

Introducción a la Gestión y Monitoreo de Redes

Network Startup Resource Center
www.nsrc.org



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license
(<http://creativecommons.org/licenses/by-nc/4.0/>)

Objetivos

Presentar Conceptos Fundamentales y Terminología

- Gestión y Monitoreo de Redes
- Que y de porque monitoreamos
- Expectativas de tiempo disponible y cálculos
- Rendimiento típico & detección de ataques
- Que y porque gestionamos
- Herramientas para gestionar y monitorear redes
- El “NOC”: consolidando sistemas

NOC: Consolidando Sistemas

NOC = Centro de Operaciones de la Red

- Coordinación de tareas, manejo de incidentes (sistema de ticketing)
- Estatus de la red y servicios (herramientas de monitoreo)
- Donde se encuentra las herramientas de gestión y monitoreo
- Almacén de documentación (wiki, base de datos, repositorios → Herramientas de documentación)

NOC: Consolidando Sistemas

Ubicación del NOC

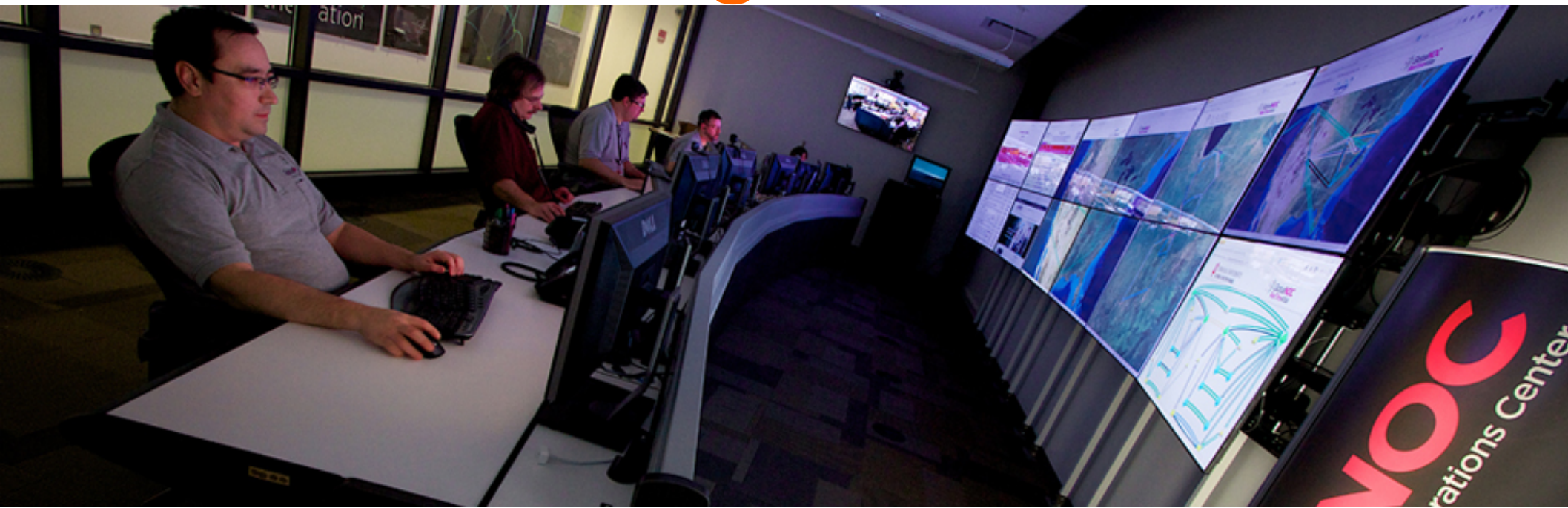
- NOC es un concepto organizacional
- No tiene que ser un lugar ni un solo servidor
- Un NOC remoto, distribuido es posible con Gestión de OoB (Fuera Banda)

Por esta semana el NOC por el curso será

<http://noc.ws.nsrc.org/>



Algunos NOCs Físicos



Gestión y Monitoreo de Redes

Monitoreo (“supervisión”)

- Comprobar el estado de una red

Gestión

- Los procesos para operar con éxito una red

Monitoreo de Sistemas y Servicios

Sistemas

- Rutadores
- Conmutadores
- Servidores

Servicios

- DNS
- HTTP
- IMAP
- SMTP
- SNMP, etc.



By Azaleos (Own work) [CC BY-SA 3.0 (<http://creativecommons.org/licenses/by-sa/3.0>) or GFDL (<http://www.gnu.org/copyleft/fdl.html>)], via Wikimedia Commons

Porque Hacemos Monitoreo?

- Estan alcanzable los sistemas y servicios?
- Estan disponible?
- Cuantos recursos usan?
- Cuál es su rendimiento?
 - Tiempos de ida y vuelta, rendimiento de la red?
 - Fallas y cortes
- Se han configurado o cambiado?
- Están bajo ataque?

Porque Hacemos Monitoreo?

- Para saber cuando haya problemas – Antes que nuestros clientes!
- Seguir utilización de recursos para cobrar clientes
- Entregar el nivel de servicio esperado (SLAs)
 - Que espera nuestra gerencia?
 - Que esperan los clientes?
 - Que espera el resto de Internet?

Porque Hacemos Monitoreo?

- Para probar que estamos entregando que fue prometido
 - Logramos un nivel de servicio de 99.9%?
- Asegurar que cumplimos con las expectativas en el futuro (SLAs)
 - Esta al punto de fallarse nuestra red?
 - Estará congestionado la red?

Expectativas de Disponibilidad

Qué hace falta para 99.9 %?

30.5 días x 24 horas = 732 horas por mes

$(732 - (732 \times .999)) \times 60 = 44$ minutos

Sólo 44 minutos de baja por mes!

Tiene que apagar 1 hora por semana?

$(732 - 4) / 732 \times 100 = 99.4 \%$

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

Cómo se mide la disponibilidad?

- En el núcleo (core)? Extremo a extremo? Desde el Internet?
- Se mide cada servidor, máquina?
- Si funciona por el jefe esta bien?

Estableciendo un Punto de Referencia

- Se puede usar monitoreo para establecer un punto de referencia (*baseline*)
- Punto de referencia = Que es normal por tu red?
 - Latencia de red típico a través rutas
 - Nivel de variabilidad (jitter) a través rutas
 - La carga en los enlaces
 - El porcentaje de uso de recursos
 - Nivel de “ruido” típicos:
 - ✓ Escaneos de la red y ataques aleatorios desde el Internet
 - ✓ Paquetes perdidas
 - ✓ Errores y fallas reportadas

Detectar Ataques

- Desviación desde el punto de referencia puede significar ataques.
- Hay mas flujos que lo usual?
- Es la carga mas alta en algunos servidores o servicios?
- Ha tenido fallas de varios servicios?

Estas cosas pueden significar un ataque

Que Gestionamos?

- Los equipos que desplegamos
 - El software corriendo en ellos
 - Su configuración (hardware y software)
 - Donde esta instalado
 - Tenemos extras?
- Cumplimos con los pedidos de los usuarios?
 - Instalar, mover, añadir o cambiar cosas?
 - Seguimiento y resolución de fallos

Por que Gestionamos?

- Saber cuando haya problemas – antes que nuestros clientes!
- Seguir el uso de los recursos (facturación)
- Cumplir al nivel de servicio esperado (SLAs)
 - Que espera nuestra gerencia?
 - Que esperan los clientes?
 - Que espera el resto de Internet?

Por que Gestionamos?

- Mejorar el producto que entregamos
 - Logramos 99.9% disponibilidad?
- Asegurar que cumplimos con las expectativas en el futuro (SLAs)
 - Esta al punto de fallar nuestra red? Esta congestionado?

Herramientas de Monitoreo y Gestión

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

Herramientas de Gestión

Sistema de Pedidos (Tickets): RT

- Administrar el aprovisionamiento y soporte

Gestión de configuración: RANCID

- Seguir configuraciones de los enrutadores

Network Documentación: Netdot

- Inventario, localización y dueño de inventario

Existe cierta coincidencia de funcionalidades entre los tres

Algunas Herramientas de Fuente Abierto

RENDIMIENTO	GESTION de CAMBIOS	GESTION de RED
Cricket	Mercurial	Big Brother
flowc	RANCID	Cacti
mrtg	CVS	Hyperic
NetFlow	Subversion	LibreNMS
NfSen	git	Nagios
ntop	Security/NIDS	OpenNMS
perfSONAR	Nessus	Sysmon
pmacct	OSSEC	Zabbix
RRDTool	Prelude	Documentation
SmokePing	Samhain	IPplan
PEDIDOS	SNORT	Netdisco
RT	Untangle	Netdot
Trac		UTILIDADES
Redmine		SNMP, Perl, Ping

Repaso de Gestión y Monitoreo

- Gestión y Monitoreo de Redes
- Cual y porque monitoreamos?
- Expectativas de tiempo de disponibilidad y como calculamos
- Rendimiento de punto de referencia
- Detección de ataques
- Cual y porque gestionamos?
- Herramientas de Gestión y Monitoreo
- El NOC: Consolidando sistemas