Gestión y Monitoreo de Redes

Claudia Inostroza
Cinostro@reuna.cl
Albert Astudillo
aastudillo@reuna.cl
Managua 05 y 06 de Diciembre de 2011

Agenda del Curso

- Lunes 5
  - Sesion 1: Introducción a Gestión de monitoreo de redes
  - Sesion 2: SNMP:
    - » Mibs y OIDs
    - » SNMPWalk
  - Sesion 3: Preparación Laboratorio
    - » Instalación Weblog
  - Sesion 4: Nagios
    - » Administración
    - » Funcionalidades

Agenda

- Martes 6
  - Sesion 1: Netflow
    - » Instalación
    - » Configuración
    - » Administración
  - Sesion 2: Smokeping
  - Sesion 3: RANCID
  - Sesion 4: Netdot

Introducción a la Gestion y Monitoreo de Redes

Claudia Inostroza
Cinostro@reuna.cl
Albert Astudillo
aastudillo@reuna.cl
Managua 05 y 06 de Diciembre de 2011

Los ámbitos que vamos a abordar

- Que es monitoreo y Gestión de redes
- Que es necesario monitorear y para que?
- Para que hacer Gestión en la Red?
- Herramientas de Monitoreo
- Detección de ataques
- Documentación
- NOC

¿Qué es Monitoreo de Red?

…

“ **Monitoreo de red**, se define como el uso de un sistema que constantemente monitoriza una red en busca de componentes defectuosos o lentos, para luego informar a los administradores de las redes mediante alarmas, que pueden ser visuales, sonoras, por e-mail, telefónicas, entre otras.”…..

¿ Que es Gestión de Redes?

….. No basta solo con monitorizar, sino que también es necesario definir y realizar actividades sobre la información, fallas y alarmas que puedan generar la monitorización de las redes….

Gestión de Redes son las actividades, métodos, procedimientos y herramientas que permitan la operación, administración, mantenimiento y aprovisionamiento de sistemas conectadas por la red.

¿Que es necesario Monitorear?

- **Servicios y sistemas**
  - Disponible, alcanzable
- **Recursos**
  - Planificación de expansión, mantener disponibilidad
- **Rendimiento**
  - Tiempo de ida y vuelta (rtt), ancho de banda
- **Cambios y configuraciones**
  - Documentación, control de revisión, logging (registro de datos)

Que es monitoreo y Gestión de redes

Que es necesario monitorear y para que?

Para que hacer Gestión en la Red?

Herramientas de Monitoreo

Detección de ataques

Documentación

NOC

Gestión de Redes: Mantenernos Informados

- Estadísticas
  - Para los propósitos de contabilidad y medición
- Fallas (detección de intrusos)
  - La detección de problemas
- Solución de problemas y el seguimiento de su historia

"Con tiempo los sistemas de ticket tienen muchos datos útiles"

Para que Monitorear??

- Una red en operación tiene que estar bajo vigilancia para:
  Cumplir con los Acuerdos de Nivel de Servicio (SLAs)

- SLAs dependen de la política local y de los compromisos adquiridos
  - Que se espera de la administración de la Red?
  - Que esperan sus usuarios?
  - Que esperan sus clientes?
  - Que espera el resto de Internet?
  - Que es aceptable? 99.999% disponibilidad?

- Disponibilidad de 100% es “muy dificil”

Expectativas de Disponibilidad

- **Que es necesario para entregar disponibilidad de 99.9%?**

  30.5 x 24 = 762 horas al mes

  (762 – (762 x .999)) x 60 = 45 minutos

  !Solo 45 minutos de mantenimiento al mes!

- **Es necesario bajar los equipos 1 hora/semana?**

  (762 - 4) / 762 x 100 = 99.4 %

  Se deben tomar en cuenta las mantenciones planificadas en los cálculos, se debe informar antes a sus usuarios/clientes si o no el periodo de mantención esta incluido en el SLA.

- **Como se mide disponibilidad?**

  En el core? Extremo a extremo? Desde Internet?

¿Que es “normal” por su red?

- Si nunca ha medido su red va a necesitar saber algunas cosas como:
  - La carga típica de los enlaces (Consumo de Ancho de Banda)
  - El nivel típico de “jitter” entre los puntos de extremo (variación de tiempo de respuesta)
  - Porcentaje típico de uso de los recursos
  - El nivel típico de “ruido”:
  - Escaneos de la red
  - Paquetes perdidos
  - Informes de errores o fallos

Los ámbitos que vamos a abordar

- Que es monitoreo y Gestión de redes
- Que es necesario monitorear y para que?
- Para que hacer Gestión en la Red?
- Herramientas de Monitoreo
- Detección de ataques
- Documentación
- NOC

¿Para que hacer Gestión en la Red?

- **Saber cuando actualizar**
  - Es el uso de su banda de ancha demasiado alto?
  - Donde va su trafico?
  - Necesita una conexión mas rápida, mas proveedores?
  - Ya están demasiadas viejas sus equipos?
- **Mantener un estado de cambios**
  - Grabar todo los cambios en su red
  - Lo hace mas fácil encontrar la causa de problemas hechas por cambios de configuración y actualizaciones
- **Mantener una historia de sus operaciones**
  - Usando un sistema de tickets mantiene una historia de eventos
  - Permite defenderse y verificar realmente que fue lo que ocurrió

¿Para que hacer Gestión en la Red? (Cont ….)

- **Contabilidad**
  - Seguir el uso de recursos
  - Facturar a los clientes
- **Saber cuando tengas problemas**
  - Mantenerse mas informado que sus usuarios!
  - Software de monitoreo puede generar tickets y notificar en forma automática a su personal de problemas.
- **Tendencias**
  - Se puede usar estés datos para ver tendencias por todo su red.
  - Esto es un parte de recompilar datos, planificación de capacidad y detección de ataques.

Los ámbitos que vamos a abordar

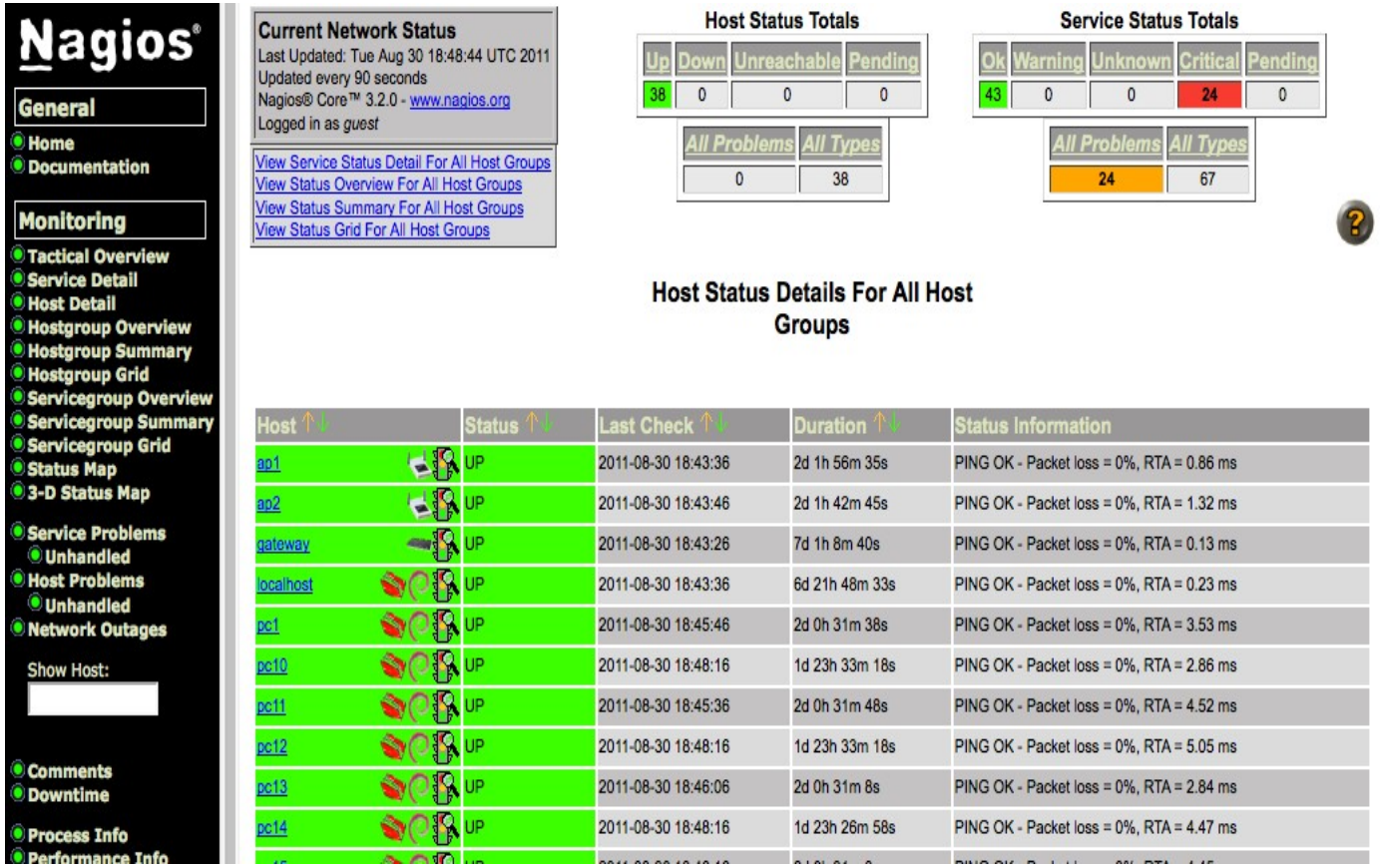
- Que es monitoreo y Gestión de redes
- Que es necesario monitorear y para que?
- Para que hacer Gestión en la Red?
- Herramientas de Monitoreo
- Detección de ataques
- Documentación
- NOC

Con que herramientas podemos medir?

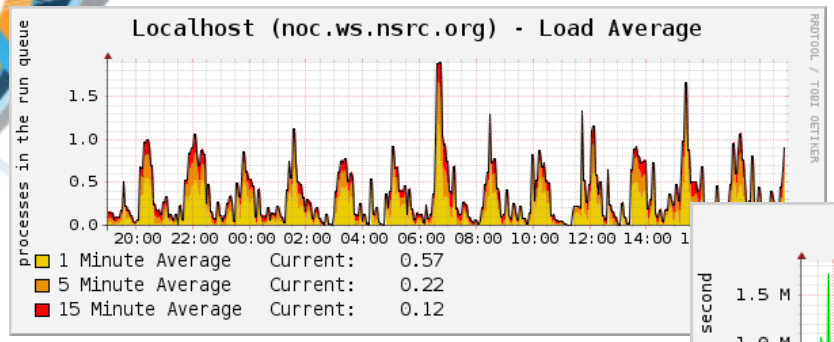
- **Disponibilidad**
  - Nagios
    - Servicios, servidores, enrutadores, switches
- **Confiabilidad**
  - Smokeping
    - Salud de conectividad, rtt, tiempo de respuesta de servicios, latencia
- **Rendimiento**
  - Cacti
    - Trafico en total, uso de puertos, CPU, Memoria Disco, procesos

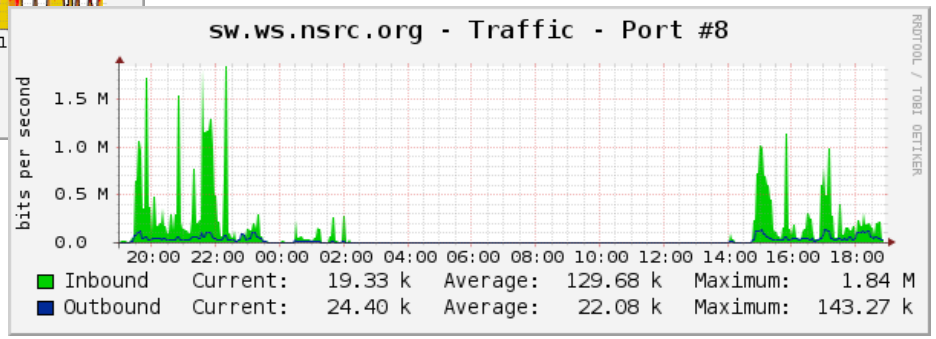
Existe superposición de funcionalidad entre estos programas!

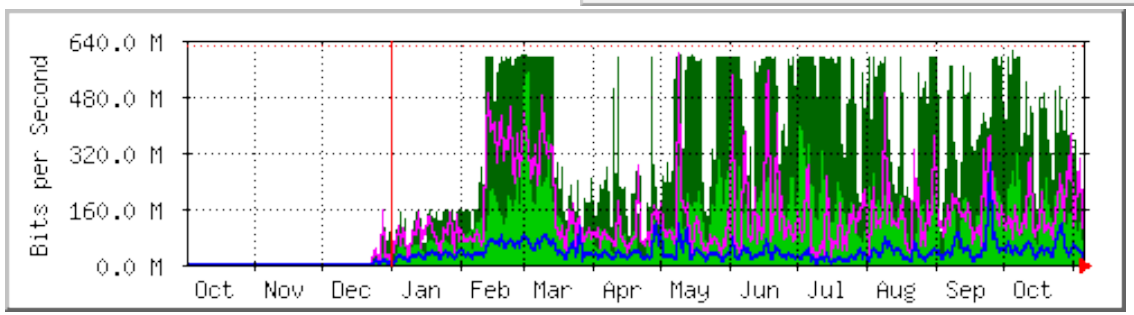
Disponibilidad



Estadísticas de Trafico: Rendimiento

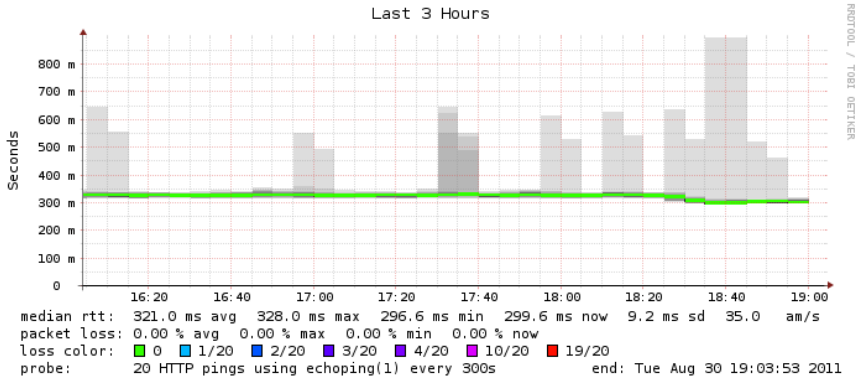


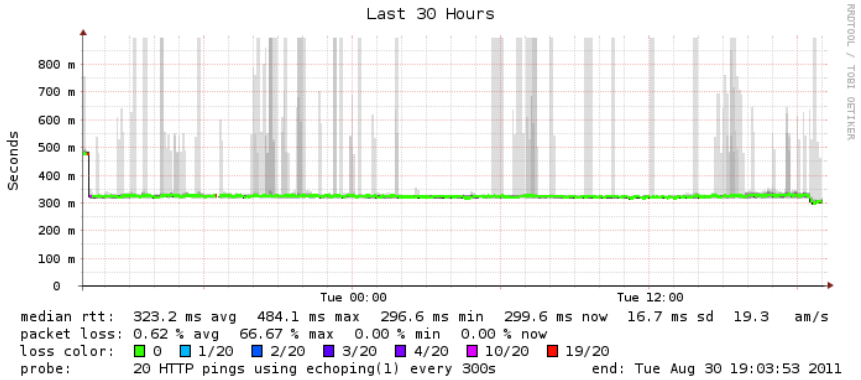




Confiabilidad

sageduck.org (Copenhagen): Tiempo de Respuesta HTTP





Tiempos de Respuesta

Que es monitoreo y Gestión de redes

Que es necesario monitorear y para que?

Para que hacer Gestión en la Red?

Herramientas de Monitoreo

Detección de ataques

Documentación

NOC

Detección de Ataques

- Tendencias y automatización le permite saber cuando se esta produciendo un ataque a su red

- Las herramientas en uso le puede ayudar a mitigar los ataques:
  - Los flujos a través de las interfaces red
  - La carga en servidores o por servicios
  - Fallas de servicios múltiples
  - Escaneos preventivos, para detectar posibles fallas

Que es monitoreo y Gestión de redes

Que es necesario monitorear y para que?

Para que hacer Gestión en la Red?

Herramientas de Monitoreo

Detección de ataques

Documentación

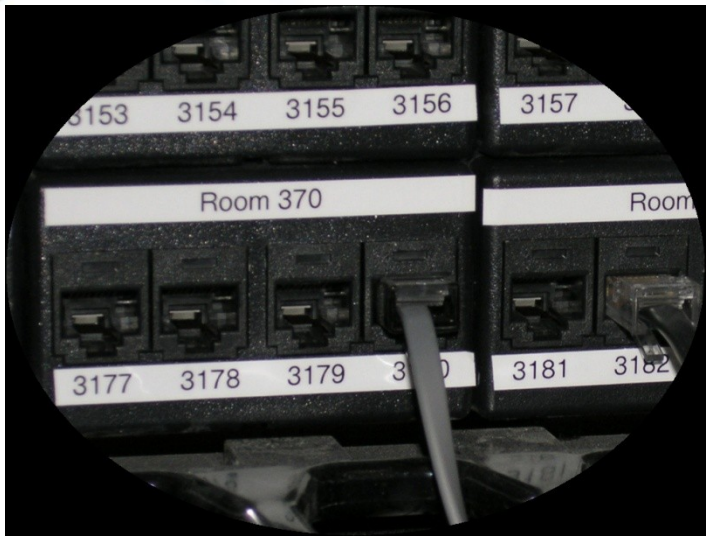
NOC

Importante Documentar Todo!!!!!

- Conocer la configuración de los dispositivos de Red
  - Permite detectar cambios en las configuraciones
- ¿Como están conectados los equipos entre si?
  - Diagrama de la red actualizado
- ¿Quienes son los proveedores de los enlaces?
  - Mantener los ID de los enlaces y procedimientos de reclamos
- ¿Que esta conectado en cada interfaz?
  - Etiquetar los cables y puertos de los equipos

Documentar: Etiquetar

- Puede ser un archivo simple de texto con una línea por cada puerto en un switch:



switch1, puerto 1, Sala 29 – Oficina Rector

¡La Información debe estar disponible para los administradores de la red!!!

Quizás sea necesario Automatizar la documentación!!!

- Un sistema automatizado de documentación de redes es algo para considerar.
  - Puede escribir Programas propios.
  - Puede considerar algunos sistemas de documentación automáticas.
  - Probablemente va a terminar haciendo los dos.

  Existen algunos programas
  - IPplan: http://iptrack.sourceforge.net/
  - Netdot: https://netdot.uoregon.edu/

Los ámbitos que vamos a abordar

- Que es monitoreo y Gestión de redes
- Que es necesario monitorear y para que?
- Para que hacer Gestión en la Red?
- Herramientas de Monitoreo
- Detección de ataques
- Documentación
- NOC

Centro de Operaciones de RED: NOC
Donde todo pasa!!!

- Coordinación de tareas
  - Estatus de los servicios y de la red
  - Recibiendo incidentes y quejas relacionados con la red.
  - Donde viven las herramientas (“servidor NOC”)
- Documentación incluyendo:
  - Diagramas de las redes
  - Base de datos y/o archivo de texto de cada puerto en cada switch
  - Descripción de la Red
  - Y … Mucho mas…

Algunas Aplicaciones de Código Abierto

Rendimiento

- Cricket
- IFPFM
- flowc
- mrtg*
- NetFlow*
- NfSen*
- ntop
- perfSONAR
- pmacct
- rrdtool*
- SmokePing*

Documentación

- IPplan
- Netdisco
- Netdot*
- Rack Table

Logging (Registro)

- swatch*
- syslog/rsyslog*
- tenshi*

Gestión de Red

- Big Brother
- Big Sister
- Cacti*
- Hyperic
- Munin
- Nagios*
- OpenNMS*
- Sysmon
- Zabbix

Preguntas???

Gracias!!!