Informe técnico sobre prácticas recomendadas del proceso de referencia

Contenido

Introducción

Este documento describe los conceptos y los procedimientos del establecimiento de líneas de base para redes de alta disponibilidad. Incluye los factores de éxito críticos para que el establecimiento de líneas de base de red y del umbral ayude a evaluar el éxito. También proporciona gran cantidad de detalle para los procesos de la línea de base y el umbral y la implementación que siguen las pautas de prácticas recomendadas identificadas por el equipo HAS (High Availability Services) de Cisco.

Este documento le guía paso a paso a través del proceso de aprobación. Algunos productos actuales del sistema de gestión de redes (NMS) pueden ayudar a automatizar este proceso; sin embargo, el proceso de referencia sigue siendo el mismo tanto si utiliza herramientas automatizadas como manuales. Si utiliza estos productos NMS, debe ajustar la configuración de

umbral predeterminada para su entorno de red único. Es importante contar con un proceso para elegir inteligentemente esos umbrales de modo que sean significativos y correctos.

Línea de base

¿Qué es una línea de base?

Una línea de base es un proceso para estudiar la red a intervalos regulares con el fin de garantizar que la red funciona según lo previsto. Se trata de más de un único informe que detalla el estado de la red en un momento determinado. Siguiendo el proceso de línea base, puede obtener la siguiente información:

- Obtenga información valiosa sobre el estado del hardware y el software
- Determinar la utilización actual de los recursos de red
- Tome decisiones precisas sobre los umbrales de alarma de red
- Identificar problemas de red actuales
- Predecir problemas futuros

En el siguiente diagrama se ilustra otra forma de observar la línea de base.

La línea roja, el punto de interrupción de la red, es el punto en el que se interrumpirá la red el cual está determinado a través del conocimiento de cómo se ejecutan el hardware y el software. La línea verde, la carga de la red, es la progresión natural de carga en la red cuando se agregan nuevas aplicaciones y existen otros factores similares.

El propósito de una línea de base es determinar:

- Dónde se encuentra la red en la línea verde
- La velocidad a la que aumenta la carga de red
- Esperemos que predigan en qué momento ambos se cruzarán

Al realizar una línea de base de forma regular, puede averiguar el estado actual y extrapolar cuándo se producirán los fallos y prepararse para ellos de antemano. Esto también lo ayuda a tomar decisiones más informadas sobre cuándo, dónde y cómo gastar dinero del presupuesto en actualizaciones de la red.

¿Por qué una línea de base?

Un proceso de línea de base le ayuda a identificar y planificar correctamente los problemas críticos de limitación de recursos en la red. Estos problemas se pueden describir como recursos del plano de control o recursos del plano de datos. Los recursos del plano de control son exclusivos de la plataforma y los módulos específicos del dispositivo y pueden verse afectados por diversos problemas, entre los que se incluyen:

- Utilización de datos
- Funciones habilitadas
- Diseño de red

Los recursos del plano de control incluyen parámetros como:

- Utilización de la CPU
- Uso de memoria
- Utilización del búfer

Los recursos del plano de datos solo se ven afectados por el tipo y la cantidad de tráfico e incluyen la utilización de enlaces y la utilización de la placa posterior. Al establecer la base de referencia de la utilización de recursos para áreas críticas, puede evitar problemas graves de rendimiento o, lo que es peor, una fusión de la red.

Con la introducción de las aplicaciones susceptibles a la latencia, como voz y video, el establecimiento de líneas de base es ahora más importante que antes. Las aplicaciones de protocolo de control de transmisión/protocolo de Internet (TCP/IP) tradicionales son indulgentes y permiten una cierta cantidad de retraso. La voz y el vídeo se basan en el protocolo de datagramas de usuario (UDP) y no permiten retransmisiones ni congestión de red.

Debido a la nueva combinación de aplicaciones, la línea de base le ayuda a comprender los problemas de utilización de recursos del plano de control y del plano de datos, así como a planificar de forma proactiva cambios y actualizaciones para garantizar el éxito continuo.

Las redes de datos existen desde hace muchos años. Hasta hace poco, mantener las redes funcionando era un proceso bastante indulgente, con algún margen de error. Con la aceptación cada vez mayor de aplicaciones sensibles a la latencia, como Voz sobre IP (VoIP), la tarea de operar una red es cada vez más difícil y requiere mayor precisión. Para ser más precisos y proporcionar a un administrador de red una base sólida sobre la que gestionar la red, es importante tener una idea de cómo funciona la red. Para ello, debe seguir un proceso denominado línea de base.

Objetivo de línea de base

El objetivo de una línea de base es:

1. Determinar el estado actual de los dispositivos de red
2. Compare ese estado con las directrices de rendimiento estándar
3. Configure los umbrales para que le avisen cuando el estado excede aquellas pautas.

Debido a la gran cantidad de datos y al tiempo que se tarda en analizarlos, primero debe limitar el alcance de una línea de base para facilitar el aprendizaje del proceso. El lugar más lógico y, a veces, más beneficioso, para comenzar es el núcleo de la red. Esta parte de la red suele ser la

más pequeña y requiere la mayor estabilidad.

En aras de la simplicidad, este documento explica cómo establecer como línea de base una base de información muy importante de Simple Network Management Protocol Management Information Base (SNMP MIB): cpmCPUTotal5min. cpmCPUTotal5min es el promedio de desintegración de cinco minutos de la unidad de procesamiento central (CPU) de un router de Cisco, y es un indicador de rendimiento del plano de control. La línea de base será realizada en un router de la serie 7000 de Cisco.

Una vez que ha aprendido el proceso, puede aplicarlo a todos los datos disponibles en la amplia base de datos SNMP que está disponible en la mayoría de los dispositivos de Cisco, como:

- Uso de la red digital de servicios integrados (ISDN)
- Pérdida de celda en el modo de transferencia asíncrona (ATM)
- Memoria del sistema libre

Diagrama de flujo de línea de base del núcleo

El siguiente diagrama de flujo muestra los pasos básicos del proceso de línea de base central. Aunque hay productos y herramientas disponibles para realizar algunos de estos pasos por usted, suelen presentar carencias en cuanto a flexibilidad o facilidad de uso. Incluso si tiene pensado utilizar las herramientas del sistema de administración de redes (NMS) para realizar la evaluación básica, sigue siendo un buen ejercicio para estudiar el proceso y comprender cómo funciona realmente la red. Además, este proceso puede develar algunas incógnitas sobre cómo funcionan algunas herramientas NMS, dado que la mayoría de las herramientas realizan básicamente las mismas tareas.

Procedimiento de línea de base

Paso 1: Compilar un inventario de hardware, software y configuración

Es extremadamente importante que compile un inventario de hardware, software y configuración por varias razones. En primer lugar, las MIB de Cisco SNMP son, en algunos casos, específicas de la versión de Cisco IOS que está ejecutando. Algunos objetos MIB son reemplazados por nuevos objetos o, en ocasiones, eliminados completamente. El inventario del hardware es muy importante una vez que recolectaron los datos, ya que los umbrales que se deben configurar después de la línea de base inicial muchas veces dependen del tipo de CPU, cantidad de memoria, etcétera, en los dispositivos Cisco. El inventario de configuración también es importante para asegurarse de conocer las configuraciones actuales: es posible que desee cambiar las configuraciones de los dispositivos después de la línea de base para ajustar los búferes, y así sucesivamente.

La forma más eficiente de llevar a cabo esta parte de la línea de base para una red Cisco es utilizar Aspectos esenciales de gestión de recursos de CiscoWorks2000 (Essentials). Si este software se instala correctamente en la red, Essentials debe tener los inventarios actuales de

todos los dispositivos en su base de datos. Simplemente necesita ver los inventarios para consultar si hay problemas.

La siguiente tabla es un ejemplo de un informe de inventario de software de clase de router de Cisco, exportado de Essentials y luego editado en Microsoft Excel. A partir de este inventario, observe que debe utilizar los datos MIB SNMP y los Identificadores de Objeto (OID) que se encuentran en las versiones 12.0x y 12.1x del IOS de Cisco.

Nombre del dispositivo	Tipo de router	Versión	Versión del software
field-2.500a.embu-mlab.cisco.com	Cisco 2511	M	12.1(1)
qdm-7200.embu-mlab.cisco.com	7204 de Cisco	B	12.1(1)E
voip-3640.embu-mlab.cisco.com	Cisco 3640	0x00	12.0(3 quater)
wan-1700a.embu-mlab.cisco.com	1720 de Cisco	0x101	12.1(4)
wan-2500a.embu-mlab.cisco.com	2514 de Cisco	L	12.0(1)
wan-3600a.embu-mlab.cisco.com	Cisco 3640	0x00	12.1(3)
wan-7200a.embu-mlab.cisco.com	7204 de Cisco	B	12.1(1)E
172.16.71.80	7204 de Cisco	B	12.0(5T)

Si Essentials no está instalado en la red, puede utilizar la herramienta de línea de comandos UNIX snmpwalk desde una estación de trabajo UNIX para encontrar la versión de IOS. Esto se muestra en el siguiente ejemplo. Si no está seguro de cómo funciona este comando, escriba man snmpwalk en el prompt de UNIX para obtener más información. La versión de IOS será importante en cuanto comience a elegir cuales MIB OID se establecerán como líneas de base, ya que los objetos MIB dependen del IOS. Observe también que al conocer el tipo de router, puede determinar más adelante cuáles deben ser los umbrales para la CPU, las memorias intermedias, etc.

```
nsahpov6% snmpwalk -v1 -c private 172.16.71.80 system
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JS-M), Version 12.0(5)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 23-Jul-2001 23:02 by kpma
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.cisco7204
```

Paso 2: Verifique que SNMP MIB esté Soportado en el Router

Ahora que tiene un inventario del dispositivo que desea sondear para su línea de base, puede comenzar a elegir los OID específicos que desea sondear. Ahorra mucha frustración si se verifica, por adelantado, que los datos que se desean están realmente allí. El objeto cpmCPUTotal5min MIB se encuentra en CISCO-PROCESS-MIB (Base de información para la administración de procesos de Cisco).

Para encontrar el OID que desea sondear, necesita una tabla de conversión que esté disponible en el sitio Web de CCO de Cisco. Para acceder a este sitio web desde un navegador web, vaya a la página Cisco MIBs y haga clic en el enlace OIDs.

Para ingresar a este sitio Web desde un servidor FTP, escriba ftp://ftp.cisco.com/pub/mibs/oid/. Desde este sitio, puede descargar la MIB específica que ha sido descodificada y ordenada por números OID.

El siguiente ejemplo se extrae de la tabla CISCO-PROCESS-MIB.oid. Este ejemplo muestra que el OID para el MIB cpmCPUTotal5min es .1.3.6.1.4.1.9.9.109.1.1.1.1.5.

Nota: No olvide agregar un "." al principio del OID o obtendrá un error cuando intente sondearlo. Es necesario agregar un ".1" al final del OID para implementarlo. Esto indica al dispositivo la instancia del OID que está buscando. En algunos casos, los OID tienen más de una instancia de un tipo particular de datos, como cuando un router tiene varias CPU.

<#root>

```
ftp://ftp.cisco.com/pub/mibs/oid/CISCO-PROCESS-MIB.oid
### THIS FILE WAS GENERATED BY MIB2SCHEMA
"org" "1.3"
"dod" "1.3.6"
"internet" "1.3.6.1"
"directory" "1.3.6.1.1"
"mgmt" "1.3.6.1.2"
"experimental" "1.3.6.1.3"
"private" "1.3.6.1.4"
"enterprises" "1.3.6.1.4.1"
"cisco" "1.3.6.1.4.1.9"
"ciscoMgmt" "1.3.6.1.4.1.9.9"
"ciscoProcessMIB" "1.3.6.1.4.1.9.9.109"
"ciscoProcessMIBObjects" "1.3.6.1.4.1.9.9.109.1"
"ciscoProcessMIBNotifications" "1.3.6.1.4.1.9.9.109.2"
"ciscoProcessMIBConformance" "1.3.6.1.4.1.9.9.109.3"
"cpmCPU" "1.3.6.1.4.1.9.9.109.1.1"
"cpmProcess" "1.3.6.1.4.1.9.9.109.1.2"
"cpmCPUTotalTable" "1.3.6.1.4.1.9.9.109.1.1.1"
"cpmCPUTotalEntry" "1.3.6.1.4.1.9.9.109.1.1.1.1"
"cpmCPUTotalIndex" "1.3.6.1.4.1.9.9.109.1.1.1.1.1"
"cpmCPUTotalPhysicalIndex" "1.3.6.1.4.1.9.9.109.1.1.1.1.2"
"cpmCPUTotal5sec" "1.3.6.1.4.1.9.9.109.1.1.1.1.3"
"cpmCPUTotal1min" "1.3.6.1.4.1.9.9.109.1.1.1.1.4"

"cpmCPUTotal5min" "1.3.6.1.4.1.9.9.109.1.1.1.1.5"
```

Hay dos formas comunes de sondear el OID de MIB para asegurarse de que esté disponible y en funcionamiento. Es una buena idea hacer esto antes de comenzar la recopilación masiva de datos para no perder tiempo consultando algo que no está ahí y terminar con una base de datos vacía. Una forma de hacerlo es utilizar un andador MIB desde la plataforma NMS, como HP OpenView Network Node Manager (NNM) o CiscoWorks Windows, e introducir el OID que desea comprobar.

A continuación se presenta un ejemplo desde OpenView SNMP MIB walker.

Otra manera fácil de sondear el OID de MIB es utilizar el comando UNIX snmpwalk como se muestra en el siguiente ejemplo.

```
nsahpov6% cd /opt/OV/bin
nsahpov6% snmpwalk -v1 -c private 172.16.71.80 .1.3.6.1.4.1.9.9.109.1.1.1.1.5.1

cisco.ciscoMgmt.ciscoProcessMIB.ciscoProcessMIBObjects.cpmCPU.cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUT
```

En ambos ejemplos, la MIB devolvió un valor de 0, lo que significa que para ese ciclo de sondeo la CPU promedió una utilización del 0 por ciento. Si tiene dificultades para que el dispositivo responda con los datos correctos, intente hacer ping en el dispositivo y acceder al dispositivo mediante Telnet. Si todavía tiene un problema, verifique la configuración SNMP y las cadenas de comunidad SNMP. Es posible que necesite encontrar una MIB alternativa u otra versión de IOS para que esto funcione.

Paso 3: Sondear y registrar un objeto MIB SNMP específico desde el router

Hay varias formas de sondear objetos MIB y registrar el resultado. Hay disponibles productos estándar, productos shareware, scripts y herramientas de proveedor. Todas las herramientas front-end utilizan el proceso SNMP get para obtener la información. Las principales diferencias residen en la flexibilidad de la configuración y en la forma en la que se registran los datos en una base de datos. Una vez más, observe la MIB del procesador para ver cómo funcionan estos diversos métodos.

Ahora que sabe que el router admite el OID, debe decidir con qué frecuencia consultarlo y cómo registrarlo. Cisco recomienda que la MIB de CPU se sondee en intervalos de cinco minutos. Un intervalo más bajo aumentaría la carga en la red o el dispositivo, y dado que el valor de MIB es un promedio de cinco minutos de todos modos, no sería útil sondearlo más a menudo que el valor promedio. También se recomienda generalmente que el sondeo de línea base tenga al menos un período de dos semanas para que pueda analizar al menos dos ciclos comerciales semanales en la red.

Las siguientes pantallas muestran cómo agregar objetos MIB en la versión 6.1 del OpenView Network Node Manager de HP. En la pantalla principal, seleccione Opciones > Recopilación de datos y umbrales.

A continuación, seleccione Edit > Add > MIB Objects.

En el menú, agregue la cadena OID y haga clic en Apply. Ahora ingresó el objeto de MIB en una plataforma OpenView de HP para que pueda ser consultado.

Luego debe permitir que HP OpenView conozca el router a interrogar para este OID.

En el menú Data Collection, seleccione Edit > Add > MIB Collections.

En el campo Origen, introduzca el nombre del sistema de nombres de dominio (DNS) o la dirección IP del router que se va a sondear.

Seleccione Store (Almacenar), No Thresholds (Sin umbrales) desde la lista Set Collection Mode (Configurar modo de colección).

Establezca el Intervalo de sondeo en 5m, para intervalos de cinco minutos.

Haga clic en Apply (Aplicar).

Debe seleccionar File > Save para que los cambios surtan efecto.

Para verificar que la recolección esté configurada correctamente, resalte la línea de resumen de recolección para el router y seleccione Acciones > Probar SNMP. Esto verifica si la identificación de comunidad es correcta y realizará el sondeo de todas las instancias de OID.

Haga clic en Cerrar y deje que la colección se ejecute durante una semana. Al final del período semanal, extraiga los datos para su análisis.

Los datos se analizan más fácilmente si los descarga en un archivo ASCII y lo importa a una herramienta para hojas de cálculo como Microsoft Excel. Para hacer esto con el NNM HP OpenView, puede usar la herramienta de línea de comando, snmpColDump. Cada colección configurada escribe en un archivo del directorio /var/opt/OV/share/database/snmpCollect/.

Extraiga los datos en un archivo ASCII llamado testfile con el siguiente comando:

<#root>

```
snmpColDump /var/opt/OV/share/databases/snmpCollect/cpmCPUTotal5min.1 >
testfile
```

Nota: cpmCPUTotal5min.1 es el archivo de base de datos que HP OpenView NNM creó cuando comenzó el sondeo de OID.

El archivo de prueba generado es similar al ejemplo siguiente.

```
03/01/2001 14:09:10 nsa-gw.cisco.com 1
03/01/2001 14:14:10 nsa-gw.cisco.com 1
```

```
03/01/2001 14:19:10 nsa-gw.cisco.com 1
03/01/2001 14:24:10 nsa-gw.cisco.com 1
03/01/2001 14:29:10 nsa-gw.cisco.com 1
03/01/2001 14:34:10 nsa-gw.cisco.com 1
03/01/2001 14:39:10 nsa-gw.cisco.com 1
03/01/2001 14:44:10 nsa-gw.cisco.com 1
03/01/2001 14:49:10 nsa-gw.cisco.com 1
03/01/2001 14:54:10 nsa-gw.cisco.com 1
03/01/2001 14:59:10 nsa-gw.cisco.com 1
03/……
```

Una vez que el resultado del archivo de prueba está en su estación UNIX, puede transferirla a la PC mediante el Protocolo de transferencia de datos (FTP).

También puede recopilar los datos mediante sus propias secuencias de comandos. Para ello, realice un comando snmpget para el OID de la CPU cada cinco minutos y vuelque los resultados en un archivo .csv.

Paso 4: Analizar datos para determinar umbrales

Ahora que tiene algunos datos, puede empezar a analizarlos. Esta fase de la línea de base determina las configuraciones del umbral que puede utilizar que son una medida precisa de rendimiento o falla y que no activará demasiadas alarmas cuando encendamos el monitoreo de umbral. Una de las formas más sencillas para hacer esto consiste en importar los datos en una hoja de cálculo como por ejemplo Microsoft Excel y hacer un cuadro de dispersión. Este método hace que sea muy fácil ver cuántas veces un dispositivo en particular habría creado una alerta de excepción si lo estuviera monitoreando para un umbral determinado. No es recomendable activar los umbrales sin realizar una línea de base, ya que esto puede crear tormentas de alerta desde dispositivos que han superado el umbral que ha elegido.

Para importar el archivo de prueba en una hoja de cálculo de Excel, abra Excel, seleccione Archivo > Abrir y seleccione el archivo de datos.

La aplicación de Excel entonces le solicita que importe el archivo.

Una vez terminado, el archivo importado debería lucir parecido a la pantalla siguiente.

Un gráfico de dispersión le permite visualizar más fácilmente cómo funcionarían varias configuraciones de umbral en la red.

Para crear el gráfico de dispersión, resalte la columna C en el archivo importado y luego haga clic en el icono del asistente para gráficos. Siga los pasos del Chart Wizard (Asistente para la creación de cuadros) para crear un cuadro de dispersión.

En el paso 1 del Asistente para gráficos, como se muestra a continuación, seleccione la ficha Tipos estándar y el tipo de gráfico XY (Dispersión). Luego haga clic en Next (Siguiente).

En el paso 2 del Asistente para gráficos, como se muestra a continuación, seleccione la ficha Rango de datos y seleccione el rango de datos y la opción Columnas. Haga clic en Next

(Siguiente).

En el paso 3 del Asistente para gráficos, como se muestra a continuación, escriba el título del gráfico y los valores de los ejes X e Y y, a continuación, haga clic en Siguiente.

En el paso 4 del Asistente para gráficos, seleccione si desea el gráfico de dispersión en una página nueva o como objeto en la página existente.

Haga clic en Finalizar para colocar el gráfico en la ubicación deseada.

"¿Qué pasaría si?" Análisis

Ahora puede utilizar el gráfico de dispersión para realizar un análisis. Sin embargo, antes de continuar, debe hacer las siguientes preguntas:

- ¿Qué recomienda el proveedor (en este ejemplo el proveedor es Cisco) como umbral para esta variable MIB?

  En general, Cisco recomienda que un router de núcleo no supere el 60% de utilización media de la CPU. Se eligió el 60% porque un router necesita cierta sobrecarga en caso de que experimente problemas o la red tenga algunos fallos. Cisco calcula que un router de núcleo necesita aproximadamente un 40 por ciento de sobrecarga de CPU en caso de que un protocolo de routing tenga que volver a calcular o a converger. Estos porcentajes varían en función de los protocolos que utiliza y la topología y estabilidad de la red.

- ¿Qué ocurre si utilizo un 60% como establecimiento del umbral?

  Si dibuja una línea en el gráfico de dispersión horizontalmente a 60, verá que ninguno de los puntos de datos supera el 60 por ciento de utilización de la CPU. Por lo tanto, un umbral de 60 establecido en las estaciones del sistema de administración de redes (NMS) no habrá activado una alarma de umbral durante el período de sondeo. Se acepta un porcentaje de 60 para este router. Sin embargo, observe en el gráfico de dispersión que algunos puntos de datos están cerca de 60. Sería bueno saber cuándo un router se está acercando al umbral del 60% para que pueda saber de antemano que la CPU se está acercando al 60% y tener un plan de qué hacer cuando llegue a ese punto.

- ¿Qué sucede si configuro el umbral en el 50%?

  Se estima que este router alcanzó el 50% de utilización cuatro veces durante este ciclo de sondeo y que habría generado una alarma de umbral cada vez. Este proceso cobra mayor importancia cuando se observan grupos de routers para ver qué harían las diferentes configuraciones de umbral. Por ejemplo, "¿Qué sucede si configuro el umbral en el 50% para toda la red principal?" Es muy difícil elegir sólo un número.

Análisis del umbral de la CPU

Una estrategia que puede utilizar para hacerlo más fácil es la metodología de umbral Ready, Set, Go . Esta metodología utiliza tres números sucesivos de umbral.

- Ready (Listo)—el umbral que estableció como indicador de qué dispositivos quizá necesiten atención en el futuro
- Set—el umbral que se usa como un indicador previo que le avisa que comienza la planificación para una reparación, actualización o nueva configuración.
- Ir: el umbral que usted o el proveedor consideran que es una condición de fallo y que requiere alguna acción para repararlo; en este ejemplo, es del 60%.

La siguiente tabla muestra la táctica de la estrategia Ready, Set, Go (listo, preparado, ya).

Umbral	Acción	Resultado
45 por ciento	Investigue más a fondo	Lista de opciones para planes de acción
50 por ciento	Formular un plan de acción	Lista de pasos del plan de acción
60 por ciento	Implementar el plan de acción	El router ya no supera los umbrales. Volver al modo Preparado

La metodología Listo, Preparado, Ya cambia el gráfico de línea de base tratado anteriormente. El siguiente diagrama muestra el cuadro cambiado de línea de base. Si puede identificar los otros puntos de intersección del gráfico, ahora dispone de más tiempo para planificar y reaccionar que antes.

Observe que en este proceso, la atención se centra en las excepciones en la red y no se ocupa de otros dispositivos. Se asume que mientras los dispositivos estén por debajo de los umbrales, están bien.

Si ha pensado en estos pasos desde el principio, estará bien preparado para mantener la red en buen estado. La realización de este tipo de planificación también resulta extremadamente útil para la planificación presupuestaria. Si sabe cuáles son sus cinco routers go principales, sus routers set medios y sus routers ready inferiores, puede planificar fácilmente cuánto presupuesto necesitará para las actualizaciones en función del tipo de routers que sean y de cuáles sean sus opciones de plan de acción. La misma estrategia se puede utilizar para los enlaces de red de área extensa (WAN) o cualquier otro OID MIB.

Paso 5: Solucione los problemas inmediatos identificados

Esta es una de las partes más sencillas del proceso de la línea de base. Una vez que haya identificado qué dispositivos exceden el paso del umbral, es recomendable que confeccione un plan de acción para devolver esos dispositivos dentro del umbral.

Puede abrir un caso en el centro de asistencia técnica Cisco Technical Assistance Center (TAC) o ponerse en contacto con su ingeniero de sistemas para conocer las opciones disponibles. No debe asumir que volver a situar las cosas por debajo del umbral le costará dinero. Algunos

problemas de CPU pueden ser solucionados cambiando la configuración para asegurar que todos los procesos se estén ejecutando de la manera más eficaz. Por ejemplo, algunas listas de control de acceso (ACL) pueden hacer que la CPU de un router se ejecute muy alto debido a la trayectoria que los paquetes toman a través del router. En algunos casos, puede implementar la conmutación de NetFlow para cambiar la trayectoria de conmutación de paquetes y reducir el impacto de la ACL en la CPU. Más allá del problema, es necesario que todos los routers vuelvan a estar bajo el umbral en este paso para que usted pueda implementar los umbrales más tarde sin correr el riesgo de inundar las estaciones NMS con demasiadas alarmas de umbral.

Paso 6: Supervisión del umbral de prueba

Este paso implica evaluar los umbrales en el laboratorio mediante las herramientas que usará en la red de producción. Existen dos enfoques comunes para la supervisión de umbrales. Debe decidir qué método es el mejor para su red.

- Método de sondeo y comparación mediante una plataforma SNMP u otra herramienta de supervisión SNMP

  Este método utiliza más ancho de banda de red para sondear el tráfico y toma los ciclos de procesamiento en su plataforma SNMP.

- Use configuraciones de alarmas y eventos RMON (Monitoreo remoto) en los routers de modo que envíen una alarma sólo cuando se exceda un umbral.

  Este método reduce el uso del ancho de banda de la red, pero también aumenta el uso de la memoria y de la CPU en los routers.

Implementación de un Umbral mediante SNMP

Para configurar el método SNMP con HP OpenView NNM, seleccione Options > Data Collection & Thresholds como lo hizo al configurar el sondeo inicial. Esta vez, sin embargo, en el menú de colecciones seleccione Store (tienda), Check Thresholds (comprobar umbrales) en lugar de Store, No Thresholds (sin umbrales). Después de configurar el umbral, puede aumentar el uso de la CPU en el router enviándole múltiples pings y/o múltiples caminatas SNMP. Tendrá que disminuir el valor del umbral si no puede hacer que la utilidad de la CPU sea lo suficientemente alta como para cruzar el umbral. En cualquier caso, debe asegurarse de que el mecanismo de umbral funciona.

Una de las limitaciones de usar este método es que no se pueden implementar umbrales múltiples en forma simultánea. Necesitará tres plataformas SNMP para establecer tres umbrales diferentes simultáneamente. Las herramientas como Concord Network Health y Trinagy TREND permiten múltiples umbrales para la misma instancia de OID.

Si el sistema solo puede gestionar un umbral a la vez, puede considerar la estrategia Ready, Set, Go de forma serial. Esto es, cuando se alcanza en forma continua el umbral ready (listo), comience su investigación y eleve el umbral para al nivel set (preparado) establecido para ese dispositivo. Cuando se alcanza el nivel “set” de manera continua, comience a formular su plan de acción y eleve el umbral hasta el nivel “go” para ese dispositivo. Luego el go threshold se alcanza

continuamente, implemente su plan de acción. Esto debería funcionar tan bien como el método de tres umbrales simultáneos. Solo se necesita un poco más de tiempo para cambiar los parámetros de umbral de la plataforma SNMP.

Implementación de un Umbral con Alarma y Evento RMON

Mediante el uso de las configuraciones de alarma RMON y de sucesos, puede hacer que el router se monitoree a sí mismo para varios umbrales. Cuando el router detecta una condición que excede el umbral, envía una trampa de SNMP a la plataforma SNMP. Debe tener un receptor de trampa SNMP establecido en la configuración de su router para que la trampa sea reenviada. Existe una correlación entre alarma y evento. La alarma verifica el OID para el umbral dado. Si se alcanza el umbral, el proceso de alarma dispara el proceso de evento que puede enviar un mensaje de trampa SNMP, crear una entrada de registro RMON o ambos. Para obtener más detalles sobre este comando, vea Comandos de configuración de eventos y alarmas RMON.

Los siguientes comandos de configuración de router tienen el monitor del router cpmCPUTotal5min cada 300 segundos. Se desencadenará el evento 1 si la CPU supera el 60 por ciento y se desencadenará el evento 2 cuando la CPU retroceda al 40 por ciento. En ambos casos, se enviará un mensaje de trampa SNMP a la estación NMS con la cadena privada de la comunidad.

Para usar el método Listos, preparados, ya, use todos los siguientes enunciados de configuración.

```
rmon event 1 trap private description "cpu hit60%" owner jharp
rmon event 2 trap private description "cpu recovered" owner jharp
rmon alarm 10 cpmCPUTotalTable.1.5.1 300 absolute rising 60 1 falling 40 2 owner jharp


rmon event 3 trap private description "cpu hit50%" owner jharp
rmon event 4 trap private description "cpu recovered" owner jharp
rmon alarm 20 cpmCPUTotalTable.1.5.1 300 absolute rising 50 3 falling 40 4 owner jharp

rmon event 5 trap private description "cpu hit 45%" owner jharp
rmon event 6 trap private description "cpu recovered" owner jharp
rmon alarm 30 cpmCPUTotalTable.1.5.1 300 absolute rising 45 5 falling 40 6 owner jharp
```

El siguiente ejemplo muestra el resultado del comando show rmon alarm que fue configurado por los enunciados anteriores.

<#root>

zack#

sh rmon alarm

```
Alarm 10 is active, owned by jharp
 Monitors cpmCPUTotalTable.1.5.1 every 300 second(s)
 Taking absolute samples, last value was 0
```

```
 Rising threshold is 60, assigned to event
1
 Falling threshold is 40, assigned to event
2
 On startup enable rising or falling alarm
Alarm 20 is active, owned by jharp
 Monitors cpmCPUTotalTable.1.5.1 every 300 second(s)
 Taking absolute samples, last value was 0
 Rising threshold is 50, assigned to event
3
 Falling threshold is 40, assigned to event
4
 On startup enable rising or falling alarm
Alarm 30 is active, owned by jharp
 Monitors cpmCPUTotalTable.1.5.1 every 300 second(s)
 Taking absolute samples, last value was 0
 Rising threshold is 45, assigned to event
5
 Falling threshold is 40, assigned to event
6
 On startup enable rising or falling alarm
```

El siguiente ejemplo muestra el resultado del comando show rmon event.

<#root>

zack#

sh rmon event

```
Event 1 is active, owned by jharp
 Description is cpu hit60%
 Event firing causes trap to community
private, last fired 00:00:00
Event 2 is active, owned by jharp
 Description is cpu recovered
 Event firing causes trap to community
private, last fired 02:40:29
Event 3 is active, owned by jharp
 Description is cpu hit50%
 Event firing causes trap to community
private, last fired 00:00:00
Event 4 is active, owned by jharp
 Description is cpu recovered
 Event firing causes trap to community
private, last fired 00:00:00
Event 5 is active, owned by jharp
 Description is cpu hit 45%
 Event firing causes trap to community
private, last fired 00:00:00
Event 6 is active, owned by jharp
 Description is cpu recovered
 Event firing causes trap to community
private, last fired 02:45:47
```

Pruebe ambos métodos para decidir cuál se adecua mejor a su entorno. Incluso puede encontrar

que una combinación de métodos funciona sin problemas. En cualquier caso, las pruebas deben realizarse en un entorno de laboratorio para garantizar que todo funciona correctamente. Después de realizar pruebas en el laboratorio, una implementación limitada en un pequeño grupo de routers le permitirá probar el proceso de envío de alertas a su centro de operaciones.

En este caso, tendrá que reducir los umbrales para probar el proceso: No se recomienda intentar aumentar artificialmente la CPU en un router de producción. También debe asegurarse de que cuando llegan las alertas a las estaciones NMS en el centro de operaciones, hay una política de escalada que le permite estar seguro de que se le informa sobre los dispositivos que excedieron los umbrales. Estas configuraciones se han probado en un laboratorio con Cisco IOS Versión 12.1(7). Si encuentra algún problema, debe consultar con Ingeniería de Cisco o Ingenieros de sistemas para ver si tiene un error en su versión de IOS.

Paso 7: Implemente el Monitoreo de Umbral usando SNMP o RMON

Una vez que usted haya testeado cuidadosamente el umbral del monitoreo en el laboratorio y en un despliegue limitado, estará listo para implementar el umbral a lo largo del núcleo de la red. Ahora puede implementar sistemáticamente este proceso de línea de base para otras variables MIB importantes en su red, como búfers, memoria libre, errores de verificación de redundancia cíclica (CRC), pérdida de celdas ATM y demás.

Si utiliza la alarma RMON y las configuraciones de eventos, ahora puede detener el sondeo desde su estación NMS. Esto disminuirá la carga en su servidor NMS y la cantidad de datos de sondeo en la red. Al pasar sistemáticamente por este proceso para obtener indicadores de estado de red importantes, fácilmente podría llegar al punto de que los equipos de red se están monitoreando a sí mismos usando Alarma y Evento RMON.

MIB adicionales

Una vez que haya aprendido este proceso, es posible que desee investigar otras MIB para establecer una línea de base y monitorear. Las siguientes subsecciones presentan una breve lista de algunas OID y descripciones que le pueden resultar útiles.

MIB del router

Las características de memoria son muy útiles para determinar el estado de un router. Un router saludable casi siempre debería tener espacio de buffer disponible con el cual trabajar. Si el router comienza a quedarse sin espacio de memoria intermedia, la CPU tendrá que trabajar más para crear nuevas memorias intermedias e intentar encontrar memorias intermedias para los paquetes entrantes y salientes. Una discusión en profundidad de las memorias intermedias está más allá del alcance de este documento. Sin embargo, como regla general, un router saludable debe tener muy pocas pérdidas de memoria intermedia, si las hay, y no debe tener ninguna falla de memoria intermedia, o una condición de memoria libre cero.

Objeto	Descripción	OID (ID del objeto)
ciscoMemoryPoolFree	La cantidad	1.3.6.1.4.1.9.9.48.1.1.1.6

	de bytes del agrupamiento de memoria que no se utilizan actualmente en el dispositivo administrado	
ciscoMemoryPoolLargestFree	El mayor número de bytes contiguos del grupo de memoria que no se utilizan actualmente	1.3.6.1.4.1.9.9.48.1.1.1.7
bufferElMiss	Cantidad de omisiones de elementos de memoria intermedia	1.3.6.1.4.1.9.2.1.12
bufferFail	Cantidad de fallas de asignación de memorias intermedias	1.3.6.1.4.1.9.2.1.46
bufferNoMem	La cantidad de memoria intermedia genera fallas debido a que no hay memoria libre	1.3.6.1.4.1.9.2.1.47

Catalyst Switch MIBs

Objeto	Descripción	OID (ID del objeto)
cpmCPUTotal5min	Porcentaje total de ocupación de CPU en el último período de	1.3.6.1.4.1.9.9.109.1.1.1.5

	cinco minutos. Este objeto desaprueba el objeto avgBusy5 de OLD-CISCO-SYSTEM-MIB	
cpmCPUTotal5sec	Porcentaje total de ocupación de la CPU en el último período de cinco segundos. Este objeto hace que el objeto busyPer de OLD-CISCO-SYSTEM-MIB se vuelva obsoleto	1.3.6.1.4.1.9.9.109.1.1.1.3
Tráfico del sistema	El porcentaje de uso del ancho de banda para el intervalo de consultas previo	1.3.6.1.4.1.9.5.1.1.8
sysTrafficPeak	El valor de medidor de tráfico máximo desde la última vez que los contadores del puerto	1.3.6.1.4.1.9.5.1.1.19

	se borraron o que se inició el sistema.	
sysTrafficPeaktime	El tiempo (en centésimos de un segundo) desde que ocurrió el valor del medidor de tráfico pico	1.3.6.1.4.1.9.5.1.1.20
portTopNUtilization	Utilización del puerto en el sistema	1.3.6.1.4.1.9.5.1.20.2.1.4
portTopNBufferOverFlow	La cantidad de sobrecargas en memoria intermedia del puerto en el sistema	1.3.6.1.4.1.9.5.1.20.2.1.10

MIB de link serial

Objeto	Descripción	OID (ID del objeto)
locIfInputQueueDrops	La cantidad de paquetes perdidos porque la cola de entrada estaba completa	1.3.6.1.4.1.9.2.2.1.1.26
locIfOutputQueueDrops	La cantidad de paquetes perdidos porque la cola de salida estaba completa	1.3.6.1.4.1.9.2.2.1.1.27

locIfInCRC	Cantidad de paquetes de entrada que presentaron errores de suma de comprobación por redundancia cíclica	1.3.6.1.4.1.9.2.2.1.1.12

Comandos de configuración de evento y alarma RMON

Alarmas

Las alarmas RMON pueden configurarse dentro de la siguiente sintaxis:

<#root>

```
rmon alarm number variable interval {delta | absolute} rising-threshold value
           [event-number] falling-threshold value [event-number]
           [owner string]
```

Elemento	Descripción
número	El número de la alarma, que es idéntico al valor de alarmIndex de la tabla alarmTable, en la MIB de RMON.
Variable	La MIB se opone al control lo que se traduce en la alarmVariable utilizada en la alarmTable de la MIB de RMON.
intervalo	El tiempo en segundos en que la alarma controla la variable MIB, que es idéntico al alarmInterval que se usó en la alarmTable de la MIB de RMON.
delta	Prueba el cambio entre las variables MIB, que afecta a alarmSampleType en alarmTable de RMON MIB.
absoluto	Prueba cada variable MIB directamente, lo que afecta el alarmSampleType en la alarmTable de la MIB de RMON.
valor de umbral ascendente	El valor en el que se dispara la alarma.

event-number	(Opcional) El número de evento que se activará cuando el umbral ascendente o descendente supere su límite. Este valor es idéntico al alarmRisingEventIndex o al alarmFallingEventIndex en la tabla de alarma del RMON MIB.
valor de umbral descendente	Valor en el que se reinicia la alarma.
La cadena owner	(Opcional) Especifique un propietario para la alarma, que sea idéntico al alarmOwner en la Tabla de la alarma del MIB de RMON.

Events

Los eventos RMON pueden configurarse dentro de la siguiente sintaxis:

<#root>

```
rmon event number [log] [trap community] [description string]
           [owner string]
```

Elemento	Descripción
número	Número de evento asignado, que es idéntico al eventIndex de eventTable en la MIB de RMON.
registro	(Opcional) Genera una entrada de registro RMON cuando se activa un evento y configura eventType en la RMON MIB en registro o en registro y trampa.
comunidad de trampa	(Opcional) Cadena de comunidad SNMP utilizada para esta trampa. Configura la configuración del eventType en la MIB de RMON para esta fila como snmp-trap o log-and-trap. Este valor es idéntico al eventCommunityValue en eventTable en RMON MIB.
cadena de descripción	(Opcional) Especifica una descripción del evento que es idéntica a la que figura en la tabla de eventos de la MIB de RMON.
La cadena owner	(Opcional) Propietario de este evento, que es idéntico al eventOwner en la tabla

	eventTable de la MIB de RMON.

Alarma RMON e implementación de eventos

Para obtener información detallada sobre la implementación de eventos y alarmas RMON, lea la sección Implementación de eventos y alarmas RMON del informe técnico Prácticas recomendadas de los sistemas de administración de redes.

Información Relacionada

- Asistencia técnica y documentación - Cisco Systems

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).