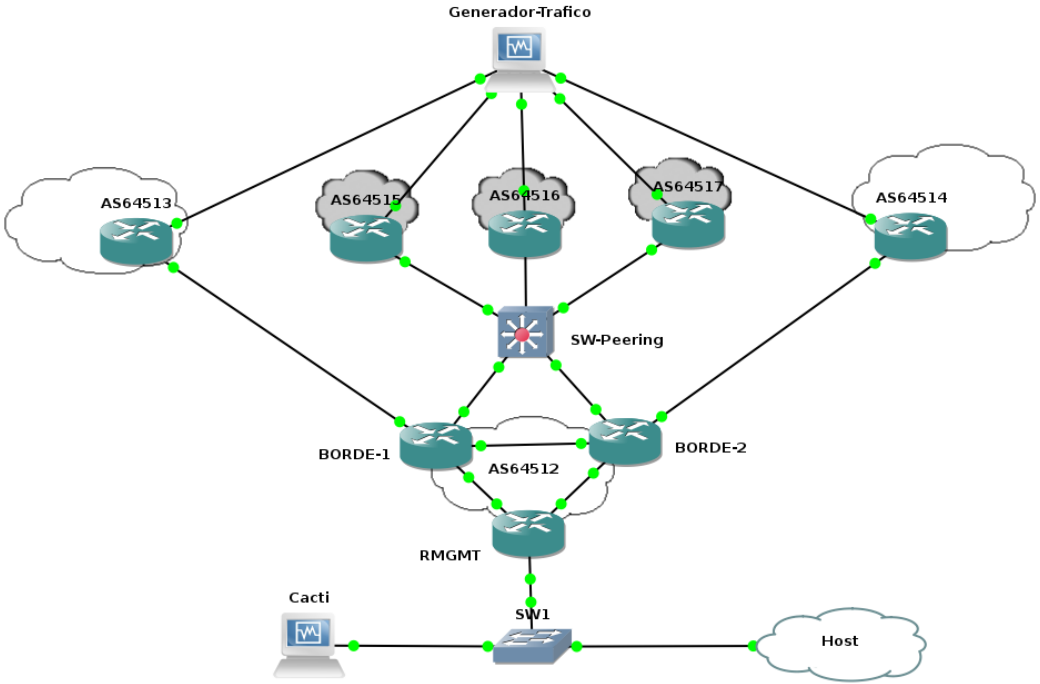
Cacti + PHP-Weathermap

Taller Monitoreo - Lacnog 2015

Monitoreo de enlaces de tránsito y peering

- Qué nos puede interesar monitorear de nuestros enlaces?
  - Utilización del CIR y el Burst (ej. percentil 95)
  - Tráfico por sistema autónomo.
  - Tráfico por zona geográfica por enlace.
  - Consumo de CDNs
  - Clientes BGP.
  - Tráfico por servicio/tecnología de acceso/usuario
  - Tráfico v4/v6, por aplicación, etc.
- Herramientas disponibles.
  - Comerciales (ej. Arbor).
  - Libres (NFCAPD, NFDUMP, NFSEN, CFLOWD, MRTG, CACTI, WEATHERMAPS, etc)
- Quienes requieren esta información?
  - Grupos de O&M, Planificación de red y Capacidad, Aseguramiento de Infraestructura, Gestión de Producto (planificación y costeo), Finanzas, etc, etc.

Maqueta de red y herramientas libres



- GNS3 para simular la red de la figura.
- Routers de borde con conexiones de tránsito (65536/65537) y peering.
- Agentes SNMP y NF v9 en routers.
- Generador de tráfico IPERF en VM Debian.
- Colector de tráfico (IPERF, NFCAPD) + Gestor (CACTI + Weathermap) en VM Debian.
- Conexión al host (via interface tap) para acceso a CACTI y Weathermap.

Cacti (www.cacti.net)

- Herramienta bajo licencia GNU-GPL.
- Brinda un front-end web completo para monitorizar hasta cientos de elementos. Basada en PHP, utiliza MySQL y RRDs para almacenar configuraciones y estadísticas.
- Administración de usuarios con permisos por áreas y funciones.
- Soporte SNMP (poller propio para manejar gran cantidad de dispositivos) y scripts externos para recolectar los datos.
- Genera, organizar y visualizar los gráficos creados.
- Creación de nuevos Templates para dispositivos y gráficos.
- Permite su modificación e integración de nuevas herramientas (add-ons).

Instalación de Cacti

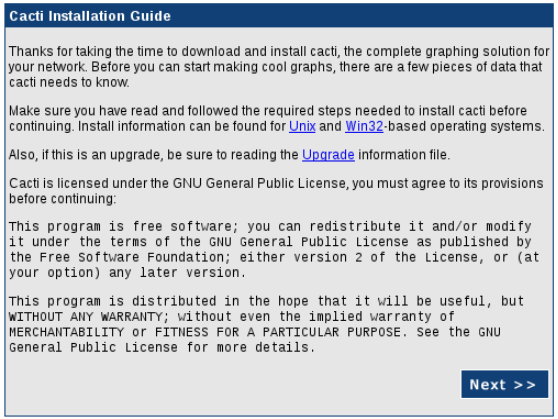
- En distribuciones basadas en Debian

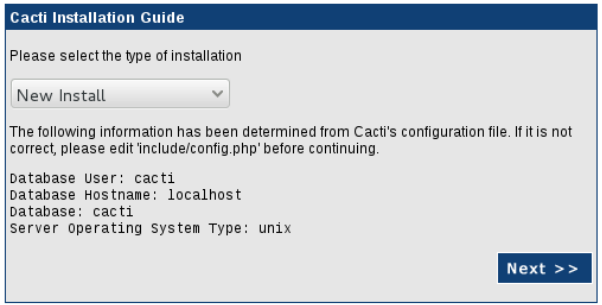
  ```
  apt-get install cacti
  ```

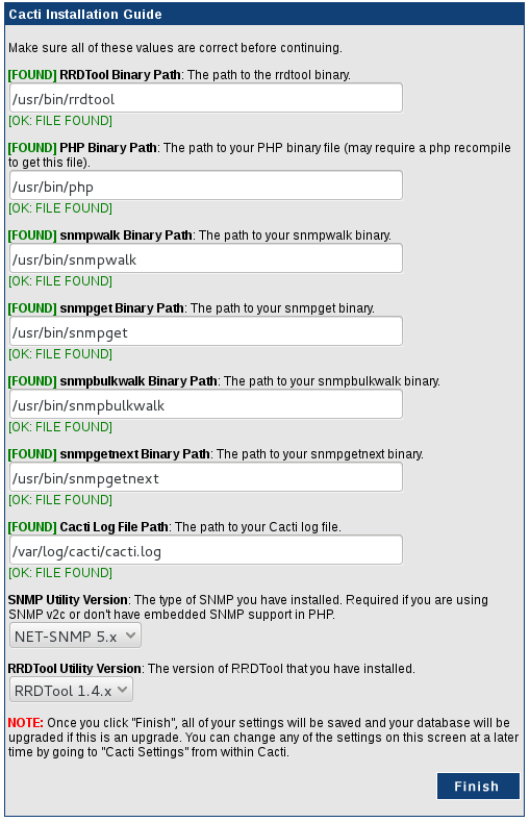
- Esto instalará cacti y sus dependencias (apache, php, mysql, etc.)
- En el proceso de instalación se nos podrá consultar y solicitar:
  - Web Server a utilizar (si tenemos más de uno instalado)
  - Password de administración para mysql (si no lo teníamos previamente instalado).
  - Password de administración de mysql para crear la base de datos que usará Cacti.
  - Password de administración para Cacti en mysql si decidimos configurarlo desde allí (no tiene que ser el mismo password que para toda la base de datos).

Configuración de Cacti

- Luego de instalar Cacti debemos configurarlo.
- Para ello utilizamos el navegador visitando el siguiente URL y finalizamos la instalación: http://IP-ADDRESS/cacti

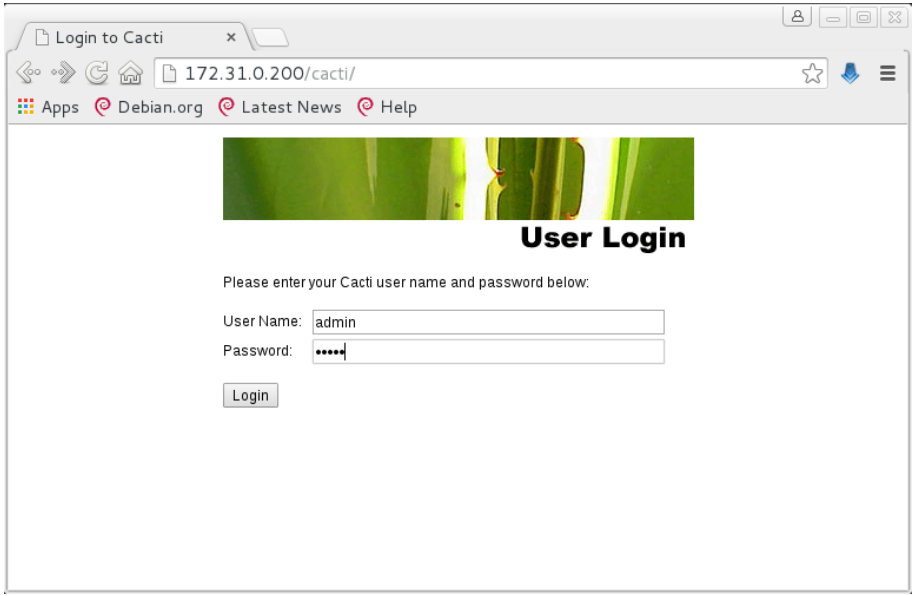


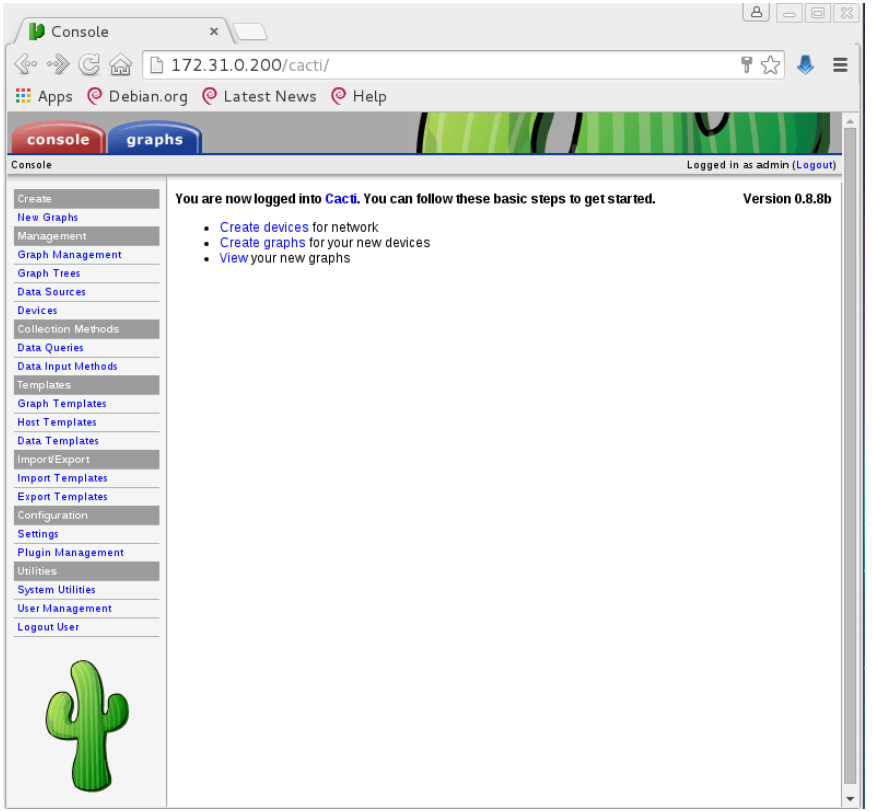




Iniciamos sesión y agregamos los dispositivos

- Usuario por defecto admin/cacti





Network-Weathermap (network-weathermap.com)

- Herramienta open source para visualizar elementos y datos en un mapa.
- Colecta información con plugins: soporte de RRDs, MRTG, archivos de texto, SNMP, fping, datos desde CACTI y scripts externos.
- Los mapas se crean “a mano” a partir de la documentación o utilizando un editor web (con funcionalidades acotadas).
- La integración con Cacti permite además brindar control de acceso a los mapas.

Instalación de Cacti Plugin.

- Requiere la instalación de la “Cacti Plugin-Architecture” (PIA) en versiones anteriores a Cacti 0.8.8.
- Obtengo el zip para la instalación:

```
wget network-weathermap.com/files/php-weathermap-0.97c.zip
```

- Descomprimir el contenido en /usr/share/cacti/site/plugins/. y dar permiso al usuario web para escribir los mapas.

```
chown www-data /usr/share/cacti/site/plugins/weathermap/output
```

- Desde Cacti se instala el plugin visitando Configuration-> Plugin Management y haciendo click en “Actions” (Install).
- Este proceso tiene bastante más pasos en versiones anteriores de Cacti.

Instalación de Cacti Editor.

- No tiene integración con el gestor de usuarios de Cacti (restringir con apache Deny, Allow o usar y luego cambiar permisos).
- Requiere la instalación de la biblioteca GD para manipular imágenes.

  ```
  apt-get install php5-gd && /etc/init.d/apache2 reload
  ```

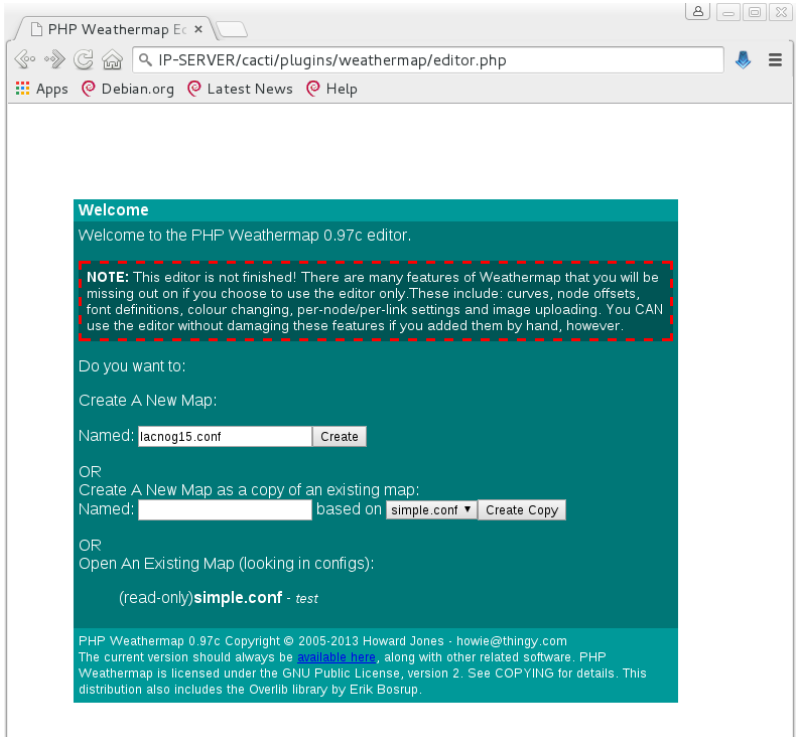
- Modifico los permisos de la carpeta donde se almacenan las configuraciones.

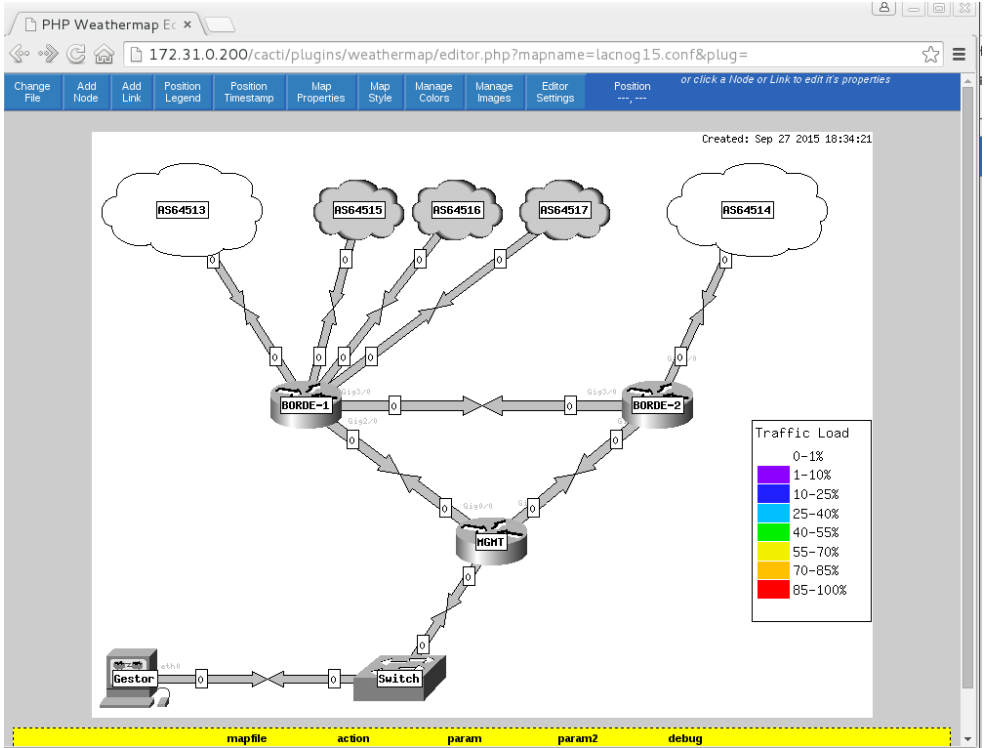
  ```
  chown www-data /usr/share/cacti/site/plugins/weathermap/configs
  ```

  Chequeo en: http://IP-SERVER/cacti/plugins/weathermap/editor.php

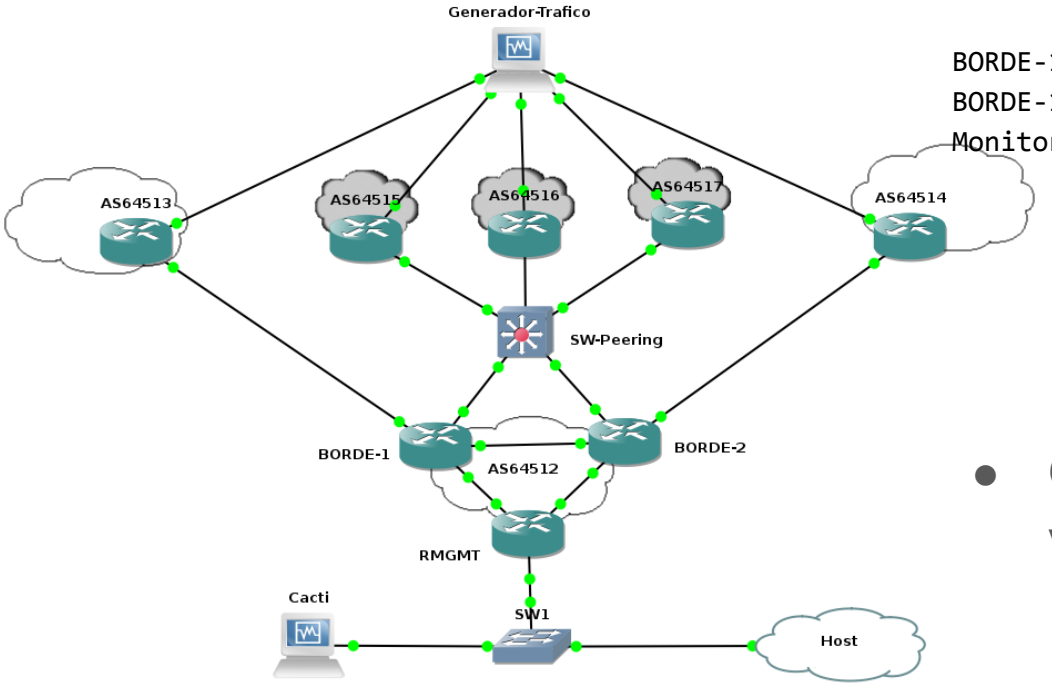
Weathermap Editor

- Elegir un nombre.conf para el mapa, crear y diseñarlo.





Configuración SNMP

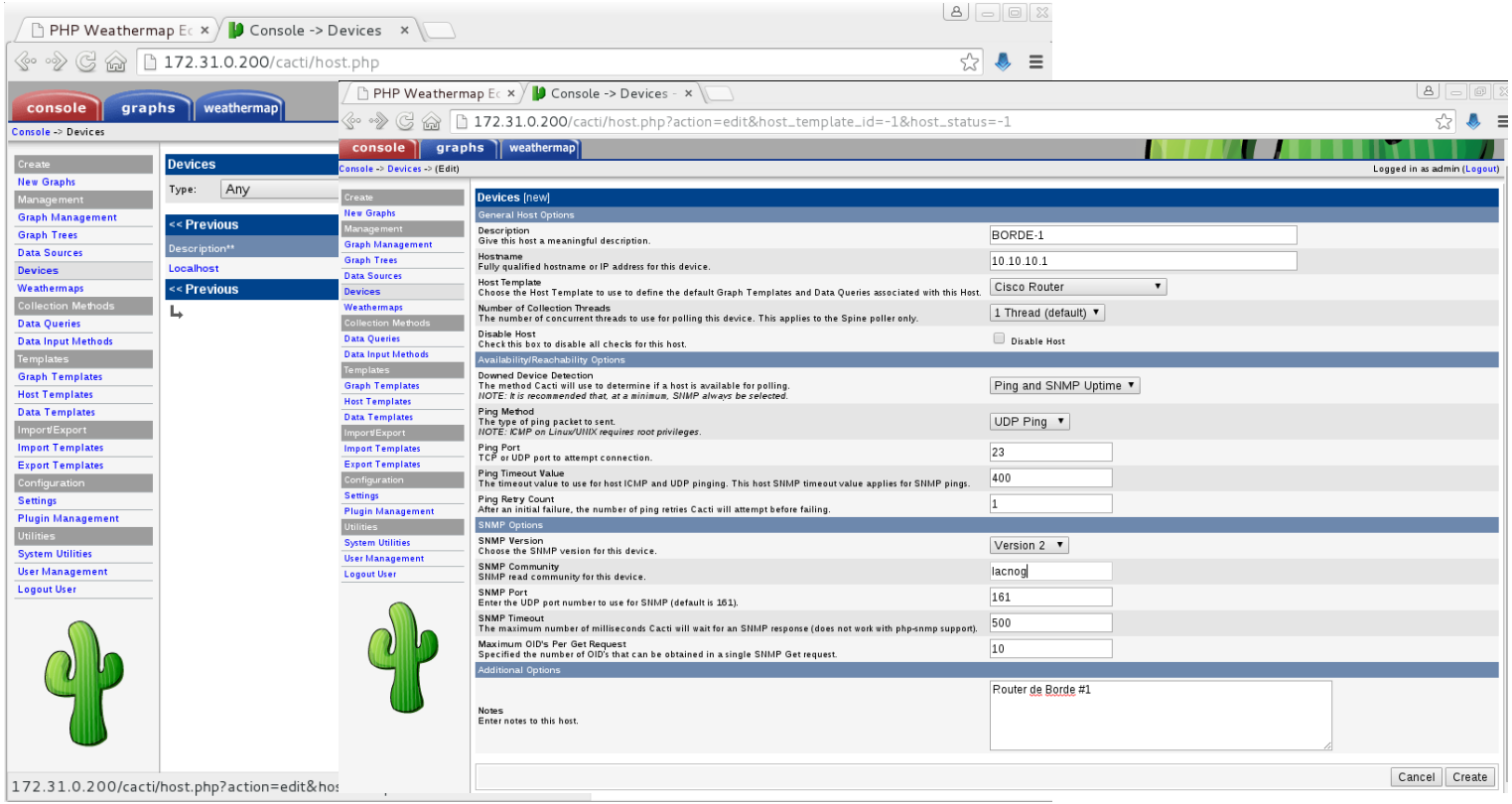


- Configuramos BORDE-1

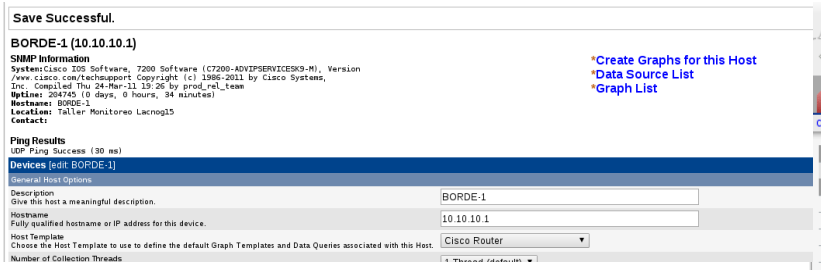
```
BORDE-1(config)#snmp-server community lacnog RO
BORDE-1(config)#snmp-server location "Taller
Monitoreo Lacnog15"
```

- Otras opciones (datos contacto, vistas, trap-managers, etc)

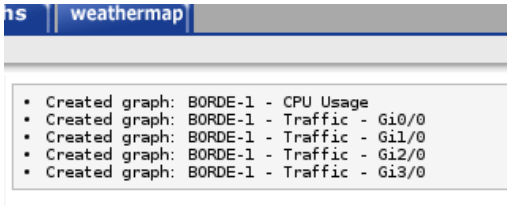
Cacti: Management>Devices>Add

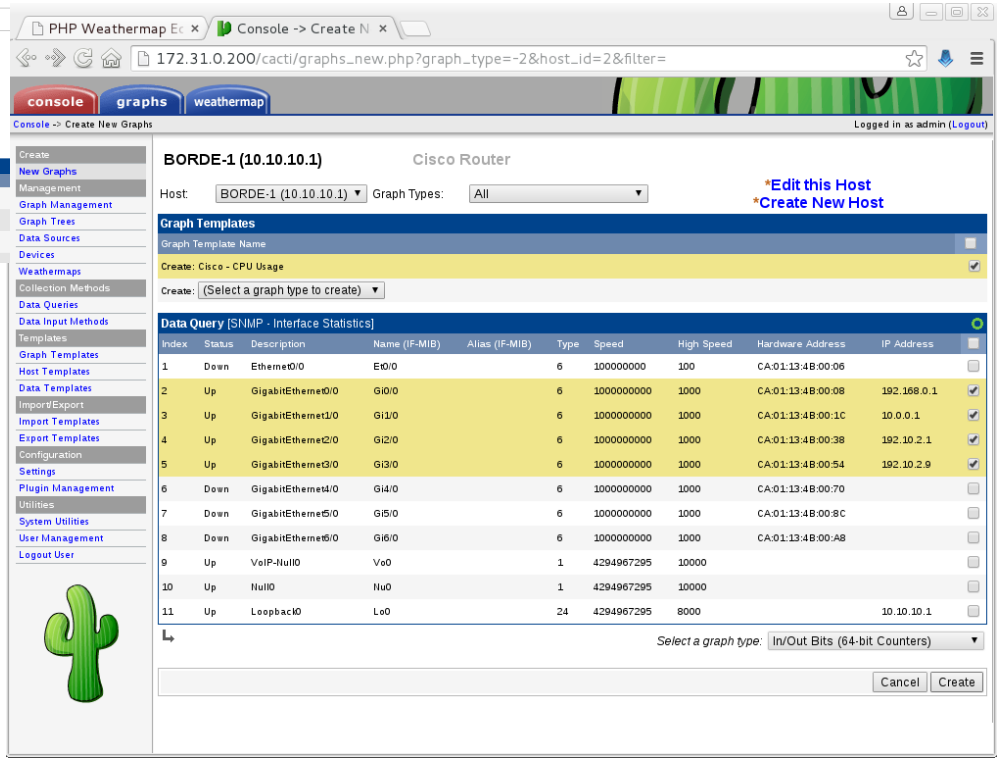


Cacti: generar gráficos (Create Graphs for this Host)



- Seleccionamos los recursos a graficar y creamos los gráficos.





Cacti: visualización de gráficos.

- Debo agregar luego el host al “Default Tree” o crear un grupo nuevo (ej. “Routers”): Management > Graph Trees > Add.
- Luego se agrega el equipo al tree: Add > ”Tree Item Type=Host”, “Host=BORDE-1” > Create.
- En la pestaña “graphs” selecciono “Routers” y visualizo los gráficos.

Iperf para generar tráfico.

- Primero en el Colector (Cacti) ejecuto el iperf como “server” para escuchar en IPv4 y en IPv6 en diferentes puertos UDP.

```
root@Cacti:~/iperf -s -u -p 12345 &
root@Cacti:~/iperf -V -s -u -p 12345 &
root@Cacti:~/iperf -s -u -p 23451 &
root@Cacti:~/iperf -V -s -u -p 23451 &
```

- En el Generador ejecuto el iperf como cliente enviando flujos UDP (controlando el throughput) hacia el server usando v4 y v6 hacia los puertos previamente configurados desde diferentes IPs de origen.

```
root@Cacti:~/iperf -B 198.51.100.254 -c 172.31.0.200 -u -p 12345 -t 3600 -b 2M&
root@Cacti:~/iperf -V -B 2001:db8:2000::fE -c 2001:db8:1000::200 -u -p 12345 -t 3600 -b 1M&
root@Cacti:~/iperf -B 172.16.0.254 -c 172.31.0.200 -u -p 23451 -t 3600 -b 3M&
root@Cacti:~/iperf -V -B 2001:db8:4000::fe -c 2001:db8:1000::200 -u -p 23451 -t 3600 -b 1M&
```

WeatherMap: asociar source a links.

- Luego de haber agregado el dispositivo al Cacti puedo asociar las fuentes de tráfico para visualizarlas en el mapa (ej. Links).
- Volviendo al editor selecciono el link y en “Data Source” selecciono “Pick from Cacti”
- Selecciono la interfaz de interés y se completan los datos, incluyendo el URL y el “Hover” Graph URL que me permitirán visualizar el gráfico de cacti al hacer “click” en el link y cuando me posiciono sobre él.
- Puedo además agregar comentarios para el link y agregar/modificar otras opciones no disponibles en el editor haciendo “Edit” y trabajando directamente sobre el texto del archivo.

WeatherMap: visualización en Cacti.

- Previo a visualizarlo en la pestaña “weathermap” debo agregarlo en Cacti.
- Management>Weathermaps>Add, selecciono el archivo de configuración y lo agrego.
- En el siguiente período de polling lo podré visualizar.

Separando tráfico en peering

- Todo el tráfico proviene de la misma interfaz.
- No tengo una separación lógica (ej. VLANs) para poder monitorizar via SNMP.
- Habilito Netflow para identificar el tráfico de cada AS Peer (o AS origen) en los routers de borde.
- Debo capturar las trazas (nfcapd), procesarlas y almacenar los octetos que provienen de cada AS de interes.
- Luego puedo utilizar CACTI + Weathermaps para su visualización.

Instalación de nfcapd

- En distribuciones basadas en Debian

```
1 apt-get install gcc flex librrd-dev make
2 cd /usr/local/src/
3 wget http://sourceforge.net/projects/nfdump/files/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz
4 gzip -dc nfdump-1.6.13.tar.gz | tar -xf -
5 cd nfdump-1.6.13
6 ./configure --enable-nfprofile
7 make && make install
```

Configuración router BORDE-1

- Configuro netflow en router de borde:

```
BORDE-1(config)#ip flow-export source Loopback0
BORDE-1(config)#ip flow-export version 9 peer-as (origin-as)
BORDE-1(config)#ip flow-export destination 172.31.0.200 16001

BORDE-1(config)#interface GigabitEthernet1/0
BORDE-1(config-if)#ip flow ingress
BORDE-1(config-if)#ip flow egress
```

Configuración del Colector netflow

- Lanzo la captura

```
root@Cacti:~/nfcapd -w -D -l /var/cache/flows/borde-1 -p 16001
```

- Verifico agregando por sistema autónomo de origen:

```
root@Cacti:/var/cache/flows/borde-1# nfdump -A srcas -r ./nfcapd.201509271855

Date first seen          Duration  Src AS   Packets  Bytes     bps  Bpp Flows
2015-09-27 15:58:14.904   144.724     0         22   1070      59   48   16
2015-09-27 15:57:21.964   182.028   64513  15555   23.3 M1.0 M   1498  3
2015-09-27 15:57:21.964   182.028   64515  15558   23.3 M1.0 M   1498  3
```

Configuración CACTI

- Defino un nuevo ***Data Input Method*** que utiliza un script para obtener en dos variables “**in**” y “**out**” los octetos con origen y destino un número de sistema autónomo que se le pasa como entrada.
- Defino un nuevo ***Data Template*** que define la base de datos (RRD) y asocia el *Data Input Method* anterior. En esta RRD se almacenará cada 5 minutos los valores que devuelve el script.
- Defino un nuevo ***Graph Template*** para generar las gráficas a partir de la RRD. Teniendo en cuenta que deben pasarse los datos a bits y promediarse durante el período de medición (nueva CDEF).
- A partir de allí puedo instanciar las ***Data Sources*** y asociarles nuevos gráficos. Estos quedarán disponibles para ser usados en el Weathermap.

Otros posibles usos

- Estadísticas de tráfico IPv6 (en equipos cuyos agentes no soportan el objeto IP-MIB::ipIfStatsInOctets.ipv6).
- Tráfico hacia subredes que alojan CDNs.
- Tráfico desde/hacia distintos países o regiones con información de RIRs (ej. ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-extended-latest)
- Segmentación de tráfico por servicio (usando BD propias de IPs).
- Tráfico por bloques publicados por enlace (balanceo de tráfico entrante).

PREGUNTAS