Gestión y Monitoreo de Redes

Introducción a la Gestión de Redes

Sección I: Panorama

Conceptos claves:

- Qué es la monitorización de redes
- Qué es la gestión de redes
- Lo básico
- Por qué gestión de redes
- Los tres grandes elementos
- Detección de ataques
- Documentación
- Consolidación de la información
- La visión completa

Detalles de la Gestión de Redes

Monitorizamos

- **Sistemas y servicios**
  - Disponible, alcanzable
- **Recursos**
  - Planificación de expansión, mantener disponibilidad
- **Rendimiento**
  - Tiempo de ida y vuelta, tasa máxima de transmisión
- **Cambios y configuraciones**
  - Documentación, control de versiones, logs

Detalles de la Gestión de Redes

Seguimos la pista de

- **Estadísticas**
  - Para fines de contabilidad
- **Fallos (Deteccion de Intrusion)**
  - Detección de problemas
  - Historial de fallos y sus soluciones

- Los sistemas de gestión de incidencias son buenos para esto
- Helps desks son un componiente util hasta critico.

Expectativas

Una red en operación debe ser monitorizada para:

- Asegurar los SLA proyectados (Acuerdos de Nivel de Servicio
- Los SLAs dependen de políticas
  - Qué espera la dirección?
  - Qué esperan los usuarios?
  - Qué esperan los clientes?
  - Qué espera el resto de la Internet?
- Qué se considera bueno? 99.999% de disponibilidad?
  - No hay tal cosa como disponibilidad 100% →

Expectativas de Disponibilidad

Qué hace falta para 99.9 %?

30.5 días x 24 horas = 732 horas por mes

(732– (732 x .999)) x 60 = 44 minutos

Sólo 44 minutos de baja por mes!

Tiene que apagar 1 hora por semana?

(732 – 4) / 732x 100 = 99.4 %

Recuerde tomar en cuenta el tiempo de baja planeado, e informe a sus usuarios si está o no incluído en el SLA

Cómo se mide la disponibilidad?

En el núcleo (core) ? Extremo a extremo? Desde la Internet?

Puntos de Referencia

Qué se considera normal en su red?

Si nunca ha monitorizado su red, tendrá que saber cosas como:

- Carga típica de los enlaces (➔ Cacti)
- Nivel de variabilidad (jitter) entre dos puntos (➔ Smokeping)
- Utilización típica de recursos
- Niveles de “ruido” típicos:
  - Escaneos de red
  - Datos descartados
  - Errores reportados y fallos

Por qué hacer todo esto?

Saber cuándo se necesita una mejora

- Su ancho de banda está saturado?
- A dónde vá su tráfico?
- Necesita un enlace de más capacidad, u otro proveedor?
- Es demasiado viejo el equipo?

Mantener una auditoría de cambios

- Anotar todos los cambios
- Facilita conocer el origen de los problemas después de cambios y actualizaciones

Mantenga un histórico de las operaciones

- Use un sistema de gestión de incidencias
- Le permite protegerse y saber lo que ha ocurrido

Por qué la gestión de redes?

Contabilidad

- Medir el uso de los recursos
- Cobrar a clientes basado en utilización

Saber cuándo hay problemas

- Entérese antes que los usuarios, sino quedará mal!
- El sistema de gestión puede crear incidencias y notificar al equipo técnico

Tendencias

- Toda esta información sirve para ver las tendencias en la red
- Esto es parte del establecimiento de un punto de referencia, planificación de la capacidad, etc.

Los tres “grandes” elementos

Disponibilidad

- Nagios — Servicios, servidores, enrutadores (routers), conmutadores (switches)

Fiabilidad

- Smokeping — Retardo, pérdidas, variabilidad, salud de enlace

Rendimiento

- Cacti — Utilización de enlaces, CPU, memoria, disco, etc.

Existe cierta coincidencia de funcionalidades entre los tres

Detección de ataques

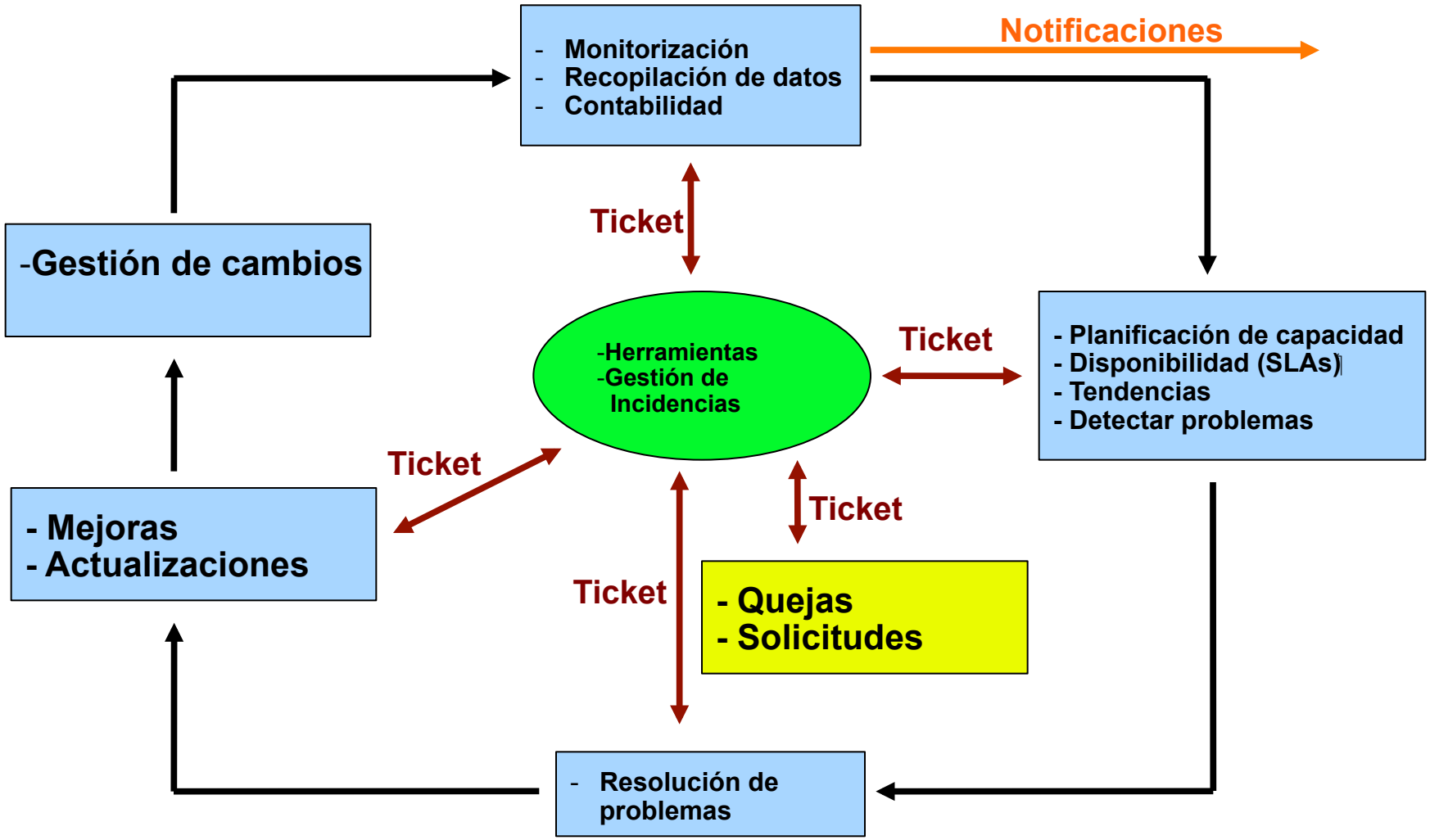
- La utilización de las tendencias y la automatización, permiten determinar cuándo es victima de un ataque
- Las herramientas le pueden ayudar a mitigar estos ataques:
  - Flujos (netflow) a través de interfaces
  - Saturación de servicios o servidores específicos
  - Fallos en múltiples servicios

Consolidación de Datos

El Centro de Operaciones de la Red (COR, o NOC) es “Donde ocurre todo”

- Coordinación de tareas
- Estado de la red y los servicios
- Atención de incidencias y quejas
- Donde residen las herramientas (”servidor NOC”)
- Documentación que incluye:
  - Diagramas de red
  - Asignación de puertos en conmutadores y enrutadores
  - Descripción de la red
  - Y como veremos mas adelante, mucho más

Visión General



Unas *pocas* soluciones Open Source…

Rendimiento

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

Manejo de Incidencias

- RT*
- Trac*
- Redmine

Gestión de Cambios

- Mercurial
- Rancid* (routers)
- CVS*
- Subversion*
- git*

Seguridad/(SDI)

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Registro de Eventos

- swatch*
- syslog-ng/rsyslog*
- tenshi*

Gestión de Redes

- Big Brother
- Cacti*
- Hyperic
- Munin
- Nagios* / Icinga*
- OpenNMS*
- Observium*
- Sysmon
- Zabbix

Documentación

- IPplan
- Netdisco
- Netdot*
- Rack Table

Protocolos/Utilidades

- SNMP*, Perl, ping

Preguntas hasta ahora?

?