Manual TRAFip

Manual TRAFip

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, protocolo TCP/IP y protocolo SNMP.

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

TRAFip es un sistema de caracterización de tráfico para redes IP. Es implementado en la red de forma no violenta y recibe informaciones sobre tráfico IP usando el protocolo Netflow o por la captura directa en una de las interfaces de la 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.
- Captura e informe de Syslog.
- Creación de fórmulas, permitiendo que el usuario defina sus proprias KPIs (Key Performance Indicators).
- Arquitectura escalable. El sistema puede crecer en el número de elementos recolectados por el uso de appliances recolectores remotos y en el número de usuarios e informes que soporta por medio de la implantación de EPMs (Expanded Processing Modules), que son appliances responsables por compartir la carga con el sistema central.
- Puede ofrecerse alta disponibilidad a través del uso de soluciones redundantes, en las que dos appliances trabajan en HOT-STANDBY.
- Informe de proyección.
- Todos los informes pueden ser guardados como modelos, programados y exportados en formato PDF, HTML y CSV.
- 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.
- Informes Top N para todos los elementos controlados.
- Clasificación de tráfico en subredes, grupos de subredes, aplicaciones, dispositivos, protocolos, sistemas autónomos y ToS (Type of Service).
- Perfiles de tráfico que permiten al usuario agrupar objetos del mismo tiempo y después usar el perfil para clasificar el tráfico de cualquier objeto del sistema. Por ejemplo, puede crearse un perfil de tráfico que contenga subredes de una red y después asociarse a cada subred para producir gráficos que exhiban el tráfico cambiado entre ellas.
- Filtros RFI (Repeated Flow Interface), que filtrarán tráficos repetidos exportados por los enrutadores.
- Captura de tráfico derecho en la interfaz de red del appliance, para ser usado en ambientes donde Netflow u otro protocolo de flujo no están disponibles.

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. Conceptos básicos

Netflow

El modo más escalable para analizar tráfico IP es a través del uso del protocolo Netflow, desarrollado por la Cisco Systems, u otro protocolo de exportación de flujo.

En el Netflow, los enrutadores exportan paquetes UDP que contienen informaciones sobre todo el tráfico que pasó por ellos.

El TRAFip permite la captura de este tráfico y usa la información para calificar el tráfico de diferentes maneras.

Cada paquete UDP puede tener hasta 1500 bytes de tamaño y cargar información de hasta 50 flujos.

Un flujo es definido como un tráfico unidireccional conteniendo 7 llaves: dirección de IP de origen, dirección de IP de destino, puerta TCP/UDP de origen, puerta TCP/UDP de destino, protocolo de nivel 3, byte de ToS e índice de entrada de interfaz lógica.

Es importante destacar que, para tener total visibilidad del tráfico que está pasando por un enrutador, se recomienda habilitar el NetFlow en todas sus interfaces.

jFlow

J-Flow es una implementación de seguimiento de tráfico de Juniper. Esta herramienta permite que dispositivos de la red recolecten datos del tráfico y exporten esta información para las recolectoras.

Esta herramienta de seguimiento también se usa como técnica de grabación de tráfico. Cada paquete que pasa por una red es comprobado y las tendencias de flujo de la red son guardadas. Después de esto, toda la información grabada es comparada y, de esta forma, es posible detectar anomalías.

IPFIX

IPFIX es un modelo propuesto por Internet Engineering Task Force (IETF).

Internet Protocol Flow Information eXport (IPFIX) es un protocolo unidireccional para exportación de datos y está basado en el formato de exportación del NetFlow v9.

La mayor ventaja del IPFIX es su soporte para campos con larguras variables. Esta funcionalidad es muy útil en el caso de que necesites exportar las URLs.

Este protocolo se destina, principalmente, a la exportación de tráfico con alta tasa de flujo y a la aplicación en enrutadores de alta velocidad.

Huawei Netstream

NetStream es una tecnología que suministra estadísticas de análisis de tráfico desarrollada por Huawei Technologies.

Es muy similar a NetFlow: cuando el sistema de gestión de red posee el software NetStream instalado, recibirá estadísticas de tráfico y del uso de recursos, que fueron recolectados por el NetStream.

sFlow

sFlow es una tecnología desarrollada por InMon.

Al contrario de otras herramientas de seguimiento antes abordadas (NetFlow, J-Flow, IPFIX y NetStream), que son más utilizadas en enrutadores, sFlow es más popular en switches.

La mayor diferencia entre sFlow y NetFlow es que mientras que NetFlow recolecta todos los paquetes, sFlow coge muestras (samples).

Esta característica hace posible saber cuál es la tendencia de la red y esto conlleva la generación de menos tráfico.

Definiciones de los objetos

Los objetos siguientes pueden ser configurados para que clasifiquen el tráfico.

Análisis de escenarios en el TRAFip

Redes full mesh

El TRAFip debe situarse lo más cerca posible del enrutador que lidia con la mayor cantidad de tráfico, para que no exista flujo de tráfico innecesario a través de la red.

Para tener todo el tráfico analizado, se recomienda que todos los enrutadores exporten tráfico en todas las interfaces.

La imagen de abajo ilustra todos los enrutadores de red MPLS exportando flujo para el TRAFip.

Redes punto-multipunto

En este caso, el TRAFip debe posicionarse lo más cercano posible al enrutador central.

Una vez que todo el tráfico pasa por el enrutador central, solo es necesario habilitar el flujo de exportación en los enrutadores del borde, excepto cuando existe tráfico fluyendo entre dos enrutadores de borde, como se ilustra a continuación.

Redes de proveedores de servicio de internet

En este ambiente, el TRAFip debe situarse lo más próximo posible del enrutador que encamina la mayor cantidad de tráfico.

El TRAFip puede utilizarse para analizar el cambio de tráfico entre ISP y otros con el objeto AS (Autonomous Systems). Esto ayudará a los administradores de red a mejorar las políticas de cambio de tráfico.

La imagen de abajo ilustra este escenario.

El gráfico de abajo es un ejemplo de calificación de tráfico AS, mostrando cuanto del tráfico que está fluyendo para fuera del ISP1 está siendo encaminado para cada ISP, representado por las curvas de los gráficos.

Capítulo 3. Guía rápida para iniciar

Accediendo a la interfaz web

Una vez que accedas al servidor TRAFip, escribe su dirección IP en el navegador, escoge el sistema TRAFip clicando en el icono del TRAFip localizado en la esquina superior derecha de la ventana.

El acceso inicial al sistema puede hacerse utilizando el usuario **telco_adm** y la contraseña **sysoper**. En este punto, se recomienda un cambio de contraseña.

Si la autentificación tiene éxito, una pantalla semejante a la que se encuentra debajo, se muestra al usuario.

La sesión puede cerrarse en cualquier momento clicando en el icono de **Logout** en la esquina superior derecha de la ventana.

La pantalla principal del sistema se divide en las siguientes áreas:

Área 1: Menú árbol. Usado para navegar por los objetos del sistema y configuración de los ítems.

Área 2: Display de datos. Usado para mostrar gráficos, informes y formas de configuración.

Área 3: Menú principal. Usado para seleccionar todos los recursos del sistema.

Área 4: Selección de gráfico Usado para seleccionar gráficos y propiedades de los objetos.

Área 5: Panel de control. Usado para acceder a las herramientas de los gráficos.

Área 6: Encabezado. Usado para indicar que usuario está conectado, cual está desconectado y cambiar entre los sistemas TRAFip y SLAview.

Análisis de tráfico de interfaces

Una vez que los enrutadores estén exportando flujo para TRAFip, podrás configurar dispositivos en el sistema y realizar un análisis de flujo en las interfaces de acuerdo con el siguiente procedimiento:

1. Tienes que estar seguro de que hay conexión entre todos los elementos de red que están exportando NetFlow y el appliance del TRAFip en la puerta UDP 161 (para tráfico SNMP), 63636 (para exportación de NetFlow) y 6343 (para exportación de sFlow).

2. Espera en torno a 5 minutos después de la configuración del enrutador y accede **Sistema** → **Diagnósticos** → **Exportadores de flujo** .

3. Clica en el botón **Editar**, que está próximo a los enrutadores identificados y rellena el formulario:

    a. Modifica los campos **Nombre** y **Dirección IP de gestión**. El segundo debe ser una dirección de IP en la que el enrutador pueda recibir consultas SNMP.

    b. Rellena la **Versión SNMP** y la **Community** de acuerdo con las configuraciones del enrutador. A continuación, con el campo (Configuración de sampling rate) en modo Manual, introduce el valor 1 en el campo **Netflow sampling rate**.

    c. En el campo **Mapeadores**, selecciona **Interfaz.** Con ello, las interfaces de los informes serán descubiertas.

4. Espera 5 minutos para que el sistema pueda mapear las interfaces del enrutador y accede a **Datos históricos** → **Dispositivos** → **Grupos de Interfaz** . Después clica en el botón Nuevo y rellena la configuración de grupos de interfaz de la forma:

    a. Rellena el campo **Nombre.**

    b. En el campo **Interfaces**, usa el carácter * para filtrar las interfaces deseadas.

    c. En las cajas de selección de **Perfil**, selecciona **Perfiles de contenido** en la guía y después selecciona **Protocolos** y **Aplicaciones**.

5. Espera en torno a 10 minutos, después accede a la interfaz de grupo creada y clica en el icono gráfico **Aplicaciones** en el área de navegación del gráfico para verificar las aplicaciones clasificadas en el tráfico del grupo de interfaz.

6. Clica en el botón derecho del ratón en el área del gráfico y selecciona la opción **Generar Informe**. En el formulario presentando clica en el botón Enviar para verificar las IPs de origen/destino y las puertas que están generando tráfico.

7. En la ventana de informe, marca la cajam4_bold(Traducir flujos para la aplicación) para verificar las aplicaciones para cada línea.

Capítulo 4. Generador de gráfico Telcomanager

Cuando clicas en un icono de objeto en el menú árbol o en el nombre del objeto en la lista de objetos, tus gráficos se mostrarán en área de selección de gráficos. Cuando clicas en un icono en esta área, el Telcographer se carga en el área de display de datos.

El Telcographer es un generador de gráficos altamente interactivo escrito en HTML5. Las funciones de esta aplicación son explicadas abajo.

Periodo

El gráfico lee informaciones del Banco de Datos de Telco, donde todas las informaciones son grabadas en una resolución de 5 minutos.

La información de la resolución de 5 minutos está disponible para todo el periodo de grabación para cada objeto controlado.

Gráfico diario

En este periodo, la información se presenta con el mayor nivel de detalles. El periodo de tiempo es de 24 horas. Posee una muestra para cada 5 minutos y 288 muestras en total.

Gráfico semanal

Cada muestra es un valor medio de 6 muestras de 5 minutos, que corresponde a 30 minutos. El periodo de tiempo es de 7 días con 336 muestras. La curva de máximo se obtiene calculando el valor máximo para cada 6 muestras de 5 minutos.

Gráfico mensual

Cada muestra es un valor medio de 24 muestras de 5 minutos, que corresponde a 2 horas. El periodo de tiempo es de 30 días con 360 muestras. La curva de máximo se obtiene calculando el valor máximo para cada 24 muestras de 5 minutos.

Gráfico trimestral

Cada muestra es un valor medio de 72 muestras de 5 minutos, que corresponde a 6 horas. El periodo de tiempo es de 90 días con 360 muestras. La curva de máximo se obtiene calculando el valor máximo para cada 72 muestras de 5 minutos.

Gráfico anual

Cada muestra es un valor medio de 288 muestras de 5 minutos, que corresponde a un día. El periodo de tiempo es de 364 días con 364 muestras. La curva de máximo se obtiene calculando el valor máximo para cada 288 muestras de 5 minutos.

Gráfico bienal

Cada muestra es un valor medio de 576 muestras de 5 minutos, que corresponde a dos día. El periodo de tiempo es de 728 días con 364 muestras. La curva de máximo se obtiene calculando el valor máximo para cada 576 muestras de 5 minutos.

Gráfico de cinco años

Cada muestra es un valor medio de 1440 muestras de 5 minutos, que corresponde a 5 días. El periodo de tiempo es de 1820 días con 364 muestras. La curva de máximo se obtiene calculando el valor máximo para cada 1440 muestras de 5 minutos.

Gráfico personalizado

Puedes escoger un periodo personalizado para tu gráfico. Para ello, selecciona el periodo **Personalizado** y define las fechas y horarios de inicio y fin.

Recursos

El Telcographer posee diversos recursos a los que se puede acceder a través del panel de control encima del gráfico. Se puede acceder también a algunos de ellos clicando con el botón derecho del ratón en cualquier punto del gráfico.

Caja de estadísticas

Al mover el ratón sobre una curva en el subtítulo del gráfico, se mostrará una caja de estadística con las siguientes informaciones: Mínimo, Máximo, Media, Total y Desvío modelo de la curva.

Mostrar valor

Este recurso hará que el puntero del ratón muestre los ejes x e y para la posición del puntero.

Zoom vertical

Para habilitar este recurso, sigue el siguiente procedimiento:

1. Selecciona la opción en el menú Opciones del panel de control del gráfico.
2. Presiona y asegura el botón del ratón en la posición inicial y deseada.
3. Mientras estés asegurando el botón, mueve el cursor del ratón para la posición final y deseada y suelta el botón del ratón.

Una curva

Clica esta opción en el menú Opciones del panel de control del gráfico y después clica en una de las curvas en los subtítulos. Esta acción hará que se muestre en el gráfico solo la curva seleccionada.

Modo relativo

Clica en esta opción en el menú Opciones del panel de control del gráfico para mostrar cada curva en el gráfico relacionado con las otras curvas. Esto significa que, para cada muestra, la suma de datos representa el 100%.

Este modo funciona solo si todas las curvas del gráfico están empiladas.

Configuración de ejes

Clica en esta opción en el menú Opciones del panel de control del gráfico para abrir la ventana en la que será posible seleccionar las curvas que aparecerán utilizando la escala derecha o izquierda del eje x.

Asociar a Graph Set

Clica con el botón derecho del ratón y después en esta opción para abrir una caja donde serás capaz de asociar el gráfico a un graphset creado anteriormente.

Guardar imagen

El icono **Guardar imagen** en el panel de control del gráfico guardará el gráfico como una imagen jpeg.

Tipo de gráfico

A través del menú **Tipo de gráfico** en el panel de control, puedes escoger el tipo de vista del gráfico: lineal, circular o de barra.

Gráfico agregado

Clica en esta opción a través del menú popup del gráfico para abrir representaciones agregadas al gráfico. Existen dos opciones de gráficos: circular y barra. Estos gráficos pueden filtrarse por un periodo de un día. Por ejemplo, si abres un gráfico redondo semanal y filtras de las 10:00h a las 17:00h, el gráfico redondo presentará los datos semanales para aquel periodo del día.

Aunque no habilites el filtro, puedes configurar el periodo del gráfico usando el campo **Horario comercial.** Cuando este campo está configurado con 1 **día**, aparece otro campo: **Últimas horas**, que se refieren a las horas que son consideradas en el gráfico. Por ejemplo, cuando este campo está configurado con un valor 1, esto significa que el gráfico está considerando solo la última hora. El calor máximo que puede ser configurado es el **24**, que representa las últimas 24 horas.

Sugerencia

Para retirar alguna curva del gráfico, basta clicar en los subtítulos.

Aproximar y alejar

Utiliza esas funciones en el menú del popup del gráfico para dar zoom in o out, respectivamente, en la escala del tiempo. Por ejemplo, utilizando esto en un gráfico anual, es posible dar un zoom in en el gráfico diario en un día particular.

Importante

Estas opciones solo son disponibles en gráficos del tipo lineal.

Exportar

Clica en el gráfico con el botón derecho del ratón y acede a esta opción. Los datos del gráfico pueden ser exportados en los formatos HTML, CSV o TSV.

Actualización automática

Selecciona esta opción para que el gráfico se actualice automáticamente cada 5 minutos. Esta opción debe ser previamente habilitada en **Sistema** → **Parámetros** → **Grafador** , donde también puedes confirmar el intervalo de actualización.

Informe

A partir de cualquier gráfico, es posible generar un informe que buscará los flujos utilizados en la construcción del gráfico.

Clica con el botón derecho en cualquier punto en el área del gráfico y mueve el ratón hasta la opción **Informe de datos brutos**. Después de esto, puedes generar un informe personalizado o uno preconfigurado.

Eso también es posible a través del menú **Informe de datos brutos** en el panel de control.

Alarmas preconfiguradas disponibles:

- Top IPs de origen
- Top IPs de destino
- Top AS de origen
- Top AS de destino
- Top conversaciones
- Tráfico no mapeado

Sugerencia

Los gráficos en **Paquetes/s** (pps) y **Bit/s** (bps) poseen una curva para configuración de sample no aplicada. Después, para verificar la información de esta curva, pasa el ratón sobre el subtítulo con el nombre "No sample total".

Teclas

Algunas teclas de tu teclado poseen funcionalidades especiales. Ve abajo cuales son y sus descripciones.

Tabla 4.1. Teclas

Tecla	Descripción
D	Transforma el gráfico para el modo derivativo.
I	Indica informaciones detalladas sobre el gráfico como resolución, curvas, samples y timestamps.
L	Relaciona el tiemestamp y el valor de cada punto de una curva.
N	Cambia el formato de las curvas del gráfico, una vez que todas ellas están empiladas.
P	Genera una curva de proyección que considera solo los puntos entre el intervalo limitado por las líneas

Tecla	Descripción
	señalizadas. Cuando mueves el ratón para abajo, el número de puntos disminuye, en caso contrario el número de puntos aumenta.
R	Ajusta el gráfico de forma que tenga la resolución máxima.
S	Guarda el gráfico como una imagen en el formato PNG.
W	Cambie la configuración de la curva para waas accell.
-	Zoom out.
+	Zoom in.
LEFT	Mueve el gráfico para la izquierda.
RIGHT	Mueve el gráfico para la derecha.
*	Gráfico retorna a su tamaño normal.

Sugerencia

Puedes convertir el tiempo de timestamp para fecha usando el comando **ts2date** en la CLI.

Capítulo 5. 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.

Resumen de la red

Esta pestaña proporciona un resumen de tráfico absoluto en tu red en la última hora.

Los datos pueden ser visualizados en forma de lista, gráfico circular o gráfico de barra.

Puedes configurar que tipo de objetos se exhibirán en ese resumen bien como que tipo de visualización cada uno tendrá.

Importante

Si arrastras los Top 10 de forma que alteres el orden de exhibición y/o borres algunos de ellos usando la "**X**", el sistema guardará estas alteraciones.

Los tipos de objetos proporcionados en este resumen son:

- Aplicación
- Dispositivo
- Grupo de aplicaciones
- Grupo de Interfaces
- Grupos de sistemas autónomos
- Grupo de subredes
- Grupo de ToS
- Objeto mapeado
- Protocolo
- Sistemas autónomos
- Subred
- ToS

Sugerencia

Clica con el ratón sobre el objeto para abrir su gráfico en una nueva pestaña.

Para abrir esta pestaña en una nueva ventana, usa el icono .

Para configurar los objetos exhibidos y sus tipos de visualización, clica en el icono  . Después, selecciona y arrastra los elementos para configurar el orden de exhibición. Ve abajo el significado de cada icono.

Tabla 5.1. Tabla de iconos

Icono	Descripción
	Muestra el top 10 de los objetos en forma de lista.
	Muestra el top 10 de los objetos en forma de gráfico circular.
	Muestra el top 10 de los objetos en forma de gráfico de barras.

Favoritos

Usando este recurso, cada usuario puede configurar los objetos de su interés con acceso directo.

Añadiendo objetos a favoritos

Para añadir objetos a tus favoritos, simplemente clica en el icono de la estrella dorada mostrado como primer elemento del área del gráfico seleccionada para el objeto deseado.

Eliminando objetos de los favoritos

Para eliminar objetos de tus favoritos, simplemente clica en el icono de la estrella dorada como primer elemento del área del gráfico seleccionada para el objeto deseado.

Totales

Esta guía contiene solo 3 gráficos, que representan el gráfico para un dominio.

Subredes

Los objetos de subredes permiten el análisis de bloques IP. También es posible usar el objeto de grupo de subred para crear un conjunto de subredes para ser analizada.

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 5.2. 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. Ves a sección Proyección para consejos sobre como configurar estos parámetros.
Habilitar TRAFWatcher	Selecciona **Sí** para habilitar el Análisis de Amenazas por el TRAFwatcher.
Grupo de subredes	Asociación de grupo de subred.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.
Caja de selección de perfil	Selecciona el perfil de tráfico de una manera que pueda ser aplicado a esta subred.
Perfil de alarma	Asociación de perfil de alarma.

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 5.3. 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 5.4. 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 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.

Grupo de subredes

Los grupos de subredes pueden ser utilizados para organizar tus subredes.

Definiciones

- El tráfico de grupo es una suma de cada bloque IP individual de la subred contenida en un grupo. Esto significa que bloques IPs duplicados serán sumados una única vez en el tráfico de grupo.
- Cuando un grupo de subred es creado, debe ser asociado a un grupo de nivel superior, lo que es solo organizativo.
- El TRAFip tiene por defecto tres de estos grupos y el usuario puede modificar su nombre y crear más en **Datos históricos** → **Subredes** → **Lista de agrupamiento** .

Configuración

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

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

Para añadir una nueva subred, rellena el formulario de abajo de acuerdo con lo estipulado:

Tabla 5.5. Formulario de grupo de subredes.

Campo	Descripción
Nombre	Nombre del grupo de subred.
Descripción	Descripción de la subred.
Habilitar proyección	Parámetros modelos de proyección. Ves a sección Proyección para consejos sobre como configurar estos parámetros.
Tráfico límite (bps)	Este valor será trazado en el objeto gráfico con una línea punteada roja.
Agrupamiento	Nivel organizativo más alto.
Subredes	Subred perteneciente a este grupo.
Perfil de alarma	Asociación de perfil de alarma.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.
Caja de selección de perfil	Selecciona el perfil de tráfico de manera que pueda ser aplicado a esta subred.

Añadir metadatos de grupos de subredes

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **Subredes**, clica en el ítem **Grupos de 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 5.6. 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 el metadato creado a un perfil de subred, accede a la lista de grupos de subredes y clica en el botón **Metadato** al lado del grupo que será configurado.

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

Agrupamiento

Este objeto es solo a nivel organizativo, puedes usarlo para organizar los grupos de subredes del TRAFip.

Cada grupo de subred solo puede situarse en un equipo.

Para gestionar el agrupamiento accede al menú **Datos históricos → Subredes → Lista de Agrupamientos** .

Para añadir un nuevo agrupamiento, rellena el formulario de acuerdo con lo descrito debajo:

Tabla 5.7. Nuevo formulario de agrupamiento

Campo	Descripción
Nombre	Nombre del agrupamiento
Grupos de agrupamiento	Asociación de grupos de subredes.

Dispositivos

Para mapear física y lógicamente los dispositivos como interfaces, el sistema posee un proceso de mapeo que se ejecuta periódicamente y mapea (ve la sección: Configuración de mapeadores). Existe un mapeador preconfigurado para mapear interfaces de dispositivos que usan la ifDescr OID para ejecutar esta tarea.

Procedimiento 5.1. Pasos de la configuración de los dispositivos

1. Selecciona **Datos históricos → Grupos → Grupos** .
2. Clica en el botón **Nuevo** y rellena el formulario de abajo:

Tabla 5.8. Formulario de nuevo dispositivo

Campo	Descripción
Nombre	Nombre del dispositivo.
Descripción	Descripción del dispositivo.
Dirección IP de gestión	Dirección de IP del dispositivo. Esta dirección de IP debe responder a las consultas SNMP para la comprobación SNMP y a las peticiones ICMP echo para comprobación ICMP.
Tipo	Tipo de dispositivo, el usuario puede usar este campo para categorizar libremente todos los dispositivos configurados.
Fabricante	Nombre del fabricante del dispositivo.
Latitud	Coordenada geográfica, en el formato de grados decimales (DD, en la sigla en inglés), usada para que el dispositivo sea localizado en mapas georreferenciados. Ejemplo: -22.9035.
Longitud	Coordenada geográfica, en el formato de grados decimales (DD, en la sigla en inglés), usada para que el dispositivo sea localizado en mapas georreferenciados. Ejemplo: -43.2096.
Credencial de SNMP	Escoge una credencial de SNMP.
Versión del SNMP	Selecciona la versión SNMP. Los posibles valores son:

Campo	Descripción
	SNMP v1 o SNMP v2c: Especifica una community SNMP SNMP v3: Especifica el tipo de autentificación y sus parámetros
Community SNMP	Rellena la community SNMP.
Utilizar configuración modelo de SNMP	Esta opción te deja definir los valores que pueden ser usados específicamente para este dispositivo. Los valores modelos están especificados en la configuración de los parámetros de los recolectores SNMP.
Considerar SysUpTime en la recolecta	Descarta la recolecta si el dispositivo no es permitido durante más de 5 minutos. Previene errores de cálculo.
SNMP Timeout	Tiempo límite en segundos para esperar una respuesta del paquete SNMP. Intervalo de valores 1-10.
Intentos SNMP	Número de nuevos intentos que serán permitidos al dispositivo si no responde a una consulta SNMP. Intervalo de valores 1-10.
Número de OIDs por paquete	Número de OIDs que serán enviadas en cada paquete SNMP. Intervalo de valores 1-100.
Tasa máxima de envío de paquetes (pps)	Número máximo de paquetes por segundo que un recolector SNMP enviará a cada dispositivo.
Ventana SNMP	Número de paquetes SNMP que serán enviados sin respuesta del dispositivo que está siendo polled.
Puerta SNMP	La puerta SNMP
Agentes	Esta opción permite que definas múltiples agentes SNMP en la misma dirección de IP y diferentes puertas. Ahora puedes especificar máscaras OID y la puerta SNMP para esta máscara. Esto significa que el recolector SNMP usará la puerta UDP especificada si la OID a ser recolectada en este dispositivo corresponde a la máscara especificada. Ejemplo: • Prefijo OID .1.3.4.6.9.9.1.2.* Puerta SNMP: 163

Campo	Descripción
	• Prefijo OID .1.3.4.6.9.9.1.3.* Puerta SNMP: 164
Credencial de conexión	Escoge una credencial de conexión.
Protocolo de conexión	Escoge entre **SSH** o **Telnet**.
Puerta SSH	Cuando el **Protocolo de conexión** es SSH, introduce la puerta SSH. El valor modelo es **22**.
Puerta Telnet	Cuando el **Protocolo de conexión** es Telnet, introduce la puerta Telnet. El valor modelo es **23**.
Usuario	Usuario para ser usado para acceder al dispositivo. Esta string está disponible como un campo libre %username% para scripts de suministro.
Contraseña del usuario	Contraseña para ser usada para acceder al dispositivo. Esta string está disponible como un campo libre %passwd% para scripts de suministro.
Contraseña de enable	La contraseña de enable es usada para acceder al dispositivo. Esta string está disponible como un campo libre %enable_passwd% para scripts de suministro.
Habilitar recolecta por el TRAFip	Habilitar la recolecta por el TRAFip
Direcciones IP del Netflow exporter	Rellena la dirección de IP que el netflow exporter usará para enviar flujos. Al lado de este campo, hay un icono de lupa. Clica en él, para rellenar automáticamente usando como base la Dirección de IP del dispositivo.
Configuración de sampling rate	Puede ser flechada manualmente o basada en un flujo.
Netflow sampling rate	Si estás exportando flujos, escoge si considerará una tasa manual configurada o si detectará la tasa de los registros de flujos.
Habilitar recolecta por el SLAview	Habilitar la recolecta por el SLAview.
Perfiles automáticos	Selecciona esta opción para habilitar el uso de este dispositivo y sus objetos mapeados en perfiles automáticos. La asociación solo sucederá si el dispositivo o sus objetos corresponden a las reglas de perfil. (Ve la sección de configuración de perfil) .
Colecta vía THA	Seleccione la forma en que se debe recopilar la información del THA. Ubicación: todas las solicitudes THA se enviarán directamente a ese dispositivo. Por lo tanto, el Telcomanager Host Agent (THA) debe estar instalado en este dispositivo. Puerta de enlace: todas las peticiones THA se enviarán a la puerta de enlace configurada en **Sistema** → **Parámetros** →

Campo	Descripción
	Telcomanager Host Agent . La puerta de enlace será responsable de recopilar la información de ese dispositivo.
Habilitar gestión de configuración	Habilita la gestión de configuración por el CFGtool.
Modo de exportación de configuración	Selecciona **Activo** para exportar la configuración periódicamente de acuerdo con el tiempo configurado en **Sistema** → **Parámetros** → **Gestión de configuración** . Para exportar la configuración usando filtro de trap, selecciona **Pasivo**.
Habilitar recolecta por CALLview	Habilita la colección por CallView.
Perfil de voz	Seleccione el perfil de voz para recopilar datos de llamadas.
Habilitar colecta JMX	Seleccione **Sí** para habilitar la recopilación de estadísticas de Java Management Extensions o **No** para deshabilitar. Para realizar la recolección JMX es necesario que el Telco JMX Agent esté configurado en **Sistema** → **Parámetros** → **Telcomanager JMX Agent** .
Método de mapeo de topología	Selecciona el protocolo que será usado para el mapeo de topología. Las acciones disponibles son: CDP - Cisco Discovery Protocol, LLDP - Link Layer Discovery Protocol o ambos. Usando ambos métodos, el SLAview utilizará el protocolo SNMP para buscar informaciones de estos protocolos en las tablas MIB de los dispositivos comprobados.
Habilitar suministro	Habilitar suministro para configurar automáticamente las Cisco IP SLA probes, Telcomanager probes y exportación de Netflow.
Recolector	Asociación del dispositivo a un recolector remoto. Este campo está disponible solo cuando la arquitectura distribuida es habilitada.
Script de autentificación	Cuando el protocolo de conexión este configurado como **Telnet**, necesitas seleccionar un script de Inicio de sesión.
Script para suministro	Rellena esta opción para suministro de Netflow en sistemas con arquitectura distribuida y configuración de probes. Este script será usado para reconfigurar la exportación de Netflow a un recolector de copia de seguridad si el recolector falla.
Modelos de polling	Escoge un modelo del polling ICMP para el dispositivo.

Campo	Descripción
	El modelo de polling permite que configures los tiempos específicos para capturar los dispositivos y que midas su disponibilidad.
Tipo de dispositivo	Campo usado para escoger un icono para representar el dispositivo gráficamente en los Mapas. Es posible escoger entre: Cámara, Firewall, Enrutador, Servidor, Switch o Inalámbrico. El tipo estándar es el **Enrutador**.
Script de exportación de configuración	Selecciona los scripts exportadores de configuración.
Dominio	Asociación de dominio del dispositivo.
Grupos	Clica en el botón **Listar** y selecciona los grupos deseados para este dispositivo en uno o más puntos en el grupo de jerarquía.
Mapeadores	Selecciona el mapeador deseado para mapear objetos, con interfaces y cpus en este dispositivo.(Ve la sección configuración de mapeadores.)
Perfiles de alarma	Asocia el dispositivo a un perfil de alarma.

Creando un dispositivo utilizando el Asistente

Existe un asistente para la creación de un dispositivo que lo guiará y validará en cada paso.

1. Selecciona **Datos históricos** → **Dispositivos** → **Asistente** .
2. Rellena los campos de acuerdo con la tabla de encima.
3. Durante la creación, serás capaz de probar la conectividad del equipo, mapear los objetos del dispositivo y probar los objetos asociados a los perfiles, por ejemplo.
4. Después de esto, puedes visualizar y guardar su nuevo dispositivo.

Verificando objetos mapeados para el dispositivo

Clica en el icono de objetos mapeados en el menú lateral del árbol para ver todos los objetos mapeados del sistema. Accediendo al formulario de cada uno de ellos, puedes habilitar proyección y añadir una descripción para el objeto.

También es posible comprobar el histórico de configuración y borrar el objeto usando, respectivamente, los botones **Histórico** y **Borrar**.

Existe un filtro encima de la página con opciones para seleccionar objetos localizados y no localizados. Objetos no localizados son objetos mapeados que no fueron localizados por un mapeador del dispositivo. Ej.: un módulo de interfaz que fue eliminado por un enrutador llevará a esta interfaz a un estado de no localizado.

En el área del menú en árbol, debajo de cada dispositivo, el sistema muestra sus respectivos objetos mapeados. El color de los iconos indica las siguientes condiciones:

Icono verde	El objeto tiene un perfil asociado a él.
Icono sin color	El objeto no tiene un perfil asociado a él.
Icono rojo parpadeando	El objeto no fue localizado por el mapeador de procesos del objeto.

Importando archivos de dispositivo

Para importar un archivo de dispositivo, accede a **Datos Históricos → Dispositivos**.

Clica en el ítem **Dispositivos** en el árbol de menú.

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

Un archivo de dispositivo importado posee los siguientes campos:

Tabla 5.9. Campos del archivo de dispositivo

Campo	Descripción
Nombre	Posibles caracteres para el campo de nombre.
Descripción	Posibles caracteres para el campo de descripción (opcional).
Dirección IP de gestión	Dirección de IP. Ej.: 10.0.0.1
Versión SNMP	Tipo **1** para versión 1, **2c** para versión 2 y **3** para versión 3.
Community SNMP	Posibles caracteres para Community SNMP.
Protocolo de conexión	Escribe **SSH** o **TELNET**.
Usuario	Posibles caracteres para el campo nombre (opcional).
Contraseña de usuario	Posibles caracteres para el campo contraseña (opcional).
Contraseña de enable	Posibles caracteres para el campo contraseña (opcional).
Habilitar recolecta por el TRAFip	SÍ para habilitar y NO para deshabilitar la recolecta por el TRAFip.
Dirección IP del Netflow exporters	Lista de direcciones IP separados por coma. Ej.: 10.0.0.1,10.0.0.2
Configuración de sampling rate	Tendrá el valor 0 para manual y el valor 1 para flujo.
Netflow sampling rate	Valor entero mayor que 0.
Habilitar recolecta por el SLAview	SÍ para habilitar y NO para deshabilitar la recolecta por el SLAview.
Perfil automático	Selecciona **SÍ** para habilitar el uso de este dispositivo y sus objetos en un perfil automático.
Tipo de dispositivo	Campo usado para escoger un icono para representar gráficamente el dispositivo en los mapas. Escoge Cámara, Firewall, Enrutador, Servidor, Switch o Inalámbrico.

Operaciones por lotes

Algunas operaciones se pueden realizar de forma simultánea para varios dispositivos. Para ello, basta con seleccionar los dispositivos deseados y utilizar la lista de opciones **Habilitar** ubicada justo encima de la lista de dispositivos. Las operaciones disponibles:

- **TRAFip**: habilita recolecta por el TRAFip.
- **SLAview**: habilita recolecta por el SLAView.
- **CFGTool**: habilita gestión de configuración.
- **Inventário físico do CFGTOOL**: habilita recolecta de inventario físico.
- **CALLview**: habilita recolecta por CALLview.

Añadir metadatos de dispositivos

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **Dispositivos**, clica en el ítem **Dispositivo** 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 5.10. 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 un metadato creado a una dispositivo, accede a la lista de dispositivos y clica en el botón **Metadato** al lado del dispositivo que será configurado.

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

Importante

Si el icono del dispositivo se pone rojo, significa que todos los exportadores están indisponibles.

Grupos de interfaces

Los grupos de interfaces permiten análisis detalladas de una única interfaz o de un grupo de interfaz, porque los perfiles pueden ser aplicados a ellos y una interfaz puede ser asociada a más de un grupo de interfaz.

Para crear un nuevo grupo de interfaz, accede al menú **Datos históricos** → **Dispositivos** y clica en el botón **Nuevo**.

Tabla 5.11. Formulario de grupo de interfaz

Campo	Descripción
Nombre	Nombre del grupo de interfaz.
Descripción	Breve descripción del grupo de interfaz.
Tráfico límite (bps)	Este valor será trazado en el gráfico de tráfico con una línea punteada roja.
Habilitar proyección	Parámetros modelo de proyección. Para consejos de como configurar estos parámetros, ves a la sección Proyección.
Agrupamiento para grupo de interfaces	Grupo de interfaz de nivel más alto, solo organizativo. Accede a **Configuración** → **Objetos** → **Agrupamiento para grupo de interfaces** para configurar nuevos grupos.
Dominio	Dominio al grupo que esta interfaz pertenece.
Interfaces	Selecciona la interfaz que pertenece a este grupo.
Perfil de alarma	Asociación a un perfil de alarma.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.
Caja de selección de perfil	Selecciona el Perfil y como debe ser aplicado a esta interfaz.

Añadir metadatos de grupos de interfaz

Para acceder a la página de configuración de metadato, accede a **Datos históricos** → **Dispositivos**, clica en el ítem **Grupos de interfaz** 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 5.12. 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 grupo de interfaz, accede a la lista de grupos de interfaz y clica en el botón **Metadato** al lado del grupo que será configurado.

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

Tráfico no mapeado

Así se llama a todo el tráfico que no posea una interfaz de entrada o una interfaz de salida. Esto puede suceder por diversas razones: pérdida de paquete, tráfico destinado u originado para el propio dispositivo, problema de enrutamiento, etc.

Aplicaciones

El objeto de aplicación es representado por una regla que combina direcciones de IP, puertas y un protocolo de la capa 4 del modelo OSI.

Accede a **Datos históricos** → **Aplicaciones** → **Aplicación** para gestionar las aplicaciones corrientes configuradas y añadir nuevas.

Tabla 5.13. Formulario de aplicación

Campo	Descripción
Nombre	Nombre de aplicación.
Descripción	Breve descripción de la aplicación.
Tráfico límite (bps)	Este valor será trazado en el gráfico con una línea punteada roja.
Identificación por ID V9 de aplicación	Habilita este campo para identificar la aplicación por su ID.
Subred(es) de origen	Subredes para combinar contra el campo de flujo de dirección de IP de origen. Ej.: 10.0.0.0/24,10.1.0.0/16,192.168.1.1/32.
Puerta de origen	Puertas para combinar contra el campo de flujo de la puerta de origen.
Operación	Operación para ser realizada entre los campos de origen y destino. Ej.: 80,443-446,455
Subred(es) de destino	Subredes para combinar contra el campo de flujo de dirección de IP de destino.
Puerta de destino	Puertas para combinar contra el campo de flujo de la puerta de destino.
Classification engine ID	Un registro específico para las atribuciones de la aplicación.
Selector ID	Un registro específico para las atribuciones de la aplicación.
Grupo de aplicación	Haz la asociación de la aplicación con los grupos de aplicación, si lo deseas.
Protocolos	Selecciona la capa 4 del protocolo OSI para usar en esta aplicación.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.

Clasificación

Las aplicaciones serán clasificadas de acuerdo con la prioridad listada en **Datos históricos** → **Aplicaciones** → **Aplicación** .

Cada flujo corresponderá a una única aplicación.

Para cambiar la prioridad de clasificación, selecciona una o más aplicaciones y clica en las flechas para ARRIBA o para ABAJO que aparecen del lado izquierdo encima de la lista de aplicación.

Importar archivos de aplicación

Para importar un archivo de aplicación, accede a **Datos Históricos** → **Aplicaciones**.

Clica en el ítem **Aplicaciones** en el árbol de menú.

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

Una importación de aplicación tiene los siguientes campos:

Tabla 5.14. Campos de archivos de aplicación

Campo	Descripción
Nombre	Posible caracteres para el campo Nombre.
Descripción	Caracteres generales (opcional).
Tráfico límite (bps)	Valor entero mayor o igual a 0.
Subred(es) de origen	Lista de subred. Formato de entrada: IP1/Máscara1,IP2/Máscara2. (IP/32 en el caso de usar una IP única). Ej.: 10.0.0.0/24,10.0.1.0/24. Puedes usar * para todas las subredes de origen.
Puerta de origen	Lista de enteros entre 1 y 65535, separados por coma. Puedes usar * para todas las puertas de origen.
Operación	Introduce 1 para operación O , 2 para operación E.
Subred(es) de destino	Lista de subred. Formato de entrada: IP1/Máscara1,IP2/Máscara2. (IP/32 en el caso de usar una IP única). Ej.: 10.0.0.0/24,10.0.1.0/24. Puedes usar * para todas las subredes de destino.
Puerta de destino	Lista de enteros entre 1 y 65535, separados por coma. Puedes usar * para todas las puertas de destino.
Protocolos	Capa 4 del protocolo OSI, separado por coma. Ej.: UDP,TCP (opcional).

Añadir metadatos de aplicaciones

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **Aplicaciones**, clica en el ítem **Aplicación** 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 5.15. 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 una aplicación, accede a la lista de aplicaciones y clica en el botón **Metadato** al lado de la aplicación que será configurada.

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

Grupos de aplicación

Los grupos de aplicación serán útiles para organizar sus aplicaciones. Usando este tipo de objeto, podrás tener una visión consolidada de un grupo de aplicaciones.

Para configurar un nuevo grupo de aplicación, accede al menú **Datos Históricos** → **Aplicaciones** → **Grupo de aplicación** .

Tabla 5.16. Formulario de grupo de aplicaciones.

Campo	Descripción
Nombre	Define un nombre.
Descripción	Describe el nuevo grupo de aplicación.
Tráfico límite (bps)	Este valor será trazado en el gráfico con una línea punteada roja.
Aplicación	Selecciona las aplicaciones que serán asociadas a este grupo de aplicación.
Perfil de Tráfico	Accede a la sección Perfiles de tráfico.

Añadir metadatos de grupos de aplicación

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **Aplicaciones**, clica en el ítem **Grupo de aplicación** 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 5.17. 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 grupo de aplicación, accede a la lista de grupos de aplicación y clica en el botón **Metadato** al lado del grupo que será configurado.

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

Protocolos

Este objeto se refiere a la capa de transporte del modelo TCP/IP. Es representado, básicamente, por un número indicando el protocolo de cada flujo. Ejemplo: 17 para tráfico UDP y 6 para tráfico TCP.

Accede a **Datos históricos** → **Protocolos** → **Protocolo** para gestionar los protocolos configurados y añadir nuevos.

Tabla 5.18. Formulario de protocolo

Campo	Descripción
Nombre	Nombre del protocolo.
Descripción	Descripción del protocolo.
Número	Número del protocolo.
Tráfico límite (bps)	Este valor será trazado en el gráfico de tráfico con una línea punteada roja.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.

Importar archivos de protocolos

Para importar un archivo de protocolos, accede a **Datos Históricos** → **Protocolos**.

Clica en **Protocolos** en el árbol del menú.

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

Un protocolo importado posee los siguientes campos:

Tabla 5.19. Campos del archivo de protocolo

Campo	Descripción
Nombre	Posible caracteres para el campo Nombre.

Campo	Descripción
Número	Valor entero entre 0 y 255.
Descripción	Caracteres generales (opcional).
Tráfico límite (bps)	Valor entero mayor o igual a 0.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.

Añadir metadatos de protocolos

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **Protocolos**, clica en el ítem **Protocolo** 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 5.20. 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 protocolo, accede a la lista de protocolos y clica en el botón **Metadato** al lado del protocolo que será configurado.

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

ASN

Como definido en el RFC 1930, un sistema autónomo es una colección de prefijos de enrutamiento IP conectados sobre control de uno o más operadores de redes que representa una común y claramente definida política de enrutamiento para internet.

Este objeto combina el campo de AS origen del flujo para formar su tráfico de origen y el campo de AS destino del flujo para formar su tráfico de destino.

Sugerencia

Algunos enrutadores pueden rellenar el campo de AS del flujo con el AS destino final/origen o con las informaciones de emparejamiento del AS. En los enrutadores Cisco, puedes configurar el comando:

```
ip flow-export version {1|5|9 [origin-AS|peer-AS/}
```

Para configurar un nuevo AS, accede a **Datos históricos** → **ASN** → **Sistema autónomo** .

Tabla 5.21. Formulario de sistemas autónomos

Campo	Descripción
Nombre	Nombre AS.
Descripción	Descripción AS.
Habilitar proyección	Parámetros modelos de proyección. Accede a sección Proyección para consejos sobre como configurar estos parámetros.
Número	Número AS. Para configurar una lista de números, sepárelos por comas.
Tráfico límite (bps)	Este valor será trazado en el gráfico de tráfico con una línea punteada roja.
Grupo de AS	Asociación de grupo AS.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.
Caja de selección de perfil	Selecciona el perfil y como debe ser aplicado a este AS.

Importar archivos de sistemas autónomos

Para importar un archivo del dispositivo, accede a **Datos Históricos** → **ASN**.

Clica en el ítem **Sistema autónomo** en el árbol de menú.

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

Un sistema autónomo importado posee los siguientes campos:

Tabla 5.22. Campos de un archivo de sistema autónomo

Campo	Descripción
Nombre	Posibles caracteres para el campo de nombre.
Número	Lista de enteros entre 1 y 65535, separados por coma.
Descripción	Caracteres generales (opcional).
Tráfico límite (bps)	Valor entero mayor o igual a 0.

Importar archivos de sistemas autónomos

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **ASN**, clica en el ítem **Sistema Autónomo** 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 5.23. 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 sistema autónomo, accede a la lista de sistemas autónomos y clica en el botón **Metadato** al lado del AS que será configurada.

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

Grupos de sistema autónomo

Puedes usar grupos AS para tener una visión consolidada de un grupo de sistemas autónomos. Por ejemplo, los ASs de cada continente.

Para configurar un nuevo AS, accede a **Datos históricos** → **Sistema autónomo** → **Grupo de sistema autónomo** .

Tabla 5.24. Formulario de grupo de sistemas autónomos

Campo	Descripción
Nombre	Nombre de AS.
Descripción	Descripción de AS.
Habilitar proyección	Parámetros modelos de proyección. Accede a sección proyección para consejos sobre como configurar estos parámetros.
Tráfico límite (bps)	Este valor será trazado en el gráfico de tráfico con una línea punteada roja.
Sistema autónomo	Sistemas autónomos que deben ser colocados en este grupo.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.
Caja de selección de perfil	Selecciona el perfil y como debe ser aplicado a este grupo de AS.

Añadir metadatos de grupos de AS

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **ASN**, clica en el ítem **Grupo de AS** 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 5.25. 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 grupo de AS, accede a la lista de grupos de sistemas autónomos y clica en el botón **Metadato** al lado del grupo que será configurado.

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

Tipo de servicio

El objeto de tipo de servicio representa el campo ToS del encabezado de la dirección IP. Esta campo es exportado para cada flujo y no tiene ni origen ni destino.

Este campo es usualmente utilizado para marcar paquetes que están en el borde de red, después pueden ser tratados con la política QoS apropiada por los enrutadores principales.

> **Importante**
>
> Se consciente de que el netflow Cisco no va a exportar el campo ToS con el valor correcto del tráfico saliendo por el borde de los enrutadores para los enrutadores de la red principal si los paquetes son marcados en la interfaz WAN. Así, solo los paquetes que vengan de los enrutadores principales poseerán valores exportados correctos en el campo de ToS, porque ya están marcados cuando llegan al borde del enrutador. Para tener el flujo de paquetes provenientes del enrutador principal marcados correctamente, debes marcar los paquetes en la interfaz LAN.

Para gestionar los objetos ToS, accede a **Datos históricos** → **ToS** → **ToS** .

Tabla 5.26. Formulario de ToS

Campo	Descripción
Nombre	Nombre ToS.
Descripción	Descripción del ToS.
Número	Número del ToS.
Tráfico límite (bps)	Este valor será trazado en el gráfico de tráfico con una línea punteada roja.
Habilitar proyección	Parámetros modelos de proyección. Accede a sección proyección para consejos sobre como configurar estos parámetros.
Grupo ToS	Asociación de grupo ToS.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.

Campo	Descripción
Caja de selección de perfil	Selecciona el perfil y como debe ser aplicado a este grupo de ToS.

Importar archivos ToS

Para importar un archivo ToS, accede a **Datos Históricos** → **ToS**.

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

Clica en el botón Importar y carga el archivo.

Un archivo de ToS importado posee los siguientes campos:

Tabla 5.27. Campos de los archivos ToS

Campo	Descripción
Nombre	Posibles caracteres para el campo de nombre.
Número	Lista de enteros entre 1 y 65535, separados por coma.
Descripción	Caracteres generales (opcional).
Tráfico límite (bps)	Valor entero mayor o igual a 0.

Añadir metadatos de ToS

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **ToS**, clica en el ítem **ToS** 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 5.28. 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 ToS, accede a la lista de ToS y clica en el botón **Metadato** al lado del ToS que será configurado.

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

Grupo de ToS

Puedes usar los grupos ToS para tener una visión consolidada de un grupo de ToS. Por ejemplo, los ToS usados para marcar el tráfico de vídeo.

Para configurar un nuevo grupo de ToS, accede a **Datos históricos** → **ToS** → **Grupo de ToS** .

Tabla 5.29. Formulario de grupo de ToS

Campo	Descripción
Nombre	Nombre del grupo de ToS.
Descripción	Nombre del grupo de ToS.
Habilitar proyección	Parámetros modelos de proyección. Accede a sección proyección para consejos sobre como configurar estos parámetros.
Tráfico límite (bps)	Este valor será trazado en el gráfico de tráfico con una línea punteada roja.
ToS	Objetivos ToS que deben ser colocados en este grupo.
Perfil de Tráfico	Comprueba la sección Perfiles de tráfico.
Caja de selección de perfil	Selecciona el perfil y como debe ser aplicado a este grupo de ToS.

Añadir metadatos de grupos de ToS

Para acceder a la página de configuración de metadato, accede a **Datos Históricos** → **ToS**, clica en el ítem **Grupos de ToS** 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 5.30. 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 grupo de ToS, accede a la lista de grupos de ToS y clica en el botón **Metadato** al lado del grupo que será configurado.

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

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 5.31. 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.
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.

Cubo de Datos

El informe de cubo de datos presenta una visión consolidada del tráfico por objeto. A través suyo, podrás construir análisis donde el tráfico puede ser quebrado por todos los objetos, no se limitando a los Perfiles de Tráfico.

Así, podrás descubrir, por ejemplo, el total de bytes, paquetes y flujos transitados de una interfaz A a una interfaz B, de la aplicación X, en el ToS CSO, de las 10:00 a las 22:00. En el modo **Tabla dinámica**podrás incluso, tener una visualización gráfica de este tráfico.

Tabla 5.32. Formulario de informe de cubo de datos

Campo	Descripción
Instante inicial	Introduce el horario de inicio del periodo en el formato dd/mm/aaaa.
Instante final	Introduce el horario final del periodo en el formato dd/mm/aaaa.
Tipo	Si escoges el tipo de **Tabla**, el informe generado mostrará una tabla con los valores de **Bytes**, **Paquetes y Flujos** para los campos escogidos. Si escoges **Tabla dinámica**, podrás configurar que objetos aparecerán como columna y cuales aparecerán como línea. Así, tendrás una matriz con los valores de **Bytes** para los campos escogidos y además podrás visualizar este resultado de forma gráfica. Para generar el gráfico, clica en el check box de la línea deseada y clica en **Generar gráficos**.
Exhibir desconocidos	Este campo solo aparece cuando el tipo de informe es **Tabla dinámica**. Selecciona **Sí** para que sean considerados, incluso, el tráfico de objetos que no están añadidos al sistema. Aparecerán en el informe como **[Desconocido]**.
Ordenar por	Este campo solo aparece cuando el tipo de informe es **Tabla**. Selecciona **Bytes**, **Paquetes** o **Flujos** de acuerdo con tu preferencia de ordenación. Los mayores valores para la unidad escogida aparecerán en la parte superior del informe.
Formato	Selecciona uno de los formatos para el informe: HTML, CSV o TSV.
Campos del informe	Selecciona que campos deben ser usados para agregación.

Importante

Este informe posee un periodo máximo de 31 días.

Top N Caracterizado

El informe Top N Caracterizado posibilita que visualices objetos por ruptura de tráfico a través de gráficos circulares.

Para cada objeto, se muestran los Top 5 de la entrada y de la salida de los objetos del perfil de tráfico seleccionado.

Para tener datos en este informe, necesitas configurar objetos y asociarlos al perfil de tráfico, que debe contener otros objetos.

De esta forma, serás capaz de obtener una visión consolidada de distribución de subredes por grupos de interfaces, por ejemplo.

Tabla 5.33. Informe Top N Caracterizado

Campo	Descripción
Instante inicial	Introduce el horario de inicio del periodo en el formato dd/mm/aaaa.
Instante final	Introduce el horario final del periodo en el formato dd/mm/aaaa.
Número de objetos	Rellena con un valor entero para definir cuantos objetos se mostrarán. El valor máximo es **100**.
Tipo de objeto	Selecciona el tipo de objeto que será roto por el perfil de tráfico.
Tipo del perfil de tráfico	Selecciona el tipo de perfil de tráfico: **ContenidoDistribución o Matriz**.
Tipo de objetos del perfil	Selecciona el tipo de objeto del perfil de tráfico.
Ordenar por	Define si los objetos serán ordenados por el m4(Media) o por el **Porcentaje del límite**.

Mapeo de IPs

IP Mapper es un agente de asignación de direcciones IP asociadas a un nombre. El usuario debe configurar una secuencia de comandos de asignación y el intervalo de ejecución del agente (en minutos). El script se puede configurar accediendo a la opción **Mapeo de IPs** en **Configuración** → **Scripts**. El IP Mapper debe estar habilitado en **Sistema** → **Parámetros** → **Mapeo de IP** , donde también es posible configurar el intervalo de ejecución y el período máximo de almacenamiento del historial.

Para ver la asignación de direcciones IP y nombres, acceda a la ruta **Datos históricos** → **Informes** → **Mapeo de IPs** .

Tabla 5.34. Formulario de Mapeo de IPs

Campo	Descripción
Filtro por nombre	Llene para filtrar por nombre.
Filtro por IP	Llene para filtrar por la dirección IP.
Filtrar por horario de asignación	Seleccione para utilizar filtros por hora inicial y final de asignación.
Horario inicial de asignación	Rellene con el horario inicial deseado.
Horario final de asignación	Preencha com o horário final desejado.

Top N

Definiciones

Los informes Top N generan estadísticas consolidadas para todos los tipos de objetos.

El informe de salida mostrará estadísticas de todos los objetos del tipo seleccionado, incluyendo el porcentaje utilizado del trafico límite.

Generando un nuevo informe

1. Accede a **Datos históricos** → **Informes** → **Top N** .
2. Escoge un tipo de objeto deseado o un modelo de la lista de modelos.
3. Rellena el formulario:

Tabla 5.35. Informe Top N

Campos	Descripción
Generar informe | Guardar modelo	Escoge un informe de una única ejecución o guarda el modelo.
Tipo de objeto	Automáticamente rellenado con el tipo de objeto seleccionado.
Filtro por nombre	Usa expresiones regulares para filtrar.
Filtro de ifAlias	Filtra por la OID ifAlias SNMP en caso de informes de interfaz.
* Fabricante	Filtro por el fabricante del objeto. Tienes que usar expresiones regulares para filtrar.
* Tipo de fabricante	Filtra por el tipo de fabricante del objeto. Tienes que usar expresiones regulares para filtrar.
Instante inicial	Selección de fecha para instante inicial.
Instante final	Selección de fecha para instante final.
Excluir fines de semana	Excluir periodo de fines de semana en el informe de datos.
Intervalo	Si todas las opciones están marcadas, este campo es ignorado, en caso contrario, el dato es seleccionado con ese intervalo para cada día.
Sentido	Escoge un sentido para filtrar el tráfico. En caso de que selecciones **Ambos**, podrásm4_bold(Agrupar por objetos), o sea, el informe será ordenado por la mayor entrada y salida, mostrando el Origen y el Destino de cada objeto en dos líneas consecutivas.
Ordenar por	Este campo solo aparece cuando el sentido es **Ambos**. Escoge si el informe será ordenado por entrada, salida, porcentaje de uso del límite o por el máximo de porcentaje de uso del límite.
Unidad	Escoge la unidad para mostrar el tráfico.
Formato de salida	Opción disponible solo para informes que no son de modelo. A partir del momento que el informe se convierte en un modelo esta opción es ignorada.
Porcentaje	Usa porcentaje para computar los resultados del informe.

* Disponible solo para informes de Dispositivos, Interfaces e Interfaces SNMP.

Sugerencia

Si seleccionas paquetes o flujos debajo del campo de unidad, serás capaz de detectar actividades sospechosas, como una subred con un número de paquetes o flujos que no es compatible con su tráfico.

Perfil de Tráfico

Definiciones

Este informe está basado en los datos resumidos.

Para tener datos en este informe, necesitas configurar objetos y asociarlos al perfil de tráfico, que debe contener otros objetos.

De esta forma, podrás ser capaz de obtener una matriz de tráfico de, por ejemplo, subredes por subredes, subredes por aplicaciones, interfaces por subredes y otros.

Generando un nuevo informe

1. Accede a **Datos históricos** → **Informes** → **Perfil de tráfico** → **Nuevo informe** .
2. Rellena el formulario:

Tabla 5.36. Informe de perfil de tráfico

Campos	Descripción
Generar informe | Guardar modelo	Escoge un informe de una única ejecución o guarda el modelo.
Dominio	Escoge el dominio:
Tipo de asociación al perfil	Escoge el tipo de asociación. Por ejemplo, para perfil de aplicaciones escoge el contenido.
Tipo de objetos del perfil	Escoge el tipo de perfil.
Filtro de tipo de objeto	Filtra para el perfil de objetos. El perfil de objetos será introducido. Filtra para el perfil de objetos. Los objetos de perfil serán situados sin una columna de informes.
Tipo de objeto	Escoge un tipo de objeto.
Filtro de objeto	Filtra para los informes de objetos. Debes usar una expresión regular para filtrar.
Análisis de tráfico	Este campo definirá las opciones de unidades del informe. Escoge entre **Absoluto** o **Tasa media**.
Medida	Escoge la unidad de los datos del informe.
Sentido	Escoge el sentido del tráfico.
Instante inicial	Escoge el instante inicial del informe para seleccionar los datos.
Instante final	Escoge el instante final del informe para seleccionar los datos.
Excluir fines de semana	Excluir periodo de fines de semana en el informe de datos.

Campos	Descripción
Intervalo	Si todas las opciones están marcadas, este campo es ignorado, en caso contrario, el dato es seleccionado con ese intervalo para cada día.
Porcentaje de límite	Escoge esta opción para tener un dato del informe del tráfico límite configurado en cada objeto. Esta opción trabajará solo cuando la unidad seleccionada sea bytes, siempre que el tráfico límite también esté en bytes.
Formato de salida	Opción disponible solo para informes no-modelos. Una vez que el informe se torna un modelo, esta opción es ignorada.
Usa prefijo SI	Usa el prefijo SI para mostrar 40.469722M en vez de 40469722, por ejemplo.
Funciones	Elija funciones de agregado para uso en el informe. Las funciones disponibles son Media, Máximo, Mínimo, Percentil y Suma.

Syslog

Definiciones

Puedes configurar cualquier dispositivo para enviar mensajes Syslog al TRAFip.

Los mensajes son recibidos por la puerta UDP 514.

Los mensajes syslog serán almacenados y borrados basados en la configuración de almacenamiento syslog.

Generando un nuevo informe

1. Accede a **Datos históricos** → **Informes** → **Syslog** → **Nuevo informe** .
2. Rellena el formulario:

Tabla 5.37. Informe Syslog

Campos	Descripción
Inicio	Introduce el horario de inicio del periodo en el formato dd/mm/aaaa.
Fin	Introduce el horario final del periodo en el formato dd/mm/aaaa.
Mensaje	Filtra el mensaje syslog. Deja en blanco para tener todos los mensajes.
Prioridad	Selecciona el mensaje prioritario Deja 0 para tener todas las prioridades.
Nivel	Selecciona el nivel de mensaje syslog. Escoge **Todas** para tener todas los mensajes.
Número de líneas	Escoge un límite de líneas para la salida del informe: **10000** o **Ilimitado**. En caso de que

Campos	Descripción
	selecciones **Ilimitado**, el informe debe generarse en el formato CSV Opción disponible solo para informes que no son modelo. Una vez que un informe se torna un modelo, esta opción es ignorada.
Formato de salida	Escoge el formato en que el informe se generará. Opción disponible solo para informes que no son modelo. Una vez que un informe se torna un modelo, esta opción es ignorada.
Filtros	Filtra los mensajes Syslog a partir de la **Dirección IP de gestión**, del **Nombre** o de un **metadato** del host. Usa expresiones regulares para filtrar los objetos. Al menos un campo de filtro debe rellenarse

3. Clica en el botón Enviar.

Dados brutos

Definiciones

Los informes de datos brutos suministran estadísticas detalladas y consolidadas para todos los flujos recolectados por el TRAFip.

Cuantos más campos selecciones, mayor y más detallado será tu informe.

Generando un nuevo informe

1. Accede a **Datos históricos** → **Informes** → **Datos brutos** .
2. Escoge la opción **Programar nuevo informe** o un modelo de la opción **informes programados.**
3. Rellena el formulario:

Tabla 5.38. Informe de datos brutos

Campo	Descripción
Generar informe | Guardar modelo	Escoge el informe de una única ejecución o guarda un modelo para guardar un informe como un modelo.
Formato de salida	Opción disponible solo para informe que no es modelo. Escoge el formato de salida deseado:
Número de líneas	Opción disponible solo para informe que no es modelo. Puedes cambiar el número máximo de líneas en **Sistema** → **Parámetros** → **Informes** en la opción **Número máximo de líneas por informe**.
Exhibir IP de las interfaces	Marca esta opción para que la IP de la interfaz se muestre en el informe cuando el campo de interfaz sea seleccionado.

Campo	Descripción
Inicio de datos	Escoge el horario inicial para seleccionar los datos brutos. El proceso de resumen se ejecuta cada cinco minutos. Después, el minuto debe rellenarse con múltiples de 5.
Tipo de objeto	Tipo de objeto que será usado en este informe.
Objeto	Selecciona el objeto para este informe. Los objetos disponibles dependerán del tipo de objeto seleccionado.
Intervalo	Selecciona el intervalo del informe. Ej.: Si seleccionas 10 min., el informe será seleccionado del campo **Inicio de los datos** más 10 minutos.
Dirección	Selecciona la dirección en la que el tráfico debe filtrarse.
Ordenar por	Selecciona la unidad para ordenar los datos del informe.
Excluir objetos del perfil	Esta opción filtrará fuera los objetos del perfil seleccionado. Esto es muy útil para encontrar tráfico indefinido.
Tratamiento de sampling rate	Escoge si el número de paquetes y bytes de los flujos deben ser multiplicados por el sampling rate o configurados por el dispositivo. Si escoges la opción de configuración, debes ir al campo Configuración de sampling rate en el formulario de configuración del dispositivo.
Resumen temporal de los flujos	Maca sí y las entradas del informe con las mismas llaves serán resumidas en el tiempo. En este caso, el tiempo inicial y el tiempo inicial del primer flujo, el tiempo final y el tiempo final del último flujo y la duración es la diferencia entre estos valores.
Formatear duración	Marca esta opciones para tener una duración de flujo formateada en horas, minutos y segundos.
Campos del Netflow	Escoge el campo de netflow para este informe. También puede ser editado en el informe generado y será recargado.
Lista de los flujos	Marca esta opción para tener todos los flujos listados.
Filtros	Los filtros serán automáticamente rellenados dependiendo de la opción del gráfico. Por ejemplo, si seleccionas solo la opción **Curva**, los filtros reflejarán esto. También puedes añadir más filtros al informe.

4. En el informe generado, puedes traducir: dirección de IP para grupo, dirección de IP para subred, dirección de IP por IP Mapper, dirección de IP para nombre de host, dirección de IP para netbios, número de AS, flujos para aplicación, flujos para ToS y flujos para grupo de ToS. Además, podrás visualizar un Top 10 de los objetos en forma de gráfico circular (para ello, clica en el icono ).

5. Clicando en la IP de origen o en la IP de destino, será exhibida una animación mostrando el flujo-a-flujo de la IP seleccionada dentro de un periodo de 5 minutos.

Sugerencia

El banco de datos de los datos brutos es indexado por exportadores de direcciones IP, por lo que si conoces el dispositivo o la interfaz que exportó el tráfico que deseas analizar, debes emitir el informe de datos brutos en el dispositivo o interfaz. De esta forma el informe será más rápido y demandará menos recursos del sistema.

Informe de Proyección

Una vez que este recurso está activado, el sistema es capaz de prever el comportamiento de cualquier curva de un gráfico e informar la violación de fecha de un determinado nivel, o, fecha a fecha, informar el valor de la curva.

Configuración

Accede a **Sistema** → **Parámetros** → **Proyección**

Tabla 5.39. Formulario de configuración de proyección

Campo	Descripción
Grados de libertad	El orden polinominal para ser usado. Actualmente, solo la primera orden polinominal es soportada.
Muestra	Configura la muestra por día, semana, o mes para el proceso de proyección.
Histórico	Configura el número de muestras que serán analizadas. Ej.: Si escoge el valor **6** para histórico y **semana** para muestra, el sistema analizará 6 semanas atrás para realizar la proyección.
Intervalo	Si la opción **Día todo** está marcada, este campo es ignorado. En caso contrario, la proyección va considerar solo el intervalo configurado para cada día.

Habilitado proyección para una curva gráfica

1. Accede a **Configuración** → **Perfiles de tráfico**.
2. Clica en el botón Editar para el perfil deseado o crea uno nuevo.
3. Clica **Sí** en la caja de selección **Habilitar proyección** y escoge **Sí** en **Usar configuraciones modelo** o personaliza las configuraciones para esa curva.

Importante

Los informes de análisis de proyección estarán disponibles un día después de habilitar el recurso, ya que el proceso de proyección se ejecuta con una base diaria.

Informes gráficos

1. Accede al gráfico que contiene la curva configurada por proyección, clica con el botón derecho en él y selecciona la opción **Violación de proyección**.

2. Selecciona la curva deseada en la caja de popup, introduce un valor para él y clica OK para tener una tasa de crecimiento y la fecha de violación.

Generando un nuevo informe

1. Accede a **Datos históricos** → **Informes** → **Proyección** → **Nuevo informe** .

2. Rellena el formulario:

Tabla 5.40. Formulario de informe de proyección

Campo	Descripción	
Tipo de proyección	Escoge el Perfil de Objeto u Objeto	
Perfil	Selecciona el perfil de objeto.	
Objeto de perfil	Selecciona el perfil de objeto.	
Tipo de objeto	Selecciona un tipo de objeto.	
Filtro de objeto	Filtra por los objetos asociados al perfil.	
Formato de salida	Opción disponible solo para informes que no son modelo. Una vez que el informe se torna un modelo, esta opción es ignorada.	
Violación de límite | Estimativa	Violación de límite	Si escoges esta opción, tendrás que seleccionar uno de los siguientes modos: **Tasa** o **Porcentaje de banda**. Seleccionando el modo **Tasa**, deberás introducir un valor entero y su unidad es bits por segundo (bps). El resultado será la fecha en que la tasa media excede el valor rellenado. Seleccionando el modo **Porcentaje de banda**, deberás introducir un valor entero entre 0 y 100 y su unidad es %. El resultado será la fecha en que la tasa

Campo	Descripción	
		media excede el valor porcentual del límite que rellenaste. Por ejemplo, puedes descubrir cuando el tráfico límite de un objeto será alcanzado.
	Estimación	Si escoges esta opción, introducirás una fecha y un horario. El resultado será el valor de la curva en el momento rellenado.
Entrada de datos	Es posible realizar una operación (**Añadir** o **Sustraer**) sobre los valores de la curva para calcular la proyección. Además puedes escoger el tipo de entrada (modo **Absoluto** o **Relativo [%]**). Basta seleccionar las opciones deseadas e introducir el valor, en bits/s.	

3. Después de rellenar el formulario, clica en **Enviar** para generar el informe, que mostrará los objetos, la dirección, la fecha estimada o el valor estimado de violación, el tráfico límite del objeto (en bps) y la cantidad usada de este límite.

Graph set

El graph set es un informe gráfico donde puedes visualizar múltiples gráficos en modo grid en el área de visualización de los datos.

Definiciones

Usuarios del tipo **Operador** y **Configurador** son capaces de gestionar solo sus propios graph sets.

Usuarios **administradores** son capaces de visualizar, editar y borrar todos los graph sets, pero no pueden crear un graph set para un usuario específico.

Creación

Accede a la ruta **Datos históricos** → **Graph set** → **Nuevo graph set** .

Tabla 5.41. Creación de graph set

Campo	Descripción
Nombre	Nombre del graphset.

Campo	Descripción
Descripción	Descripción sobre el graphset.
Tiempo entre diapositivas	Tiempo en segundos para cambiar las diapositivas utilizadas en la visualización NOC.
Exhibir en el NOC	Selecciona **Sí** para que el gráfico esté disponible en el NOC display.
Guardar en	Ruta para guardar una imagen del graphset. Ejemplo: C:\Users\Telco\Images
Dimensiones	Dimensiones de la imagen guardada.

Añadiendo gráficos

1. Accede a cualquier gráfico.
2. Clica en el gráfico con el botón derecho del ratón.
3. Accede a la opción **Asociar al Graph Set** en el popup menú y selecciona el graph set deseado.

Hay otra manera de añadir gráficos al graph set. Hace posible la adición de gráficos de los tipos barra y circular. Sigue el procedimiento de abajo:

1. Accede al graph set;
2. Clica en el símbolo **+**;
3. Rellena los campos (tipo de objeto, objetos, gráficos, tipo de gráfico y período);
4. Clica en **Introducir gráfico**.

Sugerencia

Para desasociar un gráfico, basta clicar en el símbolo **X** a su lado.

Visualizando un graph set

1. Accede a la ruta **Datos históricos → Graph Set**
2. Clica en el icono del Graph Set deseado que está en el árbol del menú.

Editando un graph set

1. Clica en **Datos históricos → Graph set**.
2. Escoge uno de los siguientes botones:
   - **Dependencias** para borrar el gráfico de un graph set.
   - **Editar** para cambiar los campos de nombre y descripción del graphset.
   - **Borrar** para borrar el graph set.

Generando gráficos para un graph set

1. Accede al graph set;
2. Clica en el símbolo ⚙;
3. Selecciona una de las opciones:
   - **Visualizar gráficos** para configurar el tiempo de inicio para los gráficos mostrados en la pantalla.
   - **Guardar imágenes** para generar y guardar cada gráfico como una imagen en el formato PNG.
4. Rellena los campos:
   - **Inicio de los datos**: Momento de inicio del gráfico;
   - **Guardar en**: Ruta para guardar una imagen del graph set. Ejemplo: C:\Users\Telco\Images;
   - **Dimensiones**: Dimensiones de la imagen que será guardada.
5. Clica en el botón **Generar gráficos**.

Capítulo 6. Configuración

Perfiles de tráfico

Definiciones

Los perfiles de tráfico te permiten construir análisis donde el tráfico de ciertos objetos pueden ser discriminados en otros objetos.

Para construir este tipo de análisis, tienes que configurar un perfil, introducir objetos en él y después asocial el perfil a otro objeto.

El banco de datos formado por esta configuración será la base para mostrar el perfil gráfico e informes como el informe de perfil de tráfico.

Algunos ejemplos de análisis de perfil son: interfaz contra aplicaciones, subredes contra subredes, subredes contra aplicaciones y así en adelante.

Configuración

1. Accede **Configuración** → **Perfiles de tráfico**.
2. Clica en el botón Nuevo para crear un nuevo perfil.
3. Rellena el formulario abajo:

Tabla 6.1. Formulario de perfil de tráfico

Campo	Descripción
Nombre	Nombre del perfil
Tipo	El tipo de perfil te permitirá seleccionar los objetos de un tipo asociado de ese perfil.
Curvas de gráfico	Escoge los objetos que pertenecerán a este perfil y los colores de sus curvas en el gráfico. Para ello, arrastra los objetos de la caja izquierda a la derecha y después clica en el botón **Editar colores**.
Subtítulo indefinido modelo	Si quieres renombrar la curva **Indefinida**, selecciona **No** y rellena el campo **Rótulo** de la manera que desees.
Proyección	Escoge si quieres habilitar la Proyección para alguna curva. Ves a la sección Proyección para informaciones sobre como configurar estos parámetros.
Caja de selección de objeto	Usa este menú para seleccionar los objetos cuyo tráfico será analizado por este perfil. En la primera capa, selecciona el tipo de objeto, luego el sistema te mostrará los objetos disponibles

Campo	Descripción
	y, en la segunda capa, selecciona los tipos de análisis.

Objetos disponibles

- Aplicación
- Grupo de aplicación
- Grupo de Interfaces
- Grupos de sistemas autónomos
- Grupo de subredes
- Grupo de ToS
- Objeto mapeado
- Protocolo
- Sistema autónomo
- Subred
- ToS

Tipos de análisis

El tipo de análisis que seleccionas cuando un objeto es asociado a un perfil dictará la forma con la que el tráfico será clasificado.

Existen tres tipos de análisis disponibles, los cuales serán explicados a continuación.

Matriz

Los objetos del perfil de tráfico se buscan en la dirección opuesta al tráfico que está siendo analizado.

Por ejemplo, vamos a suponer que un perfil de tráfico compuesto por subredes es asociado a una subred abajo de este tipo de análisis. Después, para el tráfico de destino de subred, el TRAFip intentará igualar las subredes del perfil de tráfico contra el campo de origen IP. Para el tráfico de origen de subred, el TRAFip intentará igualar las subredes del perfil de tráfico contra el campo IP de destino.

Este tipo de asociación de perfil habilita el análisis del tráfico cambiado entre la oficina central y una oficina regional de la empresa, por ejemplo.

Para establecer este análisis, sigue el procedimiento siguiente:

1. Crea una subred para cada oficina regional y una subred para la oficina central.
2. Crea un perfil de tráfico que contenga las subredes de la oficina regional.
3. Asocia un perfil de tráfico a la subred de la oficina central usando el tipo de análisis **Matriz**.

Distribución

Los objetos del perfil de tráfico se buscan en la misma dirección del tráfico que está siendo analizado.

Por ejemplo, vamos a suponer que un perfil de tráfico compuesto de subredes es asociado a una subred bajo este tipo de análisis. Después, para el tráfico de destino de subred, el sistema intentará igualar las subredes del perfil de tráfico contra el campo de origen IP. Para el tráfico de origen de subred, el sistema intentará igualar las subredes del perfil de tráfico contra el campo IP de origen.

Este tipo de asociación de perfil permite el análisis de como detallar el tráfico de entrada y salida de un grupo de subredes. Esto es útil, por ejemplo, para comprobar el balance de un grupo de servidores.

Para establecer este análisis, sigue el procedimiento siguiente:

1. Crear una subred para cada servidor.
2. Crear un grupo de subred que contenga servidores de subred.
3. Crear un perfil de tráfico que contenga servidores de subredes.
4. Asociar el perfil de tráfico al grupo de subred usando el tipo de análisis de distribución.

Contenido

El tipo de análisis de contenido se usa por objetos, donde no existe noción sobre el tráfico de origen o destino.

Estos objetos son, por ejemplo, protocolos, aplicaciones y ToS. Así, para cada flujo, existe solo un protocolo, una aplicación y un ToS.

Siempre que crees perfiles con este tipo de objeto, usa el tipo de análisis de contenido.

Dominios

Este objeto permite que todos los objetos, excepto los dispositivos, interfaces y grupos de interfaces sean resumidos, considerando solo el flujo de cada dominio.

Los dominios son generalmente usados para separar flujo de tráfico similar a través de los diferentes enrutadores. Ej.: enrutadores de borde y enrutadores de backbone.

Para cambiar de domino, usa la caja de selección que aparece en la pestaña **Datos Históricos** con cada nombre de dominio.

Definiciones

- Un dominio está compuesto de dispositivos.
- Un dispositivo solo puede ser asociada a un domino.
- Tráfico dominio total: compuesto por la suma de todos los flujos pertenecientes a los dispositivos de dominio.

Configuración

Para crear un nuevo dominio, accede a **Configuración** → **Dominios** y clica en el botón Nuevo.

Tabla 6.2. Formulario de Dominio

Campo	Descripción
Nombre	Introduce un nombre para el dominio.
Intervalo entre alarmas (seg)	Solo se emitirá una alarma del mismo tipo (de alarma) después de que este período haya pasado, en relación a la incidencia previa.
Límite de tiempo para acumular tráfico (seg)	Ese 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.
Threshold en Bytes (acumulado en el período)	Límite de bytes recibidos/enviados por/para un host para activar una alarma. Una alarma de tráfico sospechoso del tipo Alto flujo de datos entre dos IPs se activará en caso de que este límite sea alcanzado.
Threshold en Paquetes (acumulado en el período)	Límite de paquetes recibidos/enviados por/para un host para activar una alarma. Una alarma de tráfico sospechoso del tipo Alto flujo de datos entre dos IPs se activará en caso de que este límite sea alcanzado.
Threshold en Flujos (acumulado en el período)	Límite de paquetes recibidos/enviados por/para un host para activar una alarma. Una alarma de tráfico sospechoso del tipo Alto flujo de datos entre dos IPs se activará en caso de que este límite sea alcanzado.
Threshold para IP Flood (IPs acumulado en el período)	Límite de conexiones recibidas/hechas por/para un host. El valor mínimo es **2** para que una alarma sea activada.
Porcentaje mínimo para caracterización del tráfico	Cuando esté 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	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 debe ser **60**.
Lista de IPs excluidos del análisis de tráfico sospechoso (IP/máscara)	Rellena con las direcciones IP de las subredes las que se excluirán del tráfico sospechoso. Separa por comas.
Agrupamiento para grupo de interfaces	Selecciona los agrupamientos para grupos de interfaz que harán parte del Dominio.
Dispositivos del dominio	Selecciona los dispositivos que van a componer el Dominio.

Una vez que el dominio es creado, debes configurar la Interfaz RFI dependiendo de su topología de red.

Interfaces RFI

La configuración RFI hará que el sistema filtre el mismo tráfico exportado por más un enrutador en un dominio.

Este filtro se basa en el campo de entrada de interfaz, después no será usado por interfaces, grupos de interfaces y dispositivos.

Todos los flujos son gravados en disco, después el filtro será usado solo cuando el sistema resuma el tráfico o para informes de datos brutos. El filtro no evitará el recibimiento de flujos.

El ejemplo de abajo ilustra el escenario donde el filtro RFI es necesario. Para análisis correcta de este escenario, es necesario que todos los enrutadores exporten flujo en todas las interfaces.

Lo que pasa es que cuando un flujo de paquetes va de una página web central a una localización remota, es exportado dos veces. Primero entra en el enrutador de la página web central y después entra en el enrutador de una localidad.

Para resumen correcto de la subred de la página web central, por ejemplo, solo uno de los flujos debe ser considerado.

Si todas las interfaces LAN, en este caso, las interfaces FastEthernet, son configuradas como interfaces RFI, los flujos exportados que contengan estas interfaces como entrada no serán considerados, por tanto, el resultado final del resumen estará correcto.

El TRAFip puede configurar automáticamente las interfaces RFI, considerando que todas las interfaces en la misma máscara de red de 30 bits están conectadas entre sí y definidas como RFI. Este descubrimiento es realizado utilizando el protocolo SNMP y las interfaces que serán consideradas deben ser marcadas como auto rfi.

Configuración

Accede **Configuración** → **Dominios** y clica en el botón Interfaces RFI para el dominio en el que deseas configurar la interfaz RFI.

Añadir metadatos de dominio

Para acceder a la página de configuración de metadato, accede a **Configuración** → **Dominios** 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 6.3. 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, reparándolos por punto y coma (;).

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

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

Recolectoras

Esta sección debe ser usada si estás implantando el sistema de modo de arquitectura distribuida.

Para más detalles de implementación de arquitectura distribuida consulta la sección arquitectura distribuida.

Tabla 6.4. Formulario de recolectoras

Campo	Descripción
Nombre	Nombre para identificar un appliance recolector.
Llave	Rellena una llave con string. Esta string debe ser igual al campo **llave de recolector** en el menú **Sistema** → **Parámetros** → **Arquitectura distribuida** en el appliance recolector.
Dirección de IP	Dirección de IP que el recolector usará para acceder al appliance central.
IP/Máscara del Exportador	Dirección de IP usado por el recolector para recibir flujos del enrutador. Esta dirección IP se utiliza en caso de que el sistema siga recibiendo flujos si un dispositivo de colección falla.
Contraseña	Esta contraseña debe corresponder al campo **contraseña** en el menú **Sistema** → **Parámetros** → **Arquitectura distribuida** en el appliance recolector.
Recolector de copia de seguridad	Recolectora que será la copia de seguridad para esta recolectora en el caso de fallo.
Dispositivos	Dispositivos que esta recolectora irá recolectar.

Importando archivos de recolectoras

Para importar un archivo de recolectoras, accede **Configuración** → **Recolectoras**.

Clica en el botón de importar y carga el archivo.

Un archivo de dispositivo importado posee los siguientes campos:

Tabla 6.5. Campos de archivos de recolectoras

Campo	Descripción
Nombre	Posible caracteres para el campo nombre.
Llave	Caracteres alfanuméricos.
Dirección de IP	Dirección de IP. Ej.: 10.0.0.1
Contraseña	Posible caracteres para el campo de contraseña.

Añadir metadatos de recolectora

Para acceder a la página de configuración de metadato, accede a **Configuración** → **Recolectoras** 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 6.6. 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 el metadato creado a una recolectora, accede a la lista de recolectoras 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.

Objetos

En esta pantalla puedes acceder a cada forma de configuración de objeto y los objetos configurados.

Para algunos tipos de objetos, tienes la opción de hacer la subida de un archivo de configuración para configurar varios objetos.

Importando archivos de objetos

1. Accede **Configuración** → **Objetos** y clica en el botón Importar para el tipo de objeto deseado.
2. Haz la descarga de un archivo formateado de acuerdo con las instrucciones en la pantalla.
3. Clica en el botón Añadir.
4. Ajusta las configuraciones y clica en el botón Guardar.

Mapeadores

Los mapeadores son usados para descubrir objetos relacionados utilizando el protocolo SNMP o por scripts. Ejemplos de aquellos objetos son: interfaz de red, procesadores, bancos de memoria, unidades de storage, probes y otros.

Los mapeadores pueden tener dispositivos asociados automáticamente a ellos, considerando Reglas que deben ser seleccionadas como condición

Procedimiento 6.1. Creando un mapeador

1. Selecciona **Configuración** → **Mapeadores**.
2. Clica en el botón Nuevo ítem y rellena el formulario como está detallado debajo:

Tabla 6.7. Formulario de Mapedador

Campo	Descripción
Nombre	Nombre del mapeador
Icono	Imagen que se mostrará próxima a los objetos descubiertos por este mapeador en el árbol del menú. Ve el paso 3 para instrucciones de personalización de esta imagen.
Tipo	Escoge **SNMP**, **Telco script**, **Proceso** o **Servicio del Windows**.
Script	Selecciona el script. Crea uno en la sección Scripts.
Eliminado automático	Si quieres que los objetos mapeados por este mapeador sean eliminados después de un cierto número de días consecutivos en que estén perdidos, selecciona **Sí** y rellena el número de días.
Incluir prefijo	Incluye el nombre del mapeador como prefijo para los objetos descubiertos por este mapeador.
Instancia de la OID utilizada como nombre de objeto	Marca esta opción si, en vez de rellenar el nombre del objeto con el valor de la OID, el mapeador debe rellenarlo con el valor de la instancia OID. Esta opción debe ser utilizada por objetos que no tengan un OID cuyo valor puede representarlos. Después puedes utilizar una OID estadística y un mapa de instancia de objetos con esta opción.
Nombre	Nombre de la OID para ser usada para el mapeo de objetos.
OID	OID que será utilizada.
MIB	OID MIB.
Filtro por recolecta SNMP	Filtra por la respuesta de la recolectora SNMP.
Asociación de dispositivos	Habilita asociación de dispositivos automáticos al mapeador considerando las Reglas. Cuando está habilitado, el formulario mostrará la opción de eliminación automática que eliminará los dispositivos asociados cuando las condiciones no sean más conocidas.
Dispositivos	Selecciona los dispositivos que serán asociados al mapeador. En caso de que el tipo de mapeador sea **Proceso**, tras transportar el dispositivo para el lado derecho del filtro, clica en él y, a continuación, en **Listar procesos**. Hecho esto, selecciona los procesos deseados.

Sugerencia

Abajo de la sección Configuración de Mapeamiento, debes especificar la OID (Object Identifier) de una MIB (Management Information Base) donde el sistema puede encontrar nombre de instancias únicas como valores retornados, después el objeto puede ser identificado. Esta OID pode ser cargada utilizando la herramienta MIB Browse clicando en el botón buscar OID.

Usa el botón Encontrar OID para buscar la MIB y rellenar los últimos campos del formulario.

3. Configurando los iconos de mapeador.

   a. Selecciona en el menú **Configuración** → **Mapeadores** y clica en el botón Cambiar iconos.

   b. Clica en el botón Nuevo icono.

   c. Rellena el nombre del mapeador y sube un icono para cada condición de objeto.

   d. Clica en el botón Enviar.

Mapeo cruzado de OIDs

Este recurso te permite crear un mapeador especificando 2 OIDs. El mapeador encontrará el valor para la primera OID y después la usará como index para encontrar el valor de la segunda OID.

Después, el mapeador mapeará el index de la primera OID con el valor de la segunda OID.

Este mapeador puede ser usado, por ejemplo, para mapear CPUs Cisco, donde puedes especificar las siguientes OIDs:

1.3.6.1.4.1.9.9.109.1.1.1.1.2;1.3.6.1.2.1.47.1.1.1.1.7

La primera OID es la cpmCPUTotalPhysicalIndex de CISCO-PROCESS-MIB y la segunda es la entPhysicalName de ENTITY-MIB, donde puedes encontrar el nombre de cada CPU.

Asociando dispositivos a los mapeadores

Después de configurar un nuevo mapeador, debes asociarlo a un dispositivo donde el objeto debe ser descubierto. Esta asociación puede ser hecha en cada configuración de dispositivo o clicando en el botón Asociación de dispositivos en la lista de mapeadores.

Exportando e importando mapeadores

El botón **Exportar** exporta toda la configuración del mapeador a un archivo. Para importar esta configuración de vuelta, puedes utilizar el botón **importar** y después hacer la descarga de este archivo.

EPM (Extended Processing Module)

EPM es otra aplicación añadida a la ya existente instalada en el cliente. Es un módulo extendido de la solución de seguimiento.

Necesita ser habilitado en **Sistema** → **Parámetros** → **EPM** .

EPM es una solución escalable para varios usuarios accediendo al sistema por la interfaz web, visualizando gráficos e informe de datos resumidos. Los datos resumidos son replicados para las máquinas EPM realizando un acceso de datos más rápido y datos redundantes.

1. Clica **Configuración** → **EPM**.
2. Clica en Nuevo para crear una entrada EPM nueva.
3. Rellena los campos nombre y dirección IP.
4. Selecciona estatus administrativo.
5. Clica en Guardar.

Reglas

Creación de reglas

1. Selecciona **Configuración** → **Reglas** y selecciona el tipo de regla, si es dispositivo, objeto mapeado u grupos.
2. Clica en el botón Nuevo para crear una nueva regla y rellena el formulario:

Tabla 6.8. Perfil automático de reglas

Campo	Descripción
Nombre	Nombre de la regla.
Descripción	Descripción de la regla.
Filtro por campos de la base de datos	Filtro basado en los campos de la base de datos Por ejemplo, el campo **Nombre** se refiere al nombre del objeto y al campo **Mapeador** (solamente para reglas de objeto mapeado) se refiere al nombre del mapeador.
Filtro por campos de metadatos	Filtro basado en los campos de metadatos. Escoge el metadato de dispositivo (para reglas de dispositivo) o de objeto mapeado (para las reglas de objeto mapeado).
Filtro por recoleta SNMP	Filtro basado en las OIDX que serán controladas cuando las reglas sean probadas. Selecciona la opción **Usar índice de objeto mapeado** cuando se estén usando OIDs que deben ser probadas contra objetos mapeados, como por ejemplo, ifConnectorPresent.

Filtro 'No Response'

El filtro de verificación de respuesta, que está localizado en el 'Filtro por recolecta SNMP', consiste en validar un objeto en el caso de retornar un mensaje específico de error.

Para utilizarlo, debes escoger el operador 'No Response' en el filtro. En el campo 'valor' debes utilizar uno de estos valores:

- $nosuchobject$ - Es utilizado para validar la respuesta 'Sin tal objeto' de un objeto.
- $nosuchinstance$ - Es utilizado para validar la respuesta 'Sin tal instancia' de un objeto.

Scripts

Puedes crear y ejecutar scripts del tipo: **Mapeador** y **Mapeamento de IPs**.

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 Mapeador

Crea un script personalizado y asócialo a un Mapeador para mapear un dispositivo.

El script tiene que retornar una tabla. Cada entrada en esta tabla está formada por otra tabla, que tiene las siguientes entradas:

- name
- description
- version
- index

Importante

Todos los campos retornados pueden ser una string.

Usa los ejemplos a continuación para crear tus scripts de mapeador personalizado:

```
---------------------- início do script ----------------------

r = {}

t = tmlSnmp.snmpWalk('10.0.0.1','erlang2','v2c',
{[1] = '1.3.6.1.2.1.2.2.1.2', [2] = '1.3.6.1.2.1.2.2.1.5',
 [3] = '1.3.6.1.2.1.2.2.1.3', [4] = '1.3.6.1.2.1.31.1.1.1.18'})

ifDescr = t['1.3.6.1.2.1.2.2.1.2']
ifSpeed = t['1.3.6.1.2.1.2.2.1.5']
ifType = t['1.3.6.1.2.1.2.2.1.3']
ifAlias = t['1.3.6.1.2.1.31.1.1.1.18']
```

```
for key,value in pairs(ifDescr) do
 r[key] = {['name'] = value,['description'] = value,
 ['version'] = '1',['index'] = key, ['alias'] = ifAlias[key],
 ['iftype'] = ifType[key], ['speed'] = ifSpeed[key]}
end

tmlDebug.vardump(ifDescr)

return r
```

----------------------- fim do script -------------------------

Comprueba abajo el ejemplo anterior con uso de parámetros:

----------------------- início do script -----------------------

```
h = params['ipaddr']
c = params['snmp']['community']
v = params['snmp']['version']
r = {}

t = tmlSnmp.snmpWalk(h,c,v,{[1] = '1.3.6.1.2.1.2.2.1.2',
 [2] = '1.3.6.1.2.1.2.2.1.5', [3] = '1.3.6.1.2.1.2.2.1.3',
 [4] = '1.3.6.1.2.1.31.1.1.1.18'})

ifDescr = t['1.3.6.1.2.1.2.2.1.2']
ifSpeed = t['1.3.6.1.2.1.2.2.1.5']
ifType = t['1.3.6.1.2.1.2.2.1.3']
ifAlias = t['1.3.6.1.2.1.31.1.1.1.18']

for key,value in pairs(ifDescr) do
 r[key] = {['name'] = value,['description'] = value,
 ['version'] = '1',['index'] = key, ['alias'] = ifAlias[key],
 ['iftype'] = ifType[key], ['speed'] = ifSpeed[key]}
end

tmlDebug.vardump(ifDescr)

return r
```

----------------------- fim do script -------------------------

Observa algunos ejemplos más:

----------------------- início do script -----------------------

```
h = params['ipaddr']
c = params['snmp']['community']
v = params['snmp']['version']
timeout = params['snmp']['timeout']
retries = params['snmp']['retries']
mpp = params['snmp']['max_per_packet']
mpps = params['snmp']['max_pps']
w = params['snmp']['window']
port = params['snmp']['port']

r = {}
t = tmlSnmp.snmpWalk2({host = h,community = c,
version = v, timeout = timeout, retries = retries,
max_pps = mpps, max_per_packet = mpp, window = w,
port = port},{[1] = '1.3.6.1.2.1.2.2.1.2',
[2] = '1.3.6.1.2.1.2.2.1.5', [3] = '1.3.6.1.2.1.2.2.1.3',
[4] = '1.3.6.1.2.1.31.1.1.1.18'})

ifDescr = t['1.3.6.1.2.1.2.2.1.2']
ifSpeed = t['1.3.6.1.2.1.2.2.1.5']
ifType = t['1.3.6.1.2.1.2.2.1.3']
ifAlias = t['1.3.6.1.2.1.31.1.1.1.18']


for key,value in pairs(ifDescr) do
 r[key] = {['name'] = value,['description'] = value,
 ['version'] = '1',['index'] = key, ['alias'] = ifAlias[key],
['iftype'] = ifType[key], ['speed'] = ifSpeed[key]}
end

tmlDebug.vardump(t['1.3.6.1.2.1.2.2.1.2'])

return r

---------------------- fim do script  -------------------------


---------------------- início do script ----------------------

h = params['ipaddr']
c = params['snmp']['community']
v = params['snmp']['version']

r = {}

t = {['ip'] = h, ['community'] = c, ['snmpversion'] = v}
map = tmlUtils.processMapper(t)

for k,v in pairs(map) do
  tmlDebug.vardump(v)
end

return map
```

```
----------------------- fim do script  -------------------------
```

Script de Mapeamento de IPs

Cree una secuencia de comandos personalizada que será utilizada por el **IP Mapper** para asociar nombres a direcciones IP.

La secuencia de comandos tiene que devolver una tabla. Cada entrada en esta tabla está formada por otra tabla, que tiene las siguientes entradas:

- name
- ipaddr

Importante

Todos los campos devueltos pueden ser una cadena.

Utilice el siguiente ejemplo para crear su script de asignación de IP:

```
----------------------- inicio del script -----------------------

 r = {}

 r[1] = {[''name''] = ''name1'', [''ipaddr''] = ''ipaddr1''}
 r[2] = {[''name''] = ''name2'', [''ipaddr''] = ''ipaddr2''}
 r[3] = {[''name''] = ''name3'', [''ipaddr''] = ''ipaddr3''}

 return r

----------------------- fin de la secuencia de comandos  -----------------------
```

Credencial de dispositivo

Muchos dispositivos utilizan las mismas configuraciones de SNMP y de acceso remoto.

Es posible configurar estos parámetros en una credencial y después asociarlos a los dispositivos que poseen la misma configuración.

Para crear una nueva credencial, accede **Configuración** → **Credencia de dispositivo** → **Nueva credencial de dispositivo** o **Configuración** → **Filtro de trap** → **Credencial de dispositivo** y clica en el botón **Nuevo**.

Tabla 6.9. Formulario de Credencial de Dispositivo

Campo	Descripción
Nombre	Define el nombre de credencial.
Protocolo	Defina si la credencial será de **SNMP**, **SSH** om4_bold(Telnet).

Campo	Descripción
Versión del SNMP	Selecciona la versión SNMP; Los posibles valores son: SNMP v1 o SNMP v2c — Especifica una community SNMP SNMP v3 — Especifica el tipo de autentificación y sus parámetros
Community SNMP	Rellena la community SNMP.
Puerta SSH	Rellena la puerta SSH. El valor modelo es **22**.
Puerta Telnet	Rellena la puerta Telnet.. El valor modelo es **23**.
Usuario	Usuario para ser usado para acceder al dispositivo. Esta string está disponible como un campo libre %username% para scripts de suministro.
Contraseña del usuario	Contraseña del usuario que accederá al dispositivo. Esta string está disponible como un campo libre %passwd% para scripts de suministro.
Contraseña de enable	La contraseña de enable es usada para acceder al dispositivo. Esta string está disponible como un campo libre %enable_passwd% para scripts de suministro.
Dispositivos	Asocia los dispositivos que deben utilizar la credencial.

Añadir metadatos de credenciales de dispositivo

Para acceder a la página de configuración de metadato, accede **Configuración** → **Credencial de dispositivo**, clica en el ítem **Credencial de dispositivo** 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 6.10. 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 una credencial, accede a la lista de credenciales y clica en el botón **Metadato** al lado de la credencial que será configurada.

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

Capítulo 7. Herramientas

Discovery

El recurso Discovery es usado para descubrir todos los hosts que están siendo usados en una red. Para utilizar esta función, haga clic en el botón **nuevo**

Tabla 7.1. Parámetros del Discovery

Campo	Descripción
Generar informe | Guardar modelo	Escoge **Generar informe** para solo una ejecución o **Guardar modelo** para guardar el informe como modelo.
Enviar correo electrónico con ips no registrados	Una vez que se seleccionan **Guardar modelo** y Programar modelo, este campo aparecerá en el formulario. Selecciónelo para enviar correos electrónicos al propietario del modelo si el informe descubre algún host no registrado en la herramienta.
IP/Máscara	Escriba IP y la máscara de red.
Direcciones IP excluidas del análisis	Introduce una lista de IPs, separándolos por coma (,).
Agrupar IP de un mismo host	Seleccione la opción **Sí** para ver las IP que pertenecen al dispositivo descubierto.

Sugerencia

si se selecciona **Enviar correo electrónico con ips no registrados**,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.

Clica en **Enviar** para iniciar la función discovery.

Cuando el proceso termine, es posible añadir cualquiera de los hosts descubiertos como dispositivo. Puedes seleccionar cada uno, utilizar el botón **Todos** para que todos sean seleccionados o utilizar el botón **Todos SNMP** para seleccionar solos los que tuvieron respuesta SNMP de acuerdo con las credenciales de SNMP.

Después de esto, clica en **Seleccionar**, rellena los campos de los dispositivos y clica en **Añadir**

MIB Browser

Puedes explorar todas las MIBs instaladas en el sistema utilizando el MIB browser. Estos elementos están listados en la pantalla con filtros aplicados.

Si quieres explorar una MIB, clica en el botón Seleccionar en la lado derecho.

Software externo

Telcomanager Windows Collector

Descarga el ejecutable **Telcomanager Windows Collector** para instalar el recolector de Netflow para Windows.

Encamina todos los paquetes de Netflow recibidos por una máquina Windows a un appliance con TRAFip.

Telcomanager Host Agent

Descarga el ejecutable **Telcomanager Host Agent** (THA) para instalar este agente en el Windows.

Este agente recolecta informaciones sobre los procesos que se están ejecutando.

Capítulo 8. 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 8.1. 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 8.2. 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.

Importante

Este recurso no guardará el flujo de los datos brutos, ya que estos datos son más usados para solucionar problemas y normalmente necesitan de un volumen grande de espacio de almacenamiento.

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 8.3. 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 8.4. Formulario de agente de asociación automática

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

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

Agente de asociación automática de mapeadores

Configura los periodos deseados para que la asociación automática de mapeadores se ejecute.

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 8.5. 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

Campo	Descripción
	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.
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 8.6. 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
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 8.7. 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 8.8. Formulario BGP

Campo	Descripción
Habilitar BGP	Seleccione esta opción si desea anunciar o quitar una ruta.

Campo	Descripción
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 8.9. Formulario de circuito

Campo	Descripción
Modo de generación del nombre del circuito	Seleccione **Automático** para generar el nombre del circuito de forma automática.
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 8.10. 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 8.11. 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 8.12. 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 8.13. 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.
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 8.14. 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!

Filtro simples

Este filtro se muestra mucho más útil para los usuarios del sistema cuando hay una cantidad considerable de grupos de subred. Al elegir un **número de caracteres del filtro de Subredes**, aparece un filtro en el menú principal de la sección **Datos históricos** → **Subredes** donde aparecen todos los grupos de subredes, pero solo con la cantidad de caracteres que hayas establecido.

Así, cuando selecciones uno de esos grupos que se muestran en el filtro, en la sección **Grupos de subredes** solo aparecerán el grupo escogido y los posteriores a él.

Es importante recordar que al configurar el filtro simple, el menú de subredes para de exhibirse. Por eso, las subredes so pueden ser visualizadas a través de los grupos.

Importante

Cuando este campo está configurado como **0** (cero), no existe este filtro.

Grafador

Ajuste de los parámetros del grafador.

Tabla 8.15. 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 8.16. 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 de almacenamiento de máxima estadística de flujo (meses)	Este campo está relacionado solo al flujo procesado. Esta estadística puede ser visualizada en **Sistema** → **Diagnósticos** → **Estadísticas de flujo** .

Campo	Descripción
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.

Mapeador de objetos

Para más detalles sobre el mapeo de los objetos ves a la sección configuración de mapeadores.

Tabla 8.17. Formulario de configuración de parámetros de mapeador de objetos

Campo	Descripción
Intervalo de ejecución del mapeador	Programa el intervalo entre las ejecuciones del mapeador.
Periodo máximo de almacenamiento del histórico de configuración	Programa el periodo de almacenamiento de logs a través de las configuraciones realizadas por el mapeador
Límite de mapeadores TCS simultáneos	Define un límite de ejecuciones simultáneas de mapeadores del tipo TCS. Rellena un valor entre **1** y **200**. La configuración de este parámetro puede afectar al rendimiento del sistema, así que se cuidadoso.
Número de recolectas simultáneas	Define un límite de ejecuciones simultáneas de mapeadores de jobs SNMP. La configuración de este parámetro puede afectar al rendimiento del sistema, así que se cuidadoso.
Número de procesos simultáneos	Define un límite de procesos simultáneos del mapeador. La configuración de este parámetro

Campo	Descripción
	puede afectar al rendimiento del sistema, así que se cuidadoso.
Número de dispositivos en cada proceso	Define un límite de ejecuciones simultáneas de mapeadores del tipo TCS. Rellena un valor entre **1** y **200**. La configuración de este parámetro puede afectar al rendimiento del sistema, así que se cuidadoso.

Mapeo de IPs

Para más detalles sobre la asignación de IPs vaya a sección de IP Mapper.

Tabla 8.18. Formulario de configuración de parámetros de asignación de IPs

Campo	Descripción
Habilitar la asignación de IPs	Una vez seleccionada la opción Sí, el agente de asignación de IP estará habilitado. En caso contrario, no se ejecutará.
Intervalo de ejecución del asignador	Programe el intervalo entre las ejecuciones del asignador.
Período máximo de almacenamiento del historial de configuración	Programe el período de almacenamiento de historial de asociaciones de IP y nombres realizados por el asignador.

Nivel de log

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

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

Personalización de interfaz

Puedes personalizar la forma como los dispositivos se muestran en el menú en árbol en **Datos históricos → Dispositivos → Dispositivo** .

Para ello, basta con rellenar el campo **Fórmula de nombre de dispositivo** con el que deseas que aparezca en el menú.

La fórmula posee etiquetas especiales que utilizan las informaciones rellenadas en los formularios de los dispositivos. Son las siguientes:

Tabla 8.19. Fórmula de nombre de dispositivo

Etiqueta	Descripción
%n	Se refiere al **nombre** del dispositivo.
%a	Se refiera a la **dirección de IP** del dispositivo.
%t	Se refiere al **tipo** del dispositivo.
%m	Se refiere al **fabricante** del dispositivo.

Etiqueta	Descripción
%d	Se refiere al **tipo de dispositivo** (Cámara, Firewall, Router, Servidor, Switch o Inalámbrico).

En el campo **Listar interfaces por** puede seleccionar la opción **Descripción** para ver los objetos asignados por el nombre del objeto o seleccionar **Rótulo** para mostrarlos con un nombre específico.

La asignación de **Rótulo** se realiza manualmente.

Acceda a **Dispositivo elegido** → **Objeto mapeado elegido** → **Propiedades** para llenar el campo de **Rótulo** con el nombre que representará el objeto.

Esta **Rótulo** debe tener un unique key.

Preferencias locales

Tabla 8.20. 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.
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.

Proyección

Configuración estándar de parámetros para proyección. Ves a la sección proyección para consejos sobre como configurar estos parámetros.

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 8.21. Configuraciones de activación de redundancia

Campo	Descripción
Habilitar redundancia	Escoge Sí.

Campo	Descripción
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 8.22. 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 8.23. 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 8.24. 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.

Datos brutos del TRAFip

Rellena estos campos para configurar el formulario del informe de datos brutos. Para más informaciones sobre este informe, accede a la sección Informe de datos brutos.

Tabla 8.25. Datos brutos del TRAFip

Campo	Descripción
Período máximo de datos por informe (horas)	Introduce un número entero. El estándar es **18** y el máximo valor permitido es **24**.
Número máximo de líneas por informe	Introduce un número entero.
Convertir el tratamiento de sampling rate en modelo para la configuración	Selecciona **Sí** para rellenar el campo **Tratamiento de sampling rate** con **Configuración** automáticamente.

Datos Resumidos

Configura el periodo máximo de datos que un informe puede tener. El valor estándar esm4_bold(180) y el máximo valor permitido es **360**.

Informes programados

Configura las características para los informes programados.

Tabla 8.26. 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 8.27. Formulario de configuración del servidor FTP

Campo	Descripción
Servidor	Dirección de IP del servidor.
Directorio	Directorio en el servidor.
Usuario	Usuario a ser autentificado en el servidor.

Campo	Descripción
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 8.28. 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 8.29. 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.
Habilitar la recoleta por SNMP	Habilitar la recolecta SNMP para el TRAFip. Marque esta opción para habilitar el proceso InterfaceCollect para búsquedas y contador de tráfico de interfaces.
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 8.30. 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 8.31. 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.

TRAFip

Activa o desactiva la detención automática de interfaces RFI (Repeated flow interface). Para tener más informaciones sobre las RFI's, accede a la sección Interfaces RFI.

Transferencia de archivos

Estos parámetros son usados para configurar los archivos transferidos, usando el protocolo FTP, conteniendo objetos seleccionados estadísticamente durante 15 minutos.

Formulario de transferencia de archivos

Dirección de IP del servidor FTP	Dirección de IP del servidor FTP.
Puerta	Puerta TCP para conectar al servidor FTP.
Usuario del servidor	Nombre de usuario usado para conectar al servidor FTP.
Contraseña de usuario	Contraseña usada para conectar al servidor FTP.

Verificación de exportadores de flujo

Con este recurso habilitado, todos los exportadores de flujo serán comprobados de tiempo en tiempo, y para cada exportador con un tiempo sin exportación de flujos su icono cambiará, mostrando a los usuarios la falta de flujos recibidos por el exportador.

Formulario de verificación de exportadores de flujo

Habilitar verificación de exportadores	Escoge Sí o No.
Tiempo de inactividad en la exportación (min)	Escoge el límite

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 8.32. 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 8.33. 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 8.34. 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.
Habilitar favoritos	Habilita el recurso Favoritos.
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** .
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.

Campo	Descripción
Grupos de Subredes	Selecciona el grupo de subredes a las que el usuario será capaz de acceder.
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 8.1. 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 8.35. 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 8.2. 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 8.36. Formulario de usuario

Campo	Descripción
Nombre	Propiedades del perfil de usuario
Token do bot Telegram	Token obtenido tras crear un bot en el Telegram.

Campo	Descripción
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 8.37. 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 8.38. 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.

Estadística de flujo

Muestra el máximo y la media estadística de flujo por un periodo de 30 minutos, 2 horas y 24 horas.

Configura el máximo de estadística de periodo de almacenamiento de flujo en **Sistema** → **Parámetros** → **Histórico de configuración** .

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.
summarizer.log	Logs del proceso de resumen. Este proceso solicita el proceso TRAFIPsum, que procesa los datos brutos del TRAFip. Cuando el sistema está en arquitectura distribuida, el resumidor es responsable por enviar archivos sumlog (archivos que contienen datos resumidos) para la máquina central.
TRAFIPsum.log	Logs del proceso TRAFIPsum, que es responsable por el procesamiento de datos brutos del TRAFip de acuerdo con las configuraciones. Este proceso se ejecuta cada 5 minutos. En la arquitectura distribuida, el TRAFIPsum se ejecuta en los recolectores.
TRAFIPlookupd.log	Logs del proceso responsable por el rendimiento de varias traducciones que son usadas por los informes brutos del TRAFip. Ejemplos: dirección de subred IP, DNS, Netbios y aplicaciones de traducción.

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 9. 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 9.1. 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 9.2. 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 9.3. 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 9.4. 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 9.5. 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 9.6. 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

Las alarmas están basadas en el tráfico medido de objetos configurados en el sistema. Existen dos tipos de alarmas: Modelo e Histórico.

Para configurar ambos tipos de alarma, selecciona **ALARMmanager** → **Alarmas**, clica en el botón **Nuevo** y rellena el formulario.

Puedes crear una alarma para cada tipo de objeto:

- Dispositivo
- Interfaz
- Grupo de Interfaz
- Subred

- Grupos de Subred
- Aplicaciones
- Grupo de Aplicación
- Protocolos
- Sistema autónomos
- Grupos de Sistemas Autónomos
- ToS
- Grupo de ToS
- Etiqueta

Configuración de alarma estándar

Este tipo de alarma es usada para el análisis de tráfico inmediato, cuando no tiene condiciones posibles para determinar la fórmula. Usa esta alarma para mantener el control sobre las condiciones de contorno que necesitan de tratamiento cuando son detectadas.

Tabla 9.7. Formulario de alarma estándar

Campo	Descripción
Nombre	Texto descriptivo para la alarma. Ej.: alto tráfico, sin tráfico HTTP.
Tipo de alarma	Escoge modelo.
Fórmula	Ves a la sección Fórmula de alarmas modelo.
Varbind	Campo de texto libre que puede ser usado para reconocer las alarmas que son encaminadas como traps.
Correo electrónico	Ves a la sección de acciones.
Dispositivo móvil	Ves a la sección de acciones.
Trap	Ves a la sección de acciones.
Enviar correo electrónico después de (minutos)	Ves a la sección de acciones.
Enviar mensajes de dispositivo móvil después de (minutos)	Ves a la sección de acciones.
Enviar trap después (minutos)	Ves a la sección de acciones.
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.
Deshabilitar mensajes de dispositivo móvil para la alarma eliminada	Si la opción "No" es seleccionada, los mensajes de dispositivo móvil serán enviados y la condición de eliminados será indicada en ellos. La opción "Sí" después de que los mensajes de dispositivo móvil sean enviados.
Deshabilitar correo electrónico para la alarma eliminada	Si la opción "No" es seleccionada, el correo electrónico será enviado y la condición de eliminado

Campo	Descripción
	será indicada en él. La opción "Sí" evitará que el correo electrónico sea enviado.
Incidencias consecutivas para armar	Escoge el número de incidencias consecutivas de la fórmula de alarma que debe disparar la alarma. No utilizado en alarmas de Trap.
No incidencias consecutivas para desarmar	Escoge el número de no-incidencias consecutivas de la fórmula de alarma que debe desarmar la alarma. No utilizado en alarmas de Trap.
Nivel de urgencia	Selecciona el nivel para la alarma.
Perfil de alarma	Selecciona los perfiles de alarma a los cuales debe pertenecer.

Fórmula de alarma estándar

TRAFip mide y divide el tráfico de tres formas diferentes: bps (bits por segundo), paquetes y flujos. Cada uno de ellos es utilizado como una métrica en la fórmula de la alarma. Estas métricas pueden ser absolutas o pueden pertenecer al perfil de tráfico. De esta forma, podemos establecer métricas en la fórmula de alarma a través de la sintaxis:

1. **Absoluto:** "Nombre del dominio".self.<métrica>
2. **Perfil de tráfico:** "Nombre del dominio".self.<tipo de perfil>[<"nombre del perfil">.<"nombre del ítem de perfil">].<métrica>

Las métricas encima mencionadas pueden ser llamadas de **curvas**.

Los tipos de análisis de perfil pueden ser: Matriz, Distribución y Contenido, representados por **MTX**, **DST** y **CNT**, respectivamente.

Las métricas pueden ser representadas de acuerdo con la siguiente tabla:

Tabla 9.8. Representación de las métricas

Métrica	Sintaxis
Bps (bits/s) de origen	**bytAb**
Bps (bits/s) de destino	**bytBa**
Paquetes de origen	**pktAb**
Paquetes de destino	**pktBa**
Flujo de origen	**flwAb**
Flujo de destino	**flwBa**
Límite del objeto	**limit** (Ve la nota de abajo)

Importante

La métrica **limit** se refiere al límite de objeto asociado a la alarma y, en el caso de que haya un límite (dispositivo), el mismo será ignorado. Al utilizar esta métrica, no necesitarás especificar el dominio. Ve el ejemplo a continuación: (self.limit) > 0

Puedes restringir el periodo en el que la alarma será generada usando las variables **weekday** y **time**.

Los valores para **weekday** deben ser entre 1 (domingo) y 7 (sábado). Para la variable **time**, debes usar HH:MM.

Debes construir la fórmula utilizando las siguientes reglas:

- Usa paréntesis "()" para precedencia de la operación.
- Usa los operadores lógicos AND y OR.
- Usa los operadores de comparación ==,!=,<,>,<=,>=.
- Usa los símbolos *,-,+ e / para ejecutar las operaciones.

Ve los ejemplos abajo:

1. **Absoluto:** ("Default".self.bytAb) > 0 and weekday > 1 and weekday < 7
2. **Perfil de tráfico:** ("Default".self.CNT["Applications"."ssh"].bytAb) > 0 and time > 09:00

Configuración de la alarma de cambio de comportamiento

Este tipo de alarma es usualmente configurada para cuando no puedas definir los límites de forma explícita, pero quieres ser avisado de cambios en el comportamiento típico de los objetos.

Típicamente, este tipo de alarma es usada por objetos que pueden mostrar la evolución gradual sobre el tiempo (un aumento del ancho de banda, por ejemplo). En estos casos, definir límites estáticos pueden llevar a disparar alarmas innecesarias. Para resolver esto, puedes configurar el sistema para definir, con una base diaria, un comportamiento linear modelo para el objeto que deseas controlar - esta línea representa el comportamiento futuro esperado del objeto.

La alarma será disparada comparando lo esperando y la métrica recolectada, llevando en consideración una tolerancia definida por el usuario. El valor esperado para la curva configurada en la alarma es calculado considerando un periodo de tiempo definido por ti.

Tabla 9.9. Formulario de alarma histórico

Campo	Descripción
Nombre	Texto descriptivo para la alarma. Ej.: alto tráfico, ningún tráfico HTTP.
Tipo de alarma	Escoge **Histórico**.
Varbind	Un campo de texto libre que puede usarse para reconocer las alarmas que son encaminadas como traps.
Horario de activación	Ves a sección activación de fórmulas de alarma.
Curva	Ves a la sección cambio de comportamiento de la curva de alarma.
Histórico mínimo (días)	Mínima cantidad de días necesarios para rellenar el periodo de análisis.
Histórico máximo (días)	Máxima cantidad de días permitidos para rellenar el periodo de análisis.
Número de violaciones consecutivas (días)	Ves a la sección Número de violaciones consecutivas.
Factor de tolerancia superior	Ves a la sección Factor de tolerancia.

Campo	Descripción
Factor de tolerancia inferior	Ves a la sección Factor de tolerancia.
Periodo de alarma (minutos)	Ves a la sección Periodo de alarma.
Modo de activación	Define qué factores de tolerancia se considerarán para activar la alarma. Elija entre **Ambos**, **Superior** o **Inferior**.
Valor de protección (%)	Considera un valor mínimo para el umbral que es añadido a los valores esperados.
Proyección basada en el valor medio	Selecciona **Sí** para que la proyección de los valores máximos y mínimos sea calculada basándose en el valor medio.
Deshabilitar tendencias negativas	Selecciona **Sí** para que no sean consideradas tendencias negativas para la proyección.
Correo electrónico	Ves a la sección de acciones.
Dispositivo móvil	Ves a la sección de acciones.
Trap	Ves a la sección de acciones.
Enviar correo electrónico después de (minutos)	Ves a la sección de acciones.
Enviar mensajes de dispositivo móvil después de (minutos)	Ves a la sección de acciones.
Enviar trap después de (minutos)	Ves a la sección de acciones.
Deshabilitar trap para la alarma eliminada	Si la opción no es seleccionada, la trap será enviada y la condición de eliminada será indicada en la trap. La opción sí evitará que la trap sea enviada.
Deshabilitar sms para alarma eliminada	Si la condición no es seleccionada, el sms será enviado y la condición de eliminado será indicada en el sms. La opción sí evitará que el sms sea enviado.
Deshabilitar el correo electrónico para la alarma eliminada	Si la opción no es seleccionada, el correo electrónico será enviado y la condición de eliminado será indicado en el correo electrónico. La opción sí evitará que el correo electrónico sea enviado.
Incidencias consecutivas para armar	Escoge el número de incidencias consecutivas de la fórmula de alarma que debe disparar la alarma.
No incidencias consecutivas para desarmar	Escoge el número de no-incidencias consecutivas de la fórmula de alarma que debe desarmar la alarma.
Nivel de urgencia	Selecciona el nivel para la alarma.
Perfil de alarma	Selecciona los perfiles de alarma a los cuales debe pertenecer.

Fórmula de alarmas históricas

Este campo se utiliza solo para alarmas históricas. Define cuando una incidencia de alarma debe generarse.

Las variables utilizadas son **weekday**, **time**, **everyday** y **everytime**.

Usa **everyday** para disparar la alarma todos los días de la semana y **everytime** para disparar la alarma durante todo el día.

Si deseas definir cuando una alarma debe ser generada, puedes usar las variables **weekday** y **time** con los operadores definidos. Los valores para **weekday** deben ser entre 1 (domingo) y 7 (sábado). Para la variable **time**, debes usar HH:MM.

Ejemplo:

```
weekday > 1 and weekday < 7 and time > 09:00
```

En este ejemplo, la alarma se disparará si el día de la semana está entre domingo y sábado después de las 9h.

Curvas de alarma histórica

El TRAFip mide y divide el tráfico en tres formas diferentes: bps (bits por segundo), paquetes y flujos. Cada uno de ellos es usado como métrica en la curva de la alarma de cambio de comportamiento. Estas métricas pueden ser absolutas o pueden pertenecer al perfil de tráfico. De esta forma, podemos establecer la métrica de la curva de una alarma de cambio de comportamiento a través de la siguiente sintaxis:

1. **Absoluta:** "Nombre del dominio".self.<métrica>
2. **Perfil de tráfico:** "Nombre del Dominio".self.<tipo de perfil>[<"nombre del perfil">.<"nombre del ítem de perfil">].<métrica>

Los tipos de perfil puede ser Matriz, Distribución y Contenido, representados por **MTX**, **DST** y **CNT**, respectivamente.

Las métricas pueden ser representadas de acuerdo con la siguiente tabla:

Tabla 9.10. Representación de métricas

Métrica	**Sintaxis**
Bps (bits/s) de origen	**bytAb**
Bps (bits/s) de destino	**bytBa**
Paquetes de origen	**pktAb**
Paquetes de destino	**pktBa**
Flujos de origen	**flwAb**
Flujos de destino	**flwBa**

Número de violaciones consecutivas

La violación de las muestras será considerada si suceden consecutivamente y el número de violaciones es superior del parámetro especificado, en caso contrario serán descartadas de la computación del comportamiento.

Por ejemplo, supón que tienes un cambio de comportamiento en la alarma para un tráfico de interfaz y que, en algún momento, el tráfico era 500MB +- 300MB y el tráfico detectado era 3GB. Esta muestra no será usada en la computación comportamental y el tráfico esperado para el día siguiente continuará siendo 500MB. Esta muestra será solo utilizada si tiene N muestras consecutivas violadas, lo que caracteriza un nuevo comportamiento.

Factor de tolerancia

El TRAFip ejecutará el siguiente cálculo para determinar si el valor observado representa un cambio de comportamiento:

```
IF  (AV < (EV - (N * SD)) OR AV > (EV + (N * SD)))
Em seguida aciona o comportamento da mudança do alarme.

Onde
N é o fator de tolerância
SD é o desvio padrão da curva
AV é o valor médio para a atual meia-hora
EV é o valor médio esperado para a atual meia-hora
```

Periodo de alarma

El TRAFip mostrará la muestra cada 30 minutos o cada 5 minutos.

Cuando un periodo de alarma es configurado como 5 minutos, el sistema mostrará la media del valor para cada 5 minutos y lo comparará con el valor esperado, pero no lo guardará si es un cambio de comportamiento.

Cuando un periodo de alarma es configurado como 30 minutos, el sistema mostrará el valor de la media para cada media hora y determinará si el valor representa un cambio de comportamiento.

Acciones

A cada momento el sistema del TRAFip procesa un tráfico de 5 minutos, todas las fórmulas de alarma son guardadas y si retornan verdaderas, se genera la incidencia. La alarma se disparará para una incidencia de alarma solo si el número de incidencias consecutivas es superado.

Cuando marcas una acción para una alarma, tienes que rellenar tres campos:

Campo de acciones

Incidencias consecutivas para armar	Esto representa el número de veces consecutivas en las que el límite es superado.
No incidencias consecutivas para desarmar	Esto representa el número de veces consecutivas en las que el límite no es superado.
Nivel de urgencia	Escoge un nivel de urgencia adecuado para la alarma.

Tipos de acciones

Correo electrónico	Un correo electrónico será enviado a los usuarios. El servidor SMTP del TRAFip debe ser configurado, bien como el correo electrónico de cada usuario en el formulario de configuración del usuario. El correo electrónico será enviado después del número de segundos definido en el campo **Enviar correo electrónico después de (minutos)**, comenzando desde el tiempo de activación.
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. La trap debe ser interpretada usando la MIB TELCOMANAGER-ALARMMANAGER-MIB.my, que está disponible en la lista de MIB del SLAview. También debes configurar el servidor para enviar las traps en **Sistema** → **Parámetros** → **SNMP** → **SNMP trap** . La trap enviada después del número de segundos definido en el campo **Enviar trap después de (minutos)**, comenzando desde el tiempo de activación.

Gestión de eliminación de alarmas.

En esta opción aprenderás como gestionar todas las tuplas de alarma/objeto a las que el usuario tiene acceso.

Para eliminar, sigue el siguiente procedimiento:

1. Ves a la guía **ALARMmanager** → **Alarmas** y clica en el botón Alarmas eliminadas.
2. Rellena el campo de filtro de esta forma para seleccionar las alarmas/objetos deseados y clica en el botón Filtro.
3. Selecciona las alarmas/objetos de la lista.
4. Rellena el campo razón de eliminación deseado.
5. Clica en el botón Guardar para eliminar las alarmas/objetos seleccionados.

Para quitar la eliminación de las alarmas, sigue el mismo procedimiento, pero deselecciona las alarmas/objetos deseados.

Importante

Date cuenta de que si la alarma ya está eliminada, no será eliminada nuevamente y lo mismo pasa con la acción de deseliminar.

Importante

Las alarmas eliminadas pueden ser consideradas para colorear el mapa usando el flag "Considerar eliminado" en el MapView. Si una alarma eliminada es desactivada por un momento y después queda activa, es marcada como eliminada.

Añadiendo metadatos de alarma

Para acceder a la página de configuración de metadato, accede a **ALARMmanager,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 9.11. 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, selecciona **ALARMmanager** → **Perfil de alarmas**, clica en el botón **Nuevo** y rellena el formulario.

Tabla 9.12. Formulario de perfil de alarma

Campo	Descripción
Nombre	Texto descriptivo para un perfil de alarma.
Alarma	Selecciona las alarmas que pertenecerán a este perfil.
Caja de selección de objeto	En primer lugar, selecciona el tipo de objeto y se mostrarán los objetos disponibles. Después, selecciona los objetos deseados para este perfil.

Añadiendo metadatos de perfil de alarma

Para acceder a la página de configuración de metadato, accede a **ALARMmanager** → **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 9.13. 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.

Alarmas de servicio

Introducción

El recurso de alarmas de servicio permite que juntes alarmas de diferentes objetos en una única fórmula. El TRAFip puede disparar la alarma bajo condiciones más sofisticadas.

Serás capaz de crear, por ejemplo, las siguientes alarmas:

- Una alarma que es activada cuando un enlace de WAN tiene una alta latencia y también posee un bajo tráfico.
- Una alarma para decirte cuando el primario y los enlaces de copia de seguridad de locación fallarán.

Fórmula

En las fórmulas puedes usar los operadores lógicos OR, AND, NOT y XOR para construir fórmulas más complejas.

Añadiendo metadatos de alarmas de servicio

Para acceder a la página de configuración de metadato, accede a **ALARMmanager** → **Alarmas de servicio** 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**.
mm4_table(ES,Campos de un metadato) mm4_thead(Campo,Descripción) mm4_trow(Nombre,Nombre del metadato.) mm4_trow(Descripción,Descripción del metadato.) mm4_trow(Tipo de dato,Escoge si el

metadato será del tipo **Texto**, **Entero** o **Enum**.) mm4_tlastrow(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 alarma de servicio, 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.

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.
- Interfaz gráfica para crear alarmas y fórmulas personalizadas.
- 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.

Puedes configurar las columnas en **Sistema → Usuarios → Alarm consola** .

La consola posee las siguientes columnas:

Tabla 9.14. ALARMmanager consola

Columna	Descripción
INICIO	El momento de la primera incidencia

Columna	Descripción
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

El mecanismo de eliminación de alarma permite que elimines cualquier tupla de alarma/objeto, siempre que la alarma este configurada para aquel objeto. La eliminación también deshabilitará correos electrónicos, mensajes de dispositivo móvil y traps para la alarma/objeto o indicará esta condición en los correos electrónicos, mensajes de dispositivo móvil y traps. Puedes configurar el comportamiento deseado en este campo en configuración 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.

Puedes gestionar la lista de eliminación de alarma/objeto en **ALARMmanager** → **Alarmas** → **Eliminación de alarmas** .

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 10. NOC display

NOC Display

El NOC display es un modo de visualización de Graph sets. En él, todos los graph sets habilitados por el usuario se alternan automáticamente después de un periodo previamente configurado en cada graph set.

Este recurso es de gran utilidad cuando el operador debe comprobar todos los gráficos del graph set constantemente.

Capítulo 11. 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 12. Glosario

Siglas

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

Tabla 12.1. 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.