Manual para generación de reporte

Correspondiente a la herramienta mailcleaner

18/01/2019

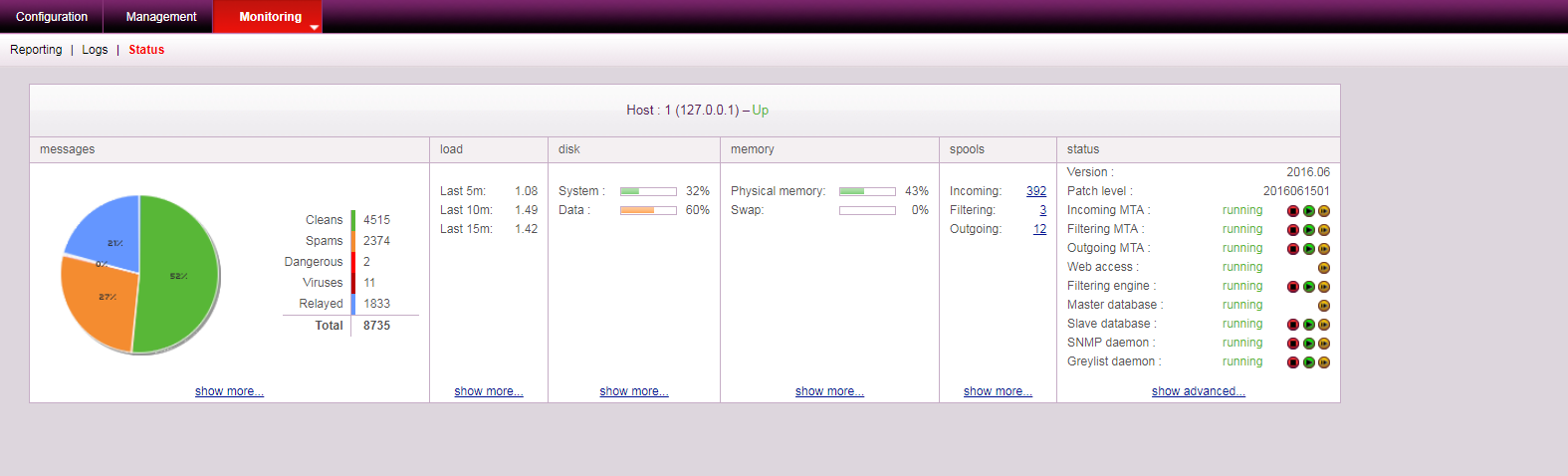
Consalud S.A

Francisco Abarca Moraga

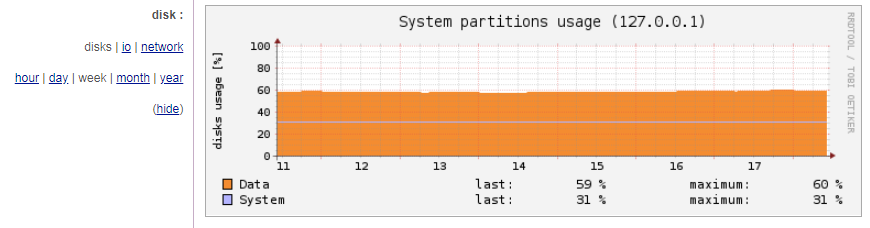
Contenido

# Uso de Recursos

Para obtener las métricas correspondientes a los elementos de hardware nos enfocamos en la pestaña *“Monitoring -> Status”*.

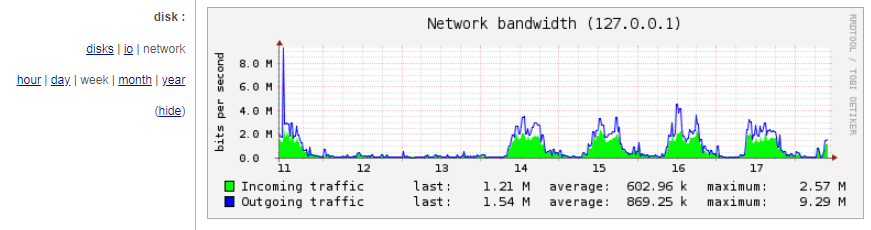


Acá primero veremos la tasa de uso de los discos (pulsando *“show more”* debajo de discos), tanto del sistema como los datos para obtener datos relevantes.



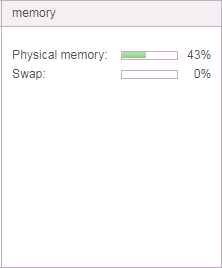
Vemos que ambas particiones no superen el 90% de utilización (viendo el grafico representativo de la semana). Tomamos los valores actuales y los anotamos en nuestro informe.

También echamos un vistazo al comportamiento de redes bajo este menú para verificar que no haya elevaciones en alguno de los tráficos.



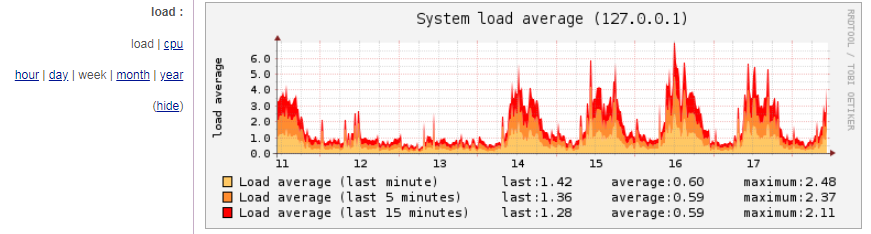
Si notamos un día con elevaciones fuera del promedio lo informamos con el día de la aparición (El día 11 en este ejemplo).

Ahora tomamos nota sobre la memoria, primero vemos los valores de uso general de la memoria física como el swap.



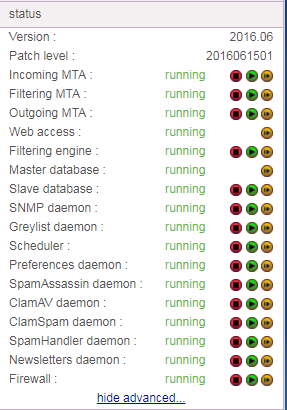
Tomamos los valores de uso y los anotamos en el informe, se recomienda notificar en caso de un uso excesivo de la memoria principal (> 90%) o uso excesivo del swap (> 25%).

Dentro de nuestras métricas aún nos falta la carga de procesamiento del sistema, para esto vamos a la pestaña de carga (“load”), y pulsamos en mostrar más debajo de ella, esto nos habilitará un gráfico, en donde podemos obtener nuestros valores.



Vemos los valores promedios de las cargas y los máximos de nuestro interés, viendo que no se supere los valores delimitados en el reporte.

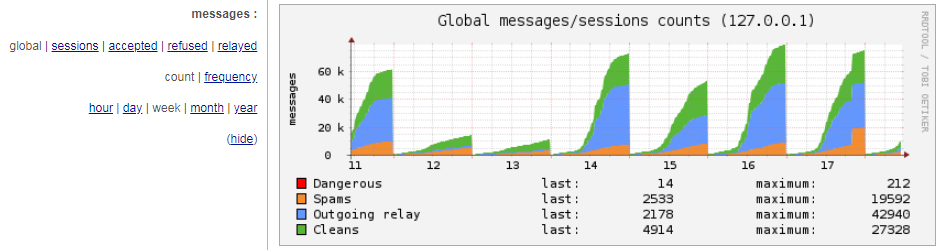
Con el hardware ya listo nos enfocaremos ahora en los servicios y su funcionamiento. Para aquello iremos a la sección de estados (“status”) donde pulsaremos en mostrar avanzados (“show advanced”) para ver todos los servicios y sus estados.



Con esta información rellenamos los estados de los servicios.

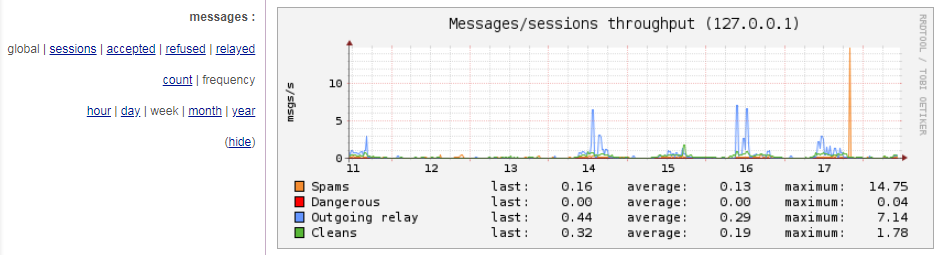
Ahora iremos a mensajes y pulsaremos en mostrar más para obtener la gráfica de los mensajes, más exactamente su cantidad y frecuencia durante la semana.

Primero tomaremos el gráfico global de la semana.



De acá nos importan los valores de las amenazas (“*Dangerous*”) y los spams, más que nada su valor de máximo semanal y lo comparamos al reporte anterior informando el delta entre las semanas.

Ahora tomamos el global de frecuencias de la semana.



Y notamos irregularidades, en caso de haberlas en el envío de spam, esto se ve al tener elevaciones de color naranjo en el gráfico en un cierto día (el día 17 en nuestro caso) y lo informamos en caso de ser positivo, para una investigación forense posterior.

Ahora miramos el gráfico de conexiones rechazadas, miramos