

1 Telediagnos

La telediagnos permite tener conocimiento del estado de SECEBIT en tiempo real, en el momento en el que algún problema es detectado, se informa e incluso se pueden llegar a tomar acciones correctoras. El sistema de telediagnos se ha construido usando **Nagios**¹, un sistema de monitorización de sistemas, ampliamente extendido y que cuenta con un sólido desarrollo.

La mayor tarea en la implantación de un sistema Nagios para monitorización, es la configuración del mismo, a grandes rasgos:

- Identificar las máquinas que deben ser monitorizadas.
- Agrupar estas máquinas por tipos a fin de facilitar las tareas de configuración y explotación.
- Para cada tipo es necesario identificar los servicios y recursos que deben ser controlados, por regla general los servicios de red pueden ser monitorizados en remoto desde el sistema que corre Nagios, mientras que otros requieren de NRPE para ser corridos remotamente en la máquina que se desea monitorizar.
- Fijar quienes van a recibir las alarmas generadas, a través de que canales y bajo que condiciones.
- Definir acciones preventivas automáticas, siempre que sean posibles y necesarias.

Es el objetivo de este documento definir como se han configurado los tres primeros apartados, entendiendo siempre que Metro cuenta ya con Nagios y que por lo tanto los dos últimos apartados se encuentran ya definidos y operativos.

1.1 Máquinas y grupos

Se han definido dos nuevos grupos:

- SECEBIT
- TELESECEBIT

El primero formado por las máquinas que portan los HSM's y que por lo tanto soportan el servicio SECEBIT, actualmente pertenecen a este grupo, 4 máquinas:

- Secebit1

¹ Para más información de nagios acudir a <http://www.nagios.org>

- Secebit2
- Secebit3
- Secebit4

El segundo grupo lo forma una única máquina, en la que se encuentra corriendo el Nagios y desde la cual se llevan a cabo las tareas de telecarga, telegestión y telediagnosís:

- Telesecebit

En esta máquina se encuentra la configuración que a continuación se describe, configuración que deberá ser traspasada al sistema Nagios existente en Metro.

1.2 Recursos y servicios monitorizados para Secebit-n

El siguiente paso en la configuración es definir los servicios y recursos de los sistemas identificados, que requieren de un control por parte de Nagios, se pueden establecer dos grandes grupos:

- Servicios ofrecidos por los SECEBIT que son accesibles vía red y por lo tanto pueden ser monitorizados directamente por Nagios
- Servicios y recursos internos a los propios SECEBIT, en este caso se usa NRPE como medio para poder ejecutar y controlar los scripts que Nagios lanza en remotamente contra los SECEBIT

Para cada servicio o recurso monitorizado se ofrece una descripción de que se está comprobando, si usa o no NRPE, el nombre del script que ejecuta en la máquina monitorizar y las acciones necesarias para solucionar el problema.

Las acciones descritas para intentar paliar las alarmas generadas, deben llevarse a cabo con los privilegios adecuados, para ellos los usuarios autorizados pueden usar comandos que requieran privilegio de root, con el comando sudo.

En cada monitorización se da la ruta del script encargado, si la monitorización usa el NRPE, la ruta pertenece a la máquina que se monitoriza, si por el contrario no usa NRPE, la ruta corresponde a la máquina donde corre Nagios.

1.2.1 Carga actual de la CPU

- Descripción. Mide la carga soportada por la CPU, comprobando la media para el último minuto, los últimos 5 y 15 minutos. Actualmente está configurado para lanzar un warning si se supera una carga de 15, 10 y 5, para 1, 5 y 15 minutos respectivamente y un critical si se supera una media de carga de 20, 25 y 20 durante 1, 5 y 15 minutos.
- Usa NRPE. SI
- Script. `/usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20`
- Acción. Comprobar con un 'top' la carga del sistema y el proceso o procesos que la están ocasionando. En el sistema SECEBIT el cuello de botella es el HSM por lo que las situaciones de carga elevadas no deberían llegar a producirse, en caso de producirse, la causa más probable es un proceso fuera de control.

1.2.2 Usuarios en el sistema

- Descripción. Cuenta el número de usuarios que se encuentran actualmente en el sistema, si se encuentran más de 2 usuarios se da un warning y si se encuentran más de 5 un critical.
- Usa NRPE. SI
- Script. `/usr/local/nagios/libexec/check_users -w 3 -c 6`
- Acción. En el caso de SECEBIT, con el número de usuarios con acceso al sistema y la configuración de esta monitorización, se trata más bien de un simple control de seguridad, que de una amenaza al rendimiento del sistema. En caso de producirse un critical, se deberá acceder al sistema y comprobar que usuarios se encuentran en él, comprobando las tareas que cada uno de ellos están llevando a cabo. Es una alarma que raramente debiera de producirse, salvo en tareas de mantenimiento o similares.

1.2.3 Disponibilidad del servicio HTTP (TOMCAT puerto 8080)

- Descripción. Comprueba que un servidor web se encuentra respondiendo con un 200 en el puerto 8080, Tomcat.
- Usa NRPE. NO
- Script. `/usr/local/nagios/libexec/check_http -p 8080`
- Acción. Si se produce una alarma, se debe comprobar que el servidor de aplicaciones Tomcat se encuentre funcionando y respondiendo. Se debe acceder a la máquina y comprobar los siguientes logs:
 - `/opt/HSMServerConfig/log`
 - `/opt/tomcat/log`

Buscando algún error de aplicación o del propio Tomcat que pueda explicar la alarma, en caso de tener que reiniciar el servidor de aplicaciones, usar:

- `/etc/init.d/tomcat restart`

1.2.4 Respuesta al PING de la máquina

- Descripción. Comprueba si la máquina responde al ping, lanzando un warning si el tiempo de respuesta excede 100 ms y el % de paquetes perdidos excede el 20 % o un critical si el tiempo de respuesta pasa de 500 ms y el número de paquetes perdidos de un 60 %.
- Usa NRPE. NO
- Script. `/usr/local/nagios/libexec/check_ping -w 100.0,20% -c 500.0,60%`
- Acción. Caso de producirse esta alarma, se debe comprobar si el problema radica en la red o en la propia máquina. Para ello podría bastar con comprobar si el resto de sistemas, están teniendo el mismo problema. Caso de que el problema se localice en la máquina, se deberá acceder y comprobar la carga del sistema y el estado de los interfaces de red, así como comprobar con un netstat el número de conexiones activas, ya sean establecidas o en proceso de ser cerradas.

1.2.5 Disponibilidad del servicio SSH

- Descripción. Comprueba que el servidor SSH se encuentra aceptando conexiones.
- Usa NRPE. NO
- Script. `/usr/local/nagios/libexec/check_ssh -p 1069`
- Acción. Esta alarma puede indicar que la conexión remota con la máquina no es posible, en caso de producirse de forma aislada, es decir sin ir asociada a una caída de red, se debería intentar acceder remotamente, no quedando más remedio que proceder con una intervención en local si la conexión no es posible. La intervención local debería tratar de determinar el estado del servidor SSH, no descartando la posibilidad de algún fallo de configuración de algún elemento de red intermedio, ya sea un router, firewall, etc.

1.2.6 Uso de memoria virtual

- Descripción. Comprueba la cantidad de memoria virtual, swap, que está usando la máquina, lanzando un warning si la cantidad de memoria virtual libre alcanza el 50 % y un critical si alcanza el 75 %.
- Usa NRPE. SI
- Script. `/usr/local/nagios/libexec/check_swap -w 50% -c 25%`
- Acción. Debido a que la aplicación encargada del servicio SECEBIT se encuentra alojada en Tomcat y que este corre en una máquina virtual Java, la probabilidad de que esta alarma ocurra es baja, ya que la máquina virtual está configurada para emplear un máximo de memoria que garantice la prestación del servicio en condiciones de carga elevadas, alrededor de 1000 operaciones/segundo, pero sin llegar si quiera a la mitad de RAM disponible. En caso de producirse este error, habría que intentar determinar mediante un 'top' que la alarma es real e identificar que procesos son los responsables del consumo de memoria.

1.2.7 Número de procesos en la máquina

- Descripción. Comprueba si el número de procesos, de cualquier tipo, que se están ejecutando en la máquina excede el configurado. Si se encuentran más de 120 procesos se produce un warning y se se sobrepasan los 150 un critical.
- Usa NRPE. SI
- Script. `/usr/local/nagios/libexec/check_procs -w 120 -c 150`
- Acción. El número de procesos que se encuentran corriendo en la máquina en un momento dado, debe ser bastante constante, la alarma se encuentra configurada con valores deliberadamente bajos a fin no tanto de alertar sobre un número de procesos que puedan poner en peligro la prestación del servicio, sino también a detectar posibles procesos 'extraños' o innecesarios. Caso de producirse esta alerta se debe comprobar el número de procesos e intentar determinar que procesos 'sobran' con un 'ps'.

1.2.8 Numero de procesos zombies en la máquina

- Descripción. Comprueba si el número de procesos zombie que se están ejecutando en la máquina excede el configurado. Si se encuentran más de 5 procesos zombies se produce un warning y se se sobrepasan los 10 un critical.
- Usa NRPE. SI
- Script. `/usr/local/nagios/libexec/check_procs -w 5 -c 10 -s Z`
- Acción. La existencia de procesos Zombie suele indicar un BUG en alguna aplicación, el proceso padre no recupera el resultado de la ejecución de alguno de sus hijos, cuando estos ya han terminado y por lo tanto sigue existiendo una entrada en la tabla de procesos aunque el proceso en si ha terminado la ejecución. Se debe buscar los procesos de este tipo con un 'ps' e identificar la aplicación que los produce, con el fin de solventar el problema.

1.2.9 Comprobación del estado del HSM y su carga

- Descripción. De entre los posibles estados del HSM, solo uno es valido para operar con él, el resto son estados de error interno o que denotan un tamper. Si el HSM no se encuentra en el estado de operación normal, se produce un critical. Por otro lado esta comprobación obtiene y comprueba la carga de trabajo del HSM, si este se encuentra por encima del 95 % se produce un warning. Por Carga no se produce un critical.
- Usa NRPE. SI
- Script. `/usr/local/nagios/libexec/check_hsmstate`
- Acción. Es importante distinguir entre un fallo producido por el estado del HSM, de uno producido por carga del mismo.
 - Estado incorrecto. Se debe acceder a la máquina y comprobar mediante el comando `/opt/PTK/hsmstate`, el estado actual del HSM, si no es - HSM in NORMAL MODE. RESPONDING -, el servicio se encuentra inoperante. Se debe forzar un reset del HSM para intentar devolverlo a su modo de funcionamiento normal, para ello usar el comando `/opt/PTK/hsmreset` y comprobar tras su ejecución el estado del HSM, si no es el correcto, contactar con Seglan.
 - Carga elevada. Un warning indicando carga elevada no es en si mismo un problema, el único problema derivado es el posible rechazo de operaciones por vencimiento de timeout. Un problema puntual de este tipo, no debe ser preocupante, pasaría a serlo si

el problema se reproduce asiduamente, ya que indicaría o un mal dimensionamiento, un problema de dimensionamiento del servicio o un que alguno de los otros SECEBIT, se encuentran fuera de servicio. La carga del HSM puede verse con el comando `/opt/PTK/hsmstate`.

1.2.10 Comprobación de las claves en el HSM y su adecuación al perfil configurado

- Descripción. El HSM es particularizado por el CRTM, quien introduce un conjunto de claves, dependiendo del ROL al que va a ser destinado el nodo SECEBIT, en el mismo proceso se guarda el ROL y las claves que lo componen. La validación que nos ocupa se encarga de comprobar que para el ROL configurado existen las claves necesarias. Se produce un critical si alguna de las claves necesarias para el ROL no existe en el HSM, en cualquier otro caso se produce un warning, producido generalmente por un fallo en la configuración de la validación.
- Usa NRPE. SI
- Script. `/usr/local/nagios/libexec/check_keys`
- Acción. Ante un warning, debe comprobarse la indicación dada por la validación, que indicará la causa, por enumerar alguna:
 - La máscara que codifica el ROL no es la misma que la guardada en el HSM.
 - No se encuentra el fichero de configuración pasado en el script que realiza la validación
 - Imposibilidad de establecer sesión con el TOKEN del HSM.
 - etc

1.2.11 Comprobación de los contadores de la aplicación SECEBIT

- Descripción. Durante el proceso de particularización del HSM por parte del CRTM, además de las claves, se insertan una serie de contadores necesarios para las operaciones requeridas por el ROL asignado al HSM. Cada contador es inicializado a un valor y además se le configura cual es su limite inferior (carece de utilidad ya que el contador solo se incrementa), limite superior y limite de alarma, es decir el valor a partir del cual se produce un aviso de contador próximo a fin. El critical en este caso está reservado para contadores que han superado su límite superior o bien para los que se ha encontrado limites configurados. El warning como en el caso anterior indica fallos de configuración y contadores con el límite de alarma superado. En cualquier caso el motivo del problema es mostrado tan para un critical como para un warning.
- Usa NRPE. SI
- Script. `/usr/local/nagios/libexec/check_cont`
- Acción. Ante un contador con límite superado, solo cabe avisar al CRTM informando de tal situación, ya que es un estado de error controlado de la aplicación, bajo el cual ciertas operaciones permanecen fuera de servicio. Ante un warning que no sea un límite de alarma superado, cabe 'tirar del hilo' para solventar el problema. Si se trata de un límite de alarma superado, como en el primer caso, el procedimiento a seguir es avisar al CRTM.

1.2.12 Comprobación del estado del proceso que gestiona las inserciones de las operaciones en BBDD

- Descripción. Las operaciones recibidas por nodo SECEBIT no son guardadas directamente por la aplicación, son llevadas a ficheros, para luego ser insertadas, este esquema posibilita seguir operando con la BBDD fuera de servicio. El proceso que se encarga de realizar las inserciones de las operaciones leyéndolas de los ficheros generados por la aplicación, es el objeto de esta monitorización, dicho proceso es arrancado a intervalos de 1 minuto por el cron. La validación consiste en comprobar si existen transacciones sin guardar con una antigüedad superior a 1 hora, en cuyo caso se produce un critical.
- Usa NRPE. SI
- Script. /usr/local/nagios/libexec/check_insertd
- Acción.

1.2.13 Comprobación del estado de la aplicación BIT

1.2.14 Comprobación del nivel de uso de la partición home

- Descripción. Realiza una comprobación del espacio de disco en la partición /home, dando un warning si menos del 20% de espacio queda libre o un critical si esta cantidad es menor a un 10%.
- Usa NRPE. SI
- Script. /usr/local/nagios/libexec/check_disk
- Acción. La partición home no debe tener uso en un nodo SECEBIT, ya que los usuarios en el sistema son unos pocos y solo realizan tareas de administración en la máquina. En cualquier caso un 'du' del directorio /home, debe proporcionar información sobre donde está el consumo de disco. Esta partición no representa un problema para el servicio ofrecido por SECEBIT.

1.2.15 Comprobación del nivel de uso de la partición opt

- Descripción. Realiza una comprobación del espacio de disco en la partición /opt, dando un warning si menos del 20% de espacio queda libre o un critical si esta cantidad es menor a un 10%.
- Usa NRPE. SI
- Script. /usr/local/nagios/libexec/check_disk
- Acción. En la partición /opt, se encuentra alojada la aplicación SECEBIT, solo existen dos motivos por los que el espacio en esta partición se puede agotar:
 - Los logs generados por la aplicación
 - Las transacciones guardadas en disco temporalmente hasta su inserción en BBDD.

La falta de espacio en esta partición si representa un problema para la continuidad del servicio SECEBIT, debiéndose determinarse el lugar o lugares donde se está consumiendo el espacio en disco, procediendo con el procedimiento de almacenamiento o borrado de logs antiguos o viendo porque las operaciones no se están guardando en BBDD.

1.2.16 Comprobación del nivel de uso de la partición raíz

- Descripción. Realiza una comprobación del espacio de disco en la partición /, dando un warning si menos del 20% de espacio queda libre o un critical si esta cantidad es menor a un 10%.
- Usa NRPE. SI
- Script. /usr/local/nagios/libexec/check_disk
- Acción. El espacio de disco sin usar en la partición raíz si puede representar un problema para la continuidad del servicio SECEBIT, si bien la aplicación SECEBIT no usa espacio de esta partición. Se debe proceder con un 'du', a identificar los puntos de consumo de disco más altos a fin de solventar el problema.

1.2.17 Comprobación del nivel de uso de la partición var

- Descripción. Realiza una comprobación del espacio de disco en la partición /var, dando un warning si menos del 20% de espacio queda libre o un critical si esta cantidad es menor a un 10%.
- Usa NRPE. SI
- Script. /usr/local/nagios/libexec/check_instd
- Acción. Dicha partición contiene entre otras cosas los logs de los procesos de sistema, /var/log, por lo que estos se convierten en los principales sospechosos si existe un problema de espacio en dicha partición. La aplicación SECEBIT no usa espacio de esta partición.

1.3 Recursos y servicios monitorizados para Telesecebit

Todo lo expuesto para los recursos y servicios monitorizados para los nodos Secebit, son de aplicación para la máquina de Telesecebit. En los puntos coincidentes se dará la referencia del apartado en cuestión del punto 1.2.

1.3.1 Carga actual de la CPU.

Ver apartado 1.2.1

1.3.2 Usuarios en el sistema.

Ver apartado 1.2.2

1.3.3 Disponibilidad del servicio HTTP (TOMCAT puerto 8080)

Ver apartado 1.2.3.

1.3.4 Disponibilidad del servicio HTTP (Apache puerto 80)

- Descripción. Comprueba que un servidor web se encuentra respondiendo con un 200 en el puerto 80, Apache.
- Usa NRPE. NO
- Script. /usr/local/nagios/libexec/check_http -p 80

- **Acción.** Si se produce una alarma, se debe comprobar que el servidor web Apache Tomcat se encuentre funcionando y respondiendo. Se debe acceder a la máquina y comprobar los siguientes logs:
 - /var/logs/apache2

Buscando algún error de aplicación o del propio Tomcat que pueda explicar la alarma, en caso de tener que reiniciar el servidor de aplicaciones, usar:

- /etc/init.d/apahce restart

1.3.5 Respuesta al PING de la máquina

Ver apartado 1.2.4.

1.3.6 Disponibilidad del servicio SSH

Ver apartado 1.2.5.

1.3.7 Uso de memoria virtual

Ver apartado 1.2.6.

1.3.8 Número de procesos en la máquina

Ver apartado 1.2.7.

1.3.9 Numero de procesos zombies en la máquina

Ver apartado 1.2.8.

1.3.10 Comprobación del resultado del tratamiento de la última lista negra

1.3.11 Comprobación del nivel de uso de la partición raíz

- **Descripción.** Realiza una comprobación del espacio de disco en la partición /, dando un warning si menos del 20% de espacio queda libre o un critical si esta cantidad es menor a un 10%.
- Usa NRPE. SI
- Script. /usr/local/nagios/libexec/check_disk
- **Acción.** Dado que esta máquina solo cuenta con una partición, el espacio de disco si representa un problema para las aplicaciones de telecarga y telegestión. Debe procederse con un 'du' a determinar el lugar donde se produce el mayor consumo de disco, empezando por los directorios:
 - /var/log. Directorio de logs de las aplicaciones del sistema.
 - Directorio de las listas negras
 - Directorio con los logs de la aplicación de telecarga y telegestión