental entre la autenticación y la autorización. Mientras más privilegios de autorización tiene un usuario, la autenticación debe ser más estricta.

Autorización

La autorización provee control de acceso remoto, lo cual incluye una autorización por única vez y autorización por cada servicio requerido por el usuario. En un router Cisco, el rango del nivel de autorización para los usuarios es de 0 a 15, donde 0 representa el nivel más bajo y 15 el más alto.

Contabilidad

La auditoría permite recopilar y enviar información de seguridad que se utiliza para la facturación, el registro y la generación de informes, como la identidad de los usuarios, los tiempos de inicio y detención, y los comandos ejecutados. La contabilidad permite a los administradores de red realizar un seguimiento de los servicios a los que acceden los usuarios, así como la cantidad de recursos de red que consumen.

En la siguiente tabla aparecen ejemplos de comandos básicos para utilizar la autenticación, autorización, contabilidad y TACACS+ en un router de Cisco y en un switch Catalyst. Consulte el documento Comandos de autenticación, autorización y auditoría para conocer los comandos con más detalle.

Comando del IOS de Cisco	**Propósito**
Router	
aaa new-model	Habilite el protocolo de autenticación, autorización y contabilización (AAA) como método principal de control de acceso.
AAA accounting {*system* | *red* | *conexión* | *exec* | *nivel de comando*} {*start-stop* | *wait-start* | *stop only*} {*tacacs+* | *radius*}	Activar contabilidad con los comandos de configuración global.
AAA authentication	Configure el router de modo que las conexiones a cualquier línea de

login default tacacs+	terminal configurada con el inicio de sesión predeterminado se autenticará con TACACS + y fallará si la autenticación falla por cualquier motivo.
AAA authorization exec default tacacs+ none	Configure el router para verificar si el usuario tiene permiso para ejecutar un shell interrogando al servidor TACACS+.
tacacs-server host *tacacs+ server ip address*	Especificar el servidor TACACS+ que será utilizado para autenticación con los comandos de configuración global.
tacacs-server key shared-secret	Especifique el secreto compartido que conocen los servidores TACACS+ y el router de Cisco mediante el comando de configuración global.
Catalyst Switch	
set authentication login tacacs enable [*all* | *consola* | *http* | *telnet*] [*primary*]	Habilite la autorización de TACACS+ para el modo de inicio de sesión normal. Use las palabras clave de la consola o Telnet con el fin de activar la autorización de TACACS+ solo para el puerto de la consola o los intentos de conexión Telnet.
set authorization exec enable {option} fallback option} [*console* | *telnet* | *ambos*]	Habilite la autorización para el modo de inicio de sesión normal. Use las palabras clave de la consola o Telnet para activar la autorización sólo para el puerto de consola o los intentos de conexión Telnet.
Set tacacs-server key *shared-secret*	Especifique el secreto compartido que conocen los servidores TACACS+ y el switch.
Set tacacs-server host tacacs+ server ip address	Especificar el servidor TACACS+ que será utilizado para autenticación con los comandos de configuración global.
Set accounting commands enable {*config* | *todo*} {*stop-only*} *tacacs+*	Habilite los comandos de configuración de cuentas.

Para obtener más información acerca de cómo configurar AAA para supervisar y controlar el acceso a la interfaz de la línea de comandos de los switches Catalyst de LAN corporativas, consulte el documento Control de acceso al conmutador mediante la autenticación, la autorización y la contabilización.

Seguridad SNMP

El protocolo SNMP puede utilizarse para hacer cambios en la configuración en routers y switches Catalyst similar a los que se ejecutan desde el CLI. Las medidas de la adecuada seguridad deberían configurarse en los dispositivos de la red para evitar el acceso no autorizado y cambiar vía SNMP. Las cadenas de comunidad deben seguir las pautas de contraseña estándar para la longitud, los caracteres y la dificultad de adivinación. Es importante cambiar los valores predeterminados público y privado de las identificaciones de comunidad.

Todos los host(s) de administración de SNMP deberían tener una dirección IP estática y habría que conferirles derechos de comunicación SNMP con el dispositivo de red predefinido por una dirección IP y una Lista de control de acceso (ACL). El software de Cisco IOS y Cisco Catalyst provee características de seguridad los que asegura que sólo las estaciones de administración autorizadas tienen permitido efectuar cambios en los dispositivos de la red.

Funciones de seguridad del router

Nivel de privilegio de SNMP

Esta función limita los tipos de operaciones que puede tener una estación de administración en un router. Existen dos tipos de niveles de privilegio en los routers: solo lectura (RO), y lectura y escritura (RW). El nivel RO sólo permite que una estación de administración consulte los datos del router. No permite la ejecución de comandos de configuración como el reinicio del router y el apagado de interfaces. Sólo puede utilizarse el nivel de privilegio RW para realizar dichas operaciones.

Listas de control de acceso SNMP (ACL)

La característica ACL SNMP puede utilizarse en conjunto con la característica de privilegio SNMP para limitar la solicitud de información de administración a los routers por parte de estaciones de administración específicas.

Vistas de SNMP

Esta característica limita la información específica que puede obtenerse de routers por medio de estaciones de administración. Puede usarse con el nivel de privilegio SNMP y las funciones ACL para asegurar el acceso restringido de datos por las consolas de administración. Para ver ejemplos de configuración de la vista de SNMP, consulte vista nmp-server.

Versión 3 de SNMP

La versión 3 de SNMP (SNMPv3) brinda intercambios seguros de datos de administración entre los dispositivos de red y las estaciones de administración. Las funciones de encripción y autenticación en SNMPv3 aseguran la máxima seguridad en el transporte de paquetes a una consola de administración. SNMPv3 es compatible con la versión de software Cisco IOS 12.0(3)T y posteriores. Para ver una descripción general técnica de SNMPv3, consulte la documentación de SNMPv3.

Lista de control de acceso (ACL) en las interfaces

La característica ACL proporciona medidas de seguridad ya que previene ataques como la simulación del IP. La ACL puede aplicarse en interfaces entrantes o salientes en routers.

Función de seguridad del switch Catalyst de LAN

Lista de permisos de IP

La característica de la lista de IP permitidas restringe el acceso entrante de SNMP y Telnet al switch a direcciones IP de origen no autorizadas. Se admiten mensajes de Syslog y notificaciones de trampa SNMP para notificar a un sistema de administración cuando ocurre una violación o acceso no autorizado.

Se puede utilizar una combinación de las funciones de seguridad de Cisco IOS para administrar los routers y los switches Catalyst. Es necesario establecer una política de seguridad que limite el número de estaciones de administración capaces de acceder a los switches y a los routers.

Para obtener más información sobre cómo mejorar la seguridad en las redes IP, consulte Mejorar la seguridad en las redes IP.

Administración de contabilidad

La administración de la contabilidad es el proceso que se utiliza en la medición de los parámetros de uso de la red para que puedan regularse de manera apropiada a los usuarios individuales o en grupo para las funciones de contabilidad o contracargo. Similar a la administración de rendimiento, el primer paso hacia una administración de contabilidad apropiada es medir la utilización de todos los recursos de red importantes. La utilización del recurso de la red se puede medir usando las características del Cisco NetFlow y Cisco IP Accounting. El análisis de los datos generados a través de estos métodos permite conocer los patrones actuales de uso.

Un sistema de facturación y contabilización basado en el uso es una parte esencial de cualquier acuerdo de nivel de servicio (SLA). Brinda tanto una manera práctica para definir las obligaciones según un SLA y las consecuencias evidentes del comportamiento fuera de los términos del SLA.

Los datos pueden recopilarse mediante sondeos o Cisco NetFlow. Cisco provee las aplicaciones NetFlow Collector y NetFlow Analyzer para reunir y analizar datos de routers y switches Catalyst. Las aplicaciones shareware como cflowd también se utilizan para recopilar datos de NetFlow. Una medición continua del uso de los recursos puede proporcionar tanto información de facturación como información de evaluación de recursos continuos óptimos y justos. Algunas de las soluciones de administración de contabilidad comúnmente implementadas son:

- Software evidente

Activación de Netflow y estrategia de obtención de datos

NetFlow (flujo de red) es una tecnología de medición de lado de entrada que permite capturar los datos requeridos para aplicaciones de planificación, supervisión y contabilidad de redes. NetFlow debería ser desplegada en las interfaces del router borde/agrupamiento para los proveedores de servicios o las interfaces del router de acceso WAN para los clientes de Enterprise.

Cisco Systems recomienda una implementación cuidadosamente planeada de NetFlow con los servicios NetFlow activados en estos routers estratégicamente ubicados. NetFlow puede ser desplegado en aumento (interfaz por interfaz) y de forma estratégica (en routers bien elegidos), en lugar de desplegar NetFlow en cada router de la red. El personal de Cisco trabajará con los clientes para determinar en qué routers e interfaces clave debe activarse NetFlow, según los

patrones de flujo de tráfico, la topología de red y la arquitectura del cliente.

Las consideraciones clave para la implementación incluyen:

- Los servicios NetFlow deben utilizarse como un medidor de borde y una herramienta de aceleración del funcionamiento de la lista de acceso y no se los debe activar en routers de núcleo/estructura básica en funcionamiento ni en erutadores que funcionan a tasas de utilización de CPU muy elevadas.
- Comprensión de los requerimientos para la recolección de datos determinada por la aplicación. Es posible que las aplicaciones de contabilidad requieran sólo información de flujo de routers de origen y terminación mientras que las aplicaciones de supervisión requieran una visión de extremo a extremo más amplia (que incluye muchos datos).
- Comprenda el impacto de la topología de red y de la política de enrutamiento en la estrategia de recopilación de flujo. Por ejemplo, evite recolectar flujos duplicados mediante la activación de NetFlow en routers de agrupamiento clave en donde el tráfico se origina o termina y no en routers de estructura básica o en routers intermedios porque esto proporcionaría vistas duplicadas de la misma información de flujo.
- Los proveedores de servicios *en la empresa del transportista de tránsito (transportar tráfico que no se origina ni se termina en su red) pueden utilizar NetFlow exportación de datos para medir el uso de tráfico de los recursos de red con fines de contabilización y facturación.*

Configuración de contabilización de IP

El soporte de contabilidad de IP de Cisco proporciona funciones básicas de contabilidad de IP. Al activar la contabilización IP, los usuarios pueden ver el número de bytes y paquetes conmutados por medio de Cisco IOS Software sobre la base de una dirección de IP de origen y destino. Únicamente se mide el tráfico de IP de tránsito que sea saliente. En las estadísticas de contabilidad, no se incluye el tráfico generado por el software o que finaliza en el software. Para mantener los totales de contabilización precisos, el software mantiene dos bases de datos de contabilización: una base de datos activa y una verificada.

El soporte de contabilidad de Cisco IP también ofrece información que identifica el tráfico IP que falla en las listas de accesos IP. La identificación de direcciones IP de origen que violan las listas de accesos IP indica posibles intentos de violación a la seguridad. Los datos también indican que debe verificarse la configuración de las listas de acceso IP. Para hacer que esta función esté disponible para los usuarios, habilite la contabilidad IP de las violaciones de la lista de acceso mediante el uso del comando ip accounting access-violations. Los usuarios pueden exhibir la cantidad de bytes y de paquetes de una única fuente que intentó violar la seguridad, contra con la lista de acceso del par de destino de origen. La contabilidad IP muestra de manera predeterminada la cantidad de paquetes que pasaron listas de acceso y se rutearon.

Para activar la contabilización de IP, utilice uno de los siguientes comandos para cada interfaz, en el modo de configuración de interfaz:

Comando	Propósito
contabilidad IP	Habilita la contabilización de IP básica.
violaciones de acceso de contabilidad ip	Habilite la contabilidad IP con la capacidad de identificar el tráfico de IP que falla en las listas de acceso IP.

Para configurar otras funciones de contabilidad IP, utilice uno o más de los siguientes comandos en modo de configuración global:

Comando	Propósito
ip accounting-threshold threshold	Establece la cantidad máxima de entradas de contabilización que deben crearse.
ip accounting-list ip-address wildcard	Información de la cuenta de filtro para hosts.
ip accounting-transits count	Controle el número de registros de tránsito que se almacenarán en la base de datos de contabilidad IP.

Consulte Convenciones de sugerencias técnicas de Cisco para obtener información sobre las convenciones utilizadas en este documento.