

Problema 2 Administración de rendimiento de servicios en Red

Parte 1 – Establecer un 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. SLA consiste en la métrica convenida en entre el proveedor y sus clientes. Los valores configurados para las mediciones deben ser realistas, significativos y cuantificables para ambas partes.

Las diversas estadísticas de la interfaz se pueden recoger de los dispositivos de red para medir el nivel de rendimiento. Estas estadísticas pueden incluirse como métricas en el SLA. Las estadísticas tales como caídas de entradas en la cola, pérdidas de la cola de salida, y paquetes ignorados son útiles para diagnosticar los problemas relacionados con el rendimiento.

A nivel de dispositivos, la medición del rendimiento puede 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.

Parte 2 - Análisis y ajuste del rendimiento (línea de base)

Para realizar un análisis y ajuste del rendimiento es necesario implementar la técnica de línea de base. El módulo de análisis debe mostrar un inventario de la configuración.

Tarea 1- Inventario de la configuración.

El inventario es muy importante una vez que se recolectaron los datos, ya que los umbrales que se deben configurar después de la línea de base muchas veces dependen del tipo de CPU, cantidad de memoria, etcétera, en los dispositivos.

A continuación se muestra una tabla con la información esencial del inventario:

Nombre del dispositivo	Versión del software (sistema operativo)	Tiempo de actividad del sistema	Fecha y hora del host	Número de procesos que se ejecutan en el sistema

Tarea 2: Verificar que SNMP MIB se admita en el host.

Para el proceso de línea de base es necesario recopilar la información de almacenamiento, procesamiento y memoria del host. Para realizar este procedimiento, es necesario explorar el grupo HOST-RESOURCES-MIB enlistado en .1.3.6.1.2.1.25.

Nota: Revisar el material de la plataforma hostMIBObjects.pdf

Responda las siguientes preguntas:

1. ¿Cuál es el OID para conocer el uso del procesador?
2. ¿Cuál es el OID para obtener el uso de la memoria RAM?
3. ¿Cuál es el OID para sondear el uso del almacenamiento del dispositivo?

Tarea 3: Consultar y registrar objetos MIB del SNMP específicos del HOST

Hay varias maneras de sondear los objetos de MIB y de registrar la salida. Los productos comerciales, los productos gratuitos, los scripts están disponibles. Todas las herramientas utilizan el SNMP 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.

Partiendo del OID que es soporta en el host, es necesario decidir cuantas veces se debe sondear y cómo se va a registrar la información recopilada. Cisco recomienda que el CPU MIB esté sondeado en intervalos de cinco minutos. Un intervalo más bajo aumentaría la carga en la red o el dispositivo. Se recomienda también generalmente que el sondeo de línea de base se ejecute por lo menos en un periodo de dos semanas.

Tarea 4: Analice los datos para determinar los umbrales

Una vez de que se almacenaron ciertos datos, se puede comenzar con el análisis. 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.

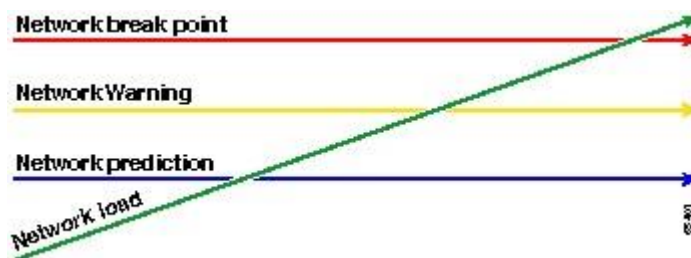
Una estrategia que se puede utilizar para hacer este más fácil el análisis, es la metodología de umbral. Esta metodología utiliza tres números sucesivos de umbral.

- Ready (Listo) —el umbral que se estableció como indicador de qué dispositivos tal vez necesiten atención en el futuro
- Set (preparado) —el umbral que se usa como un indicador previo que avisa el inicio de la planificación para una realizar una reparación, actualización o una configuración nueva.
- Go (ya) — el umbral es una condición de falla y requiere una cierta acción repararla; en este ejemplo es el 60 por ciento.

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

Umbral	Acción	Resultado
45 por ciento	Investigue más lejos	Lista de opciones para los planes de acción
El 50 por ciento	Formule el plan de acción	Lista de pasos en el plan de acción
60 por ciento	Implemente el plan de acción	El router ya no supera los umbrales. De nuevo al modo listo

El siguiente diagrama muestra el cuadro cambiado de línea de base usando la metodología Listo, Preparado, ya.



Al implementar la metodología Listo, preparado, ya, se puede decir que se mantiene la red sana. La ejecución de este tipo de hojas de operación (planning) es también extremadamente útil para la planificación del presupuesto.

Tarea 5: Problemas inmediatos identificados arreglo

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.

Parte 3 - Supervisión del rendimiento, medición e informes

Las diferentes mediciones del rendimiento en la interfaz, en el dispositivo o en los niveles de protocolo deben 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

El módulo de supervisión de rendimiento es capaz de medir el tiempo de respuesta hacia un dispositivo IP de destino, que puede ser un enrutador 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. El módulo de supervisión de

rendimiento puede alertar a las consolas de administración si el tiempo de respuesta excede los umbrales predefinidos.

El módulo de supervisión de rendimiento puede medir y/o informar alguna de las siguientes opciones:

- Rendimiento del servicio de Protocolo de transferencia de hipertexto (HTTP)
- Búsqueda del sistema de nombres de dominio (DNS)
- Conexión del 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 puntos extremos para un Calidad de Servicio (QoS) específico
- Bits de tipo de servicio (ToS) IP
- Pérdida del paquete usando los paquetes generados mediante CSAA

Parte 4 -Detección de comportamiento anómalo al monitorizar una red

El problema de recolectar, almacenar y visualizar información de un servicio de red usando series de tiempo se puede solucionar usando el software RRDtool.

Administrar un servicio de red en tiempo real no es una tarea trivial. Cada variable es monitorizada, ya sea el tráfico en bytes en un puerto de un switch, la carga del CPU en un host, o las peticiones atendidas por un demonio, generan series de tiempo. Todas esas series reflejan una parte de la salud del servicio de red.

El primer desafío, por lo tanto, es recopilar, almacenar y proporcionar acceso en tiempo real a esta vasta y diversa información. El software de código abierto RRDtool cumple con este primer desafío.

Es probable que un técnico de red esté interesado en un comportamiento aberrante; es decir, cambios en el comportamiento a corto plazo de una serie temporal (del orden de minutos u horas) que son inconsistentes con el historial pasado. Las tendencias a largo plazo (del orden de semanas o meses) no son de interés desde la perspectiva del monitoreo del servicio porque se espera que una serie temporal evolucione en un entorno dinámico. El comportamiento aberrante puede indicar un cuello de botella de rendimiento, una falla en el componente de la aplicación o un tiempo de inactividad del sistema. En algunos casos, se puede anticipar un comportamiento aberrante.

El segundo desafío del monitoreo de red es identificar automáticamente un comportamiento aberrante en medio de miles de series de tiempo de servicios de red. Una vez que se identifica ese comportamiento, se puede activar una alerta para llamar la atención del técnico sobre el problema potencial. Las herramientas de software existentes proporcionan parte de esta funcionalidad, pero estas soluciones generalmente se basan en reglas o umbrales simples (es decir, la utilización de la

memoria debe ser inferior al 80%). Estas reglas y umbrales son suficientes para muchas aplicaciones, pero no pueden detectar cambios más sutiles en el comportamiento y aplican un criterio estático para detectar comportamientos aberrantes en lugar de dinámicos.

Para informar un comportamiento anómalo es necesario implementar un algoritmo de predicción y tendencia. El algoritmo de predicción permite conocer cuando extrapolarán la carga de la red y el punto de interrupción definido. RRDtool permite proporcionar el análisis de datos (a través del algoritmo de pronóstico de Holt-Winters), umbrales definidos y el comportamiento anómalo en la serie temporal del conjunto de datos.

La detección de comportamiento anómalo es descompuesta en tres partes, cada una se construye sobre su predecesor:

- Un algoritmo para predecir los valores de una serie temporal en un valor esperado.
- Una medida de desviación entre los valores esperados y los valores observados.
- Un mecanismo para decidir si un valor observado o una secuencia de valores observados son “demasiado desviados” de los valores esperados

Haciendo predicción de la tendencia y análisis, el módulo es capaz de “predecir” dónde y cuándo un determinado valor se producirá en cierta fecha con un grado de certeza.

Tarea 1 - Predicción de la tendencia de series temporales lineales

Para analizar una serie temporal con comportamiento lineal se usará el método de mínimos cuadrados para encontrar la línea del mejor ajuste al comportamiento de una variable monitorizada. Dicho método cumple la siguiente función:

$$y = a(x) + b$$

Donde ‘a’ denota la pendiente y ‘b’ es el valor de la constante de la ecuación (intercepción en y)

Tarea 2 - Predicción de la tendencia de series temporales no lineales

Para conjunto de datos no lineales se usará el algoritmo de Holt Winters.

Parte 5 Detección y notificación de comportamiento anómalo

Un desafío del monitoreo de red es identificar automáticamente un comportamiento aberrante en medio de miles de series de tiempo de servicios de red. Una vez que se identifica ese comportamiento, se puede activar una alerta para llamar la atención del técnico sobre el problema potencial.

Lista de cotejo.

Servicio IP (solo se evalúan cinco más SNMP)	Configuración del servicio según el contrato de nivel de servicio (1 punto)		Análisis y ajuste del rendimiento (línea de base) (1 punto)		Supervisión del rendimiento, medición e informes (1punto)		Detección de comportamiento anómalo al monitorizar una red				Detección y notificación de comportamiento anómalo (1 punto)	
							Predicción de la tendencia de series temporales no lineales (3 puntos)		Predicción de la tendencia de series temporales no lineales (3 puntos)			
	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No
FTP												
DNS												
HTTP												
SSH												
SMTP												
DHCP												
HTTPS												
SNMP												