Manual TRAFwatcher

Manual TRAFwatcher

Tabla de contenidos

Lista de tablas

Prefacio

Público objetivo

Este manual está destinado a los administradores de red, consultores de red y asociados de Telcomanager.

Para entender completamente este manual, el lector debe tener un conocimiento medio sobre gestión de redes y protocolo TCP/IP.

Convenciones utilizadas en este manual

Este documento utiliza las siguientes convenciones:

Tabla 1. Convenciones del manual

Item	Convenciones
Seleccionando un ítem del menú:	**Menú → Submenú → Ítem del menú**
Comandos, botones y palabras clave.	Fuente en **negrita**.

Capítulo 1. Introducción

Sobre

TRAFwatcher es un módulo que actúa junto con el TRAFip para ayudar a detectar amenazas en tu red.

Principales recursos

- Soporte para NetFlow, jFlow, sFlow, IPFIX y Huawei netstream.
- Acceso a todos los recursos del sistema a través de un web browser.
- Puede ofrecerse alta disponibilidad a través del uso de soluciones redundantes, en las que dos appliances trabajan en HOT-STANDBY.
- Exportación de imagen de gráfico en masa.
- Flexibilidad en la creación de gráficos.
- Gráfico en HTML5 interactivo, con recursos como zoom vertical y horizontal, auto-escala y gráficos agregados.
- Banco de datos de alto rendimiento para datos históricos almacenados.
- Perfiles de amenaza que pueden ser asociados a las subredes para que direcciones IPs dentro de ellas sean alarmadas en caso de que los límites definidos sean superados.
- Creación de scripts para anunciar direcciones IPs sospechosas en blackhole.

Requisitos mínimos

Estos requisitos son para los computadores que irán a acceder al sistema por el web browser.

Hardware

- Procesador Pentium 2 400 MHZ o superior.
- 128 MB de memoria RAM.

Navegador

- Internet explorer 9+.
- Chrome 4.0+.
- Firefox 7.0+.

Capítulo 2. Datos históricos

Este capítulo describe los elementos de la guía de datos históricos.

Abajo de esta guía puedes acceder a todos los datos procesados por los objetos controlados.

Se puede acceder a los datos a través de gráficos e informes.

Panel de Control

Esta pestaña muestra los límites y el resumen de las IPs que tuvieron tráfico sospechoso detectado en el momento para cada subred.

Límites

Para cada subred, se mostrará una tabla conteniendo los límites, los valores máximos, las medias y las distancias porcentuales entre las medias y los valores máximos de **Bytes de origen**, **Bytes de destino**, **Flujos de origen**, **Flujos de destino**, **Paquetes de origen**, **Paquetes de destino**, **IP Flood de origen e IP Flood de destino**.

Si la subred está usando el límite automático, aparecerá un **(auto)** al lado de los valores de los límites.

La distancia porcentual del valor máximo a la media es calculada de la siguiente forma:

```
Distância = [(Máximo/Média)-1] * 100
```

Resumen de las últimas amenazas

Se mostrarán las IPs (origen o destino), la duración de ataque, el tipo de ataque detectado, el tipo de límite que fue superado, el valor del límite y el valor que fue observado en el tráfico.

Clicando en el botón **Añadir a la lista de exclusión**la IP pasará a ser excluida del análisis de tráfico sospechoso.

Para ejecutar el script de **Blackhole** manualmente, clica en el icono que aparece en la columna **Blackhole**.

Para obtener estadísticas detalladas y consolidadas para cada flujo, genera un **informe de datos brutos** clicando en el icono  .

Importante

Solo aparecerá en esta pantalla las subredes que usan límite automático o que están asociadas a algún Perfil de Amenaza.

Subredes

Los objetos de subredes permiten el análisis de bloques IP.

Definiciones

- **Tráfico de destino de subred**: compuesto por la suma de todos los flujos en los que la dirección de IP de destino pertenece al bloque de IP de subred.

- **Tráfico de origen de subred**: compuesto por la suma de todos los flujos en los que la dirección de IP de origen pertenece al bloque de IP de subred.
- **Tráfico absoluto de la subred**: compuesto por la suma de todos los flujos en que la dirección IP de origen o destino pertenece al bloque de IP de subred.
- **Tráfico absoluto externo de la subred**: compuesto por la suma de todos los flujos en que la dirección IP pertenece al bloque de IP de la subred, pero la dirección IP de origen o de destino pertenecen a una subred desconocida.

Configuración

Para gestionar el sistema de subredes, accede a **Datos Históricos** → **Subredes**.

Clica en el ítem de menú del árbol **Subredes** para tener la lista de subredes configuradas.

Para añadir una nueva subred, clica en el botón **Nuevo** y rellena el formulario.

Tabla 2.1. Formulario de nueva subred

Campos	**Descripción**
Nombre	Nombre de la subred.
Descripción	Descripción de subred.
Bloques de dirección IP	Las subredes pueden tener más de una banda de direcciones. Ej.: 10.0.0.0/24, 10.0.1.0/24, 2001:db8:abcd:2000::/64, 2001:cdba:9abc:5678::/64.
Tráfico límite (bps)	Este valor será trazado en el gráfico del objeto con una línea punteada roja.
Threshold del Factor de Actividad de origen	Límite del **Factor de Actividad** de origen.
Threshold del Factor de Actividad de destino	Límite del **Factor de Actividad** de destino.
Habilitar proyección	Usa los parámetros modelo de proyección o defínalos.
Habilitar TRAFWatcher	Selecciona **Sí** para habilitar el Análisis de Amenazas por el TRAFwatcher.
Usar límite automático	Selecciona **Sí** para que el sistema calcule los límites automáticamente de acuerdo con el tipo del **Factor de tolerancia**. Si seleccionas **No**, la detección de amenazas será realizada a partir de los límites configurados manualmente en el **Perfil de amenaza.**
Factor de tolerancia	Este campo solo está disponible cuando el campo **Usar límite automático** es **Sí**. El factor **Extremo** es más tolerante a las amenazas, o sea, los thresholds serán mayores en caso de que se seleccione esta opción. Para una evaluación moderada de amenazas selecciona **Moderado**.
Perfil de amenaza	Este campo solo está disponible cuando el campo **Usar límite automático** es **No**. Selecciona el perfil

Campos	Descripción
	de amenaza para esta subred para que sea usado en el Análisis de amenazas o déjelo en blanco.
Perfil de alarma	Asociación de perfil de alarma.

Sugerencia

Puedes habilitar el TRAFwatcher para varias subredes simultáneamente. Para ello, en la lista de todas las subredes, selecciona las que deseas habilitar para el TRAFwatcher y clica en el botón **Habilitar TRAFwatcher**.

Importando archivos de subredes

Para importar un archivo de subredes, accede a **Datos Históricos** → **Subredes**.

Clica en el ítem **Subredes** en el menú del árbol.

Clica en el botón **Importar** y carga el archivo.

Una subred importada posee los siguientes campos:

Tabla 2.2. Campos de un archivo de subred

Campo	Descripción
Nombre	Nombre de la subred.
Descripción	Descripción de la subred (opcional).
Bloques de dirección IP	Las subredes pueden tener más de una banda de direcciones. Formato de entrada: IP1/Máscara1,IP2/Máscara2 (IP/32 en el caso de usar una IP única). Ej.: 10.0.0.1/32,10.0.1.0/24
Tráfico límite (bps)	Rellena con valores enteros mayores o iguales a 0.
Habilitar TRAFwatcher	Rellena con **YES** o **NO**.

Añadir metadatos de subredes

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **Subredes**, clica en el ítem **Subredes** en el menú del árbol y clica en el botón **Metadato**.

Clica en el botón **Nuevo** para crear un nuevo metadato. Puede ser del tipo **Texto**, **Entero** o **Enum**.

Puedes alterar el metadato cuando desees usando el botón **Editar** y verificar el histórico de alteraciones a través del botón **Histórico**.

Para borrar un metadato, clica en el botón **Borrar**.

Tabla 2.3. Campos de un metadato

Campo	Descripción
Nombre	Nombre del metadato.
Descripción	Descripción del metadato.

Campo	Descripción
Tipo de dato	Escoge si el metadato será del tipo **Texto**, **Entero** o **Enum**.
Valores	Este campo solo está disponible si el **Tipo de dato** es **Enum**. Introduce una lista de valores, separándolos por punto y coma (;).

Para asociar el metadato creado a una subred, accede a la lista de subredes y clica en el botón **Metadato** al lado de la subred que será configurada.

Después, rellena los metadatos de acuerdo con el tipo. Puedes rellenar todos ellos o solo los que desees.

Estadísticas

Al acceder a una subred a través del menú lateral, el display de datos mostrará sus estadísticas cada 5 minutos.

Se muestran los valores de **Media** y **Máximo** de los bytes, paquetes, flujos e IP Flood de origen y de destino.

En el inicio de la página, se exhiben los valores más altos registrados.

Importante
Es necesario que la subred esté asociada a un Perfil de Amenaza para que estos valores sean obtenidos.

Importante
Al subred que supere el umbral definido en el perfil de amenaza asociado al ella tendrá su célula resaltada en rojo.

Informes

Modelos

Para la mayoría de los informes disponibles en el sistema, tienes la opción de guardarlos como modelo.

Guardando

1. Abre el informe deseado y selecciona la opción Guardar modelo.

2. Rellena los campos de abajo:

Tabla 2.4. Forma del modelo

Campo	Valores
Nombre	Nombre del informe.
Permiso de escritura	Selecciona quien puede alterar este informe. Esta opción de grupos está basada en el grupo de usuarios.

Campo	Valores
Permiso de lectura	Selecciona quien puede leer este informe. Esta opción de grupos está basada en los grupos de usuarios.
Enviar informe por correo electrónico	Enviar por correo electrónico
Enviar informe al servidor FTP	Enviar al servidor FTP.
Formato del anexo	Escoge el formato deseado: PDF or CSV.

3. Rellena los otros campos de informe y clica en el botón Enviar.

Después de ejecutar los pasos de encima, el informe guardado estará disponible en la **Lista de modelo** para cada tipo de informe.

Programación

1. Abre la lista de modelo para el informe creado o crea un nuevo informe.
2. Selecciona la opción Programar modelo;
3. Selecciona la opción de programación apropiada.

Opciones de programación

- Una ejecución: Puede ser **Inmediata** o **Programada**. Los instantes inicial y final de los datos son configurados en el propio formulario.
- Diario: Define el **Horario de Ejecución** de todo día, en este horario, será ejecutado un informe con periodo de 1 día. Si la opción **Considerar el día de la ejecución** está marcada, el día de ejecución será considerado en este período.
- Semanal: Define un **Día de la semana** y un horario para que el informe sea ejecutado. Los datos tendrán inicio el Domingo a las 00h y fin el Sábado de la semana anterior a las 23h59min. Si la opción **Considerar el día de la ejecución** está marcada, la semana del día de ejecución será considerada en este período.
- Mensual: Define un **Día de ejecución** y un horario para que el informe sea ejecutado. Los datos tendrán inicio el Domingo a las 00h y fin el Sábado del mes anterior a las 23h59min. Si la opción **Considerar el día de la ejecución** está marcada, el mes del día de ejecución será considerado en este período.

Sugerencia

Para programar un informe, debes guardarlo como modelo.

Sugerencia

Cuando un informe está listo, es enviado al correo electrónico de los usuarios. El servidor SMTP debe ser configurado, así como el correo electrónico de cada usuario en el formulario de configuración del usuario.

Editando

Después del modelo estar guardado, un botón **Editar** aparecerá en la lista del modelo y puede ser usada para cambiar los parámetros del informe.

Visualizando informes

Después del sistema ejecutar un modelo, un nuevo informe se generará.

Se puede acceder a todas las instancias del informe a través del botón Detalles para cada modelo.

Para visualizar una instancia del informe, sigue el procedimiento de abajo:

1. Clica en el botón **Detalles** para el modelo deseado.
2. Escoge el formato de salida deseado, entre HTML, CSV y PDF.
3. Clica en el botón **Mostrar** para la instancia de informe deseada.

Gestionando espacio de disco

El espacio total disponible y actualmente usado por los modelos de informes es listado debajo de la lista de modelo.

El sistema tiene un área de almacenamiento reservada que es compartida por todos los informes.

Puedes aumentar o disminuir este espacio yendo a **Sistema** → **Parámetros** → **Almacenamiento de datos** .

Puedes borrar informes generados clicando en el botón Detalles en la lista de modelo, para el modelo deseado.

Análisis de Amenazas

El informe de análisis de amenazas proporciona informaciones detalladas de tráficos sospechosos, mostrando IPs de origen y de destino, cuando el flujo comenzó o cuando terminó. Además, muestra que parámetro del perfil de amenaza fue superado: Bytes/s, Paquetes/s, Flujos/s o Direcciones IP/s.

Para generar un nuevo informe, accede a **Datos Históricos** → **Informes** → **Análisis de Amenazas** .

El formulario ya estará rellenado, pero podrás editarlo. Entonces, clica en el botón **Enviar**.

Tabla 2.5. Informe de Análisis de Amenazas

Campo	Descripción
Instante inicial	Rellena con el horario de inicio del periodo.
Instante final	Rellena con el horario de fin del periodo.
Filtro por subred	Selecciona **Ninguno** para no filtrar por Subred o selecciona la subred deseada.
Número de líneas	Establece un límite de líneas para la salida del informe.
Tipo de Ataque	Puedes escoger entre **Alto flujo de datos entre dos IPs**, **Alto flujo de datos entre dos IPs (Porta 0)**, **Amplificación de DNS**, **Amplificación de NTP**, **Amplificación de SNMP**, **ICMP Flood**, **IP Flood** y **Syn flood**.

Sugerencia

Puedes generar **informes de datos brutos** para obtener estadísticas detalladas y consolidadas para cada flujo. Para ello, basta clicar en el icono que aparece al lado de cada dirección IP.

Lista de IPs en blackhole

Esta pestaña muestra las direcciones IP que fueron anunciadas en blackhole manualmente o automáticamente.

Para cada IP, se mostrará una tabla conteniendo el horario en el que la IP tuvo un tráfico sospechoso detectado, el horario que fue anunciado en blackhole y el horario en que fue eliminado del blackhole.

Accediendo a **Sistema** → **Parámetros** → **Análisis de Amenazas** puedes configurar el período máximo, en minutos, en el que las direcciones IP continuarán siendo exhibidas en la lista después de su eliminación del blackhole.

Eliminando direcciones IPs de la lista de blackhole

Para eliminar direcciones IP del blackhole manualmente, clica en el icono mostrado en la columna **Ejecutar script de eliminación**.

Capítulo 3. Configuración

Perfil de amenaza

Puedes crear perfiles de amenaza y asociarlos a las subredes deseadas. En estos perfiles, definirás los límites de las tasas por segundo de los datos acumulados en el periodo configurado en **Sistema** → **Parámetros** → **Análisis de Amenazas** , así, en caso de que sean superados en alguna red asociada, una alarma será disparada.

Puedes configurar el perfil para detectar si se superaron los límites de **tráfico absoluto** y **ataques comunes** como SYN flood, ICMP flood, amplificación de DNS, amplificación de SNMP, amplificación de NTP y **ataques en la puerta 0**.

Para crear un nuevo perfil de amenaza, accede **Configuración** → **Perfiles de amenaza** y clica en el botón **Nuevo**.

Visualiza el histórico de configuración del perfil a través del botón **Histórico**.

Los perfiles pueden ser editados a través del botón **Editar** y eliminados con el botón **Borrar**:

Tabla 3.1. Formulario de Perfil de Amenaza

Campo	Descripción
Nombre	Define un nombre para el perfil.
Origen Mb/s	Límite de tasa de megabits por segundos enviados para un host para activar una alarma.
Destino Mb/s	Límite de tasa de megabits por segundos enviados para un host para activar una alarma.
Origen Paquete/s	Límite de tasa de paquetes por segundos enviados para un host para activar una alarma.
Destino Paquetes/s	Límite de tasa de paquetes por segundos enviados para un host para activar una alarma.
Origen Flujos/s	Límite de tasa de flujos por segundos enviados para un host para activar una alarma.
Destino Flujos/s	Límite de tasa de flujos por segundo recibidos por un host para activar una alarma.
Número de Direcciones IP de origen	Límite de conexiones hechas para un host en el periodo de 60 segundos.
Número de Direcciones IP de destino	Límite de conexiones recibidas por un host en el periodo de 60 segundos.
Threshold para syn flood (flujos/s)	Límite de tasa de flujos por segundo con la flag SYN para un único destino.
Threshold para ICMP flood (paquetes/s)	Límite de tasa de paquetes por segundo con la ICMP echo request para un único destino.
Threshold para amplificación de DNS (Mb/s)	Límite de tasa de megabits por segundo de DNS response para un único destino.

Campo	Descripción
Threshold para amplificación de SNMP (Mb/s)	Límite de tasa de megabits por segundo de SNMP response para un único destino.
Threshold para amplificación de NTP (Mb/s)	Límite de tasa de megabits por segundo de NTP response para un único destino.
Origen Mb/s - Puerta 0	Límite de tasa de megabits por segundos enviados para un host en la puerta 0 (cero).
Destino Mb/s - Puerta 0	Límite de tasa de megabits por segundos recibidos por un host en la puerta 0 (cero).
Origen Paquetes Mb/s - Puerta 0	Límite de tasa de paquetes por segundos enviados para un host en la puerta 0 (cero).
Destino Paquetes Mb/s - Puerta 0	Límite de tasa de paquetes por segundos recibidos por un host en la puerta 0 (cero).
Origen Flujos/s - Puerta 0	Límite de tasa de flujos por segundos enviados para un host en la puerta 0 (cero).
Destino Flujos/s - Puerta 0	Límite de tasa de flujos por segundos recibidos por un host en la puerta 0 (cero).
Direcciones IP excluidas del análisis	Rellena con las direcciones IP o subredes que serán excluidas del análisis de amenazas. Sepáralos por comas.
Subredes	Selecciona las subredes que harán parte de este perfil de amenaza.

Sugerencia

Para configurar los límites de las tasas, puedes usar las estadísticas de **Media** y **Máximo** exhibidas en la pantalla inicial de cada subred en **Datos Históricos** → **Subredes**

Añadir metadatos de perfiles de amenaza

Para acceder a la página de configuración de metadato, accede a **Configuración** → **Perfiles de amenaza** y clica en el botón **Metadato**.

Clica en el botón **Nuevo** para crear un nuevo metadato. Puede ser del tipo **Texto**, **Entero** o **Enum**.

Puedes alterar el metadato cuando desees usando el botón **Editar** y verificar el histórico de alteraciones a través del botón **Histórico**.

Para borrar un metadato, clica en el botón **Borrar**.

Tabla 3.2. Campos de un metadato

Campo	Descripción
Nombre	Nombre del metadato.
Descripción	Descripción del metadato.
Tipo de dato	Escoge si el metadato será del tipo **Texto**, **Entero** o **Enum**.

Campo	Descripción
Valores	Este campo solo está disponible si el **Tipo de dato** es **Enum**. Introduce una lista de valores, reparándolos por punto y coma (;).

Para asociar el metadato creado a un perfil de alarma, accede a la lista de perfiles y clica en el botón **Metadato** al lado del perfil de la alarma que será configurada.

Después, rellena los metadatos de acuerdo con el tipo. Puedes rellenar todos ellos o solo los que desees.

Scripts

Puedes crear y ejecutar scripts de los tipos: **Inicio de sesión** y **Blackhole**.

Los tipos de scripts aparecerán en una caja de selección en el menú lateral a la izquierda de la página. Al seleccionar uno de ellos, se instalarán los scripts ya existentes para este tipo.

Creando scripts

Para crear un nuevo script, clica en la señal de **+**. La caja de texto aparecerá con un ejemplo del tipo de script seleccionado. Edita la caja de texto y, después de eso, selecciona el modo de ejecución (**Lua**, **Send/Expect** o **Texto**, dependiendo del tipo de script), clica en **Ejecutar** y selecciona el objeto en el que el script será ejecutado.

Sugerencia

Puedes guardar o eliminar un script en cualquier momento utilizando los iconos que se encuentran encima de la caja de texto.

Funciones

El sistema suministra algunas funciones para dar más poder a los scripts:

- **tmlSnmp.snmpGet**: Ejecuta SNMP GET en el dispositivo.
- **tmlSnmp.snmpGet2**: Ejecuta SNMP GET en el dispositivo cuando la configuración SNMP no es la estándar.
- **tmlSnmp.snmpWalk**: Ejecuta SNMP WALK en el dispositivo.
- **tmlSnmp.snmpWalk2**: Ejecuta SNMP WALK en el dispositivo cuando la configuración SNMP no es la estándar.
- **tmlSSH.sshNew**: Se conecta a un servidor remoto a través de SSH.
- **tmlTelnet.telnetNew**: Se conecta a un servidor remoto a través de Telnet.
- **tmlUtils.processMapper**: Mapea los procesos del dispositivo.
- **tmlUtils.removeTerminalEscape**: Elimina caracteres de terminales.
- **tmlDebug.log**: Imprime el log en la pestaña **Debug** del **Resultado**.
- **tmlDebug.vardump**: Imprime el log de la variable en la pestaña **Debug** del **Resultado**.
- **tmlJson:encode**: Convierte una tabla en Lua en un JSON en texto libre.

- **tmlJson:decode**: Convierte un JSON en texto libre en una tabla en Lua.
- **tmlPing.pingNew**: Envía paquetes a través del protocolo ICMP.
- **tmlMsSql.msSqlNew**: Accede a dbms (Database Management System) Microsoft SQL server.
- **setTimeout**: Altera el timeout de la conexión.
- **tmlSocket.http**: Ejecuta solicitud HTTP. Para ello, basta con indicar una URL y un método. Los métodos válidos son **GET** y **POST** en caja alta.
- **tmlSequence.getNext**: Generar números secuenciales y sin repetición. Devuelve el valor actual sumado a 1 y la secuencia comienza con el número 1.
- **tmlBGP.addToBlackHole**: Agrega la subred al blackhole.
- **tmlBGP.removeFromBlackHole**: Elimina las subredes del blackhole.

Las funciones en Lua permitidas en los scripts son las siguientes:

- abs
- clock
- difftime
- exp
- floor
- ipairs
- max
- min
- next
- pairs
- pow
- sqrt
- time
- tonumber
- tostring
- type
- unpack

Variables

También existen variables que están disponibles en todos los scripts y son rellenadas de acuerdo con el objeto relacionado.

Ellas son almacenadas en la tabla params (params['variable_name']):

- **params['ipaddr']**: Dirección IP.
- **params['name']**: Nombre del dispositivo.
- **params['description']**: Descripción del dispositivo.
- **params['type']**: Tipo del dispositivo.
- **params['snmp']['community']**: Comunidad SNMP del dispositivo.
- **params['snmp']['version']**: Versión SNMP del dispositivo.
- **params['snmp']['timeout']**: SNMP Timeout del dispositivo.
- **params['snmp']['retries']**: Nuevas tentativas SNMP del dispositivo.
- **params['snmp']['max_per_packet']**: Número de OIDs por paquete.
- **params['snmp']['max_pps']**: Tasa máxima de envío de paquetes (pps).
- **params['snmp']['window']**: Ventana SNMP del dispositivo.
- **params['snmp']['port']**: Puerta SNMP del dispositivo.
- **params['mobj'][<MAPEADOR>][<DESCRIPCIÓN>]['ifindex']**: ifIndex del objeto mapeado, donde MAPEADOR es el nombre del mapeador y DESCRIPCIÓN es el nombre del objeto mapeado (sin el nombre del dispositivo).
- **params['mobj'][<MAPEADOR>][<DESCRIPCIÓN]['description']**: Descripción del objeto mapeado, donde MAPEADOR es el nombre del mapeador y DESCRIPCIÓN es el nombre del objeto mapeado (sin el nombre del dispositivo).
- **params['username']**: Nombre del usuario para autentificación.
- **params['passwd']**: Contraseña para autentificación.
- **params['enable_passwd']**: Contraseña de enable para autentificación.
- **params['protocol']**: Protocolo para conexión.
- **params['alarm']['active']**: Estatus de la alarma. Retorna **true** o **false**.
- **params['alarm']['name']**: Nombre de la alarma.
- **params['alarm']['urgency']**: Niveles de urgencia de la alarma.
- **params['alarm']['object']['name']**: Nombre del objeto alarmado.
- **params['alarm']['object']['description']**: Descripción del objeto alarmado.
- **params['alarm']['object']['type']**: En alarmas de dispositivo, es el tipo del dispositivo alarmado.
- **params['alarm']['object']['manufacturer']**: En alarmas de dispositivo, es el fabricante del dispositivo alarmado.
- **params['alarm']['object']['device']['name']**: En alarmas de objeto mapeado, es el nombre del dispositivo al cual el objeto mapeado alarmado pertenece.
- **params['alarm']['object']['device']['description']**: En alarmas de objeto mapeado, es la descripción del dispositivo al cual el objeto mapeado alarmado pertenece.

- **params['alarm']['object']['device']['type']**: En alarmas de objeto mapeado, es el tipo de dispositivo al cual el objeto mapeado alarmado pertenece.
- **params['alarm']['object']['device']['manufacturer']**: En alarmas de objeto mapeado, es el fabricante del dispositivo al cual el objeto mapeado alarmado pertenece.
- **params['blackhole']['ipaddr']**: Anuncio o eliminación del IP en blackhole.
- **params['connection']**: Objeto de conexión a un dispositivo.
- **params['metadata'][<NOMBRE_DE_METADATOS>]**: Valor de metadatos del dispositivo, donde NOMBRE_DE_METADATOS es el nombre de los metadatos.

Ejecutando scripts

Para ejecutar algún script ya creado, clica en él en el menú a la izquierda. Puedes editarlo usando la caja de texto. Entonces, clica en **Ejecutar** y selecciona el objeto en el que el script será ejecutado.

Además, es posible acompañar los detalles de la última ejecución usando la pestaña **Resultado** dispuesta en el final de la página.

Sugerencia

Es posible guardar las alteraciones realizadas en el script clicando en el icono de guardar, que se encuentra encima de la caja de texto.

Script de Inicio de Sesión

Este tipo de script se usa para hacer la autentificación cuando el protocolo de conexión de un dispositivo es del tipo **Telnet**, una vez que, al contrario del SSH, no posee una capa propia de autentificación.

Ve a continuación el ejemplo del script de autentificación Cisco Telnet escrito en el modo Lua.

```
c = params['connection']
u = params['username']
p = params['passwd']

if (c:send(u) == false) then
 return nil
end
if (c:expect('Pass') == false) then
 return nil
end
if (c:send(p) == false) then
 return nil
end
if (c:expect('>') == false) then
 return nil
end
```

Script de Blackhole

Este tipo de script es utilizado para hacer el anuncio de direcciones IP en la lista blackhole, bien como para retirarlos.

Puede ser escrito de tres modos: **Texto**, **Lua** y **Send/Expect**.

En **Configuración → Blackhole**, asociarás un dispositivo a dos scripts de este tipo, uno para el anuncio de los IPs en blackhole y otro para eliminar.

En **Sistema → Parámetros → Análisis de Amenazas** puedes configurar el período máximo, en minutos, en el que una dirección IP quedará en blackhole antes que este script de eliminación se ejecute.

El script a continuación ya viene configurado en el TRAFwatcher y es un script genérico para dispositivos Cisco.

```
c = params['connection']
c:setTimeout(10)

if(c:send('enable') == false) then
  return false
end
if(c:expect('Password:') == false) then
  return false
end
if(c:send(params['enable_passwd']) == false) then
  return false
end
if(c:expect('#') == false) then
  return false
end

if(c:send('conf t') == false) then
  return false
end
if(c:expect('(config)') == false) then
  return false
end

for k,v in pairs(params['blackhole']) do
 if (c:send('ip route ' .. k .. ' 255.255.255.255 Null0') == false) then
  return false
 end
 if (c:expect('(config)') == false) then
  return false
 end
end

if (c:send('router bgp XXX') == false) then
 return false
end
if (c:expect('(config-router)') == false) then
 return false
end

for k,v in pairs(params['blackhole']) do
   if (c:send('network ' .. k .. ' mask 255.255.255.255
 route-map blackhole') == false) then
```

```
  return false
 end
 if (c:expect('(config-router)') == false) then
  return false
 end
end
if (c:send('route-map blackhole permit 10') == false) then
   return false
end
if (c:expect('(config-route-map)') == false) then
   return false
end

if (c:send('set community 6939:666') == false) then
   return false
end
if (c:expect('(config-route-map)') == false) then
   return false
end
if (c:send('end') == false) then
   return false
end
if (c:expect('#') == false) then
   return false
end
```

Wildcards

Tabla 3.3. Lista de wildcards

Variables	Descripción
%username%	Campo de usuario del formulario de configuración del dispositivo.
%passwd%	Campo de contraseña de usuario del formulario de configuración del dispositivo.
%enable_passwd%	Habilitar campo de contraseña del formulario de configuración del dispositivo.
%blackhole_ipaddr%	Dirección IP que se anunciará en Blackhole.
%blackhole_ipaddr_mask_N%	Bloque de red de la dirección IP que se anunciará en Blackhole con la máscara N aplicada a él.

Blackhole

Asocia scripts para anunciar y eliminar direcciones IP del blackhole, o sea, de la lista de IPs sospechosos.

Tabla 3.4. Formulario de Blackhole

Campo	Descripción
Tipo de ejecución	Selecciona **Manual** para anunciar una determinada dirección IP en Blackhole manualmente a través del

Campo	Descripción
	Informe de Análisis de Amenazas o **Automático** para que el sistema anuncie automáticamente todas las direcciones IP en Blackhole.
Script	Selecciona el script que anunciará una dirección IP en blackhole.
Script de eliminación	Selecciona el script que eliminará la dirección IP del blackhole.
Dispositivo	Selecciona el dispositivo deseado.

Capítulo 4. ALARMmanager

Informes

Para acceder a los informes ALARMmanager, ves a **ALARMmanager → Informes**

Informes eliminados

Este informe suministra los logs de todas las operaciones de eliminación realizadas por los usuarios.

Tabla 4.1. Formulario de informe de alarmas eliminadas

Campo	Descripción
Formato de salida	Selecciona uno de los formatos para el informe: HTML, CSV o PDF.
Tipo de objeto	El tipo de objeto para la alarma.
Instante inicial	El instante inicial para el informe.
Instante final	El instante final para el informe.
Operación	Filtro para operación de eliminación.
Filtro de usuario	Filtra por el usuario que ejecutó la operación.
Filtro de objeto	Filtra por el objeto en que la operación se ejecutó.
Filtro de alarma	Filtra por la alarma en que la operación se ejecutó.

Informes consolidados

Este informe suministra una visión de todos los eventos de alarma de manera detallada o resumida.

Este informe puede ser guardado como un modelo. Para instrucciones sobre como trabajar con modelos de informes, ves a la sección modelos en este manual.

Tabla 4.2. Formulario de alarmas consolidadas

Campo	Descripción
Filtro de alarma	Usa expresión regular y clica en el botón Filtrar para seleccionar la alarma deseada.
Filtro de objeto	Usa expresión regular para filtrar los objetos deseados.
Fabricante	Filtra por el fabricante del objeto. Tienes que usar expresión regular para filtrar.
Tipo de fabricante	Filtrar por el tipo de fabricante. Tienes que usar expresión regular para filtrar.
Tipo de objeto analizado	Tipo do objeto.
Filtro ifAlias	Filtra basándose en la interfaz OID ifAlias. Debes usar expresión regular para filtrar.
Instante inicial	Periodo inicial de análisis.

Campo	Descripción
Instante final	Periodo final de análisis.
Periodo	Si la opción **Día todo** está marcada, este campo es ignorado, en caso contrario, el dato es seleccionado con aquel intervalo para cada día.
Excluir fines de semana	Excluir periodo de fines de semana en el informe de datos.
Solamente activos	Muestra solo las alarmas activas.
Consolidado	Esta opción resumirá todas las incidencias de alarma para cada objeto.
Solamente generados por trap	Muestra solo alarmas generadas por traps **link down**.
Formato de salida	Selecciona uno de los formatos para el informe: HTML, PDF o CSV.
Grupos	Este campo puede ser usado para filtrar objetos asociados solo a algunos grupos de root.

Sugerencia

Para ordenar los resultados del informe, clica en cada encabezado de la columna.

Modelo de correo electrónico

Introducción

Puedes seleccionar el formato del correo electrónico de ALARMmanager y escoger si deseas utilizar el modelo estándar o personalizarlo.

Tabla 4.3. Modelo de correo electrónico

Campo	Descripción
Habilitar modelo del correo electrónico estándar	Selecciona **No** para personalizar el modelo del correo electrónico.
Contenido del correo electrónico	Puedes escoger el formato de correo electrónico que recibirás (HTML o Txt).

Personaliza el correo electrónico

Cuando estás editando tu modelo de correo electrónico, es posible restaurar el modelo solo clicando en el modelo **Restaurar modelo estándar**.

Si el contenido del correo electrónico está en formato HTML, puedes ver una previsualización antes de guardar el nuevo modelo. Para hacer esto, clica en el botón **Preview**.

Tendrás las siguientes palabras clave entre '**$**' y puedes sustituirlas para tu configuración de alarma:

Tabla 4.4. Variables del correo electrónico

Variables	Descripción
$date$	Fecha de activación/desactivación de la alarma.

Variables	Descripción
$objtype$	Tipo do objeto: Objeto mapeado o Device. Alarma de servicio no posee tipo de objeto.
$object$	Nombre del objeto.
$path$	Exhibe el camino para el objeto en el SLAView.
$alarm$	Nombre de la alarma.
$action$	Estado de la alarma: activado o desactivado.
$level$	Niveles de urgencia de la alarma.
$formula$	Fórmula de la alarma.
$varbind$	Varbind.
$suppressed$	Indica si la alarma fue suprimida.
$color$	Variable para ser usada en el correo electrónico HTML. Verde para desactivado y rojo para activado.

Niveles de urgencia de alarma

Los niveles de urgencia en la aplicación ALARMmanager son personalizados y puedes configurar todos los que quieras.

Para gestionar los niveles de alarma, accede al menú **ALARMmanager → Niveles de urgencia de alarma**

Aquí posees una lista de niveles preconfigurados. Puedes editar niveles y añadir otros.

Cambiando el nivel de prioridad de urgencia

Para cambiar el nivel de prioridad de urgencia, selecciona el nivel deseado y clica en las flechas UP o DOWN localizadas en la esquina superior izquierda.

Añade un nuevo nivel de urgencia

Para añadir un nivel de urgencia, clica en el botón Nuevo y rellena el formulario.

Tabla 4.5. Formulario de nivel de urgencia de alarma

Campo	Descripción
Rótulo	Define un subtítulo para el nivel de urgencia. Se mostrará en una columna de la consola ALARMmanager.
Color del plano de fondo	El color de plano de fondo que se mostrará en la consola ALARMmanager.
Color de texto	Color del texto que se mostrará en la consola ALARMmanager.
Aviso sonoro	Habilita el sonido de aviso para esta alarma. El sonido de aviso sonará en la consola del ALARMmanager, cuando esta función también este habilitada en la consola. Habilítala en

Campo	Descripción
	ALARMmanager → **Consola** → **Habilitar aviso sonoro** .
Alarmas	Selecciona las alarmas que recibirán esta prioridad.
Alarmas de servicio	Selecciona las alarmas de servicio que recibirán esta prioridad.

Añade metadatos de nivel de urgencia

Para acceder a la página de configuración de metadato, accede a **ALARMmanager** → **Niveles de urgencia de alarma** y clica en el botón **Metadato**.

Clica en el botón **Nuevo** para crear un nuevo metadato. Puede ser del tipo **Texto**, **Entero** o **Enum**.

Puedes alterar el metadato cuando desees usando el botón **Editar** y verificar el histórico de alteraciones a través del botón **Histórico**.

Para borrar un metadato, clica en el botón **Borrar**.

Tabla 4.6. Campos de un metadato

Campo	Descripción
Nombre	Nombre del metadato.
Descripción	Descripción del metadato.
Tipo de dato	Escoge si el metadato será del tipo **Texto**, **Entero** o **Enum**.
Valores	Este campo solo está disponible si el **Tipo de dato** es **Enum**. Introduce una lista de valores, separándolos por punto y coma (;).

Para asociar un metadato creado a un nivel de urgencia, accede a la lista de niveles y clica en el botón **Metadato** al lado del nivel que será configurado.

Después, rellena los metadatos de acuerdo con el tipo. Puedes rellenar todos ellos o solo los que desees.

Alarmas

El TRAFwatcher ya viene con ocho alarmas del tipo **Posible amenaza** preconfiguradas: **DNS Amplification threshold reached**, **ICMP Flood threshold reached**, **IP Flood threshold reached**, **NTP Amplification threshold reached**, **Port 0 threshold reached**, **SNMP Amplification threshold reached**, **Syn Flood threshold reached** y **Traffic threshold reached**.

No puedes borrar estas alarmas, pero sus campos pueden ser editados.

Tabla 4.7. Formulario de alarma TRAFwatcher

Campo	Descripción
Nombre	Nombre de la alarma.
Tipo de alarma	Clasificación de la alarma.

Campo	**Descripción**
Varbind	Campo de texto libre que puede ser usado para reconocer las alarmas que son encaminadas como traps.
Correo electrónico	Un correo electrónico será enviado a los usuarios. El servidor SMTP debe ser configurado, así como el correo electrónico de cada usuario en el formulario de configuración del usuario.
Dispositivo móvil (SMS)	Mensajes más cortos que los enviados por correo electrónico. Esta alarma puede ser enviada a un correo electrónico por el gateway de SMS si el campo de SMS está configurado en el siguiente formato: 88888888@operador.com. Si el SMS es un número de teléfono, los protocolos SMPP o HTTP también pueden ser usados para enviar el mensaje. Para hacer esto, necesitas configurar el siguiente ítem: **Sistema** → **Parámetros** → **Servidor SMS** .
Dispositivo móvil (Telegram)	Un mensaje será enviado a un chat del Telegram por un bot. Para configurar esta funcionalidad, debes crear un bot en el Telegram, para hacerlo, una vez en el Telegram, inicia una conversación como el usuario @BotFather. Escoge la opción/newbot y sigue las instrucciones para finalizar la creación del bot. Al terminar anota el token del bot Telegram. Asocia el bot al chat en el que los mensajes serán enviados. Accede al formulario de perfil de usuarios, rellena el campo "Token del bot Telegram" y clica en Validar. Si todo va bien, el campo "ID del chat Telegram" será automáticamente rellenado. El mensaje será enviado después de los segundos definidos en el campo **Enviar mensaje después de**, iniciando por el tiempo de activación de la alarma.
Trap	Una trap se enviará para cada alarma.
Enviar correo electrónico después de (minutos)	El correo electrónico será enviado después del número de minutos definido en este campo, a partir del horario de activación.
Enviar mensajes de dispositivo móvil después de (minutos)	los mensajes móvil serán enviados después del número de minutos definido en este campo, a partir del horario de activación.
Enviar trap después de (minutos)	La trap será enviada después del número de minutos definido en este campo, a partir del horario de activación.
Deshabilitar correo electrónico para la alarma eliminada	Si la opción "No" es seleccionada, el correo electrónico será enviado y la condición de eliminado será indicada en él. La opción "Sí" evitará que el correo electrónico sea enviado.

Campo	Descripción
Deshabilitar sms para alarma eliminada	Si la opción "No" es seleccionada, el sms será enviado y la condición de eliminado será indicada en él. La opción "Sí" evitará que el sms sea enviado.
Deshabilitar trap para la alarma eliminada	Si la opción "No" es seleccionada, la trap será enviada y la condición de eliminada será indicada en ella. La opción "Sí" evitará que la trap sea enviada.
Nivel de urgencia	Selecciona un nivel de urgencia para la alarma.
Perfiles de Alarma	Selecciona los perfiles de alarma a los cuales esta alarma pertenecerá.

Añadiendo metadatos de alarma

Para acceder a la página de configuración de metadato, accede a **Alarmas** → **Alarmas** y clica en el botón **Metadato**.

Clica en el botón **Nuevo** para crear un nuevo metadato. Puede ser del tipo **Texto**, **Entero** o **Enum**.

Puedes alterar el metadato cuando desees usando el botón **Editar** y verificar el histórico de alteraciones a través del botón **Histórico**.

Para borrar un metadato, clica en el botón **Borrar**.

Tabla 4.8. Campos de un metadato

Campo	Descripción
Nombre	Nombre del metadato.
Descripción	Descripción del metadato.
Tipo de dato	Escoge si el metadato será del tipo **Texto**, **Entero** o **Enum**.
Valores	Este campo solo está disponible si el **Tipo de dato** es **Enum**. Introduce una lista de valores, separándolos por punto y coma (;).

Para asociar un metadato creado a una alarma, accede a la lista de alarmas y clica en el botón **Metadato** al lado de la alarma que será configurada.

Después, rellena los metadatos de acuerdo con el tipo. Puedes rellenar todos ellos o solo los que desees.

Perfiles de alarma

Los perfiles de alarma son usados para juntar las alarmas y los objetos controlados.

Para configurar un perfil de alarma, ves a **ALARMmanager** → **Perfil de alarmas**, clica en el botón **Nuevo** y rellena el formulario.

Tabla 4.9. Formulario de perfil de alarma

Campo	Descripción
Nombre	Texto descriptivo para un perfil de alarma.

Campo	Descripción
Alarma	Selecciona las alarmas que pertenecerán a este perfil.
Subred	Selecciona las subredes que pertenecerán a este perfil.

Añadiendo metadatos de perfil de alarma

Para acceder a la página de configuración de metadato, accede a **Alarmas** → **Alarmas** y clica en el botón **Metadato**.

Clica en el botón **Nuevo** para crear un nuevo metadato. Puede ser del tipo **Texto**, **Entero** o **Enum**.

Puedes alterar el metadato cuando desees usando el botón **Editar** y verificar el histórico de alteraciones a través del botón **Histórico**.

Para borrar un metadato, clica en el botón **Borrar**.

Tabla 4.10. Campos de un metadato

Campo	Descripción
Nombre	Nombre del metadato.
Descripción	Descripción del metadato.
Tipo de dato	Escoge si el metadato será del tipo **Texto**, **Entero** o **Enum**.
Valores	Este campo solo está disponible si el **Tipo de dato** es **Enum**. Introduce una lista de valores, separándolos por punto y coma (;).

Para asociar el metadato creado a un perfil de alarma, accede a la lista de perfiles y clica en el botón **Metadato** al lado del perfil de la alarma que será configurada.

Después, rellena los metadatos de acuerdo con el tipo. Puedes rellenar todos ellos o solo los que desees.

Consola

Introducción

El aplicativo ALARMmanager trabaja de forma integrada entre los sistemas y es capaz de general alarmas basadas en fórmulas.

También posee los siguientes recursos:

- Interfaz gráfica en HTML5.
- Alarma a través de correo electrónico, mensajes de dispositivo móvil y traps.
- Las alarmas pueden emitir sonidos.
- Perfiles de alarma para facilitar la asociación de alarmas a los objetos gestionados.
- Reconocimiento de alarmas y comentarios.

- Eliminación de alarmas para evitar correos electrónicos, mensajes de dispositivo móvil y traps para alarmas repetidas.

Operación de Consola

Para acceder a la consola operacional de alarma, va a **ALARMmanager → Consola**

Autentificación

Un usuario debe estar autentificado para acceder al ALARMmanager.

Consola

La consola del ALARMmanager mostrará todas las alarmas activas y también desactivadas que todavía no fueron desactivados por el parámetro de periodo de almacenamiento del ALARMmanager. Las alarmas que puedes visualizar dependerán del permiso que su usuario posea.

La consola posee las siguientes columnas:

Tabla 4.11. ALARMmanager consola

Columna	Descripción
INICIO	El momento de la primera incidencia
TÉRMINO	El momento de la última incidencia Muestra ACTIVO si la alarma todavía no terminó.
USUARIO	Usuario que programó la alarma.
TIPO	Tipo de objeto, puede ser dispositivo u objeto mapeado.
OBJETO	Nombre del objeto.
DESCRIPCIÓN	Si el objeto es una interfaz, muestra su ifAlias.
CAMINO	Muestra el primer camino para el objeto en los grupos SLAview.
ESTADO	Estado de la alarma, puede ser activo o inactivo.
ALARMA	Nombre de la alarma.
NIVEL	El nivel de la alarma definido en configuración de nivel.
TRAP	Sí, si fue generado por un trap y no en cualquier otro caso.
COMENTARIOS	Comentario del operador. Para introducir un comentario, clica dos veces en aquella célula.

Reconocimiento de alarma

Cuando la alarma es reconocida, la línea de alarma muestra el nombre del usuario que ejecutó la operación y su información también pude verse en informes de alarmas consolidadas. Después de reconocer una alarma, puedes ser capaz de introducir comentarios para la alarma.

Para el reconocimiento de alarma, clica con el botón derecho en él y después selecciona la opción Reconocer alarmas en el menú. La alarma se muestra después en la tabla de alarmas reconocidas para todos los operadores.

Para múltiples reconocimientos de una vez, selecciona con el botón izquierdo del ratón y después clica con el botón derecho en la lista para mostrar el menú.

La alarma puede ser liberada del operador solo por el usuario administrador. Para ello, el administrador debe seleccionar la alarma de reconocimiento en la lista y seleccionar la opción de alarma Liberar alarmas en el menú.

Eliminación de alarma

Para eliminar una alarma, sigue el siguiente procedimiento:

1. Selecciona la alarma deseada con el botón izquierdo del ratón. Para escoger más de una alarma, asegura la tecla CTRL y selecciona las alarmas con el botón izquierdo del ratón.
2. Clica con el botón derecho del ratón para mostrar el popup menú. Clica en la opción Eliminar alarmas en el popup menú.
3. Rellena la caja de texto con la razón de la eliminación. También puedes dejarlo en blanco.
4. Clica en el botón Confirmar.

Puedes comprobar las operaciones de eliminación de log ejecutadas por los usuarios en informe de alarmas eliminados.

Comentario de alarmas

Para introducir comentarios para una alarma, en primer lugar necesitas reconocerla.

Para introducir un comentario, sigue el procedimiento siguiente:

1. Clica en la tabla "Reconocidos".
2. Da un clic doble en la columna COMENTARIOS para la alarma.
3. Rellena la caja de texto en la ventana Comentarios de Alarma y clica en el botón Confirmar.

Habilitar sonido para una alarma

El sonido de la alarma funcionará si esta activa, no reconocido, Critical o Major en la consola ALARMmanager.

Selecciona la opción **ALARMmanager** → **Consola** → **Habilitar aviso sonoro** .

Sincronización de alarma

El ALARMmanager sincroniza tus alarmas con el banco de datos del sistema cada 2 minutos. Esta sincronización puede accionarse inmediatamente en el menú **ALARMmanager** → **Consola** → **Sincronizar alarmas** .

Eliminando alarmas

El ALARMmanager borra automáticamente las alarmas que hayan terminado, pero puedes visualizarlas después en la consola hasta que el almacenamiento máximo de alarmas inactivas haya pasado. Para configurar este parámetro ves al menú **Sistema** → **Parámetros** → **ALARMmanager** .

El operador puede borrar las alarmas en cualquier momento si están en estado inactivo, seleccionando las alarmas con el botón derecho en el ratón y clicando en la opción Borrar en el popup menú.

Abrir gráficos

Selecciona una línea de alarma y clica en el botón Abrir gráficos para abrir los gráficos del objeto.

Filtro de alarma

Este filtro puede accionarse para cualquier objeto en cualquier mapa. Esto filtrará las alarmas de los objetos y también de los objetos relacionados a él jerárquicamente.

Sugerencia

Los niveles de urgencia se muestran en el final de la página. Al clicar en alguno de ellos, se filtrarán todas las alarmas de este nivel. Al clicar nuevamente en el nivel, el filtro es eliminado.

Capítulo 5. Sistema

Registro de acceso

Acceso de usuario

Esta opción muestra un informe resumido por día que contiene el registro de acceso de los usuarios. Cada línea del informe es un enlace a un informe diario detallado.

Acceso simultáneo

Este informe muestra el número de usuarios que están conectados en el sistema en cada grupo de usuario.

Copia de Seguridad/Restaurar

Puedes ejecutar una copia de seguridad y restaurar todos los datos del sistema de cualquier servidor fijo o descargar/subir un archivo simple con todas las configuraciones del sistema.

Va en **Sistema** → **Copia de seguridad/Restaurar** para trabajar con las siguientes opciones de copia de seguridad/restaurar:

Copia de seguridad local de configuración

Clica en este icono para mostrar todos los archivos de copia de seguridad de configuración.

Puedes crear un nuevo archivo clicando en el botón Crear nuevo.

El botón Configurar se usa para seleccionar el número de archivos que se mantendrán.

Clica en el botón Descarga para hacer la descarga de un archivo de configuración para tu escritorio.

El botón Copiar a Restaurar se usa para copiar un archivo de configuración en el área de restaurar para que pueda ser restaurado.

Restauración local de configuración

Esta opción se usa para restaurar un archivo de copia de seguridad. Haciendo esto, todas las configuraciones actuales del sistema se sustituirán por las definiciones contenidas en el archivo restaurado.

Para ejecutar una restauración del sistema debes subir el archivo de configuración de tu ordenador local o copiar un archivo de copia de seguridad antiguo disponible en el sistema y después clicar en el botón Restaurar para ese archivo.

Copia de seguridad Remota

Esta opción puede ser usada para guardar los archivos de configuración y datos históricos del sistema en un servidor de copia de seguridad remoto. Seleccione el tipo de protocolo que desea utilizar para realizar una copia de seguridad remota. Las opciones disponibles son los protocolos FTP y S3.

Tabla 5.1. Copia de seguridad remota utilizando un servidor FTP

Campo	Descripción
Versión de IP	Escoge si es IPv4 o IPv6
Servidor de copia de seguridad	Dirección de IP del servidor de copia de seguridad.
Directorio de copia de seguridad	Directorio en el servidor de copia de seguridad.
Usuario	Usuario a ser autentificado en el servidor de copia de seguridad.
Contraseña del usuario	Contraseña.
Protocolo utilizado en la copia de seguridad	Protocolo para ser usado en las copias de seguridad.
Puerta utilizada por el protocolo	Número de la puerta.
Tamaño del servidor (GB)	Tamaño del servidor en Gigabytes.
Activar copia de seguridad	Selecciona **Sí** para activar el recurso de copia de seguridad
Hora para realizar la copia de seguridad	Selecciona el momento del día para que se ejecuten las copias de seguridad.

Tabla 5.2. Copia de seguridad remota utilizando un servidor S3

Campo	Descripción
Versión de IP	Escoge si es IPv4 o IPv6
Directorio de la copia de seguridad	Directorio en el servidor de copia de seguridad.
Tamaño del servidor (GB)	Tamaño del servidor en Gigabytes.
Activar copia de seguridad	Selecciona **Sí** para activar el recurso de copia de seguridad
Hora para realizar la copia de seguridad	Selecciona el momento del día para que se ejecuten las copias de seguridad.
Clave de acceso	Clave de acceso de usuario.
Llave secreta	Llaves secretas de usuario.
Nombre del bucket	Nombre del bucket donde se almacenan las copias de seguridad.
Host base	URL do Servidor S3.
Host bucket	URL de estilo alojado virtual.

Restauración Remota

Selecciona un único sistema para ejecutar la restauración de los datos o clica Requerir la restauración completa para buscar datos de todos los sistemas.

Importante

- El servidor ftp debe estar en línea, ya que los datos se buscan en él.
- Solo ejecute esta operación durante la instalación de un TRAFip o SLAview nuevos y vacíos, ya que todos los datos serán sustituidos.

Situación de restauración

Esta opción mostrará el estatus de restauración cuando se solicite una operación de restauración remota.

Parámetros

Esta sección se usa para configurar varios parámetros del sistema que no son usados por diferentes procesos.

Active directory

Esta opción hace posible que los usuarios inicien sesión en el RAFip usando el método de autentificación Active Directory Kerberos.

Para que un usuario sea autentificado por este método, es necesario que el TRAFip este configurado.

Tabla 5.3. Formulario de Active directory

Campo	Descripción
Habilitar autentificación por el Active Directory	Cuando la opción **Sí** este seleccionada, el campo **Autentificación local** aparecerá en el formulario de usuario.
Servidor	Escribe la dirección del servidor Active Directory. Ejemplo: kerberos.example.com
Dominio	Escribe el domino del Active Directory. Ejemplo: ATHENAS.MIT.EDU

Cuando este método está activado, no existe autentificación local, o sea, cualquier usuario que no sea del tipo **Administrador** inicia sesión por el TACACS.

> **Importante**
> El usuario **Administrador** tiene la opción de elegir iniciar sesión localmente o no, de todas formas, se recomienda que haya siempre una cuenta de **Administrador** con **Autentificación local** activada, en el caso de que sea utilizado el control de acceso externo.

Agentes de asociación

Configura los períodos adecuados para cada tipo de asociación automática se ejecute. Esto sucederá dos veces al día.

Tabla 5.4. Formulario de agente de asociación automática

Campo	Descripción
Primer horario de ejecución	Escoge el horario para que se realice la primera ejecución.
Segundo horario de ejecución	Escoge el horario para que se realice la primera ejecución.

Análisis de amenazas

En esta sección, configurarás los parámetros de detección de amenazas.

Tabla 5.5. Formulario de parámetros del Análisis de amenazas

Campo	Descripción
Ventana de tiempo para descartar flujos (seg)	Es el límite de tiempo, en segundos, para acumular tráfico, o sea, este límite define el periodo en que los análisis suceden. En este caso, solo se considerarán los datos con diferencia de tiempo entre el primero y el último que estén dentro de este límite.
Porcentaje mínimo para caracterización del tráfico	Cuando este en arquitectura distribuida, puede establecerse que el tráfico sea caracterizado como sospechoso en los recolectores cuando solo se alcance un porcentaje del total de los thresholds. Define este porcentaje mínimo usando este campo.
Tolerancia de diferencia entre horario local y del exportador (en segundos)	Define el tiempo de tolerancia, en segundos, para considerar que un determinado flujo está dentro del periodo que se está analizando y no sea descartado. El valor mínimo que puede rellenarse debe ser **60**.
Período máximo de almacenamiento de Tráfico sospechosos (días)	Configura el máximo periodo de tiempo, en días, en el que los eventos de tráfico sospechoso serán almacenados en el sistema.
Intervalo para rodar script para deshabilitar blackhole (m)	Período, en minutos, en el que una dirección IP estará en blackhole antes de que un script de remoción la retire.
Máximo permitido de IPs alarmados	Define un límite para la cantidad de IPs alarmados. Cuando este valor se supere, significa que el perfil de amenaza está mal configurado para la subred con muchos IPs alarmados. Entonces, se muestra un Warning al lado del Logotipo. Este parámetro preserva el rendimiento del sistema.
Número de amenazas que serán exhibidas	Define el número de amenazas que serán exhibidas en el Panel de Control.
Período máximo de almacenamiento de IPs retirados del blackhole (min)	Configura el máximo periodo de tiempo, en minutos, en el que los IPs retirados del blackhole serán almacenados en el sistema.

Importante

Se necesita habilitar el análisis de amenazas en el formulario de cada subred deseada.

Almacenamiento de datos

En esta área, puedes configurar el almacenamiento de espacio que debería ser colocado para cada tipo de dato del sistema.

El campo **Espacio de distribución disponible** mostrará el espacio que todavía puede ser distribuido.

Para comprobar cuanto espacio de cada área está siendo consumido, debes iniciar sesión en el sistema deseado (TRAFip, SLAview o CFGtool) y acceder a **Sistema** → **Diagnósticos** → **Almacenamiento de datos** . El ítem del banco de datos TDB corresponde a los datos resumidos para cada tipo de sistema.

Puedes realizar la redistribución de espacio de almacenamiento entre diferentes áreas en cualquier momento.

Tabla 5.6. Formulario de almacenamiento de datos

Campo	Descripción
Iniciar proceso a partir de la ocupación en %	Cuando este valor se alcance, el proceso de limpieza se ejecutará de acuerdo con el tipo de ejecución configurada. Rellena un valor entre **1** y **85**.
Tipo de ejecución	Escoge si un agente funcionará a cada **Intervalo de tiempo** o en un **Horario programado.**
Intervalo de tiempo para ejecución (minutos)	Define el intervalo de tiempo, en minutos, para la ejecución del agente. El valor mínimo es **10**.
Horario de ejecución	Define el horario en el que se realice la ejecución del agente.
Espacio disponible para los archivos SYSLOG	Almacenamiento dedicado para datos brutos de archivos SYSLOG.
Espacio disponible para los archivos de Informes programados	Almacenamiento dedicado a informes programados.
Trap receiver storage	Almacenamiento dedicado para archivos de Trap receiver.
Espacio disponible para archivos de captura	Almacenamiento dedicado a archivos de captura.
Limpiar datos históricos	Habilita la eliminación del datos históricos antiguos.
Limpiar alarmas	Habilita la eliminación del historial de alarmas antiguas.
Datos brutos del TRAFip	Área de almacenamiento destinada a los archivos de datos brutos del TRAFip. Este almacenamiento normalmente crece mucho más rápido que los datos resumidos. De esta forma, si los configuras con el mismo tamaño que los datos resumidos, vas a terminar con 10 veces menos datos históricos.
Datos resumidos del TRAFip	Almacenamiento dedicado para el TRAFip, datos procesados o TDB - Telco database. Este dato se usa para gráficos e informes TOPN.
Archivos de resumen remoto del TRAFip	Almacenamiento dedicado a los datos procesados del TRAFip enviados por los recolectores en un ambiente de arquitectura distribuida.
Datos de alteración de comportamiento del TRAFip	Almacenamiento dedicado para los datos de alteración de comportamiento, como datos de alarmas históricas, por ejemplo.
Datos brutos del SLAview	Almacenamiento dedicado para datos brutos del SLAview. Esto es, en general, de las recolectas SNMP de las OIDs.
Datos resumidos del SLAview	Almacenamiento dedicado para datos procesados del SLAview. Este dato se usa para gráficos e informes.
Archivos de resumen remoto SLAview	Almacenamiento dedicado a los datos procesados para los archivos de los datos SLAview enviados por los recolectores en un ambiente de arquitectura distribuida.

Campo	Descripción
Datos de alteración de comportamiento del SLAview	Almacenamiento dedicado para los datos de alteración de comportamiento, como datos de alarmas históricas, por ejemplo.
Datos de versiones del CFGtool	Almacenamiento dedicado para versiones de configuraciones de los dispositivos. Aunque este valor sea superado, los datos de versión de dispositivos con solo una versión no se excluirán.

Cuando los campos **Datos brutos (MB)** y **Datos resumidos (MB)** están rellenados con '**0**' (cero), significa que el sistema está distribuyendo de manera automática el **Espacio disponible para distribución** entre los **Datos brutos del TRAFip**, **Datos brutos del SLAview**, **Datos resumidos del TRAFip** y **Datos resumidos del SLAview**.

Puedes configurar manualmente estos valores, pero no olvides que los datos brutos tienden a crecer mucho más rápido que los datos resumidos. Para redistribuir los espacios, divide el valor de **Espacio disponible para distribución** por 4. Así, tendrás el valor de cada espacio.

Atención

Si reduces el espacio de almacenamiento de cualquiera de estas áreas, la próxima vez que el recolector de papelera sea ejecutado, limpiará los datos para adecuar el espacio de almacenamiento.

Arquitectura distribuida

Estos parámetros deben ser usados si deseas ejecutar el sistema en el modo de arquitectura distribuida.

Para más detalles de la arquitectura distribuida ves a sección arquitectura distribuida.

Tabla 5.7. Formulario de los parámetros de la arquitectura distribuida

Campo	Descripción
Número máximo de fallos consecutivos del recolector	Este número representa cuantas veces el nudo de la central esperará los archivos procesados de un nudo del recolector mientras este nudo se considere desactivado. Esta comprobación se realiza cada 5 minutos por un proceso de control para los sistemas TRAFip y SLAView. Después que el recolector está definido como deshabilitado por el nudo central, el recolector de copia de seguridad, si está definido, sustituirá las operaciones con los recolectores defectuosos.
Habilitar arquitectura distribuida	Selecciona esta opción si el appliance será parte de un sistema de arquitectura distribuida.
¿Es recolector?	Marque **Sí** en esta opción si el appliance tendrá un papel de recolector en el sistema. En el caso contrario este appliance será considerado un nudo central.
Llave del recolector	Rellena con una string de identificación para identificar este recolector en el nudo central.
Versión de IP	Escoge si es IPv4 o IPv6

Campo	Descripción
IP de la consolidadora	Rellena con la dirección IP del appliance para que sea usado como nudo central.
Contraseña	Contraseña usada para autentificación

Aviso de Expiración

Configura cuantos días antes de la expiración de la licencia se te recordará sobre ella.

Tabla 5.8. Formulario de aviso de expiración

Campo	Descripción
Alterar expiración faltando	Define un valor entre 10 y 30.

Copia de seguridad

- Datos: Parámetros para ejecutar copia de seguridad remota.. Vea la sección copia de seguridad remota.
- Configuración: configura el número de antiguas configuraciones de las copias de seguridad de los archivos para mantener en el sistema.

BGP

Anuncie o quita rutas de sus tablas de enrutamiento

Tabla 5.9. Formulario BGP

Campo	Descripción
Habilitar BGP	Seleccione esta opción si desea anunciar o quitar una ruta.
Identificador BGP	Valor entero que identifica únicamente el emisor.
Número de AS local	Número del AS del emisor.
Número de AS del peer	Número del AS del receptor.
Ip del peer	IP del router del AS receptor.
Comunidad BGP	Conjunto de etiquetas genéricas que se pueden utilizar para señalar varias directivas administrativas entre enrutadores BGP.

Circuito

Establezca el metadato deseado para crear una carpeta.

Los datos se agrupan de acuerdo con el metadato elegido.

Tabla 5.10. Formulario de circuito

Campo	Descripción
Modo de generación del nombre del circuito	Seleccione **Automático** para generar el nombre del circuito de forma automática.

Campo	Descripción
Script	Este campo solo está disponible si el Modo de generación del **nombre del circuito** es **Automático**. Selecciona el script. Crea uno en la sección Scripts.
Metadatos para la agrupación	Seleccione el nombre del metadato.

Cisco WAAS

Cisco WAAS (Wide Area Application Services) es una herramienta desarrollada por Cisco que es capaz de acelerar sus aplicaciones.

Tabla 5.11. Formulario de Cisco WAAS

Campo	Descripción
Habilitar control al Cisco WAAS	Escoge **Sí** o **No**.

Configuración de HTTPS

Configura el modo HTTPS (HyperText Transfer Protocol Secure).

Tabla 5.12. Formulario de HTTPS

Campo	Descripción
Habilitar https	Escoge **Sí** y el servidor será reiniciado en el modo HTTPS.
Certificado	Importe el certificado https. El archivo debe tener la extensión .pem y debe estar firmado por una CA (Certification Authority) para que sea válido.

Configuración del agente de captura

Configura el número permitido de agentes en ejecución simultánea.

Tabla 5.13. Formulario de configuración del agente de captura

Campo	Descripción
Número de agentes en ejecución simultánea	Entre con un entero menor o igual a 10. El valor modelo es **3**.

Configuración regional

Tabla 5.14. Formulario de configuración regional

Campo	Descripción
Separador de decimal	Separador decimal para informes del sistema.
Lenguaje del sistema	Escoge el lenguaje modelo del sistema. Cada usuario puede definir su propia configuración de idioma en configuración del usuario.

Campo	Descripción
Número de decimales en los archivos de exportación	Configuración usada para formatear campos de números en los informes exportados.
Separador de archivos CSV	Separador de informes CSV

EPM

EPM (Extended Processing Module) es otra aplicación adicionada a la ya instalada en el equipo. Es un módulo extendido de la solución de seguimiento.

Tabla 5.15. Formulario EPM

Campo	Descripción
Habilitar EPM	Selecciona esta opción si deseas habilitar el módulo de solución de seguimiento.
¿Es EPM?	Marca **Sí** en esta opción si esta aplicación es utilizada como EPM.

Importante

Cambiando esta configuración perderás todos tus datos históricos, por lo tanto, ¡ten cuidado!

Grafador

Ajuste de los parámetros del grafador.

Tabla 5.16. Formulario de parámetros del grafador

Campo	Descripción
¿Habilitar gráfico derivativo como modelo?	En el modo estándar, puntos de gráficos son conectados usando interpolación linear. En el modo derivativo, se utiliza la interpolación por partes.
Habilitar actualización automática	Selecciona esta opción para tener todos los gráficos actualizados automáticamente. También puedes habilitar esta opción en tiempo de ejecución para cada gráfico.
Excluir fines de semana	Habilitando esta opción, los días del fin de semana se mostrarán con color más claro en los gráficos.
Intervalo de actualización	Intervalo de actualizaciones.
Horario comercial	Esta opción permite modificaciones en la visualización de los gráficos de acuerdo con el horario comercial definido en Preferencias locales. Elija entre **Sin acciones**, **Destacar horario comercial** o **Mostrar solo horario comercial**.

Histórico de configuración

Selecciona el periodo de almacenamiento para diferentes áreas de configuración.

Tabla 5.17. Parámetros de históricos de configuración

Campo	Descripción
Periodo máximo de almacenamiento de histórico de configuración	Esto incluye todos los cambios de configuración, excepto para el usuario relacionado con las operaciones. Este dato se mostrará en **Sistema** → **Diagnósticos** → **Logs de configuración** .
Periodo máximo de almacenamiento de histórico de configuración de usuarios	Esto es específico para las operaciones de usuario. Estos datos pueden exhibirse en **Sistema** → **Diagnósticos** → **Logs de configuración** seleccionando la opción usuario en el campo **Tipo de objeto**.
Periodo máximo de almacenamiento de estadísticas de resumen	Esto está solo relacionado al proceso de resumen. Esta estadística puede ser comprobada en **Sistema** → **Diagnósticos** → **Resumidor** .

Inicio de sesión automático

Este recurso habilita la autentificación bypass para solicitudes URL provenientes de otro sistema.

Para habilitar este recurso, sigue el siguiente procedimiento:

1. Ves al **Sistema** → **Parámetros** → **Inicio de sesión automático** .
2. Selecciona "Sí" en la opción **Habilitar Inicio de sesión automático**.
3. Rellena la URL en el formato requerido, que es la página cuyas solicitudes serán originadas.
4. En su servidor web, rellena la siguiente URL: **http://<IP>/cgi-bin/login?dip=<USUÁRIO>**.

Logotipo

Escoge un archivo de imagen de tu Escritorio y súbelo, después la imagen se exhibirá en la esquina derecha superior.

Recuerda que la imagen debe estar con una altura fija de 43 píxeles y un ancho variable de 20 a 200 píxeles.

Nivel de log

Escoge el nivel del ALARMDaemon: **BajoAlto**.

Este nivel determinará la cantidad de detalles en el log de alarma.

Preferencias locales

Tabla 5.18. Formulario de preferencias locales

Campo	Descripción
Tamaño de la página en PDF	Tamaño de la página en los informes en PDF
Limitador de búsqueda	Rellena con un valor positivo entero para limitar tus búsquedas. El valor modelo es 2500.

Campo	Descripción
Primer periodo del horario útil	Define los horarios inicial y final para el primer periodo de horario útil.
Segundo periodo del horario útil.	Define los horarios inicial y final para el segundo periodo de horario útil.

Redireccionamiento de inicio de sesión

Rellena el campo **página de destino tras inicio de sesión** para ser redireccionado a otro sistema tras el inicio de sesión. En el sistema redireccionado, serás capaz de acceder a todos los objetos sin autentificación del TRAFip/SLAview.

Redundancia

Esta sección es utilizada para especificar las configuraciones de redundancia.

Activación

Tabla 5.19. Configuraciones de activación de redundancia

Campo	Descripción
Habilitar redundancia	Escoge Sí.
IP de sincronización local	Rellénalo con la dirección de IP configurada para la interfaz directamente conectada a otro appliance.
IP de sincronización remota	Rellénalo con la dirección de IP configurada para el appliance remoto.
Tamaño máximo de histórico	Configura el tamaño máximo de histórico en MB. El tamaño de histórico mínimo es de 16MB.
Estado preferencial	Selecciona **Maestro** o **Slave**.

Ves a sección redundancia para detalles de habilitación de este recurso.

Conmutación

Tabla 5.20. Configuraciones de conmutación de redundancia

Campo	Descripción
Interfaces	Selecciona la interfaz que compartirá las direcciones de IP entre los dos appliances. Usa el botón **Añadir** para añadir múltiples interfaces. Por lo menos debe reservarse una interfaz para poseer una dirección de IP exclusiva para fines de gestión. Una interfaz debe ser usada para la conexión back-to-back y otras pueden ser usadas para compartir IPs.

Redundancia de la recolección de flujos

Esta sección es utilizada para especificar las configuraciones de redundancia de la recolección de flujos.

Tabla 5.21. Configuraciones de redundancia de la recolección de flujos

Campo	Descripción
Habilitar redundancia de la recolección de flujos	Escoge Sí.
Interface para conmutación	Seleccione la interfaz que se utilizará para compartir la dirección IP de exportador entre la recolectora y la recolectora que está configurada como copia de seguridad.

Registro de acceso de usuarios

El sistema ofrece una herramienta que proporciona un informe resumido diario que contiene el registro de acceso de usuarios. Para más informaciones consulta la sección **Registro de acceso**.

Puedes configurar el tiempo máximo en que estos registros estarán en el sistema.

Tabla 5.22. Formulario de registro de acceso de usuarios

Campo	Descripción
Periodo máximo de almacenamiento de los registros de acceso de usuarios (meses)	Escoge un valor menor o igual a 36. El valor estándar es **12**, o sea, el equivalente a 1 año.

Informes

Esta sección permite hacer configuraciones avanzadas de los informes.

Informes programados

Configura las características para los informes programados.

Tabla 5.23. Formulario de configuración de los informes programados

Campo	Descripción
Tiempo de actualización de la página de espera (segundos)	Introduce un número entero.
Tiempo Máximo de Ejecución (minutos)	Introduce un número entero.
Número Máximo de Procesos Simultáneos	Introduce un número entero.
Prefijo del asunto del correo electrónico	Define un prefijo para el asunto del correo electrónico.
Hostname para enlace del correo electrónico	Configura un hostname para el correo electrónico.

También es posible enviar los informes programados a un servidor FTP.

Tabla 5.24. Formulario de configuración del servidor FTP

Campo	Descripción
Servidor	Dirección de IP del servidor.
Directorio	Directorio en el servidor.

Campo	Descripción
Usuario	Usuario a ser autentificado en el servidor.
Contraseña	Contraseña.
Puerta	Número de la puerta.
Límite de almacenamiento (MB)	Establezca el tamaño máximo que los informes pueden ocupar.

Para enviar un informe al servidor FTP, vaya a **Informe** y guarde o edite una modelo seleccionando la opción **Programar modelo** y luego marque **Sí** en el campo **Enviar informe al servidor FTP**.

Servidor SMS

Método SMPP(Protocolo Short message peer-to-peer)

Use este método si tu operador móvil proporciona una cuenta SMPP.

Tabla 5.25. Formulario de servidor SMPP

Campo	Descripción
Protocolo SMS	Escote la opción SMPP
Host	Host SMPP.
Puerta	Puerta SMPP.
Sistema ID	Sistema ID SMPP.
Tipo de sistema	Tipo de sistema SMPP.
Contraseña	Contraseña SMPP.
URL	Ves a la sección de URL.
Número de teléfono de origen	Número de teléfono que se exhibirá como llamada SMS.

Los SMSs pueden enviarse utilizando distintos métodos. Ambos pueden ser configurados por este formulario.

Método URL(Uniform Resource Locator)

Este método debe usarse si tienes un gateway http.

SLAview ejecutará una operación http GET utilizando la URL suministrada.

Debes usar las wildcars $CELLPHONE$ y MSG en la URL.

La wildcard $CELPHONE$ será sustituida por el campo wildcard SMS que rellenaste en el formulario de configuración del usuario.

La wildcard MSG será sustituida por un mensaje de alarma que contiene las siguientes informaciones:

- Nombre de la alarma.
- Niveles de urgencia de la alarma.

- Estado de la alarma.
- Fecha y horario que la alarma cambió de estado.
- Variable de alarma

SMTP

Rellena este formulario con los parámetros SMTP para enviar correos electrónicos.

Tabla 5.26. Formulario de parámetros SMTP

Campo	Descripción
Servidor SMTP	Configura el servidor SMTP. La puerta usada por el servidor SMTP puede ser alterada en este campo. Siga el ejemplo: smtp.server.com:port
Usuario SMTP	Introduce el correo electrónico.
Contraseña SMTP	Introduce la contraseña. Si el servidor SMTP no solicita autentificación en este campo puede dejarse en blanco.
Remitente SMTP	Configura un remitente para el correo electrónico.

Puedes verificar las configuraciones SMTP antes de guardar: clica en **Prueba SMTP** e introduce la dirección de correo electrónico para la prueba.

SNMP

Recolector SNMP

Estos parámetros se usarán para todos los procesos que ejecutan SNMP polling. Estas son configuraciones modelo, pero pueden ser ajustadas a nivel del dispositivo.

Para una referencia de todos los procesos del sistema, ves a sección archivos de log.

Parámetros SNMP

SNMP Timeout	Tiempo límite en segundo que el colector esperará por un paquete de respuesta SNMP. Intervalo de valores 1-10.
Nuevos intentos SNMP	Número de intentos que serán permitidos para el dispositivo si no responde a una consulta SNMP. Intervalo de valores 1-10.
Número de OIDs por paquete	Número de OIDs que el recolector enviará en cada paquete SNMP. Intervalo de valores 1-100.
Tasa máxima de envío por paquete	Número máximo de paquetes por segundo que un recolector SNMP enviará a cada dispositivo.
Tasa máxima general de envío de paquetes (pps)	Límite global para la cantidad de paquetes enviados por segundo. Considera todos los dispositivos registrados. Rellena 0 si quieres que no tenga límites.

Ventana SNMP	Número de paquetes SNMP que serán enviados sin respuesta del dispositivo que está siendo sondado.
Puerta SNMP	Puerta TCP estándar para conectar con el agente SNMP.
Ignorar interfaces	Rellena la expresión para ignorar estas interfaces.
Interfaces high counter	Rellena la expresión para usar, en estas interfaces, el contador de OID más alto(ifHCInOctets e ifHCOutOctets).
Interfaces SecRate	Rellena la expresión para usar la sec rate OIDs (IfHCIn1SecRate y IfHCOut1SecRate) en estas interfaces.

Trap SNMP

Rellena los campos de abajo para especificar los hosts que recibirán los traps. Estos traps pueden ser alarmas de ALARMmanager o traps auto generados por los TELCOMANAGER MIBS.

Tabla 5.27. Campos de TRAP

Campo	Descripción
Hosts para enviar Traps	Direcciones de IP de los hosts. Ej.: 10.0.0.1,10.0.0.2.
Comunidad para enviar Traps	Comunidades SNMP de los hosts de trap.

TACACS

Habilita el método de autentificación TACACS+. Se pueden configurar hasta dos servidores para Redundancia.

El nombre de usuario y contraseña de cada usuario debe ser configurado en el sistema, exactamente como el servidor TACACS.

Cuando este método está activado, no existe autentificación local, o sea, cualquier usuario que no sea del tipo **Administrador** inicia sesión por el TACACS.

Importante

El usuario **Administrador** tiene la opción de elegir iniciar sesión localmente o no, de todas formas, se recomienda que haya siempre una cuenta de **Administrador** con **Autentificación local** activada, en el caso de que sea utilizado el control de acceso externo.

Telcomanager Host Agent

Rellene este formulario con la dirección IP del servidor donde está instalado el Telcomanager Host Agent. Esta dirección se utilizará para recopilar todos los dispositivos configurados para utilizar la colección THA en el modo de puerta de enlace.

Importante

Para que el THA pueda recopilar información de forma remota en un Active Directory (AD), es necesario que los siguientes servicios estén habilitados en las máquinas remotas:

- Llamada a procedimiento remoto (RPC)

- Registro remoto

Telcomanager JMX Agent

Rellene este formulario con la dirección IP y el puerto del servidor donde está instalado el Telcomanager JMX Agent. Esta dirección se utilizará para recopilar todos los dispositivos configurados para utilizar la colección JMX.

Tema

En esta sección, puedes ver el tema modelo del sistema.

Tabla 5.28. Configuración del tema

Campo	Descripción
Tema modelo	Escoge el tema modelo para el sistema: **Dark**, **Green & Yellow**, **Red & white** or **Telcomanager**.

Sugerencia

Date cuenta de que cada usuario puede definir su proprio tema en configuración de usuario.

Verificación de versión del sistema

Todos los días entre 2h y 3h de la madrugada, hay una verificación de la versión del sistema para comprobar si hay una nueva build disponible. Cuando exista, el usuario será informado.

Web Services

API de Configuraciones

Tabla 5.29. Formulario de API de configuraciones

Campo	Descripción
Hosts con acceso permitido a la API de configuraciones	Configura los hosts que son habilitados para acceder a la API de configuraciones.
Nombre de usuario utilizado por la API de configuraciones	Escribe el usuario.

Datos brutos del TRAFip

Configura el acceso a los datos brutos del TRAFip.

Tabla 5.30. TRAFip's raw data form

Campo	Descripción
Ip con permisos de acceso	Escribe el IP.
Contraseña	Escribe la contraseña.

Usuarios

El sistema posee tres tipos de usuarios:

Tipos de usuario

Administrador	Tiene total acceso al sistema.
Configurador	Puede crear, borrar y editar cualquier objeto del sistema. No puede hacer cambios en las configuraciones del sistema.
Operador	Solo puede visualizar el sistema de objetos comprobados e informes.

Cuando asocias grupos a usuarios, restringes la visualización de este usuario al objeto con jerarquía de grupos.

También pueden limitarse los menús a los que los usuarios pueden acceder y el número de usuarios simultáneos que accederán al sistema.

Editando usuarios

1. Selecciona **Sistema** → **Usuarios** → **Lista de usuarios** .
2. Clica en los botones Nuevo o Editar y rellena el formulario siguiente:

Tabla 5.31. Formulario de usuario

Campo	Descripción
Nombre de usuario	Inicio de usuario.
Nombre	Nombre de usuario.
Contraseña	Contraseña.
Confirmación de contraseña	Repite la contraseña.
Correo electrónico	Correo electrónico para enviar alarmas y el informe programado cuando esté disponible. Debes configurar el servidor SMTP.
SMS	Número de celular para enviar alarmas utilizando el protocolo SNMP o celular@teste.com para enviar pequeños correos electrónicos con alarmas. El sistema también puede enviar SMSs a través de la integración con un portal web.
Usar gráfico compacto	Compacta los gráficos para que quepan en la misma página o visualízalos en el tamaño normal.
Usar resumen de grupo	Habilita la visualización del Resumen de grupo para el usuario.
Autentificación local	Habilita autentificación basada en el Active Directory o TACACS. Para configurar el Active Directory accede a **Sistema** → **Parámetros** → **Active Directory** y para configurar el TACACS accede a **Sistema** → **Parámetros** → **TACACS** .

Campo	Descripción
Tema	Selecciona el tema del usuario. Escoge el Tema Estándar en **Sistema** → **Parámetros** → **Tema**
Grupo de usuario	Asocia este usuario a un usuario del grupo de forma que se restrinja el número de accesos simultáneos al sistema con el grupo.
Idioma	Selecciona el idioma del usuario.
Perfil	Selecciona el perfil de usuario para restringir la alarma y el servicio de visualización de alarma y notificación.
Tipo	Tipos de usuario.
Menú	Usa la opción estándar para restringir al usuario a menús específicos.
Subredes	Selecciona las subredes a las que el usuario será capaz de acceder.

Deshabilitar usuarios

Puede deshabilitar un usuario haciéndolo inactivo. Un usuario inactivo no puede iniciar ni recibir notificaciones del sistema. Para desactivar un usuario, utilice el botón **Deshabilitar** al lado del usuario deseado.

Grupo de usuarios

Los grupos de usuarios son usados para gestionar cuantos usuarios pueden estar conectados simultáneamente en el sistema.

Procedimiento 5.1. Gestionando grupos de usuarios

1. Selecciona **Sistema** → **Usuarios** → **Grupos de usuarios** .
2. Clica en los botones Nuevo o Editar y rellena el formulario siguiente:

Tabla 5.32. Formulario de usuario

Campo	Descripción
Nombre	Nombre del grupo de aplicación
Descripción	Descripción del grupo de aplicación
Limitar el número de accesos simultáneos	Selecciona un número entre 1 y 255. Este será el límite de accesos simultáneos en el sistema para los usuarios de este grupo.
Usuarios	Especifica los usuarios que serán colocados en el grupo. Un usuario puede pertenecer solo a un grupo.

Perfiles de usuarios

Los perfiles de usuarios son usados para asociar alarmas a los usuarios.

Procedimiento 5.2. Gestionando perfiles de usuarios

1. Selecciona **Sistema** → **Usuarios** → **Perfiles de usuarios** .

2. Clica en los botones Nuevo o Editar y rellena el formulario siguiente:

Tabla 5.33. Formulario de usuario

Campo	Descripción
Nombre	Propiedades del perfil de usuario
Token do bot Telegram	Token obtenido tras crear un bot en el Telegram.
ID del chat Telegram	ID del chat en el que el bot está participando.
Usuarios	Asocia los usuarios a un perfil.
Perfiles -> Alarmas	Asocia un par de Perfil -> Alarma para este perfil.
Alarmas de servicio	Asocia servicios de alarmas a este perfil.

Alarma Consola

Puedes seleccionar las columnas que se mostrarán en el ALARMmanager consola. Además, estás habilitado para configurar el orden en que las columnas aparecerán. Para esto, basta clicar y arrastrar las líneas.

Tabla 5.34. Columnas ALARMmanager consola

Columna	Descripción
INICIO	Tiempo de la primera incidencia.
TÉRMINO	Tiempo de la última incidencia. Muestra ACTIVO si la alarma no terminó.
USUARIO	Usuario que programó la alarma.
TIPO	Tipo de objeto, puede ser dispositivo u objeto mapeado.
OBJETO	Nombre del objeto.
DESCRIPCIÓN	Descripción del objeto.
IFALIAS	Si el objeto es una interfaz, muestra su ifAlias.
ESTADO	Estado de la alarma, puede ser activado o desactivado.
ALARMA	Nombre de la alarma.
NIVEL	El nivel para la alarma definido en configuración de nivel.
TRAP	Sí, si fue generado por un trap y no en cualquier otro caso.
COMENTARIOS	Comentarios del operador. Para introducir un comentario, clica dos veces en la célula.
CAMINO	Muestra el primer camino de grupo del SLAview para el objeto.

Diagnósticos

Información de red

Muestra la fecha y la hora del sistema, interfaces de rede y gateway modelo.

Pruebas de conexión

Pruebas como ping, nslookup y traceroute para probar la conexión entre el appliance y los elementos de red.

Captura de paquetes

Usando esta herramienta, puedes analizar los paquetes que están pasando por las interfaces del appliance.

Clica en **Sistema** → **Diagnósticos** → **Captura de paquetes** .

Clica en Nuevo.

Tabla 5.35. Captura de paquetes

Columna	Descripción
Interfaz de red	Escoge la interfaz que se analizará.
Tamaño máximo del archivo	Escoge el tamaño máximo del archivo donde el resultado del análisis se registrará.
Cantidad máxima de paquetes	Rellena el número máximo de paquetes que serán analizados. Rellena 0 si quieres que no tenga límites.
Puerta	Filtra puertas a analizar. Escribe * para todas las puertas o coma para valores separados.
Excluir puerta	Excluir puertas para analizar. Escribe * para todas las puertas o coma para valores separados.
Host	Escoge un host para filtrar o selecciona **Todos** para todos los hosts.

Clica Enviar para iniciar la captura y después Volver para volver a la lista de archivos de captura.

Si desean cerrar la captura, clica Parar. Un botón de Descarga aparecerá y puedes hacer la descarga del archivo capturado.

Objetos

Muestra el número de objetos y perfiles configurados.

Resumidor

Esta sección muestra el tiempo que el proceso resumidor lleva para ejecutar por el último día

Al implantar el sistema en arquitectura distribuida, el tiempo para enviar los archivos resumidos de todos los recolectores también se muestra.

Importante

El proceso de resumen se ejecuta cada cinco minutos, por lo que el tiempo del proceso ejecutado debe ser menor que cinco minutos para el buen funcionamiento del sistema.

Uso de disco

Muestra información sobre el uso de almacenamiento de las áreas.

Logs del sistema	Logs del sistema operacional.
Logs SLAview	Logs del SLAview.
Logs TRAFip	Logs TRAFip.
SLAview Banco de datos TDB,Uso del almacenamiento para el banco de datos SLAview Telco, que se usa para asegurar los datos resumidos del SLAview.	
TRAFip Banco de datos TDB	Uso del almacenamiento para el banco de datos TRAFip Telco, que se usa para asegurar los datos resumidos del TRAFip.
TRAFip datos brutos	Almacenamiento usado para los datos brutos del TRAFip.
SLAview datos brutos	Almacenamiento usado para los datos brutos del SLAview.
Detalles de los datos brutos	Almacenamiento de los datos brutos por día para el sistema en el que estás conectado.

Archivos de Log

En esta área puedes visualizar los archivos de log del sistema. Abajo, una lista de archivos.

Archivos de LOG

createMark.log	Logs del proceso de actualización de la versión.
backupgen.log	Configuración de copia de seguridad diaria de procesos de logs.
dbackupArchive.log	Logs de proceso remoto de copia de seguridad.
Gc*	Logs del proceso de recolector de papelera.

Logs de configuración

Esta opción proporciona los logs de la configuración del sistema.

Estos logs se mantienen por un periodo definido en **Sistema** → **Parámetros** → **Histórico de configuración** → **Período máximo de almacenamiento de histórico de configuración** .

Huso horario

Este menú se usa para configurar el huso horario correcto para el servidor. Puedes seleccionar uno de los husos predefinidos en el sistema o subirlo otra vez.

Este procedimiento es usualmente necesario si existen modificaciones de datos durante el día.

Soporte

Inicio de solicitud

Clica en el botón **Iniciar solicitud** y serás redireccionado al formulario de soporte técnico de Telcomanager a través de una pestaña nueva en tu navegador.

Importante

Necesitar estar conectado a Internet.

Verificar si hay actualizaciones del sistema

Clica en el botón **Verificar actualizaciones** para descubrir si hay patches disponibles para tu versión o si es posible actualizar el sistema para nuevas versiones.

Importante

Necesitas estar conectado a Internet.

Configuración de túnel para soporte remoto

Esta opción puede usarse para establecer una conexión segura para los servidores de soporte de Telcomanager.

Una vez que la conexión sea establecida, puedes contactar al equipo de soporte de Telcomanager con el código de solicitud.

Sugerencia

Si tu código de solicitud no funciona, intenta introducir un valor diferente.

Sobre

Esta sección muestra la versión que está actualmente instalada y las opciones de licencia.

También, puedes comprobar el número de dispositivos existentes, la serie de datos históricos y el límite de bits/s o flow/s.

Capítulo 6. Recursos habilitados con licencia

Redundancia

La solución de redundancia te permite implantar dos appliances idénticos trabajando en modo HOT-STANDBY.

Importante

Esta funcionalidad solo funcionará si los dos appliances tienen la misma versión.

Sugerencia

Es aconsejable que los appliances tengan las mismas configuraciones de hardware. En caso de que haya diferencias, el sistema mostrará un aviso.

Conceptos

- Cuando este recurso es habilitado, el sistema trabaja con dos máquinas idénticas en HOT-STANDBY realizando la sincronización de los datos y observando cada uno de los estados en todo momento.
- Un protocolo de comunicación se ejecuta entre los dos servidores y si un fallo es detectado en uno de los servidores, el otro actuará como el servidor activo - si ya no lo está - y la trap tmTSRedundancyStateChangeTrap se enviará. Esta trap es documentada en la MIB TELCOMANAGER-TELCOSYSTEM-MIB.
- Ambos appliances comparten la misma dirección IP, que es usada para enviar flujos de los enrutadores. Esta dirección IP está activa solo en el servidor ACTIVO y cuando cambia de estado, la dirección MAC de la interfaz migrará al servidor ACTIVO.

Habilitando la redundancia

1. Usando dos appliances Telcomanager idénticos con la opción de licencia de redundancia habilitada, haz una conexión back-to-back usando la misma interfaz en cada dispositivo y configura una dirección de IP no-válida entre estas interfaces, usando CLI (command line interface) en cada dispositivo.
2. En la CLI, configura la dirección de IP que será compartida entre dos servidores solo en el servidor activo.
3. Ves al menú **Sistema** → **Parámetros** → **Redundancia** y rellena el formulario de ambos dispositivos.
4. Espera 20 minutos para verificar el estado de cada servidor en **Sistema** → **Diagnósticos** → **Información de red** .

Arquitectura distribuida

Conceptos

La arquitectura distribuida debe ser usada para dimensionar la capacidad del sistema para recolectar flujos IP y datos SNMP y para procesar los datos brutos, una vez que estas tareas son designadas al appliance recolector.

Prerrequisitos

- Todas las máquinas relacionadas deben tener el mismo acceso SNMP para todos los dispositivos controlados.
- Los flujos de IP debe exportarse para los appliance recolectores.
- Debe poseer anchura de banda suficiente para transferir los archivos de resumen entre los appliances recolectores y el appliance central. Ten en cuenta que un recolector requiere en torno a 64 Kbps de anchura de banda para controlar 1000 interfaces con 10 variables de resumen en cada interfaz.
- Las puertas TCP 22 y 3306 deben estar disponibles entre el appliance recolector y el central. La puerta 22 es usada para transferir archivos en el protocolo SSH y la 3306 es utilizada para emitir la consulta del banco de datos para el appliance central.

Establecimiento

1. En el appliance central, ves a **Sistema** → **Parámetros** → **Arquitectura distribuida** y rellena el formulario.
2. En el appliance recolector, ves a **Sistema** → **Parámetros** → **Arquitectura distribuida** .
3. En el appliance central, ves a **Configuración** → **Recolectoras** y rellena el formulario.
4. Espera en torno a 20 minutos y ves al menú **Configuración** → **Recolectoras**, para ver si las recolectoras listadas están con el menú en estatus **ON**.

Capítulo 7. Glosario

Siglas

Esta sección muestra las siglas y abreviaturas presentes en este manual.

Tabla 7.1. Lista de siglas y abreviaturas

Sigla	Descripción
AD	Active Directory.
API	Interfaz de programación de aplicaciones. Del inglés, Application Programming Interface.
AS	Sistema autónomo Del inglés, Autonomous system.
ASN	Número de sistema autónomo. Del inglés, Autonomous system number.
Avg	Media. Del inglés, average.
CDP	Protocolo Cisco Discovery. Del inglés, Cisco Discovery Protocol.
CLI	Interfaz de línea de comando. Del inglés, Command line interface.
CNT	Es un tipo de análisis de perfil de tráfico: Contenido.
CPU	Unidad central de procesamiento. Del inglés, Central processing unit.
DNS	Sistema de Nombres de Dominios. Del inglés, Domain Name System.
DoS	Negación de servicio. Del inglés, Denial of service.
DST	Es un tipo de análisis de perfil de tráfico: Distribución.
Enum	Enumerate.
EPM	Es un módulo extendido del SLAview. Del inglés, Expanded Processing Modules.
FTP	Protocolo de Transferencia de Archivos. Del inglés, File Transfer Protocol.
GB	Gigabyte.
GIS	Sistema de Información Geográfica. Del inglés, Geographic Information System.
HTTP	Protocolo de Transferencia de Hipertexto. Del inglés, Hypertext Transfer Protocol.
HTTPS	Protocolo de Transferencia de Hipertexto Seguro. Del inglés, Hyper Text Transfer Protocol Secure.
ICMP	Protocolo de Mensajes de Control de Internet. Del inglés, Internet Control Message Protocol.
IETF	Internet Engineering Task Force.
IP	Protocolo de internet. Del inglés, Internet Protocol.

Sigla	Descripción
IPFIX	IP Flow Information Export.
IPv4	Protocolo de internet en la versión 4. En ella, las direcciones IP son compuestas por 32 bits.
IPv6	Protocolo de internet en la versión 6. En ella, las direcciones IP son compuestas por 128 bits.
ISP	Proveedor de Servicio de Internet. Del inglés, Internet Service Provider.
Kb	Kilobit.
KPI	Indicador-Llave de Desempeño. Del inglés, Key Performance Indicator.
LAN	Red de área local. Del inglés, Local Area Network.
LLDP	Link Layer Discovery Protocol.
Máx.	Máximo.
Mb	Megabit.
MIB	Base de informaciones de gestión. Del inglés, Management information base.
Mín.	Mínimo.
MPLS	Multi-Protocol Label Switching.
MTX	Es un tipo de análisis de perfil de tráfico: Matriz.
NaN	Cuando el valor no es un número. Del inglés, Not a number.
NTP	Network Time Protocol.
OID	Identificador de objeto. Del inglés, Object Identifier.
QoS	Calidad de Servicio. Del inglés, Quality of Service.
RFC	Request for Comments.
RFI	Repeated Flow Interface.
SMS	Servicio de mensajes cortos. Del inglés, Short Message Service.
SMPP	Protocolo de mensaje corto peer-to-peer. Del inglés, Short Message Peer-to-Peer.
SMTP	Protocolo de transferencia de correo simple. Del inglés, Simple Mail Transfer Protocol.
SNMP	Protocolo Simple de Gestión de Red. Del inglés, Simple Network Management Protocol.
SSH	Secure Shell.
TACACS	Terminal Access Controller Access-Control System.
TCP	Protocolo de control de transmisión. Del inglés, Transmission Control Protocol.
TCS	Telcomanager Custom Script.

Sigla	Descripción
THA	Telcomanager Host Agent.
ToS	Tipos de Servicios. Del inglés, Type of Services.
TSA	Telcomanager Windows Security Agent.
UDP	User Datagram Protocol.
URL	Localizador Uniforme de Recursos. Del inglés, Uniform Resource Locator.
WAAS	Wide Area Augmentation System.
WAN	Red de larga distancia. Del inglés, Wide Area Network.