IXP: Mediciones y monitoreo

Hernán Galperin*, J. Ignacio Alvarez-Hamelin†‡§ y Esteban Carisimo**

*CONICET – Universidad de San Andrés
†Instituto Tecnológico de Buenos Aires
‡CONICET – Facultad de Ingeniería UBA
§GRCyCD – Facultad de Ingeniería UBA
http://cnet.fi.uba.ar/
**GRCyCD – Facultad de Ingeniería UBA
http://cnet.fi.uba.ar/

Noviembre 2014

¿Para qué sirve el monitoreo?

Frases de Lord Kelvin:

- *“Medir es saber”*
- *“Si no puedes medirlo, no puedes mejorarlo”*

¿Para qué sirve el monitoreo?

Frases de Lord Kelvin:

- *“Medir es saber”*
- *“Si no puedes medirlo, no puedes mejorarlo”*

¿Para qué sirve el monitoreo?

Frases de Lord Kelvin:

- *“Medir es saber”*
- *“Si no puedes medirlo, no puedes mejorarlo”*

¿Para qué sirve el monitoreo?

Frases de Lord Kelvin:

- *“Medir es saber”*
- *“Si no puedes medirlo, no puedes mejorarlo”*

Métricas de medición

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia *(cantidad de saltos)*
- Tasa de pérdida de paquetes

Métricas de medición

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia *(cantidad de saltos)*
- Tasa de pérdida de paquetes

Métricas de medición

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia *(cantidad de saltos)*
- Tasa de pérdida de paquetes

Métricas de medición

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia *(cantidad de saltos)*
- Tasa de pérdida de paquetes

Métricas de medición

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia *(cantidad de saltos)*
- Tasa de pérdida de paquetes

Métricas de medición

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia *(cantidad de saltos)*
- Tasa de pérdida de paquetes

Métricas de medición

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia *(cantidad de saltos)*
- Tasa de pérdida de paquetes

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute, ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute, ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute, ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute, ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute, ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

Desarrollada *ad-hoc* para PIT Bolivia:

- PladMeD

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

Desarrollada *ad-hoc* para PIT Bolivia:

- PladMeD

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

Desarrollada *ad-hoc* para PIT Bolivia:

- PladMeD

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

Desarrollada *ad-hoc* para PIT Bolivia:

- PladMeD

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

Desarrollada *ad-hoc* para PIT Bolivia:

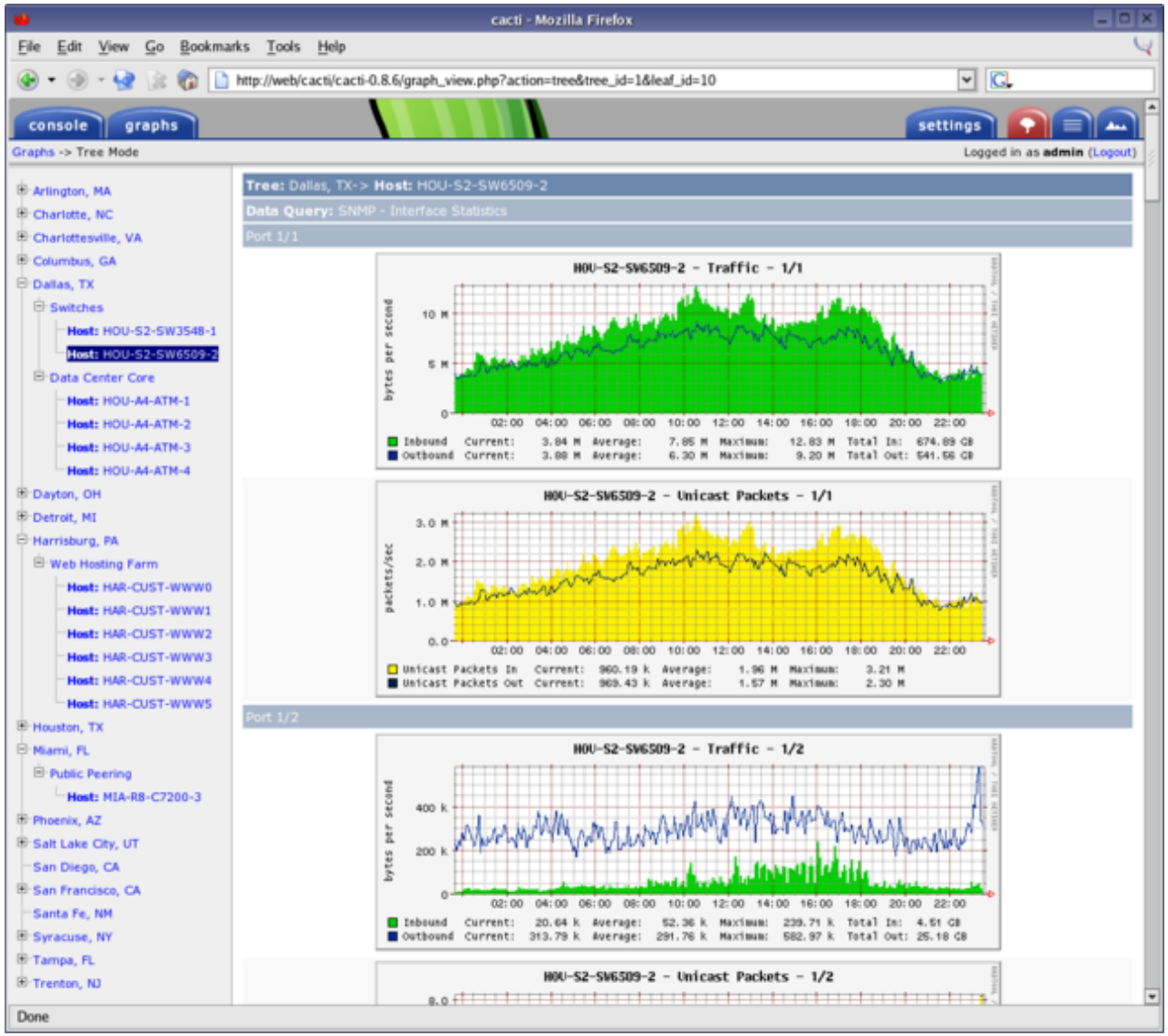
- PladMeD

Cacti

Acerca de Cacti:

- Front-end en PHP para generar gráficos de variables de red
- Fuentes de datos:
  - Cualquier fuente externa
  - A través de RRDTool
  - Almacenados en MySQL
- Soporte SNMP y creación de MRTG
- Capacidad para estrcuturar la información de forma jerárquica a través de árboles

Ejemplo Cacti

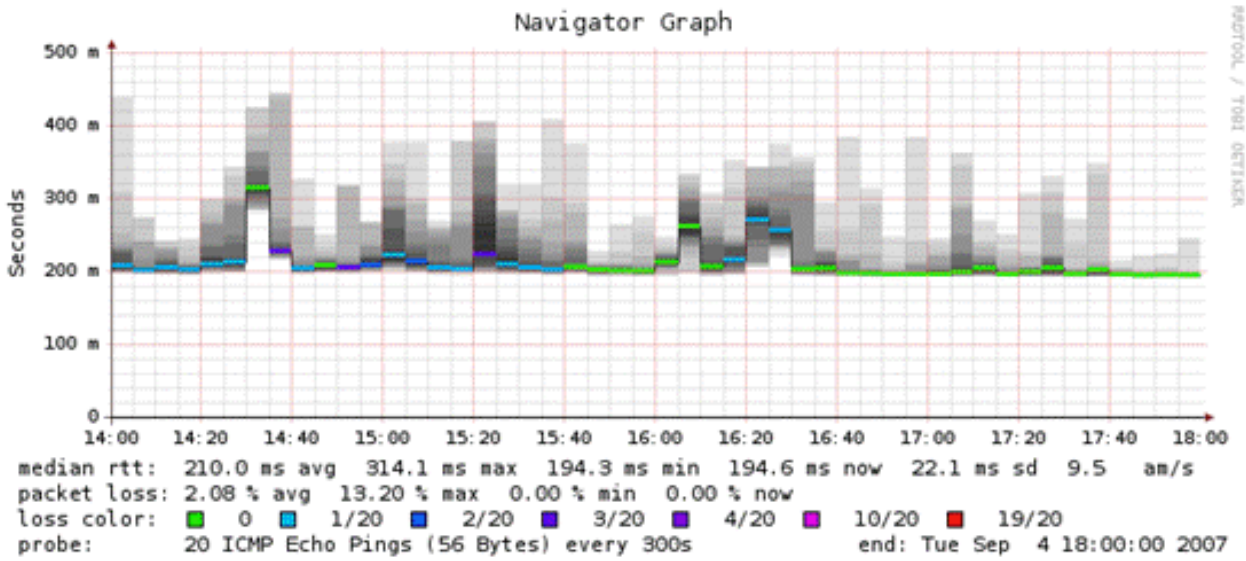


SmokePing

Acerca de SmokePing:

- Herramienta para medir latencia y tasa de pérdida de paquetes
- Herramienta divida en dos:
  - *back-end*: Obtención y almacenamiento de datos
  - *front-end*: Presentación web
- Almacena y gráfica la distribución de los parámetros
- Puede calcular la latencia de distintos protocolos:
  - ICMP (`ping`)
  - HTTP
  - DNS
- Almacena los datos a través de RRDTool
- Capacidad para generar alarmas
- Capacidad *Master-Slave*: Poder generar pruebas desde puntos remotos

Ejemplo SmokePing



Sistema de monitoreo con multiples prestaciones tienendo como destacadas las siguientes áreas:

- Capacidad de detectar los servicios prestados en la red monitoreada
- Almacenamiento y reportes:
  - Capacidad propia o de fuentes externas para obtener información
  - Disponibilidad para enviar reportes por e-mail o SMS
- Medición de performance
  - Capacidad de almacenamiento de SNMP y JMX
  - Comparación contra umbrales sofisticados (cambios absolutos y relativos)
  - Capacidad de generar gráfico “TOP N”

Sistema de monitoreo con multiples prestaciones tienendo como destacadas las siguientes áreas:

- Capacidad de detectar los servicios prestados en la red monitoreada
- Almacenamiento y reportes:
  - Capacidad propia o de fuentes externas para obtener información
  - Disponibilidad para enviar reportes por e-mail o SMS
- Medición de performance
  - Capacidad de almacenamiento de SNMP y JMX
  - Comparación contra umbrales sofisticados (cambios absolutos y relativos)
  - Capacidad de generar gráfico “TOP N”

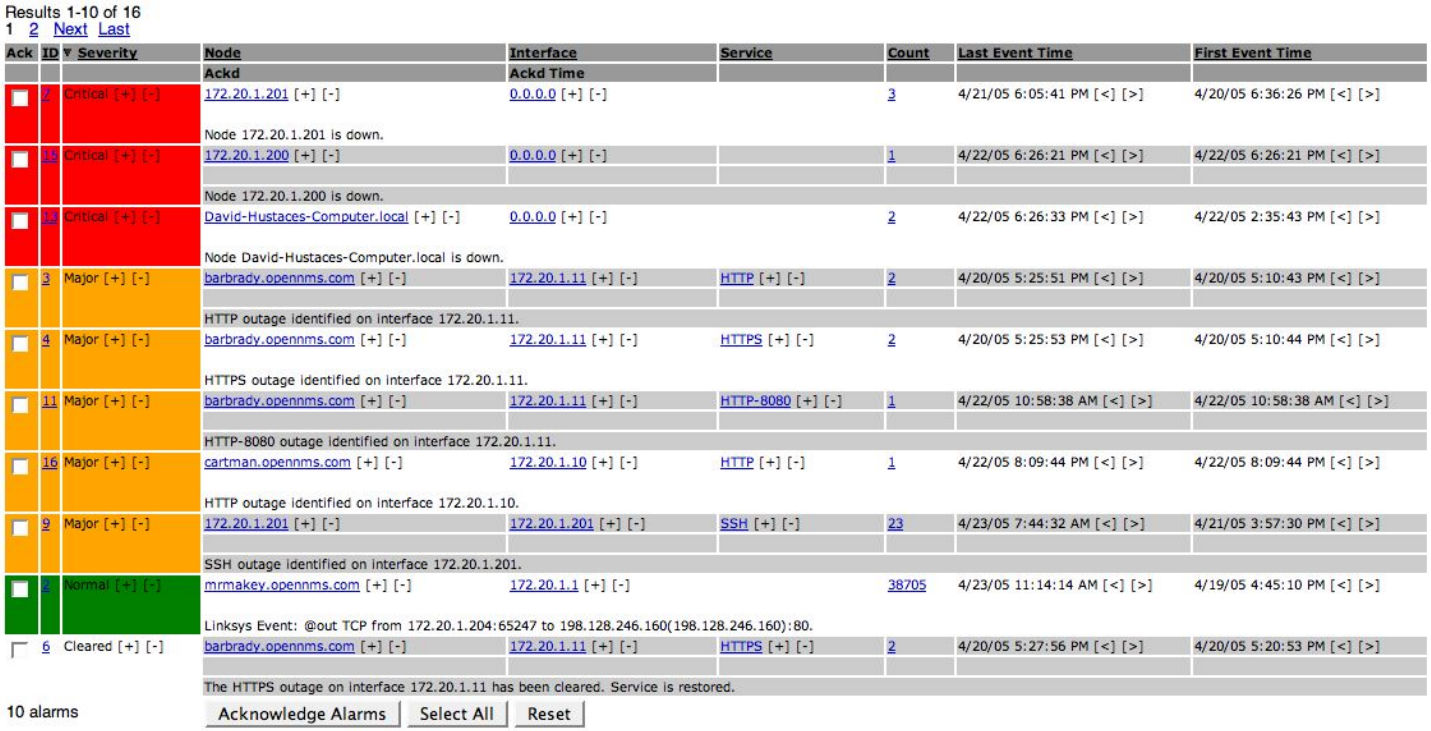
Sistema de monitoreo con multiples prestaciones tienendo como destacadas las siguientes áreas:

- Capacidad de detectar los servicios prestados en la red monitoreada
- Almacenamiento y reportes:
  - Capacidad propia o de fuentes externas para obtener información
  - Disponibilidad para enviar reportes por e-mail o SMS
- Medición de performance
  - Capacidad de almacenamiento de SNMP y JMX
  - Comparación contra umbrales sofisticados (cambios absolutos y relativos)
  - Capacidad de generar gráfico “TOP N”

Sistema de monitoreo con multiples prestaciones tienendo como destacadas las siguientes áreas:

- Capacidad de detectar los servicios prestados en la red monitoreada
- Almacenamiento y reportes:
  - Capacidad propia o de fuentes externas para obtener información
  - Disponibilidad para enviar reportes por e-mail o SMS
- Medición de performance
  - Capacidad de almacenamiento de SNMP y JMX
  - Comparación contra umbrales sofisticados (cambios absolutos y relativos)
  - Capacidad de generar gráfico “TOP N”

Ejemplo openNMS (I)



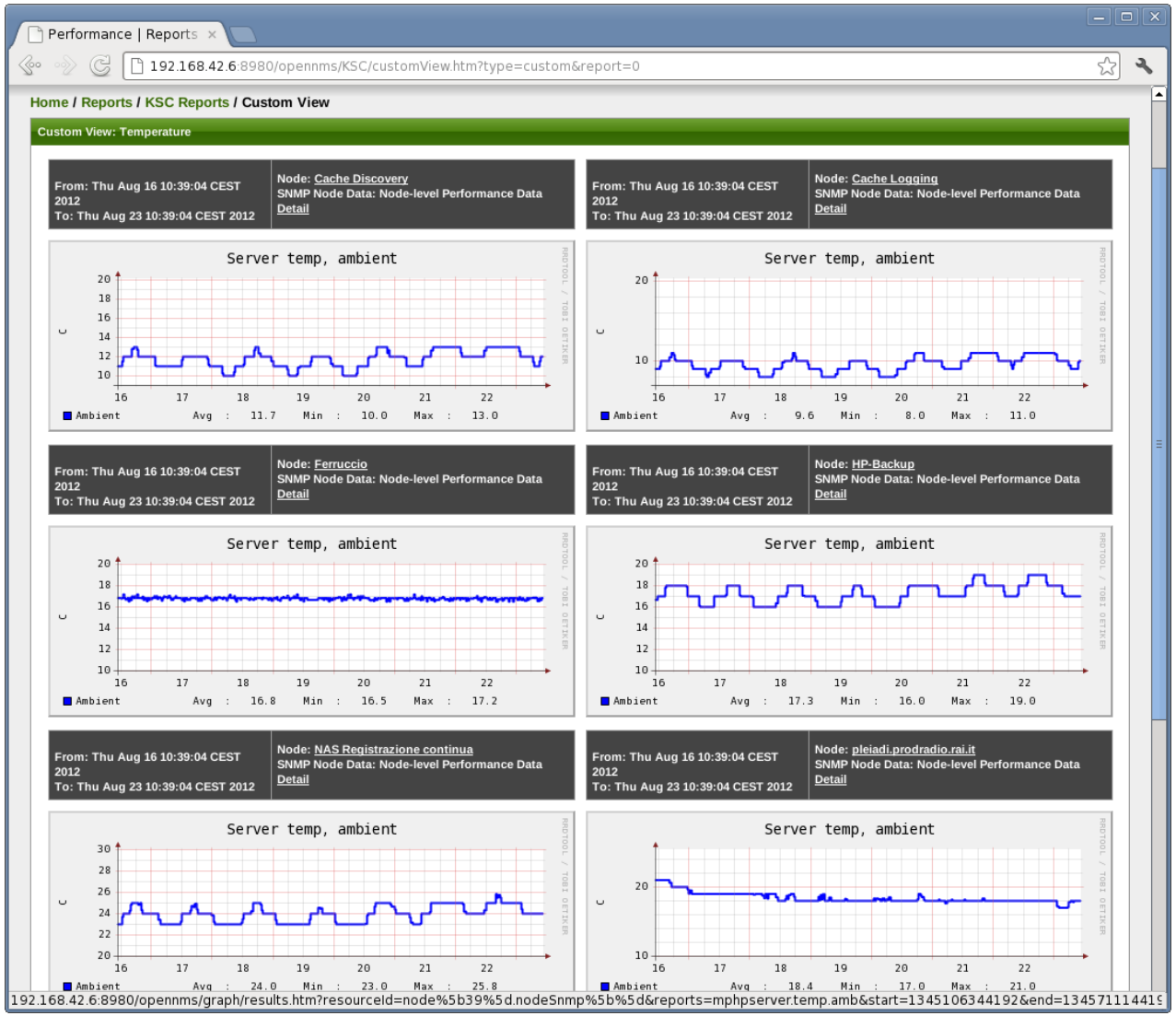
Results 1-10 of 16
1 2 Next Last

Ack	ID	Severity	Node	Interface	Service	Count	Last Event Time	First Event Time
			Ackd	Ackd Time				
☐	7	Critical [+] [-]	172.20.1.201 [+] [-]	0.0.0.0 [+] [-]		3	4/21/05 6:05:41 PM [<] [>]	4/20/05 6:36:26 PM [<] [>]
			Node 172.20.1.201 is down.					
☐	13	Critical [+] [-]	172.20.1.200 [+] [-]	0.0.0.0 [+] [-]		1	4/22/05 6:26:21 PM [<] [>]	4/22/05 6:26:21 PM [<] [>]
			Node 172.20.1.200 is down.					
☐	15	Critical [+] [-]	David-Hustaces-Computer.local [+] [-]	0.0.0.0 [+] [-]		2	4/22/05 6:26:33 PM [<] [>]	4/22/05 2:35:43 PM [<] [>]
			Node David-Hustaces-Computer.local is down.					
☐	3	Major [+] [-]	barbrady.opennms.com [+] [-]	172.20.1.11 [+] [-]	HTTP [+] [-]	2	4/20/05 5:25:51 PM [<] [>]	4/20/05 5:10:43 PM [<] [>]
			HTTP outage identified on interface 172.20.1.11.					
☐	4	Major [+] [-]	barbrady.opennms.com [+] [-]	172.20.1.11 [+] [-]	HTTPS [+] [-]	2	4/20/05 5:25:53 PM [<] [>]	4/20/05 5:10:44 PM [<] [>]
			HTTPS outage identified on interface 172.20.1.11.					
☐	11	Major [+] [-]	barbrady.opennms.com [+] [-]	172.20.1.11 [+] [-]	HTTP-8080 [+] [-]	1	4/22/05 10:58:38 AM [<] [>]	4/22/05 10:58:38 AM [<] [>]
			HTTP-8080 outage identified on interface 172.20.1.11.					
☐	16	Major [+] [-]	cartman.opennms.com [+] [-]	172.20.1.10 [+] [-]	HTTP [+] [-]	1	4/22/05 8:09:44 PM [<] [>]	4/22/05 8:09:44 PM [<] [>]
			HTTP outage identified on interface 172.20.1.10.					
☐	9	Major [+] [-]	172.20.1.201 [+] [-]	172.20.1.201 [+] [-]	SSH [+] [-]	23	4/23/05 7:44:32 AM [<] [>]	4/21/05 3:57:30 PM [<] [>]
			SSH outage identified on interface 172.20.1.201.					
☐	2	Normal [+] [-]	mrmakey.opennms.com [+] [-]	172.20.1.1 [+] [-]		38705	4/23/05 11:14:14 AM [<] [>]	4/19/05 4:45:10 PM [<] [>]
			Linksys Event: @out TCP from 172.20.1.204:65247 to 198.128.246.160(198.128.246.160):80.					
☐	6	Cleared [+] [-]	barbrady.opennms.com [+] [-]	172.20.1.11 [+] [-]	HTTPS [+] [-]	2	4/20/05 5:27:56 PM [<] [>]	4/20/05 5:20:53 PM [<] [>]
			The HTTPS outage on interface 172.20.1.11 has been cleared. Service is restored.					

10 alarms

Acknowledge Alarms | Select All | Reset

Ejemplo openNMS (II)



Siguiente presentación