

Plataformas de datos de InterSystems y su rendimiento - Parte 5: Supervisión con SNMP

Artículo

[Mario Sanchez Macias](#) · Nov 5, 2019



Lectura de 11 min

Plataformas de datos de InterSystems y su rendimiento - Parte 5: Supervisión con SNMP

¡Hola Comunidad!

En publicaciones anteriores, mi compañero Murray mostró cómo se pueden recopilar métricas históricas de rendimiento utilizando los pButtons. Hablamos primero de los pButtons porque se instalan con cada instancia de las plataformas de datos (Ensemble, Caché, ...). Sin embargo, existen otras formas para recopilar, procesar y desplegar las métricas de rendimiento de Caché, en tiempo real, ya sea con la finalidad de realizar una supervisión sencilla o, lo más importante, para llevar a cabo operaciones analíticas mucho más sofisticadas y obtener la capacidad de planificación. Uno de los métodos utilizados más comunes para recopilar datos es el SNMP (Protocolo simple de administración de la red).

El SNMP es una forma estándar para que Caché proporcione información acerca de la administración y la supervisión en una amplia variedad de herramientas de administración. En la documentación en línea de Caché se incluyen detalles de la interfaz entre Caché y SNMP. Mientras que SNMP debería 'funcionar únicamente' con Caché, existen algunos trucos y trampas en su configuración. Es común encontrarse con algunos problemas para configurar SNMP si es la primera vez que se hace por lo que esta publicación te puede ayudar para evitar caer en dichos errores.

En este artículo repasaré la instalación y la configuración de SNMP para Caché en Red Hat Linux pero deberías ser capaz de utilizar los mismos pasos para instalar otras variedades de *nix. Estoy escribiendo esta publicación utilizando Red Hat ya que Linux puede ser un poco más complicado de configurar. En Windows Caché se instala automáticamente una DLL para conectarse con el servicio estándar SNMP de Windows, por lo que debería ser más fácil configurarlo.

Una vez que SNMP se configure del lado del servidor, se puede comenzar con la monitorización utilizando un gran número de herramientas. Mostraré el resultado de la monitorización utilizando la popular herramienta PRTG, pero existen muchas otras -[Aquí encontrará una lista parcial.](https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems)

Hay que tener en cuenta que los archivos Caché y Ensemble MIB se incluyen en la carpeta Caché_installation_directory/SNMP. Los archivos son: ISC-CACHE.mib e ISC-ENSEMBLE.mib

Aquí encontrarás artículos previos de esta serie >>

- [Part 1 - Getting started on the Journey, collecting metrics.](#)
- [Part 2 - Looking at the metrics we collected.](#)
- [Part 3 - Focus on CPU.](#)
- [Part 4 - Looking at memory.](#)

Empieza aquí...

Comienza revisando la supervisión de Caché mediante SNMP en la [documentación en línea de Caché.](#)

1. Configuración de Caché

Sigue los pasos descritos en la sección "Administración de SNMP en Caché", que se encuentra en la [documentación en línea de Caché](#) para habilitar el servicio de supervisión de Caché y configurar el subagente SNMP para que inicie automáticamente con el arranque de Caché.

Verifica que el proceso de Caché está ejecutándose, por ejemplo eche un vistazo en la lista de procesos o en el sistema operativo.

```
ps -ef | grep SNMP
```

```
root 1171 1097 0 02:26 pts/1 00:00:00 grep SNMP
```

```
root 27833 1 0 00:34 pts/0 00:00:05 cache -s/db/trak/hs2015/mgr -cj -p33 JOB^SNMP
```

Eso es todo, ¡la configuración de Caché está lista!

2. Configuración del sistema operativo

Aún hay algo más que hacer aquí. Primero verifica que snmpd daemon está instalado y en funcionamiento. Si no es así, instala e inicia snmpd.

Verifica el estado de snmpd con:

```
service snmpd status
```

Inicia o para snmpd con:

```
service snmpd start|stop
```

Si snmp no está instalado, tendrás que instalarlo como se indica en las instrucciones del sistema operativo, por ejemplo:

```
yum -y install net-snmp net-snmp-utils
```

3. Configurar snmpd

Como se detalla en la documentación de Caché, en los sistemas Linux la tarea más importante es verificar que el agente maestro SNMP del sistema sea compatible con el protocolo Agent Extensibility (AgentX), que Caché ejecuta como subagente, y el maestro esté activo y recibiendo las conexiones en el AgentX TCP estándar (puerto 705).

Aquí es donde nos podemos encontrar con algunos problemas. Por ejemplo, puedes tener algunos errores básicos con el archivo "snmp.conf" lo cual implica que el subagente SNMP de Caché no se comunica con el agente maestro del sistema operativo. En el siguiente ejemplo de un archivo "/etc/snmp/snmp.conf" se configuró para iniciar agentX y proporcionar el acceso a Caché y a las Bases de información gestionada (MIB) SNMP de Ensemble.

Ten en cuenta que deberá confirmar si la siguiente configuración cumple con las políticas de seguridad de su organización.

Como mínimo, las siguientes líneas deben editarse para reflejar la configuración de su sistema.

Por ejemplo, cambiar:

```
syslocation "System_Location"
```

a

```
syslocation "Primary Server Room"
```

Edite también las dos líneas siguientes:

```
syscontact "Your Name"
```

```
trapsink Caché_database_server_name_or_ip_address public
```

Edita o reemplaza el archivo que existe en /etc/snmp/snmp.conf para que coincida con lo siguiente:

```
#####  
#  
# snmpd.conf:  
# An example configuration file for configuring the NET-SNMP agent with Cache.  
#  
# This has been used successfully on Red Hat Enterprise Linux and running  
# the snmpd daemon in the foreground with the following command:  
#  
# /usr/sbin/snmpd -f -L -x TCP:localhost:705 -c./snmpd.conf  
#  
# You may want/need to change some of the information, especially the  
# IP address of the trap receiver of you expect to get traps. I've also seen  
# one case (on AIX) where we had to use the "-C" option on the snmpd command  
# line, to make sure we were getting the correct snmpd.conf file.  
#  
#####  
#####  
# SECTION: System Information Setup  
#  
# This section defines some of the information reported in  
# the "system" mib group in the mibII tree.  
# syslocation: The [typically physical] location of the system.  
# Note that setting this value here means that when trying to  
# perform an snmp SET operation to the sysLocation.0 variable will make  
# the agent return the "notWritable" error code. IE, including  
# this token in the snmpd.conf file will disable write access to  
# the variable.  
# arguments: location_string  
syslocation "System Location"  
# syscontact: The contact information for the administrator  
# Note that setting this value here means that when trying to  
# perform an snmp SET operation to the sysContact.0 variable will make  
# the agent return the "notWritable" error code. IE, including  
# this token in the snmpd.conf file will disable write access to  
# the variable.  
# arguments: contact_string  
syscontact "Your Name"  
# sysservices: The proper value for the sysServices object.  
# arguments: sysservices_number  
sysservices 76  
#####  
# SECTION: Agent Operating Mode  
#  
# This section defines how the agent will operate when it  
# is running.  
# master: Should the agent operate as a master agent or not.  
# Currently, the only supported master agent type for this token  
# is "agentx".  
#  
# arguments: (on|yes|agentx|all|off|no)  
master agentx
```

```
agentXSocket tcp:localhost:705
#####
# SECTION: Trap Destinations
#
# Here we define who the agent will send traps to.
# trapsink: A SNMPv1 trap receiver
# arguments: host [community] [portnum]
trapsink Caché_database_server_name_or_ip_address public
#####
# Access Control
#####
# As shipped, the snmpd demon will only respond to queries on the
# system mib group until this file is replaced or modified for
# security purposes. Examples are shown below about how to increase the
# level of access.
#
# By far, the most common question I get about the agent is "why won't
# it work?", when really it should be "how do I configure the agent to
# allow me to access it?"
#
# By default, the agent responds to the "public" community for read
# only access, if run out of the box without any configuration file in
# place. The following examples show you other ways of configuring
# the agent so that you can change the community names, and give
# yourself write access to the mib tree as well.
#
# For more information, read the FAQ as well as the snmpd.conf(5)
# manual page.
#
####
# First, map the community name "public" into a "security name"
# sec.name source community
com2sec notConfigUser default public
####
# Second, map the security name into a group name:
# groupName securityModel securityName
group notConfigGroup v1 notConfigUser
group notConfigGroup v2c notConfigUser
####
# Third, create a view for us to let the group have rights to:
# Make at least snmpwalk -v 1 localhost -c public system fast again.
# name incl/excl subtree mask(optional)
# access to 'internet' subtree
view systemview included .1.3.6.1
# access to Cache MIBs Caché and Ensemble
view systemview included .1.3.6.1.4.1.16563.1
view systemview included .1.3.6.1.4.1.16563.2
####
# Finally, grant the group read-only access to the systemview view.
# group context sec.model sec.level prefix read write notif
access notConfigGroup "" any noauth exact systemview none none
```

Después de editar el archivo `/etc/snmp/snmp.conf`, reinicia el `snmpd` daemon.

[service snmpd restart](#)

Verifica el estado de `snmpd`, ten en cuenta que se inició `AgentX` y observa la línea de estado: **Turning on AgentX master support.**

```
h-4.2# service snmpd restart
Redirecting to /bin/systemctl restart snmpd.service
sh-4.2# service snmpd status
Redirecting to /bin/systemctl status snmpd.service
? snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
Loaded: loaded (/usr/lib/systemd/system/snmpd.service; disabled; vendor preset: disabled)
Active: active (running) since Wed 2016-04-27 00:31:36 EDT; 7s ago
Main PID: 27820 (snmpd)
CGroup: /system.slice/snmpd.service
??27820 /usr/sbin/snmpd -LS0-6d -f
Apr 27 00:31:36 vsan-tc-db2.iscinternal.com systemd[1]: Starting Simple Network Management Protocol (SNMP)
Daemon....
Apr 27 00:31:36 vsan-tc-db2.iscinternal.com snmpd[27820]: Turning on AgentX master support.
Apr 27 00:31:36 vsan-tc-db2.iscinternal.com snmpd[27820]: NET-SNMP version 5.7.2
Apr 27 00:31:36 vsan-tc-db2.iscinternal.com systemd[1]: Started Simple Network Management Protocol (SNMP)
Daemon..
sh-4.2#
```

Después de reiniciar snmpd debes hacer lo mismo con el subagente SNMP de Caché utilizando la rutina ^SNMP:
%SYS>do stop^SNMP()
%SYS>do start^SNMP(705,20)

El sistema operativo snmpd daemon y el subagente de Caché deben ser accesibles y ejecutarse ahora.

4. Comprueba el acceso a la MIB

Para probar el acceso a la MIB puedes realizar la verificación con las siguientes líneas de comando.

snmpget devuelve un valor único:

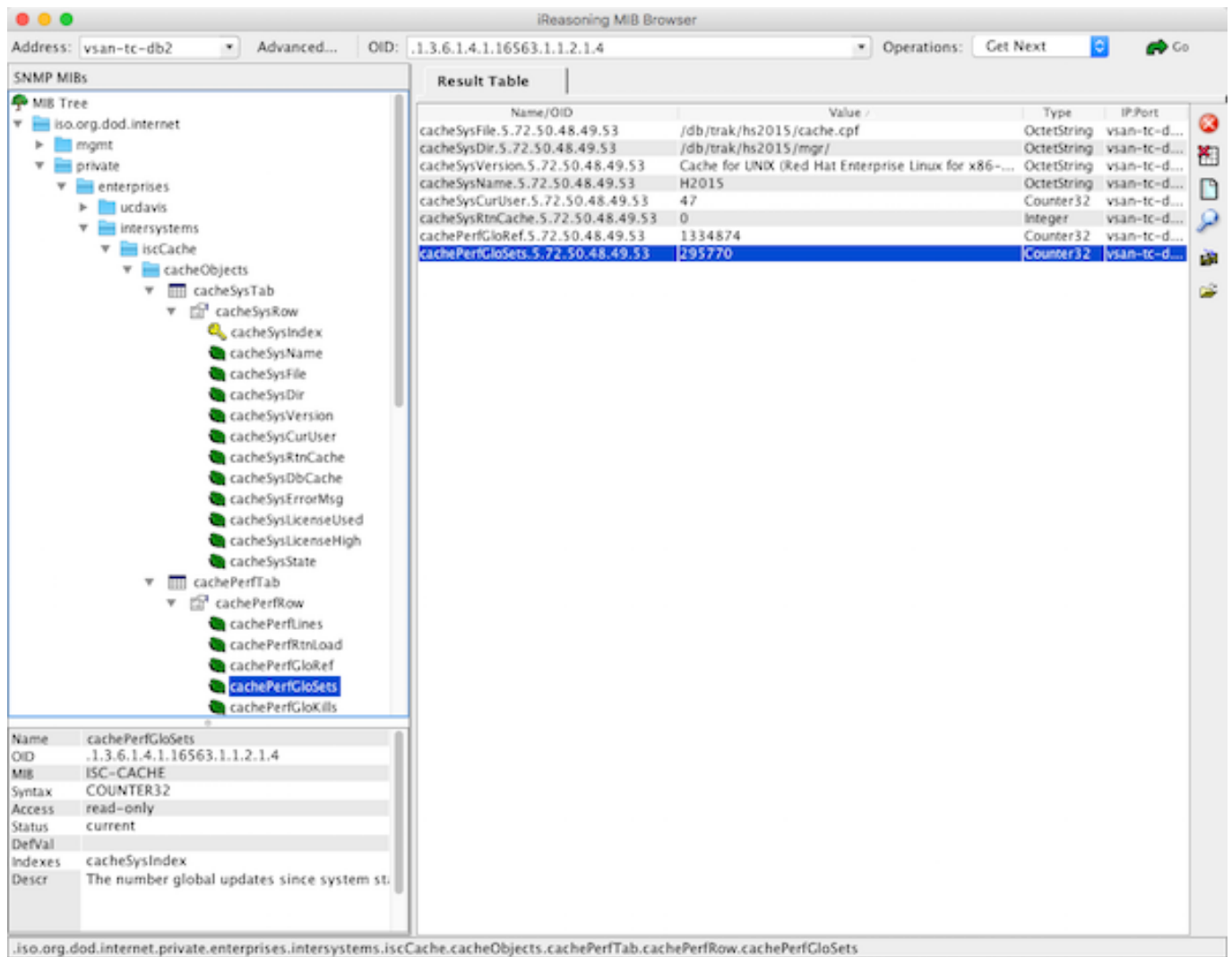
```
snmpget -mAll -v 2c -c public vsan-tc-db2 .1.3.6.1.4.1.16563.1.1.1.1.5.72.50.48.49.53
SNMPv2-SMI::enterprises.16563.1.1.1.1.5.72.50.48.49.53 = STRING: "Cache for UNIX (Red Hat Enterprise
Linux for x86-64) 2015.2.1 (Build 705U) Mon Aug 31 2015 16:53:38 EDT"
```

Y snmpwalk will 'walk' the MIB tree or branch:

```
snmpwalk -m ALL -v 2c -c public vsan-tc-db2 .1.3.6.1.4.1.16563.1.1.1.1
SNMPv2-SMI::enterprises.16563.1.1.1.1.2.5.72.50.48.49.53 = STRING: "H2015"
SNMPv2-SMI::enterprises.16563.1.1.1.1.3.5.72.50.48.49.53 = STRING: "/db/trak/hs2015/cache.cpf"
SNMPv2-SMI::enterprises.16563.1.1.1.1.4.5.72.50.48.49.53 = STRING: "/db/trak/hs2015/mgr/"
etc
etc
```

Además, existen varias ventanas y clientes *nix disponibles para visualizar los datos del sistema. Me gusta utilizar la herramienta gratuita iReasoning MIB Browser. Tendrás que cargar el archivo ISC-CACHE.MIB para el cliente con el fin de que conozca la estructura de MIB.

La siguiente imagen muestra el iReasoning MIB Browser en OSX.

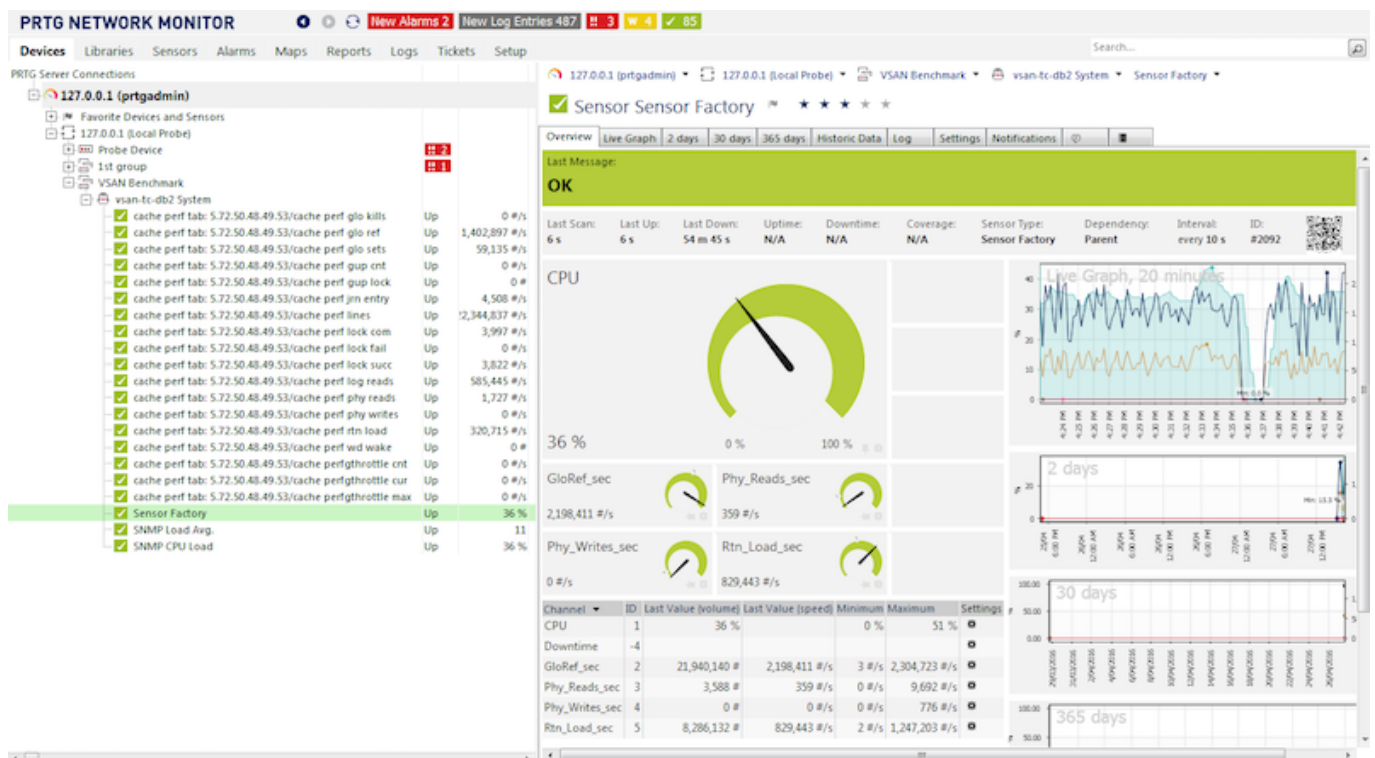


Incluyendo herramientas de monitorización

Aquí es donde pueden existir grandes diferencias en la implantación. Dejo a tu consideración la elección de la herramienta para monitorización, supervisión o análisis.

Por favor, deja un comentario detallando las herramientas y los valores que obtengas para supervisar y administrar tus sistemas. Esto será de gran ayuda para otros miembros de la comunidad.

A continuación, se muestra una captura de pantalla del popular PRTG Network Monitor con las métricas de Caché. Los pasos para incluir las métricas de Caché en PRTG son similares a los que se emplean con otras herramientas



Ejemplo de flujo de trabajo - añade Caché MIB a la herramienta de monitorización.

Paso 1.

Asegúrate de que puedes conectarte a las MIB del sistema operativo. Un consejo es identificar el problema en el sistema operativo y no en Caché. Es muy probable que las herramientas de supervisión sean conocidas y estén preconfiguradas para las MIB de sistemas operativos comunes, por lo que puede ser más fácil ayudar a los proveedores u otros usuarios.

Dependiendo de la herramienta de supervisión que elijas, es posible que tenga que añadir un 'módulo' o una 'aplicación' de SNMP, los cuales generalmente son gratuitos o de código abierto. Las instrucciones del proveedor suelen ser bastante claras para este primer paso.

Después de que realices la supervisión de las métricas del sistema operativo, es momento de añadir a Caché..

Paso 2.

Importa los archivos ISC-CACHE.mib y ISC-ENSEMBLE.mib en la herramienta para que reconozcan la estructura de la MIB.

Los pasos que se muestran aquí pueden variar. Por ejemplo, PRTG tiene la utilidad 'MIB Importer'. Los pasos básicos son abrir el archivo de texto ISC-CACHE.mib en la herramienta e importarlo al formato interno de la herramienta. Por ejemplo, Splunk utiliza un formato Python, etc.

Nota: Nos encontramos que en la herramienta PRTG se agotaba el tiempo si trataba de agregar un sensor para todas las ramas de MIB en Caché. Asumo que recorrió todo el árbol y se agotó el tiempo para algunas métricas como en las listas de procesos, no pasé mucho tiempo solucionando este problema, sino que trabajé en torno a él importando solo la rama correspondiente al rendimiento (cachePerfTab) desde ISC-CACHE.mib.

Una vez importada/convertida la MIB puede reutilizarse para recopilar los datos de otros servidores en tu red. En la imagen anterior se muestra que PRTG utiliza un sensor de tipo "Sensor Factory" para combinar varios sensores en una sola gráfica.

Resumen

Existen muchas herramientas para monitorización, supervisión, de alerta, otras que incluyen análisis muy inteligentes, algunas son gratuitas, otras necesitan licencias de soporte y existen las que combinan las funcionalidades anteriores.

Debes supervisar tu sistema y definir las actividades que son normales y las que están fuera de ese rango, y por lo tanto deben investigarse. SNMP es una manera sencilla para mostrar las métricas de Caché y de Ensemble.

[#Administración del sistema](#) [#Monitorización](#) [#Rendimiento](#) [#Otro](#)

00 2 0 0 109

Log in or sign up to continue
Añade la respuesta

URL de fuente: <https://es.community.intersystems.com/post/plataformas-de-datos-de-intersystems-y-su-rendimiento-parte-5-supervisi%C3%B3n-con-snm>