Manual CFGtool

Manual CFGtool

Tabla de contenidos

Lista de tablas

Prefacio

Público objetivo

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

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

Convenciones utilizadas en este manual

Este documento utiliza las siguientes convenciones:

Tabla 1. Convenciones del manual

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

Capítulo 1. Introducción

Sobre

CFGtool es un sistema de gestión de configuración de dispositivos.

Principales recursos

- Acceso a todos los recursos del sistema a través de un web browser.
- Puede ofrecerse alta disponibilidad a través del uso de soluciones redundantes, en las que dos appliances trabajan en HOT-STANDBY.
- Banco de datos de alto rendimiento para datos históricos almacenados.
- Alarmas de alteración de configuración de un dispositivo y de integridad de archivos.
- Gestión de scripts de suministro, exportación de configuración e inicio se sesión.

Requisitos mínimos

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

Hardware

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

Navegador

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

Capítulo 2. Datos históricos

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

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

Grupos

Los grupos sirven para organizar objetos. Son jerárquicos y pueden tener los niveles que sean necesarios.

Los grupos pueden ser utilizados para restringir el acceso de usuarios a los objetos comprobados. Al asociar un perfil de usuario a un grupo, los usuarios de este perfil solo pueden visualizar los objetos asociados a este grupo y a los grupos debajo suyo, de acuerdo con la jerarquía.

Los objetos pueden ser asociados a grupos de manera manual o automática. Durante la configuración del grupo, cuando sea asociado manualmente, el formulario mostrará **Dispositivos** y **Objetos mapeados** disponibles para ser asociados. Cuando sea asociado automáticamente, el formulario de grupo mostrará las reglas de asociación de Dispositivos y de Objetos mapeados.

Los objetos pueden ser eliminados del grupo automáticamente cuando no atiendan más a las reglas de asociación. Esta opción está solo disponible cuando el grupo posee la asociación automática habilitada.

Importante

Cuando el icono del grupo es una carpeta amarilla, no hay gráficos en este grupo. Cuando el icono es una carpeta verde, hay por lo menos un objeto con perfil asociado a este grupo, o sea, hay gráficos para ser exhibidos.

Procedimiento 2.1. Pasos de configuración

1. Selecciona **Datos históricos** → **Grupos** → **Grupos** .

2. Clica en el botón **Nuevo** para crear un nuevo grupo y rellena el formulario.

Tabla 2.1. Formulario de nuevo grupo

Campo	Descripción
Nombre	Define un nombre para el grupo.
Descripción	Define una descripción para el grupo.
Asociación automática	Selecciona **Sí** para habilitar la asociación automática de objetos a este grupo considerando las Reglas de Asociación.
Grupo superior	El grupo raíz en relación a este. Si ningún grupo raíz es seleccionado, este grupo será un grupo raíz en el sistema.
Eliminado automático	Selecciona **Sí** para habilitar la eliminación automática de objetos a este grupo. Cuando esta opción está habilitada, los objetos son automáticamente eliminados del grupo cuando no responden más a las reglas de asociación. Esta

Campo	Descripción
	opción está disponible solo cuando la **Asociación automática** está habilitada.
Dispositivos	Dispositivos que pertenecerán a este grupo.
Perfiles de Usuario	Perfiles de usuarios que tendrán acceso a este grupo.

3. Clica en el botón **Guardar**.

4. Para añadir más grupos debajo de este grupo, clica en el icono Grupos, selecciona Subgrupos en el área de selección del gráfico y repite los pasos de encima.

Añadir metadatos de grupos

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

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

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

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

Tabla 2.2. Campos de un metadato

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

Dispositivos

Un dispositivo es cualquier elemento de red que posee una dirección de IP y soporte para protocolos SNMP y ICMP.

Procedimiento 2.2. 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 2.3. 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: 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.

Campo	Descripción
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 • 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,

Campo	Descripción
	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** → **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 verificación de seguridad	Selecciona **Sí** para habilitar la Integridad de Seguridad o **No** para deshabilitarla.
Habilitar recolecta de inventario físico	Selecciona **Sí** para habilitar la recolecta del informe de inventario físico o **No** para deshabilitarlo.
Recolectar lista de software	Selecciona **Sí** para habilitar la recolecta de lista de software o **No** para deshabilitarla.
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

Campo	Descripción
	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. 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 de los tipos habilitados en **Configuración** → **Tipos 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.

Campo	Descripción
Perfiles de alarma	Asocia el dispositivo a un perfil de alarma.

Exportando la configuración del dispositivo

Clicando en el botón **Agente de exportación de configuración** ejecutarás los scripts exportadores de configuración.

Comprueba el resultado de la exportación clicando en **Resumen** en el área de selección.

Configurando la Integridad de Seguridad de dispositivos

El sistema de Integridad de Seguridad sirve para hacer el seguimiento de archivos en servidores. Debe ser habilitado en el formulario del dispositivo para tener sus archivos comprobados.

Es necesario hacer la instalación del agente **Telcomanager Windows Security Agent (TSA)** en la máquina que contiene los archivos que serán comprobados. Está disponible para Descarga en **Herramientas → Software Externo** y, después de instalado, recolectará informaciones sobre los archivos que están siendo comprobados por el CFGtool.

En la lista de dispositivos, en **Datos Históricos → Dispositivos → Dispositivo** , es posible obtener un informe sobre los archivos comprobados, bien como el estatus de cada uno de ellos (ausente, alterado o normal). Para ello, basta clicar en el botón **Verificación de Seguridad** al lado del dispositivo.

Sugerencia

Los archivos ausentes serán marcados en amarillo y los archivos que tengan algún tipo de alteración serán marcados en rojo.

Hay también 2 alarmas del tipo **Integridad de Seguridad**: file change and file missing. Consulta la sección de alarmas para más informaciones sobre ellas.

Configurando la lista de software de dispositivos

El sistema de lista de software sirve para hacer el seguimiento de los programas instalados en servidores. Debe ser habilitado en el formulario del dispositivo.

Es necesario hacer la instalación del **Telcomanager Host Agent (THA)** en la máquina que se desea comprobar. Está disponible para Descarga en **Herramientas → Software Externo** y, después de instalado, recolectará informaciones sobre los programas instalados y las enviará al CFGtool.

En la lista de dispositivos, en **Datos Históricos → Dispositivos → Dispositivo** , es posible obtener la lista de los programas instalados. En ella encontrará el nombre, versión, tamaño, editor y fecha de instalación de cada programa. Para ello, basta clicar en el botón **Lista de Software** al lado del dispositivo.

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 2.4. 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 2.5. 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.

Informes

Modelos

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

Guardando

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

2. Rellena los campos de abajo:

Tabla 2.6. Forma del modelo

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

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

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

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

Programación

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

Opciones de programación

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

Sugerencia

Para programar un informe, debes guardarlo como modelo.

Sugerencia

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

Editando

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

Visualizando informes

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

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

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

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

Gestionando espacio de disco

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

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

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

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

Histórico de configuración

Las alteraciones de configuración pueden ser visualizadas directamente en la pantalla del dispositivo clicando en **Resumen** en el área de selección de gráfico.

El informe de histórico de configuración proporciona todas las alteraciones de configuración en un determinado periodo. El resultado del informe contiene los dispositivos, los tipos del script de exportación de configuración, las versiones y las fechas de creación.

Tabla 2.7. Formulario del informe de histórico de configuración

Campo	Descripción
Filtro por nombre	Filtra el dispositivo por el nombre.
Dispositivos sin configuración	Si esta opción está habilitada, el filtro buscará solo los dispositivos que no poseen configuración del tipo seleccionado en el campo **Tipo de configuración.**
Instante inicial	Introduce el horario de inicio del periodo.
Instante final	Introduce el horario del final del periodo.
Tipo de configuración	Escoge **Todos** o un tipo de configuración específico.
Formato de salida	Selecciona uno de los formatos para el informe: HTML o CSV.

Importante

Puedes comparar versiones seleccionando dos ítems que contengan el mismo dispositivo y el mismo tipo de script.

Policy Compliance

El informe de policy compliance muestra una relación entre dispositivos, reglas y políticas. De esta forma, podrás visualizar que reglas no están siendo respetadas por los dispositivos, o sea, que equipos no están de acuerdo con las políticas de conformidad.

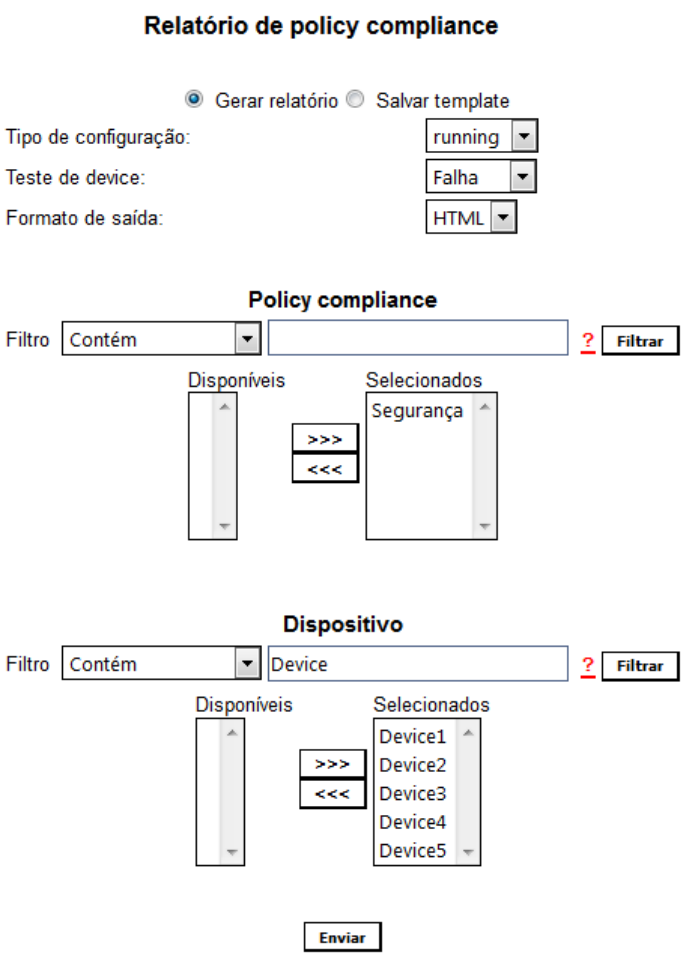
Cuando la versión del dispositivo este de acuerdo con una regla, aparecerá un check en verde. En caso contrario, aparecerá un "X" en rojo.

Tabla 2.8. Formulario de informe de Policy Compliance

Campo	Descripción
Generar informe | Guardar modelo	Escoge **Generar informe** para solo una ejecución o **Guardar modelo** para guardar el informe como modelo.
Tipo de configuración	Selecciona si quieres analizar versiones de un tipo específico o **Todos** los tipos.
Prueba de device	Selecciona **Fallo** para mostrar todos los dispositivos que tuvieron un fallo por lo menos en una de las reglas pertenecientes a las policies asociadas. Para mostrar solo los dispositivos con éxito en todas las reglas, selecciona **Éxito.** En caso de que quieras que todos los dispositivos se muestren, independientemente de que estén de acuerdo con las reglas, selecciona **Todos**.
Formato de salida	Escoge el formato deseado de salida: HTML, PDF o CSV. Opción disponible solo para informe que no es modelo.
Policy compliance	Selecciona las policies que serán analizadas.
Dispositivo	Asocia los dispositivos que tendrían sus versiones de configuración analizadas.

Por ejemplo, con el objetivo de verificar la seguridad de la red, creaste una regla para comprobar si la AAA (Autentificación, Autorización y Contabilidad, del inglés "Authetication, Authorization and Account") está habilitada. Esta regla verifica si la configuración de los equipos presenta el texto "aaa new-model" y fue asociada a la policy **Seguridad**.

Puedes saber si algún dispositivo no está de acuerdo con esta regla, o sea, está con la AAA deshabilitada. Para ello, puedes generar un informe como el mostrado en el ejemplo de abajo:



Ejemplo de Informe de Policy Compliance

Sugerencia

Puede comparar una política con cualquier versión de configuración en la pantalla del dispositivo haciendo clic en **Resumen** en el área de selección de gráficos. Una vez allí, seleccione la versión que desea probar y haga clic en **Probar policy compliance** botón.

Inventario Físico

El informe de inventario físico proporciona informaciones sobre las clases de componentes físicos de los equipos comprobados en el sistema e indica cuantos componentes poseen las mismas características.

Con él, es posible visualizar las características de los componentes físicos de los dispositivos, como nombre, descripción, modelo, fabricante, proveedor y versión.

Tabla 2.9. Formulario de informe de Inventario Físico

Campo	Descripción
Clase	Selecciona **Todas**, **Otros**, **Desconocido**, **Chasis**, **Backplane**, **Container**, **Fuente**, **Ventilador**, **Sensor**, **Módulo**, **Puerta**, **Pila** o **CPU**.

Campo	Descripción
Filtro por nombre	Rellena para filtrar por el nombre del equipo.
Filtro por ip	Rellena para filtrar por la dirección IP del equipo.
Filtro por metadatos de dispositivo	Añade filtros por campos de metadatos de dispositivo.
Filtro por campos de inventario	Añade filtros por campos de inventario. Selecciona **Descripción**, **Proveedor**, **Nombre**, **Versión de hardware**, **Versión de firmware**, **Versión de software**, **Serial**, **Fabricante**, **Modelo**, **Alias** o **Asset**.

Importante

Se necesita habilitar la recolecta de inventario físico en el formulario de cada dispositivo deseado.

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 2.10. 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.

Capítulo 3. Aprovisionamento

Scripts

Puedes ejecutar fácilmente, en un dispositivo, algún script ya existente o puedes crear uno nuevo y ejecutarlo sin ser necesario que sea guardado.

Esta ejecución puede ser inmediata o programada y los logs estarán disponibles en **Aprovisionamento** → **Tareas** por un período de tiempo que puedes definir en **Sistema** → **Parámetros** → **Aprovisionamento** .

Además, es posible acompañar los detalles del último Aprovisionamento usando la pestaña **Última tarea** dispuesta en el final de la página.

Creando scripts

Para crear un nuevo script, clica en la señal de **+** y edita la caja de texto. Después de esto, selecciona el modo de ejecución (**Lua**, **Send/Expect** om4_bold(Texto)), clica en **Ejecutar** y selecciona el dispositivo 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.

Ejecutando scripts

Para ejecutar algún script ya creado, clica en él en el menú de la izquierda. Puedes editarlo usando la caja de texto. También es posible seleccionar el modo de ejecución: **Lua**, **Send/Expect** om4_bold(Texto). Por último, clica en **Ejecutar** y selecciona el dispositivo en el que el script será ejecutado.

En caso de que quieras programa la ejecución, selecciona la opción **Programar modelo**. Necesitarás definir un nombre y el tipo de programación (**Una ejecución Diario**, **Semanal** o **Mensual**). Puedes acceder y editar tus programaciones en cualquier momento en **Aprovisionamento** → **Tareas**.

Tareas

En esta pestaña, se exhibirá una lista de tareas con informaciones sobre los últimos scripts ejecutados.

Las tareas se muestran de acuerdo con la fecha y la hora de ejecución.

Usando el botón **Script**, es posible ver más detalles del script como su nombre o modo de ejecución y el contenido del script.

Ya el botón **Exhibir** muestra detalles del Aprovisionamento como el estatus y el dispositivo. El resultado del Aprovisionamento puede verse clicando nuevamente en el botón **Exhibir**.

Las tareas pueden ser borradas en cualquier momento a través del botón **Borrar.**

Las tareas programadas pueden ser interrumpidas con el botón **Suspender** y retomadas con el botón **Retomar.**

Capítulo 4. Configuración

Reglas

Creación de reglas

1. Selecciona **Configuración** → **Reglas**.
2. Clica en el botón Nuevo para crear una nueva regla y rellena el formulario:

Tabla 4.1. 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.

Tipos de configuración

Existen 5 tipos preconfigurados de exportación de configuración. Puedes crear nuevos, pero puedes editar las propiedades de los ya existentes usando el botón **Editar**. De esta forma, es posible nombrarlos de acuerdo con tus preferencias.

Para visualizar el histórico de alteraciones, clica en el botón **Histórico**.

Los tipos de configuración que estén marcados como **activos** se mostrarán en el formulario de dispositivo.

Tabla 4.2. Tipos de configuración

Campo	Descripción
Nombre	Nombre del tipo de configuración
Descripción	Descripción del tipo de configuración
Activo	Selecciona **Sí** para activar el tipo de configuración y hacerlo visible en el formulario de configuración de dispositivo.

Scripts

Puedes crear y ejecutar scripts de los tipos: **Exportador de configuración**, **Inicio de sesión**, **Suministro** e **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 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  -----------------------
```

Agente de Exportación de Configuración

Crea un Script de Exportación de Configuración para hacer la gestión de la configuración de un dispositivo.

Sugerencia

Puede asociar un script a uno o más dispositivos utilizando el icono de **Configuración** sobre el cuadro de texto.

Usa el ejemplo a continuación para crear tu scripts de exportación de configuración:

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

h = params['ipaddr']
u = params['username']
p = params['passwd']

c=tmlSSH.sshNew({host=h,port='22',user=u,passwd=p,timeout='5'})

if(c == nil) then
 return nil
end

if (c:connect() == false) then
 return nil
end
if(c:expect('#') == false) then
 return nil
end

c:send('show config')

r = c:read()
if(r == nil) then
 return nil
end
c:disconnect()

r=tmlUtils.removeTerminalEscape(r)

return r

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

Script de Inicio de Sesión

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

Así como los scripts de suministro, los scripts de Inicio de sesión pueden ser escritos en tres modos: **Texto**, **Lua** y **Send/Expect**.

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

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

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

Script de Suministro

El script de suministro ejecuta una secuencia de preguntas y respuestas esperadas por el dispositivo.

Este tipo de script puede ser creado de tres modos: **Texto**, **Lua** y **Send/Expect**.

Puedes programar la ejecución de este tipo de script. Para ello, después de clicar en **Ejecutar**, selecciona la opción **Programar**. Necesitarás definir un nombre y el tipo de programación (**Una ejecución Diario**, **Semanal** o **Mensual**). Estas programaciones pueden accederse y editarse en cualquier momento en **Suministro** → **Tareas**.

Modo Texto

En este modo, el script será constituido, básicamente, por todos los comandos que son ejecutados en un dispositivo.

Modo Lua

En este formato, es posible convertir el suministro más personalizado a través de la programación.

Tendrá como modelo la variablem4_bold(params['connection']), que es el objeto de conexión al dispositivo que está siendo suministrado.

Modo Send/Expect

Este modo es el más utilizado para suministro. Ve abajo el script de Probe IP/SLA ICMP Echo [ip sla monitor] escrito en este modo y, a continuación, la descripción del mismo:

```
send: enable
expect: pass
send: %enable_passwd%
expect: #
send: configure terminal
expect: (config)
send: ip sla monitor %probe_index%
abort: invalid;#
send: type echo protocol ipIcmpEcho $ip_destination$ source-ipaddr $ip_source$
abort: incomplete;#
send: tag %probe_name%
expect: #
send: frequency 300
expect: #
send: exit
expect: (config)
send: ip sla monitor schedule %probe_index% life forever start-time now
expect: #
send:exit
```

- Los campos **send** son los comandos que serán ejecutados en el dispositivo.
- Los campos **expect** son strings esperadas por el dispositivo.
- Los campos **abort** son usados para introducir una string que causará el cierre del script si es recibido por el dispositivo. El texto introducido después del carácter, trabajará de la misma forma que el campo esperado.
- Cuando los campos son cerrados con el carácter **%**, pueden ser caracterizados como wildcards especiales. Ve la lista de las wildcards soportadas en la próxima sección.

Wildcards

Tabla 4.3. Lista de wildcards

Variables	Descripción
%username%	Campo de usuario del formulario de configuración del dispositivo.
%passwd%	Campos de contraseña de usuario del formulario de configuración del dispositivo.
%enable_passwd%	Habilitar campo de contraseña del formulario de configuración del dispositivo.
%probe_index%	Index SNMP de la probe.
%probe_name%	Campo de nombre del formulario de configuración de probe.
%collector_ip%	Dirección de IP del nuevo recolector o actual recolector que está abajo en la arquitectura distribuida..
%current_collector_ip%	Dirección de IP del actual recolector en la arquitectura distribuida.

Policy Compliance

Crea políticas de conformidad formadas por reglas que garanticen que las configuraciones de tus dispositivos están de acuerdo con lo esperado.

Puedes generar informes que muestren de manera clara como los dispositivos se están comportando en relación a las policies y reglas, o sea, si las están respetando o no.

De esta forma, tendrás mayor facilidad en el control y administración de posibles riesgos de seguridad, además de tener tu tiempo optimizado, ya que no necesitarás analizar manualmente cada configuración.

Regla

Puedes crear reglas que busquen, en sus versiones de configuración de dispositivos, expresiones específicas y que verifiquen que las configuraciones de tus dispositivos están correctas.

Para ello, accede a **Configuración** → **Policy Compliance** → **Nueva regla** o **Configuración** → **Policy Compliance** → **Regla** y clica en el botón **Nuevo**.

Tabla 4.4. Formulario de Regla de Policy Compliance

Campo	Descripción
Nombre	Define el nombre de la regla.
Descripción	Describe la regla, en caso que lo desees.
Texto de búsqueda	Añade filtro de strings. Puedes añadir todos los filtros que quieras y escoger las operaciones entre ellos: Y u **O.**

Las reglas pueden ser editadas en cualquier momento a través del botón **Editar** y ser eliminadas con el botón **Borrar**:

Importante
No podrás eliminar una regla que esté asociada a alguna policy.

Policy policy.

La policy es, básicamente, un conjunto de reglas.

Para crear una nueva policy, accede **Configuración** → **Policy Compliance** → **Nueva policy** o **Configuración** → **Policy Compliance** → **Policy** y clica en el botón **Nuevo**.

Tabla 4.5. Formulario de Policy Compliance

Campo	Descripción
Nombre	Define el nombre de la Policy.
Regla	Asocia una regla o más a la policy compliance.

Puedes editar la policy y las reglas que la componen. Para ello, clica en el botón **Editar**.

En caso de que quieras eliminar una policy, usa el botón **Borrar**.

Filtro de Trap

Algunos equipos disparan traps siempre que sus configuraciones son alteradas.

Crea filtros para estas traps y así todas las veces que el sistema las reciba, exportará la nueva configuración del equipo.

Importante

Es necesario que el dispositivo tenga el modo de exportación de configuración configurado como **Pasivo**.

Para crear un nuevo filtro, accede a **Configuración** → **Filtro de trap** → **Nuevo filtro de trap** o **Configuración** → **Filtro de trap** y clica en el botón **Nuevo**.

Tabla 4.6. Formulario de Filtro de Trap

Campo	Descripción
Nombre	Define un nombre para el filtro de trap.
Varbind identificador	Introduce las varbinds que deben estar presentes en la trap. Sepáralas por coma.
Varbind de usuario	Introduce la varbind que informa el usuario que efectuó la alteración. Este campo es opcional.
Varbind de host	Introduce la varbind informando el host que efectuó la alteración. Este campo es opcional.

Usa el botón **Editar** para alterar el filtro y el botón **Borrar** para eliminarlo.

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 4.7. 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).
Versión del SNMP	Selecciona la versión SNMP; Los posibles valores son: SNMP v1 o SNMP v2c Especifica una community SNMP

Campo	Descripción
	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 4.8. Campos de un metadato

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

Para asociar 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 5. 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 5.1. 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.

Telcomanager Windows Security Agent

Descarga el ejecutable **Telcomanager Windows Security Agent** (TSA) para instalar este agente en el Windows.

Este agente recolecta información sobre los archivos controlados por el sistema de Integridad de Seguridad y los envía al CFGtool.

Instalación del TSA

Después de bajar el ejecutable, serás encaminado a un asistente de instalación.

El asistente te dará las sugestiones de como seguir con la instalación y al final tendrás que rellenar los parámetros del archivo de configuración.

Una vez que los parámetros hayan sido rellenados, serás conducido a la etapa final del asistente. Certifícate que la opción "Run Telcomanager Security Agent <version>" esté habilitada y clica en **Finish**.

Tabla 5.2. Parámetros del archivo de configuración del TSA

Campo	Descripción
Files	Este parámetro se refiere a los archivos que serán controlados. Debe rellenarse con la dirección completa del archivo o de la carpeta que se desea comprobar, por ejemplo: **C:\Program Files (x86)\Telcomanager Security Agent**. En caso de que sea rellenado con una carpeta, todos los archivos pertenecientes a esta carpeta y a sus subcarpetas serán comprobados. Es posible añadir una lista de carpetas o archivos, basta separarlos con comas.
Ignore files	Este parámetro se refiere a los archivos que serán excluidos del seguimiento. Debe rellenarse con la dirección completa del archivo o de la carpeta que se desea excluir del seguimiento, por ejemplo: **C:\Program Files (x86)\Telcomanager Security Agent\excluded_file**. Es posible añadir una lista de carpetas o archivos, basta separarlos con comas.
Registry	Este parámetro debe rellenarse con el registro de Windows que se desear comprobar,

Campo	Descripción
	por ejemplo: **SOFTWARE\Microsoft\Windows \CurrentVersion\Installer**. Todos los registros debajo de lo rellenado serán controlados. Es posible añadir una lista de registros, basta separarlos con comas.
Ignore registry	Este parámetro se refiere a los registros que serán excluidos del seguimiento. Todos los registros que estén debajo de él, también serán excluidos del seguimiento. Es posible añadir una lista de registros, basta separarlos con comas.
Trafip IP	Dirección IP del TRAFip.
Port	Puerta que recibirá los datos en el TRAFip. Este parámetro debe rellenarse con el valor **59999**.
Interval	Intervalo, en segundos, introduce los seguimientos, o sea, si este parámetro fue rellenado con el valor **60**, los archivos y registros serán controlados cada minuto.

Archivo de configuración

El archivo de configuración es un archivo de texto creado automáticamente a través del asistente de instalación del TSA. Está localizado en la misma carpeta de instalación del servicio y tiene el nombre **config**.

Para alterarlo, es necesario interrumpir el servicio TSA en Windows antes y, entonces, editar el archivo usando el modo Administrador. Después de realizar las alteraciones, tendrás que iniciar el serviciom4_bold(TSA) nuevamente.

Tabla 5.3. Parámetros del archivo de configuración del TSA

Campo	Descripción
file_path	Se refiere al campo **Files**.
ignore_file_path	Se refiere al campo **Ignore files**.
registry_path	Se refiere al campo **Registry**.
ignore_registry_path	Se refiere al campo **Ignore registry.**
server_ip	Se refiere al campo **Trafip IP**.
server_port	Se refiere al campo **Port**.
Interval	Se refiere al campo **Interval**.

Capítulo 6. 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 6.1. 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 6.2. 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 6.3. 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 6.4. 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 6.5. 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

Campo	Descripción
	este habilitada en la consola. Habilítala en **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 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 un metadato creado a un nivel de urgencia, accede a la lista de niveles y clica en el botón **Metadato** al lado del nivel que será configurado.

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

Alarmas

El CFGtool proporciona 3 tipos de alarmas: **Configuration Check**, **Integridad de Seguridad** y **Connection Failure**.

El tipo **Configuration Check** posee 5 alarmas preconfiguradas que son disparadas en el caso de que suceda un cambio de configuración de un dispositivo.

El tipo **Integridad de Seguridad posee** 2 alarmas preconfiguradas (file change and file missing) que son disparadas en el caso de una alteración o falta de algún archivo.

El tipo **Connection Failure** posee 1 alarma preconfigurada (Connection Failure) que se dispara en el caso de que suceda algún fallo en la tentativa de obtener la configuración de algún dispositivo. No es posible crear nuevas alarmas de este tipo.

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

Además, puedes crear nuevas alarmas para saber cuándo las configuraciones de tus dispositivos no están respetando las políticas y reglas de Policy Compliance.

Tabla 6.7. Formulario de alarma CFGtool

Campo	**Descripción**
Nombre	Define un nombre para la alarma
Tipo de alarma	Escoge entre **Configuration check** e **Integridad de Seguridad.**
Tipo de configuración	Escoge el tipo de configuración.
Varbind	Campo de texto libre que puede ser usado para reconocer las alarmas que son encaminadas como traps.
Correo electrónico	Un correo electrónico será enviado a los usuarios. El servidor SMTP debe ser configurado, así como el correo electrónico de cada usuario en el formulario de configuración del usuario.
Dispositivo móvil (SMS)	Mensajes más cortos que los enviados por correo electrónico. Esta alarma puede ser enviada a un correo electrónico por el gateway de SMS si el campo de SMS está configurado en el siguiente formato: 88888888@operador.com. Si el SMS es un número de teléfono, los protocolos SMPP o HTTP también pueden ser usados para enviar el mensaje. Para hacer esto, necesitas configurar el siguiente ítem: **Sistema** → **Parámetros** → **Servidor SMS** .
Dispositivo móvil (Telegram)	Un mensaje será enviado a un chat del Telegram por un bot. Para configurar esta funcionalidad, debes crear un bot en el Telegram, para hacerlo, una vez en el Telegram, inicia una conversación como el usuario @BotFather. Escoge la opción/ newbot y sigue las instrucciones para finalizar la creación del bot. Al terminar anota el token del bot Telegram. Asocia el bot al chat en el que los mensajes serán enviados. Accede al formulario de perfil de usuarios, rellena el campo "Token del bot Telegram" y clica en Validar. Si todo va bien, el campo "ID del chat Telegram" será automáticamente rellenado. El mensaje será enviado después de los segundos definidos en el campo **Enviar mensaje después de**, iniciando por el tiempo de activación de la alarma.
Trap	Una trap se enviará para cada alarma.
Suministro	Selecciona **Sí** para habilitar el suministro para esta alarma.
Script de suministro	Selecciona un script de suministro para ser ejecutado.

Campo	Descripción
Enviar correo electrónico después de (minutos)	El correo electrónico será enviado después del número de minutos definido en este campo, a partir del horario de activación.
Enviar mensajes de dispositivo móvil después de (minutos)	los mensajes de dispositivo móvil serán enviadas después del número de minutos definido en este campo, a partir del horario de activación.
Enviar trap después de (minutos)	La trap será enviada después del número de minutos definido en este campo, a partir del horario de activación.
Ejecutar suministro después de (minutos)	Un script de suministro será ejecutado después del número de minutos definido en este campo, a partir del horario de activación.
Deshabilitar correo electrónico para la alarma eliminada	Si la opción "No" es seleccionada, el correo electrónico será enviado y la condición de eliminado será indicada en él. La opción "Sí" evitará que el correo electrónico sea enviado.
Deshabilitar sms para alarma eliminada	Si la opción "No" es seleccionada, el sms será enviado y la condición de eliminado será indicada en él. La opción "Sí" evitará que el sms sea enviado.
Deshabilitar trap para la alarma eliminada	Si la opción "No" es seleccionada, la trap será enviada y la condición de eliminada será indicada en ella. La opción "Sí" evitará que la trap sea enviada.
Deshabilitar suministro para alarma eliminada	Selecciona "Sí" para impedir que el suministro suceda cuando la alarma este eliminada.
Nivel de urgencia	Selecciona un nivel para la alarma.
Policy Compliance	Asocia las policies que serán controladas.
Perfiles de Alarma de dispositivo	Selecciona los perfiles de alarma a los cuales esta alarma pertenecerá.

Gestión de eliminación de alarma

Para eliminar una alarma, sigue el siguiente procedimiento:

1. Ves a la guía **ALARMmanager** → **Alarmas** y clica en el botón Alarmas eliminadas.
2. Rellena el campo del filtro en el formulario para seleccionar las alarmas/objetos y clica en el botón Filtro.
3. Selecciona las alarmas/objetos en la lista.
4. Rellena el **Motivo de la eliminación** si lo deseas.
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.

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 6.8. Campos de un metadato

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

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

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

Perfiles de alarma

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

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

Tabla 6.9. Formulario de perfil de alarma

Campo	Descripción
Nombre	Texto descriptivo para un perfil de alarma.
Tipo de asociación de objeto	Escoge **Manual** para asociar manualmente o **Automático** para usar una regla para asociar.
Alarma de dispositivo	Selecciona las alarmas deseadas para pertenecer al perfil.
Dispositivos	Este campo aparece cuando el **Tipo de asociación de objeto** es Manual. Selecciona los dispositivos que serán controlados.
Regla de asociación	Este campo aparece cuando el **Tipo de asociación de objeto** es Automático. Selecciona las reglas usadas para asociar los objetos que serán controlados.

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

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

Consola

Introducción

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

También posee los siguientes recursos:

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

Operación de Consola

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

Autentificación

Un usuario debe estar autentificado para acceder al ALARMmanager.

Consola

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

La consola posee las siguientes columnas:

Tabla 6.11. ALARMmanager consola

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

Reconocimiento de alarma

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

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

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

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

Eliminación de alarma

Para eliminar una alarma, sigue el siguiente procedimiento:

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

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

Comentario de alarmas

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

Para introducir un comentario, sigue el procedimiento siguiente:

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

Habilitar sonido para una alarma

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

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

Sincronización de alarma

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

Eliminando alarmas

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

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

Abrir gráficos

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

Filtro de alarma

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

Sugerencia

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

Capítulo 7. 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 7.1. 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 7.2. Copia de seguridad remota utilizando un servidor S3

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

Restauración Remota

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

Importante

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

Situación de restauración

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

Parámetros

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

Active directory

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

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

Tabla 7.3. 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 7.4. Formulario de agente de asociación automática

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

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 7.5. 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 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.

Campo	Descripción
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 7.6. 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

Campo	Descripción
	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 7.7. 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 7.8. Formulario BGP

Campo	Descripción
Habilitar BGP	Seleccione esta opción si desea anunciar o quitar una ruta.
Identificador BGP	Valor entero que identifica únicamente el emisor.
Número de AS local	Número del AS del emisor.
Número de AS del peer	Número del AS del receptor.
Ip del peer	IP del router del AS receptor.

Campo	Descripción
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 7.9. 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 7.10. 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 7.11. 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 7.12. 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 7.13. 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 7.14. 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!

Gestión de configuración

Selecciona el intervalo para recolectar todas las configuraciones de los dispositivos con un script asociado. Este script puede ser creado en la sección Scripts.

Tabla 7.15. Intervalo de gestión de configuración

Campo	Descripción
Límite de número de versiones	Define el número máximo de versiones que serán mantenidas por cada dispositivo. Cuando este límite sea alcanzado, las versiones más antiguas serán descartadas. El valor máximo es 4320.

Campo	Descripción
Intervalo de gestión	Configura el intervalo en horas para exportar la configuración del dispositivo. El modelo es de 8 horas.

Histórico de configuración

Selecciona el periodo de almacenamiento para diferentes áreas de configuración.

Tabla 7.16. 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 máximo de almacenamiento de estadísticas de resumen	Esto está solo relacionado al proceso de resumen. Esta estadística puede ser comprobada en **Sistema** → **Diagnósticos** → **Resumidor** .

Integridad de Seguridad

Selecciona el periodo de tiempo en el que las alarmas del tipo **Integridad de Seguridad** permanecerán activas.

Tabla 7.17. Integridad de Seguridad

Campo	Descripción
Límite de modificación (segundos)	Periodo de tiempo en que la alarma **Security integrity - file change** permanecerá alarmada.
Límite de ausencia (segundos)	Periodo de tiempo en que la alarma **Security integrity - file missing** permanecerá alarmada.

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.

Mapeo de IPs

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

Tabla 7.18. 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 7.19. 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 7.20. 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.

Suministro

Configura los parámetros para el suministro de scripts.

Tabla 7.21. Parámetros de suministro

Campo	Descripción
Período máximo de log para mantener (meses)	Define el tiempo en el que los logs de los scripts se mantendrán. Escoge un valor menor o igual a 120. El valor modelo es 1.
Límite de procesos de suministro simultáneos	Define el límite de procesos de suministro que serán ejecutados simultáneamente. Escoge un valor menor o igual a 50. El valor modelo es 10.
Límite de tiempo de espera de ejecución (minutos)	Define el tiempo límite de espera en el caso de que el límite de procesos simultáneos alcance el valor máximo definido. Escoge un valor menor o igual a 120. El valor modelo es 60.

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 7.22. Configuraciones de activación de redundancia

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

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

Conmutación

Tabla 7.23. 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 7.24. 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 7.25. Formulario de registro de acceso de usuarios

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

Informes

Esta sección permite hacer configuraciones avanzadas de los informes.

Informes programados

Configura las características para los informes programados.

Tabla 7.26. 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 7.27. 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.
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 7.28. 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 7.29. 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.

Campo	Descripción
Contraseña SMTP	Introduce la contraseña. Si el servidor SMTP no solicita autentificación en este campo puede dejarse en blanco.
Remitente SMTP	Configura un remitente para el correo electrónico.

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

SNMP

Recolector SNMP

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

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

Parámetros SNMP

SNMP Timeout	Tiempo límite en segundo que el colector esperará por un paquete de respuesta SNMP. Intervalo de valores 1-10.
Nuevos intentos SNMP	Número de intentos que serán permitidos para el dispositivo si no responde a una consulta SNMP. Intervalo de valores 1-10.
Número de OIDs por paquete	Número de OIDs que el recolector enviará en cada paquete SNMP. Intervalo de valores 1-100.
Tasa máxima de envío por paquete	Número máximo de paquetes por segundo que un recolector SNMP enviará a cada dispositivo.
Tasa máxima general de envío de paquetes (pps)	Límite global para la cantidad de paquetes enviados por segundo. Considera todos los dispositivos registrados. Rellena 0 si quieres que no tenga límites.
Ventana SNMP	Número de paquetes SNMP que serán enviados sin respuesta del dispositivo que está siendo sondado.
Puerta SNMP	Puerta TCP estándar para conectar con el agente SNMP.
Ignorar interfaces	Rellena la expresión para ignorar estas interfaces.
Interfaces high counter	Rellena la expresión para usar, en estas interfaces, el contador de OID más alto(ifHCInOctets e ifHCOutOctets).
Interfaces SecRate	Rellena la expresión para usar la sec rate OIDs (IfHCIn1SecRate y IfHCOut1SecRate) en estas interfaces.

Trap SNMP

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

Tabla 7.30. 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 7.31. 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.

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 7.32. 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 7.33. 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 7.34. 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.
Permiso para definir configuración de baseline	Esta opción está disponible solo para usuarios de los tipos **Administrador** y **Configurador**. Selecciona **Sí** para que el usuario pueda indicar una versión de configuración como ideal para un equipo.
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.

Campo	Descripción
Menú	Usa la opción estándar para restringir al usuario a menús específicos.

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 7.1. 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 7.35. 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 7.2. 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 7.36. 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 7.37. 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 7.38. 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.

Resumidor

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

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

Importante

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

Uso de disco

Muestra información sobre el uso de almacenamiento de las áreas.

Logs del sistema	Logs del sistema operacional.
Logs SLAview	Logs del SLAview.
Logs TRAFip	Logs TRAFip.

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

Archivos de Log

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

Archivos de LOG

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

Logs de configuración

Esta opción proporciona los logs de la configuración del sistema.

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

Huso horario

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

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

Soporte

Inicio de solicitud

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

Importante

Necesitar estar conectado a Internet.

Verificar si hay actualizaciones del sistema

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

Importante

Necesitas estar conectado a Internet.

Configuración de túnel para soporte remoto

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

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

Sugerencia

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

Sobre

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

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

Capítulo 8. 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 9. Glosario

Siglas

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

Tabla 9.1. 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.