Monitorización remota

Monitorización remota

Monitorización remota

Introducción

El Network server ejecuta las tareas asignadas a él mediante un sistema de colas multiproceso, puede trabajar con otros servidores de red (modo HA).

Debe tener una visibilidad completa (direcciones IP y puertos) sobre los que se van a realizar las pruebas. En este capítulo también cubre el Plugin server y WMI server.

Monitorización básica de red

1. Pruebas ICMP: Son pruebas básicas de red que permiten saber si un anfitrión o *host* está en línea y accesible, además del tiempo que se tarda en llegar a dicho dispositivo a través de la red.
2. Pruebas TCP: Se forma remota se comprueba que un sistema tiene abierto el puerto TCP especificado en la definición del módulo.
3. Pruebas SNMP: Es posible lanzar peticiones SNMP (*SNMP Polling*) a sistemas que tengan dicho servicio activado para obtener datos como el estado de las interfaces, el consumo de red por interfaz, etc.

El Network server es quien ejecuta las diferentes pruebas de red asignadas en cada agente. Cada agente se asigna a un servidor de red, y es este quien se encarga de su ejecución, insertando los resultados en la base de datos Pandora FMS.

Configuración genérica de un módulo para monitorización de red

Para monitorizar de forma remota un equipo o un servicio de un equipo (FTP, SSH, etc.), primero se debe crear el agente correspondiente, se accede por el menú Management → Resources → Manage agents → Create agent. Rellene los datos para su nuevo agente y pulse el botón Create.

Una vez que haya creado el agente, se pulsa sobre la solapa superior de los módulos (Modules). Allí seleccione crear un nuevo módulo de red pulsando botón Create. En el siguiente formulario que se muestre se selecciona Create a new network server module, y cuando se cargue el menú desplegable de la derecha, seleccione la comprobación deseada.

Monitorización ICMP

Son las comprobaciones más básicas que dan una información importante y exacta.

- icmp_proc: Comprobación en línea (ping) que permite saber si una dirección IP responde o no.
- icmp_data: Comprobación de *latencia* que indica el tiempo en milisegundos para responder a una consulta básica ICMP.

Monitorización TCP

TCP está orientado hacia la conexión por lo que a un envío TCP Send corresponderá una respuesta TCP Receive que indica el estado de un puerto o un servicio a monitorizar. Opcionalmente se puede enviar una cadena de texto y esperar a recibir una respuesta que será tratada directamente por Pandora FMS como un dato.

- TCP Send: Campo para configurar los parámetros que enviar al puerto TCP. Para enviar varias cadenas en secuencia envío/respuesta, hay que separarlas con el carácter `|`; admite la cadena `^M` para reemplazarla por el envío de un retorno de carro.
- TCP receive: Campo para configurar las cadenas de texto que se deben comparar con las repuestas recibidas de la conexión TCP. Si se envían/reciben en varios pasos, cada paso se debe separar con el carácter `|`.

Ejemplo:

TCP Send

```
HELO myhostname.com^M|MAIL FROM: ^M| RCPT TO: ^M
```

TCP Receive

```
250|250|250
```

Módulos de ejecución remota

Enterprise versión 741 o superior.

Para poder utilizar con éxito estos módulos se necesitan las credenciales de conexión del agente a monitorizar. Por tanto todo esto se debe registrar en el almacén seguro de credenciales. Se repiten las instrucciones para la configuración genérica de un módulo pero se selecciona alguno de los siguientes:

- `remote_execution_data`: numérico.
- `remote_execution proc`: *booleano* (0 FALSO, distinto de cero VERDADERO).

- `remote_execution_data_string`: alfanumérico (cadena).
- `remote_execution_data_inc`: incremental (ratio).

Además, se deben definir los siguientes parámetros:

1. Target IP: opcionalmente la IP del objetivo (si no, se usará la del agente).
2. Port: opcionalmente el puerto al que conectar (22 en GNU/Linux, indiferente en MS Windows®).
3. Command: el comando a ejecutar para realizar la monitorización.
4. Credential identifier: el juego de credenciales a utilizar para conectar.
5. Connection method: opcionalmente el método de conexión del objetivo (si no, se usará el del Agente).

El comportamiento del módulo es idéntico a la hora de asignar alertas, generar eventos o visualizar informes.

A partir de la versión 743 en el fichero `pandora_server.conf` se debe disponer de *tokens* para la configuración de los siguientes parámetros relacionados con la ejecución remota de módulos: `ssh_launcher`, `rcmd_timeout` y `rcmd_timeout_bin`.

Propiedades avanzadas comunes de los módulos de red

- Custom ID: permite almacenar un ID de una aplicación externa para facilitar la integración de Pandora FMS con aplicaciones de terceros. Por ejemplo, una *Configuration management database* (CMDB).
- Interval: Intervalo de ejecución del módulo, el cual puede ser personalizado por un usuario Administrador de manera predefinida y luego ser utilizado por usuarios estándar.
- Post process: para posprocesado del módulo (multiplicar o dividir el valor devuelto), por ejemplo cuando se obtienen bytes y se desea mostrar el valor en Megabytes.
- Min. Value y Max. Value: cualquier valor por debajo del mínimo o por encima del máximo se tomará como inválido y se descartará.
- Export target: solo disponible en la versión Enterprise con Export server.
- Category: Solamente se usa en conjunto con la Metaconsola de la versión Enterprise.
- Si *Cron from* está activado, el módulo se ejecutará una vez cuando la fecha y hora actuales coincidan con la fecha y hora configuradas en *Cron from*, ignorando el propio intervalo del módulo.

Monitorización SNMP

Introducción a la monitorización SNMP

- Polling SNMP: Se realiza cada cierto tiempo de forma activa e implica ordenar que Pandora FMS ejecute un comando `get` contra un dispositivo SNMP.
- Trap SNMP: Ocurre con cambios o eventos en el dispositivo, que pueden suceder en cualquier momento o no. Es necesario activar la consola de *traps* SNMP en Pandora FMS, donde se mostrarán los que se reciban de cualquier dispositivo. Se pueden definir alertas mediante reglas de filtrado de

traps por cualquiera de sus campos.

Pandora FMS trabaja con SNMP manejando Identificadores de Objetos u *Object IDentifier* (OID) individuales, así cada OID es un módulo de red.

Pasos necesarios para trabajar con SNMP

- Activar la gestión SNMP del dispositivo para que desde el servidor de red se pueda hacer consultas SNMP.
- Conocer la IP y la comunidad SNMP del dispositivo remoto.
- Conocer el OID concreto del dispositivo remoto (o utilizar uno de los múltiples *wizards* de que dispone Pandora FMS o su explorador de OID SNMP).
- Saber cómo gestionar el dato que devuelve el dispositivo. Los dispositivos SNMP devuelven datos en diferentes formatos. Pandora FMS puede tratar casi todos. Los datos de tipo contador son los que Pandora FMS gestiona como `remote_snmp_inc` y son de especial importancia, ya que al ser contadores no pueden tratarse como datos numéricos sino como tasa de elementos por segundo. La mayoría de datos estadísticos SNMP son de tipo contador y se han de configurar como `remote_snmp_inc` si se quiere monitorizar de forma adecuada.

Monitorizando con módulos de red tipo SNMP

Pandora FMS incluye algunos OID en su base de datos que puede usar directamente. Las MIB son una colección de definiciones que definen las propiedades del objeto gestionado dentro del dispositivo a gestionar.

Existen más MIB incluidas en Pandora FMS y con la versión Enterprise se incluyen paquetes de MIB para distintos dispositivos.

Para poder monitorizar cualquier otro elemento por SNMP se debe conocer su comunidad SNMP. Durante la creación del módulo debe seleccionar Manual setup. En el campo Type existen tres opciones para SNMP, al seleccionar una de ellas se expandirá el formulario mostrando los campos adicionales para SNMP.

- SNMP community: es como una identificación de usuario o una contraseña que permite el acceso a las estadísticas de un enrutador u otro dispositivo (versiones SNMPv1 y SNMPv2c ya que SNMPv3 utiliza autenticación por credenciales). Por defecto los dispositivos traen la comunidad pública (public) de solo lectura y generalmente cada administrador de red cambia todas las cadenas de la comunidad a valores personalizados en la configuración del dispositivo.
- SNMP OID: identificador OID que monitorizar, el cual consiste en una cadena de números y puntos. Estas cadenas son automáticamente traducidas por cadenas alfanuméricas más descriptivas si las MIB correspondientes se encuentran instaladas en el sistema.

Monitorizando SNMP desde los Agentes Software

Un Agente Software es generalmente es utilizado para obtener datos locales, sin embargo también puede realizar monitorización SNMP.

En GNU/Linux®

snmpget suele estar instalado por defecto, por lo que puede ser llamado desde la línea *module_exec*.

```
module_exec snmpget -v <versión> -c <comunidad> <dirección IP> <OID numérica>
```

Cabe destacar que solo las OID "básicas" son traducibles por su equivalente numérico, y que es recomendable usar siempre OID numéricas, ya que no se sabe si la herramienta va a saber traducirla o no. En cualquier caso siempre se pueden cargar los MIB en el directorio:

```
/usr/share/snmp/mibs.
```

En MS Windows®

snmpget.exe (el cual forma parte del proyecto net-snmp, con licencia BSD) está añadido al Agente Software junto con las MIB básicas, además de un empaquetador o guión (*wrapper* o *script*) para encapsular la llamada. De similar manera que en Linux, se pueden cargar los MIB en el directorio:

```
/util/mibs.
```

Gestor de MIB

Pandora FMS de manera predeterminada utiliza las MIB que están alojadas por el sistema operativo en:

```
 /usr/share/snmp/mibs.
```

Se pueden incorporar nuevas MIB (y gestionarlas luego) por medio de la funcionalidad MIB uploader desde el menú Operation → Monitoring → SNMP.

Estas MIB solamente son usadas por Pandora FMS y están almacenadas en la ruta:

```
 {PANDORA_CONSOLE}/attachment/mibs.
```

Esta funcionalidad solo gestiona las MIB para *Polling SNMP*,
en el caso de las *Trap SNMP* consulte el capítulo
Monitorización con traps SNMP.

Navegador SNMP de Pandora FMS

Versión Enterprise NG 744 o superior

El Navegador SNMP realiza un recorrido completo del árbol del dispositivo. Dicha operación puede tardar varios minutos y es posible recorrer ramas precisas y acortar el recorrido. Se accede desde Monitoring → SNMP → SNMP Browser.

El sistema pedirá esa información al sistema y además mostrará (si está disponible) la información del OID solicitado. Si no existe información sobre el OID del dispositivo, esta se muestra únicamente en formato numérico. La información descriptiva de los OID se almacena mediante las bases de información gestionada o MIB. Si no dispone de una MIB para el dispositivo que desea explorar, probablemente tenga que recurrir a buscar “trozos de información” en la información visualizada por Pandora FMS, lo cual es complejo y lleva tiempo.

El explorador SNMP también permite buscar una cadena de texto tanto en los valores de OID obtenidos como en los valores traducidos de los propios OID (si están disponibles). Esto es especialmente útil para buscar cadenas conocidas concretas y localizar su OID. Si localiza varias entradas nos permitirá ir saltando de una ocurrencia a otra, y las mostrará resaltadas en amarillo.

Es posible seleccionar varios OID y añadirlos a un agente pulsando el botón Create agent modules. Para ello se selecciona los agentes que serán monitorizado con dichos OID y se añaden al cuadro de la derecha. También se puede seleccionar varios OID para añadirlos a una política de monitorización.

SNMP Wizard

Vista de administración de un agente.

Se debe definir la dirección IP de destino, la comunidad y otros parámetros opcionales (SNMP v3 está soportado) para hacer un *Walk SNMP* al objetivo. Una vez se reciba la información

correctamente, aparecerá un formulario para la creación de módulos tales como Devices, Processes, Free space on disk, Temperature sensors y Other SNMP data.

Se selecciona el tipo de módulo y se agregan a la lista de creación, cuando acabe este proceso se podrá hacer clic en el botón de Create Modules.

Este *wizard* creará dos tipos de módulos:

- Módulos SNMP para las consultas con OID estático: Sensores, Memoria, CPU, etcétera.
- Módulos Plugin para las consultas con OID dinámico o los datos calculados: Procesos, Espacio en disco, Memoria usada expresada en porcentaje, etcétera.

Para los módulos de tipo plugin usaremos el plugin de SNMP remoto, por lo que si el *plugin* no está instalado en el sistema, estas características permanecerán desactivadas. El plugin deberá tener el nombre snmp_remote.pl sin importar su localización.

Para que el *wizard* SNMP pueda obtener datos de un dispositivo SNMP gracias a los componentes remotos, es necesario cumplir 2 requisitos:

- Tener registrado en Pandora el Private Enterprise Number (PEN) del fabricante del dispositivo.
- Tener registrados y habilitados en Pandora componentes del wizard SNMP para el fabricante del dispositivo.

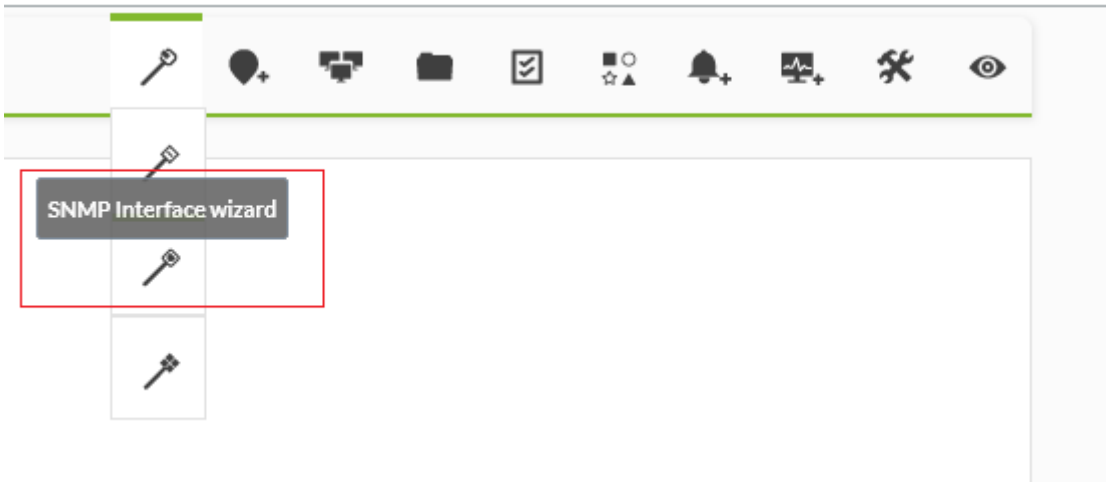
Si el dispositivo explorado cumple estos requisitos, se mostrarán todos los módulos de los cuales se hayan podido obtener datos para dar la oportunidad de seleccionar cual crear y cual no.

Una vez pulsado el botón *Create modules* se mostrará un listado resumen de los módulos elegidos con su configuración. En este listado se verán los módulos que no se puedan crear, ya sea porque ya existen en el agente o porque se han configurado 2 o más módulos con el mismo nombre en el propio *wizard*.

Tenga en cuenta que si el valor del Módulo recogido por el *wizard* es de tipo incremental o incremental absoluto, dicho valor no es el incremento en sí sino un valor referencial. Para obtener un valor incremental son necesarias dos lecturas, por ello el valor del Módulo indicará “cero” hasta que se realice la próxima lectura.

Antes de que se añadan al agente, habrá una última oportunidad de confirmar la creación de estos módulos o de cancelarla y seguir modificando el resultado del *wizard*.

SNMP Interface wizard



Este *Wizard* navega por la rama de SNMP IF-MIB::interfaces, ofreciendo la posibilidad de crear múltiples módulos de varios interfaces con la selección múltiple. Después de seleccionar la dirección IP de destino, comunidad, etc., el sistema hará una consulta SNMP a la máquina destino y rellenará el formulario para la creación de módulos.

Para que el wizard SNMP de interfaces pueda obtener datos de un dispositivo SNMP el dispositivo SNMP debe devolver datos de la rama IF-MIB.

Una vez confirmada la creación de los módulos, se volverá a evaluar uno a uno si se pueden crear o no, para evitar módulos duplicados en el caso de que en el lapso de tiempo de la confirmación se hayan creado los mismos módulos por otro medio.

Se nos notificará si el proceso se ha podido completar con éxito o, si por el contrario, ha habido algún módulo que no se haya podido crear.

Monitorización remota de MS Windows con WMI

WMI es una tecnología empleada en el sistema operativo (S.O.) de Microsoft® para obtener información remota de equipos funcionando con Windows®; está disponible desde la versión Windows XP hasta las versiones más actuales. WMI permite obtener todo tipo de información del S.O., las aplicaciones e incluso el hardware. Las consultas de WMI se pueden realizar localmente con el Agente Software (llamando a la API del S.O.) o de forma remota.

En algunos sistemas el acceso remoto a WMI no está activado y es preciso activarlo para poder ser consultado

desde el exterior.

Es necesario habilitar el componente wmiserver en el fichero de configuración del servidor de Pandora FMS.

```
# wmiserver : 1 or 0. Set to 1 to activate WMI server with this setup
# DISABLED BY DEFAULT
  wmiserver 1
```

Las consultas se hacen en WQL, una especie de lenguaje SQL específico de Microsoft®, para todo objeto que aparezca en la base de datos del sistema WMI.

Para comenzar a monitorizar por WMI, primero se deberá crear el agente correspondiente, luego se pulsará sobre la solapa superior de los módulos (Modules). Una vez en ella, se selecciona Create a new WMI server module y se pulsa el botón Create.

Campos específicos WMI:

- Namespace: Espacio de nombres WMI; en algunas consultas este campo es diferente de cadena vacía (por defecto), dependiendo del proveedor de información de la aplicación que se monitorice.
- Key string: Opcional, campo para comparar con la cadena devuelta por la consulta, y de existir el módulo devuelve 1 o 0, en lugar de la cadena en sí.
- Field number: El número del campo devuelto empezando desde 0 (las consultas WMI pueden devolver más de un campo). En la mayoría de las veces es 0 o 1.
- WMI Query: Consulta WMI, similar a una sentencia en SQL.

Wizard WMI

Utilizado para navegar y crear módulos con consultas WMI a un agente específico. En el *Wizard* de agente (pestaña en la vista de administración de un agente), haga clic en el icono:

Debe especificar el nombre de usuario y contraseña que tenga permisos para hacer consultas WMI (o en su defecto la del Administrador) en el servidor de destino para hacer las primeras consultas

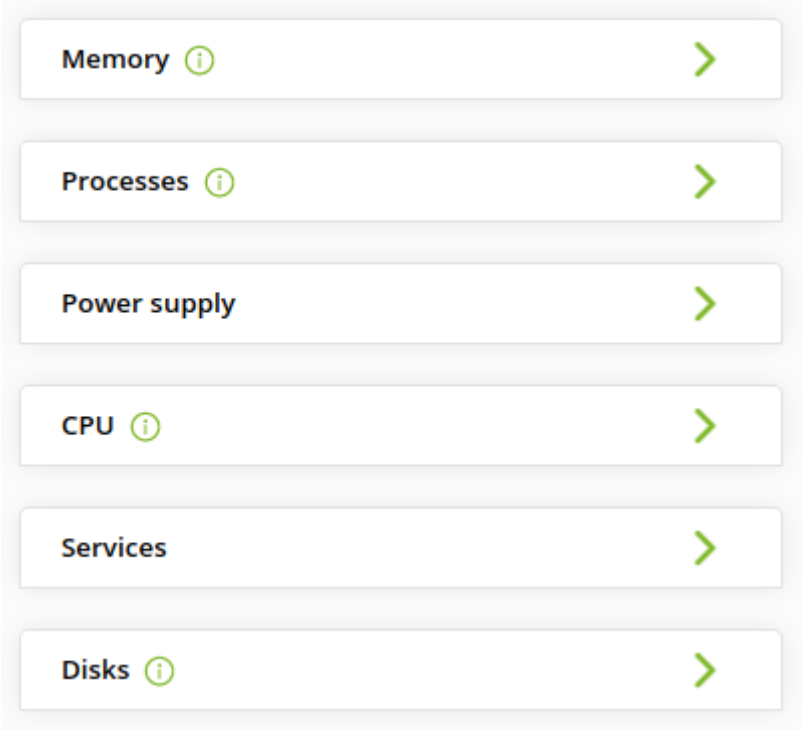
WMI. Esta información será utilizada para la creación de módulos.

Con el Wizard WMI es posible crear módulos de diferentes tipos de información WMI:

- Servicios: Se crearán monitores booleanos en estado normal si el servicio está corriendo y en estado crítico cuando se encuentre detenido.
- Procesos: Los monitores de procesos recibirán información solamente cuando el proceso esté activo. De lo contrario, caerán en estado desconocido.
- Espacio libre en disco
- Componentes WMI: En este caso escogerá entre los componentes WMI registrados en el sistema.

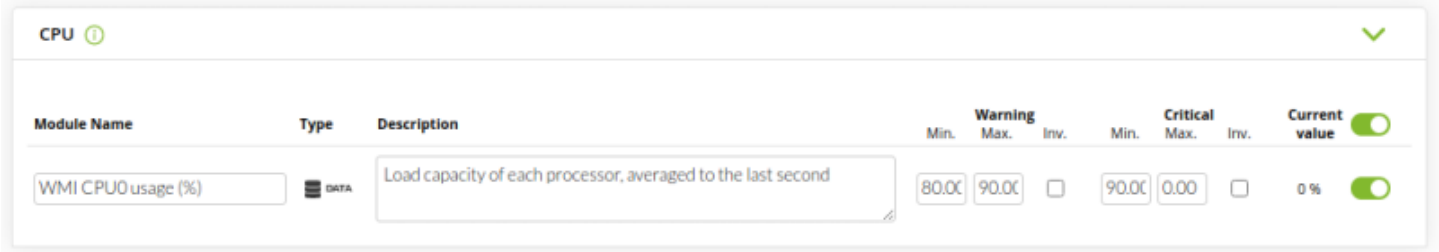
Debe tener registrados y habilitados en Pandora componentes del wizard WMI: de esta manera se mostrarán todos los módulos de los cuales se hayan podido obtener datos para tener la oportunidad de crearlos o no.

Estos módulos se mostrarán organizados en bloques en base al grupo al que pertenezca el componente del wizard que los haya generado.



Todos los bloques se mostrarán comprimidos en un primer momento para facilitar la visualización y se podrán ir expandiendo para modificar los seleccionados o los datos. Además, en cada bloque donde se hayan marcado módulos para su creación se verá un icono informativo que indicará.

Si desplegamos un bloque, se podrán elegir los módulos que se agregarán y los que no, así como la opción de modificar el nombre, la descripción o los umbrales de cada módulo individualmente.



Una vez pulsado el botón *Create modules* se mostrará un listado con un resumen de los módulos elegidos con su configuración. En este listado se verán los módulos que no puedan ser creados, ya sea porque ya existen en el agente o porque se han configurado dos o más módulos con el mismo nombre en el mismo *wizard*.

A pesar de todas las modificaciones que se realicen habrá una última oportunidad de confirmar la creación de estos módulos o de cancelarla y seguir modificando el resultado del *wizard*.

Una vez confirmada la creación de los módulos, se volverá a evaluar uno a uno si se pueden crear o no, para evitar módulos duplicados en el caso de que en el lapso de tiempo de la confirmación se hayan creado los mismos módulos por otro medio.

El asistente notificará si el proceso se ha podido completar con éxito o si por el contrario ha habido algún módulo que no haya podido ser creado.

Monitorización con plugins remotos de servidor

Un *plugin remoto* es un *script* o fichero ejecutable que admite parámetros y devuelve un solo y único valor. El resultado podría ser un número, un valor booleano (0 = error, OK <> 0) o una cadena de texto. Un *plugin* remoto generalmente permite parámetros de entrada. Por defecto varios *plugins* de servidor vienen instalados y listos para utilizarse y el usuario puede siempre añadir los que necesite.

Existen dos clases de *plugin* remoto: estándar y tipo Nagios. La diferencia estriba principalmente en que los de tipo Nagios responden con un nivel de errores (*error level*) y además, de manera opcional, con una cadena descriptiva.

Administración de plugins remotos

Se accede por Management → Servers → Plugins, se abrirá una nueva ventana con un listado de los *plugins* registrados. Cada ítem tiene sus correspondientes botones de edición y borrado, excepto si tiene módulos en uso los cuales se pueden listar por medio del botón Lock.

Al editar un *plugin*:

- Plug-in type: Permite establecer si es de tipo estándar o tipo Nagios.

- Max. timeout: Para fijar el tiempo de espera para su ejecución, *se debe prestar especial atención en este valor ya que debe abarcar suficiente tiempo para la ejecución* de lo contrario no obtendrá valor alguno.
- El campo de la descripción es importante ya que se verá en la interfaz de uso del *plugin* por parte del usuario, escoja una leyenda corta y explicativa.

- En la ejecución de un *plugin* existen tres valores de espera: el del servidor, el del *plugin* y el del módulo. El del servidor prevalece sobre los demás, y en segundo lugar, el del *plugin*. Ej. con valores de *timeout* del servidor en 10 segundos, el del *plugin* en 20 y el del un módulo con este *plugin* en 30, el máximo tiempo que se esperará a la ejecución de ese módulo será de 10 segundos.
- Al editar un *plugin* y este se encuentra en uso por al menos un agente, no podrá *agregar o borrar* las macros.

Macros internas

De una forma similar a las alertas, también se pueden utilizar macros internas en la configuración de *plugins*. Las macros soportadas son las siguientes:

- `_agent_` o `_agentalias_`: Alias del agente al que pertenece el módulo.
- `_agentname_`: Nombre del agente al que pertenece el módulo.
- `_agentdescription_`: Descripción del agente al que pertenece el módulo.
- `_agentstatus_`: Estado actual del agente.
- `_address_`: Dirección del agente al que pertenece el módulo.
- `_module_`: Nombre del módulo.
- `_modulegroup_`: Nombre del grupo del módulo.
- `_moduledescription_`: Descripción del módulo.
- `_modulestatus_`: Estado del módulo.
- `_moduletags_`: Etiquetas (*tags*) asociados al módulo.
- `_id_agent_`: ID del agente, útil para construir directamente la URL o redireccionar a la Consola de Pandora FMS.
- `_id_module_`: ID del módulo.
- `_policy_`: Nombre de la política a la que pertenece el módulo si está establecida alguna.
- `_interval_`: Intervalo de ejecución del módulo.
- `_target_ip_`: Dirección IP del destino del módulo.
- `_target_port_`: Puerto del destino del módulo.
- `_plugin_parameters_`: Parámetros de *plugin* del módulo.
- `_email_tag_`: correos electrónicos asociados a *tags* de módulos.

Macros de campos personalizados para monitorización remota

Las macros de campos personalizados permiten utilizar los campos personalizados de agentes como macros para ciertas opciones de configuración de módulos.

Las macros de campos personalizados funcionan con módulos de tipo SNMP, WMI, *plug-in* e inventario. Se pueden utilizar en módulos independientes, componentes de red y en módulos de política.

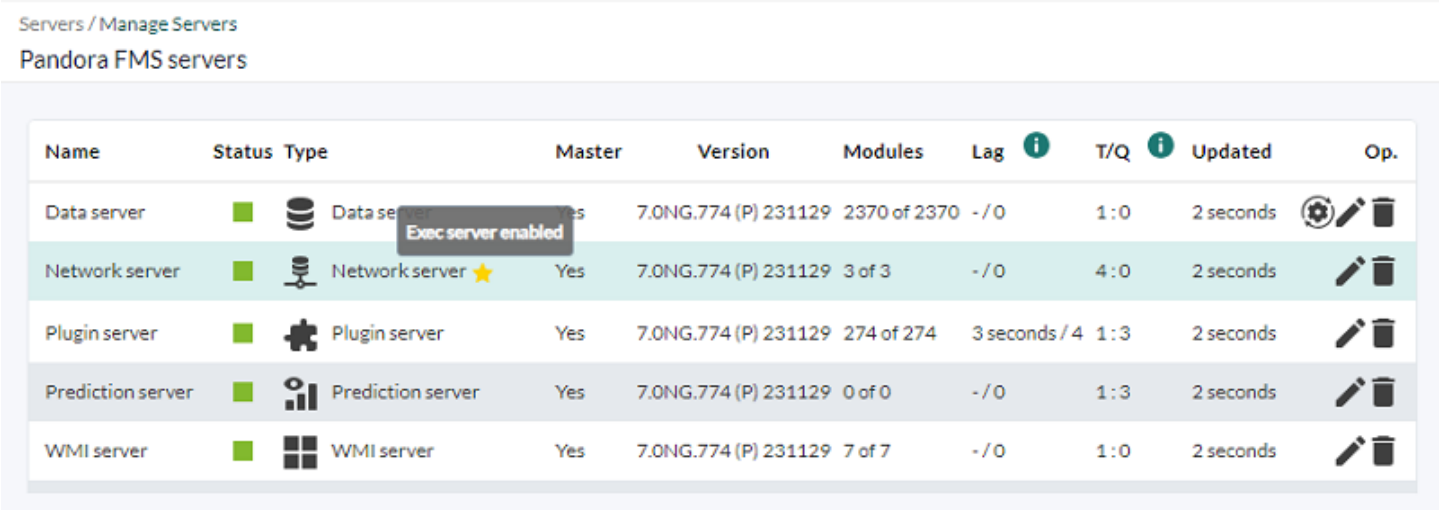
Se accede por Management → Resources → Custom fields → Create field en este nuevo campo personalizado se almacenará la cadena de comunidad SNMP. Apunte su ID, ya que más tarde formará parte de la macro, y rellene la cadena de comunidad con el valor adecuado en sus agentes SNMP.

Luego se debe crear un componente de red SNMP al que se debe introducir `_agentcustomfield_<n>_` *como cadena en* SNMP community*, donde* n *es el ID del campo personalizado creado.*

Ejecución remota de wizards y pruebas de red (Exec Server)

Solamente para servidores PFMS instalados en GNU/Linux.

Esta funcionalidad permite que desde la consola de Pandora FMS se puedan ejecutar algunas acciones en servidores remotos de Pandora FMS.



Con un Exec server configurado se podrá elegir desde:

- El SNMP browser en la sección SNMP.
- En los Event responses en la sección de eventos.
- En los wizards de SNMP de agente.
- En los wizards de WMI de agente.
- En los wizards de interfaces SNMP de agente (excepto para los Satellite Server).

Dependiendo del servidor seleccionado a la hora de lanzar cada *wizard*, se crearán los módulos adaptados para servidor o Satellite Server. En este último caso se escribirán los módulos en el fichero de configuración remota para que puedan ser ejecutados por el servidor.

Los Exec server funcionan internamente a través de la ejecución de comandos remotos SSH desde la consola de Pandora FMS a los servidores habilitados, llamados Exec Server. Estos pueden ser Network servers o Satellite servers de Pandora FMS.

El proceso de configuración requerirá el concurso de la persona encargada de la administración de red para configurar tanto los servidores PFMS como para los ordenadores destino y el tráfico de conexiones y datos, entre otros aspectos como los cortafuegos y las VLAN para aumentar la seguridad.

- Se debe contar con un agente lógico configurado con la configuración remota habilitada.

Sin la configuración remota habilitada se carecerá de la creación de módulos de Satellite desde los asistentes (*wizards*).

- Se debe tener llaves digitales creadas (clave pública y clave privada) para la conexión SSH.
- La clave pública debe ser copiada a los servidores destino y se debe configurar para que solamente conecte de esa manera, mediante llave digital.
- En el servidor que ejecuta la Consola web PFMS se debe tener un usuario creado a nivel de sistema operativo y con acceso debido a su propio directorio y que permita ejecutar una *shell* válida para las tareas a encomendar.
- En la Consola web PFMS se deberá acceder como usuario *superadmin* o *Pandora Administrator*.

Consulte el anexo técnico para más información.

Monitorización de rutas

Versión NG 715 o superior.

Pandora FMS ofrece por defecto la monitorización de rutas completas entre dos puntos de la red, indicando visualmente el camino que se está siguiendo en todo momento para comunicarse entre estos dos puntos. El analizador de rutas de Pandora FMS utiliza un *plugin* de agente para trazar un mapa de la ruta.

Para utilizar este sistema se necesita:

- Un Agente software en el punto de origen de la ruta a analizar.
- Alcance vía ICMP desde el punto de origen.

De manera opcional, si desea hacer escaneos de rutas a través de Internet, se recomienda que despliegue la aplicación MTR en el equipo origen de ruta.

Se accede a la pestaña de configuración de *plugins* en agente y se agrega la siguiente línea:

```
route_parser -t <target_address>
```

Por último active la ejecución del *plugin*.

Volver al índice de documentación de Pandora FMS