

Manual SLAview

Manual SLAview

Tabla de contenidos

Prefacio	xii
Público objetivo	xii
Convenciones utilizadas en este manual	xii
1. Introducción	1
Sobre	1
Principales recursos	1
Requisitos mínimos	2
Hardware	2
Navegador	2
2. Conceptos básicos	3
SNMP Polling, resumen y gráficos	3
Alarmas	3
3. Guía rápida para iniciar	4
Accediendo a la interfaz web	4
Configurando métricas SNMP en los dispositivos	4
Seguimiento de alarma	5
4. Generador de gráfico Telcomanager	6
Periodo	6
Gráfico diario	6
Gráfico semanal	6
Gráfico mensual	6
Gráfico trimestral	6
Gráfico anual	6
Gráfico bienal	7
Gráfico de cinco años	7
Gráfico personalizado	7
Recursos	7
Caja de estadísticas	7
Mostrar valor	7
Zoom vertical	7
Una curva	7
Modo relativo	8
Configuración de ejes	8
Administrar alarmas	8
Crear una alarma	8
Recolecta on-line	8
Asociar a Graph Set	8
Ejecutar suministro	8
Guardar imagen	8
Tipo de gráfico	8
Gráfico agregado	8
Aproximar y alejar	9
Exportar	9
Actualización automática	9
Teclas	9
5. Datos históricos	11
Favoritos	11
Añadiendo objetos a favoritos	11
Eliminando objetos de los favoritos	11
Dashboards	11
Agregar nuevo dashboard	11

Agregar nuevo widget	12
Grupos	12
Añadir metadatos de grupos	14
Carpetas de enlace	14
Dispositivos	16
Creando un dispositivo utilizando el Asistente	20
Verificando objetos mapeados para el dispositivo	21
Importando archivos de dispositivo	21
Exportar datos	22
Operaciones por lotes	22
Añadir metadatos de dispositivos	22
Informe de configuración de inventario	23
Probes	24
Tareas	31
Prerrequisitos	31
Añadir metadatos de probes	31
Informes	32
Modelos	32
Análisis de variable	34
Top N	35
Syslog	36
Informe de Proyección	37
Mapeo de IPs	40
Graph set	40
Definiciones	40
Creación	40
Añadiendo gráficos	41
Visualizando un graph set	41
Editando un graph set	41
Generando gráficos para un graph set	42
Circuito	42
Histórico de ruta	43
Definiciones	43
Creación	43
Visualizando una prueba de ruta	43
6. Configuración	44
Perfiles	44
Definiciones	44
Gestionando perfiles	44
Exportando Perfiles	52
QoS	52
Definiciones	52
Habilitando el recurso de QoS	52
Habilitando seguimiento de QoS en las interfaces	52
Recolectoras	53
Importando archivos de recolectoras	53
Exportar datos	54
Añadir metadatos de recolectora	54
Objetos	54
Importando archivos de objetos	54
Mapeadores	55
Mapeo cruzado de OIDs	56
Asociando dispositivos a los mapeadores	57
Exportando e importando mapeadores	57

Mantenimiento	57
ICMP polling	57
Añadir metadatos de ICMP Polling	57
EPM (Extended Processing Module)	58
Tipos de probe	58
Añadir metadatos de tipos de probe	59
Reglas	60
Creación de reglas	60
Filtro 'No Response'	61
Trap Receiver	61
Configuraciones del Trap Receiver	61
Lógica del Trap Receiver	62
Alarma de Trap	62
Informe del Trap Receiver	62
Lógica de la fórmula del Trap Receiver	62
Añadir metadatos de Trap Receiver	63
Scripts	63
Creando scripts	63
Funciones	64
Ejecutando scripts	73
Script de Acción de alarma	73
Script de Recolector	74
Script de Mapeador	77
Script de Mapeamiento de IPs	81
Script de Suministro	81
Script de validación de metadatos	83
Credencial de dispositivo	83
Añadir metadatos de credenciales de dispositivo	84
Filtro de Syslog	85
Añadir metadatos de filtro de Syslog	85
Plantilla de Tiempo	86
7. Herramientas	87
Discovery	87
Exportar datos	87
MIB Browser	88
Software externo	88
Telcomanager Windows Collector	88
Telcomanager Host Agent	88
8. Sistema	89
Registro de acceso	89
Acceso de usuario	89
Acceso simultáneo	89
Copia de Seguridad/Restaurar	89
Copia de seguridad local de configuración	89
Restauración local de configuración	89
Copia de seguridad Remota	89
Restauración Remota	90
Situación de restauración	91
Parámetros	91
Active directory	91
Agente de las carpetas de enlace	91
Agentes de asociación	91
Alarmas	92
Almacenamiento de datos	93

Arquitectura distribuida	95
Aviso de Expiración	95
Copia de seguridad	96
BGP	96
Circuito	96
Cisco WAAS	97
Recolector personalizado	97
Configuración de HTTPS	97
Configuración del agente de captura	97
Configuración regional	98
Configuraciones del trap receiver	98
EPM	98
Exportación	98
Grafador	100
Histórico de configuración	101
ICMP	101
Inicio de sesión automático	102
Logotipo	102
Mapa GIS	103
Mapeador de objetos	103
Mapeo de IPs	103
Modo seguro	104
Nivel de log	105
Personalización de interface	105
Preferencias locales	107
Proyección	107
QoS	107
Redireccionamiento de inicio de sesión	107
Redundancia	107
Registro de acceso de usuarios	108
Informes	108
Servidor SMS	109
SMTP	110
SNMP	111
TACACS	112
Telcomanager Host Agent	112
Telcomanager JMX Agent	112
Tema	112
Verificación de versión del sistema	113
Web Services	113
Gest. de MIBs	113
Usuarios	113
Editando usuarios	114
Deshabilitar usuarios	115
Grupo de usuarios	115
Perfiles de usuarios	116
Log de modo seguro	116
Alarma Consola	117
Diagnósticos	117
Información de red	117
Pruebas de conexión	117
Captura de paquetes	118
Objetos	118
SNMP	118

Resumidor	118
Uso de disco	118
Archivos de Log	119
Logs de configuración	120
Consulta de datos brutos del SLAview	120
Plugins	120
Huso horario	121
Soporte	121
Inicio de solicitud	121
Verificar si hay actualizaciones del sistema	121
Configuración de túnel para soporte remoto	121
Sobre	121
9. Alarmas	123
Informes	123
Informes eliminados	123
Informes consolidados	123
Informes avanzados	124
Modelo de correo electrónico	126
Introducción	126
Personaliza el correo electrónico	126
Niveles de urgencia de alarma	127
Cambiando el nivel de prioridad de urgencia	127
Añade un nuevo nivel de urgencia	127
Añade metadatos de nivel de urgencia	128
Alarmas	128
Configuración de alarma fórmula	128
Configuración de las alarmas de cambio de comportamiento (Alarmas Históricas)	132
Configuración de alarmas syslog	137
Gestión de eliminación de alarmas.	138
Añadiendo metadatos de alarma	138
Perfiles de alarma	139
Añadiendo metadatos de perfil de alarma	140
Alarmas de servicio	140
Introducción	140
Creando una nueva Alarma de Servicio.	141
Fórmula	141
Añadiendo metadatos de alarmas de servicio	141
Consola	142
Introducción	142
Operación de Consola	142
10. Eagle Watcher	147
Configuración	147
11. NOC display	148
NOC Display	148
12. MapView	149
Introducción	149
Principales recursos	149
Operación	149
Navegación en el mapa	149
Filtro	150
Filtro de alarma para el mapa	150
Filtro de alarma de objeto	150
Datos detallados	150
Guardando el mapa	151

Cambiando el modo de visualización	151
Layout en grid	151
Creando y eliminando conexiones	151
Estilo de conexión	152
Seleccionando objetos	152
Alineando objetos	152
Editando las propiedades del objeto del mapa	152
Editando las propiedades del texto del mapa	152
Cambiando la imagen de fondo	153
Zoom in/out	153
Ajustar la pantalla	153
Habilitar cambio de tamaño de la imagen	153
Adición de texto y formas geométricas	153
13. Metadato	154
Introducción	154
Creación de un metadato	154
.....	154
14. Recursos habilitados con licencia	155
Redundancia	155
Conceptos	155
Habilitando la redundancia	155
Arquitectura distribuida	155
Conceptos	155
Prerrequisitos	156
Establecimiento	156
15. Glosario	157
Siglas	157

Lista de tablas

1. Convenciones del manual	xii
4.1. Teclas	9
5.1. Nuevo formulario de dashboard	11
5.2. Nuevo formulario de widget	12
5.3. Formulario de nuevo grupo	13
5.4. Campos de un metadato	14
5.5. Formulario para nueva carpeta de enlace	15
5.6. Campos de un metadato	15
5.7. Formulario de nuevo dispositivo	16
5.8. Campos del archivo de dispositivo	21
5.9. Campos de un metadato	23
5.10. Formulario de informe de inventario de configuración	23
5.11. Formulario de nivel de filtro	23
5.12. Telco ICMP/Jitter probe	25
5.13. Telco HTTP probe	25
5.14. Telco DNS probe	26
5.15. Telco SSH probe	26
5.16. Telco TCPConnect probe	27
5.17. Telco Twamp	27
5.18. Cisco IP/SLA Jitter probe	28
5.19. Cisco IP/SLA ICMP Echo probe	29
5.20. Cisco IP/SLA Path Echo probe	30
5.21. Cisco IP/SLA UDP Echo probe	30
5.22. Campos de un metadato	31
5.23. Forma del modelo	32
5.24. Informe de Análisis de variable	34
5.25. Señalización de Análisis de variable	35
5.26. Informe Top N	36
5.27. Informe Syslog	37
5.28. Formulario de configuración de proyección	38
5.29. Formulario del informe de proyección	38
5.30. Formulario de Mapeo de IPs	40
5.31. Creación de graph set	41
5.32. Formulario de nuevo circuito	42
5.33. Creación de prueba de ruta	43
6.1. Formulario de perfil	44
6.2. Variable de resumen	48
6.3. Gráfico	49
6.4. Curva del gráfico	49
6.5. Formulario de asociación de perfil	50
6.6. Formulario de Asistente de QoS	52
6.7. Formulario de recolectoras	53
6.8. Campos de archivos de recolectoras	53
6.9. Campos de un metadato	54
6.10. Formulario de Mapedador	55
6.11. Campos de un metadato	57
6.12. Formulario de tipo de probe	58
6.13. Campos de un metadato	60
6.14. Perfil automático de reglas	60
6.15. Configuración Trap Receiver	61
6.16. Lógica Trap Receiver	62

6.17. Informe del Trap Receiver	62
6.18. Campos de un metadato	63
6.19. Target	64
6.20. Parámetro	66
6.21. Parámetro	66
6.22. Comando	67
6.23. Parámetros	67
6.24. Parámetro	68
6.25. Comando	69
6.26. Parámetro	69
6.27. Comando	69
6.28. Lista de wildcards	82
6.29. Formulario de Credencial de Dispositivo	83
6.30. Campos de un metadato	84
6.31. Formulario de Filtro de Syslog	85
6.32. Campos de un metadato	85
6.33. Formulario de Filtro de preferencias locales.	86
7.1. Parámetros del Discovery	87
8.1. Copia de seguridad remota utilizando un servidor FTP	90
8.2. Copia de seguridad remota utilizando un servidor S3	90
8.3. Formulario de Active directory	91
8.4. Formulario de agente de asociación automática	91
8.5. Formulario de parámetros del Alarmas	92
8.6. Formulario de almacenamiento de datos	93
8.7. Formulario de los parámetros de la arquitectura distribuida	95
8.8. Formulario de aviso de expiración	95
8.9. Formulario BGP	96
8.10. Formulario de circuito	97
8.11. Formulario de Cisco WAAS	97
8.12. Formulario del recolector personalizado	97
8.13. Formulario de HTTPS	97
8.14. Formulario de configuración del agente de captura	98
8.15. Formulario de configuración regional	98
8.16. Formulario EPM	98
8.17. Protocolo Syslog	99
8.18. Formulario de parámetros del grafador	100
8.19. Parámetros de históricos de configuración	101
8.20. Formulario de parámetros del proceso ICMP	101
8.21. Formulario de configuración de parámetros de mapeador de objetos	103
8.22. Formulario de configuración de parámetros de asignación de IPs	103
8.23. Formulario de modo seguro	104
8.24. Formulario de personalización de interfaz	105
8.25. Etiqueta en el campo Fórmula del nombre del dispositivo (menú de árbol).	105
8.26. Etiqueta en el campo Dispositivo (Gráfico).	106
8.27. Etiqueta en el campo Interfaz (Gráfico).	106
8.28. Formulario de preferencias locales	107
8.29. Configuraciones de activación de redundancia	107
8.30. Configuraciones de conmutación de redundancia	108
8.31. Formulario de registro de acceso de usuarios	108
8.32. Formatear	109
8.33. Formulario de configuración de los informes programados	109
8.34. Formulario de configuración del servidor FTP	109
8.35. Formulario de servidor SMPP	109
8.36. Formulario de parámetros SMTP	110

8.37. Campos de TRAP	112
8.38. Configuración del tema	112
8.39. Formulario de API de configuraciones	113
8.40. TRAFip's raw data form	113
8.41. Formulario de usuario	114
8.42. Formulario de usuario	115
8.43. Formulario de usuario	116
8.44. Formulario de Log de modo seguro	116
8.45. Columnas Alarmas consola	117
8.46. Captura de paquetes	118
8.47. Consulta de datos brutos del SLAview - Paso 1	120
8.48. Consulta de datos brutos del SLAview - Paso 2	120
9.1. Formulario de informe de alarmas eliminadas	123
9.2. Formulario de alarmas consolidadas	123
9.3. Formulario de informe avanzado de alarma	124
9.4. Informe de señalización de alarma avanzado	126
9.5. Modelo de correo electrónico	126
9.6. Variables del correo electrónico	126
9.7. Formulario de nivel de urgencia de alarma	127
9.8. Campos de un metadato	128
9.9. Formulario de alarma fórmula	128
9.10. OPCIÓN	131
9.11. TIPO_DE_OBJETO	132
9.12. Formulario de cambio de comportamiento	133
9.13. Formulario de alarma syslog	137
9.14. Campos de un metadato	139
9.15. Formulario de perfil de alarma	139
9.16. Campos de un metadato	140
9.17. Formulario de alarmas de servicio	141
9.18. Alarmas consola	143
9.19. Menú de contexto	143
13.1. Formulario de un nuevo metadato	154
15.1. Lista de siglas y abreviaturas	157

Prefacio

Público objetivo

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

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

Convenciones utilizadas en este manual

Este documento utiliza las siguientes convenciones:

Tabla 1. Convenciones del manual

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

Capítulo 1. Introducción

Sobre

SLAview es un gerente de sistema de red enfocado en el análisis de rendimiento.

Las principales tecnologías utilizadas son el protocolo SNMP, protocolo ICMP y Cisco SLA Probes, Telcomanager Software Probes y algoritmos de análisis comportamental.

Principales recursos

- Seguimiento de cualquier dispositivo de la red usando protocolos SNMP v1, v2c y v3.
- Acceso a todos los recursos del sistema a través de un web browser.
- Visiones jerárquicas.
- Captura e informe de Syslog.
- Plataforma multi-tenant, que suministra aislamiento del ambiente del usuario.
- Creación de fórmulas, permitiendo que el usuario defina sus propias KPIs (Key Performance Indicators).
- Alarma de análisis de comportamiento en cualquier KPI controlada.
- Arquitectura escalable. El sistema puede crecer en el número de elementos recolectados por el uso de appliances recolectores remotos y en el número de usuarios e informes que soporta por medio de la implantación de EPMs (Expanded Processing Modules), que son appliances responsables por compartir la carga con el sistema central.
- Puede ofrecerse alta disponibilidad a través del uso de soluciones redundantes, en las que dos appliances trabajan en HOT-STANDBY.
- Informe de proyección.
- Todos los informes pueden ser guardados como modelos, programados y exportados en formato PDF, HTML y CSV.
- Polling de SNMP en línea con 10 segundos de intervalo, clicando en cualquier gráfico.
- Exportación de imagen de gráfico en masa.
- Flexibilidad en la creación de gráficos.
- Gráfico en HTML5 interactivo, con recursos como zoom vertical y horizontal, auto-escala y gráficos agregados.
- Descubierta de objetos SNMP.
- Banco de datos de alto rendimiento para datos históricos almacenados.
- Informes Top N para todos los elementos controlados.
- Informes de alarmas avanzados que permiten la agregación de datos a través de la técnica de pivote.

- Polling, consolidación y perfiles de gráfico.
- Asociación de perfiles automáticos, facilitando las tareas administrativas diarias.
- Herramienta MAP nombrada MAPview, con topología de recurso de mapeo y navegación de interfaz intuitiva.
- Herramienta Alarmas, que permite que los usuarios configuren alarmas como una fórmula con las métricas controladas para cada objeto. Las alarmas pueden ser visualizadas en una consola o enviadas por correo electrónico, SMS y traps SNMP.
- Agente de auto QoS (Quality of Service) desarrollado para MIB Cisco Class Based QoS

Requisitos mínimos

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

Hardware

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

Navegador

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

Capítulo 2. Conceptos básicos

SNMP Polling, resumen y gráficos

La principal tecnología empleada en el sistema del SLAview es el protocolo SNMP (Simple Network Management Protocol).

El SLAview es capaz de realizar el seguimiento de cualquier equipo que ejecute el agente SNMP o que solo responda al ping de consulta.

El protocolo SNMP trabaja con el MIB (Management Information Base) del equipo. El MIB es un banco de datos que puede ser consultado para suministrar información de configuración y rendimiento. El agente SNMP controla el acceso al MIB y responde a las consultas a su banco de datos.

El sistema SLAview posee un proceso de polling muy flexible. Puede mapear instancias de una amplia variedad de objetos en los archivos de MIB, como interfaces de red, procesadores, unidades de almacenamiento y muchos otros. El mapeo de objetos es definido por el usuario y se referirá a ellos como objetos comprobados o mapeados. Una vez que los mapeos fueron realizados, las instancias de los objetos encontrados pueden ser asociadas a los perfiles donde las OIDs que son usadas en el proceso de polling fueron definidas.

El sistema suministra perfiles, donde el usuario puede definir fórmulas de resúmenes basadas en la OIDs, que son, en realidad, las métricas o KPIs que deben comprobarse.

Los gráficos también son definidos en los perfiles y las curvas son fórmulas basadas en los resúmenes de variables predefinidas.

Alarmas

Las alarmas son definidas como fórmulas basadas en el resumen de variables. Puedes definir fórmulas libremente usando la anotación infija.

Capítulo 3. Guía rápida para iniciar

Accediendo a la interfaz web

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

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

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

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

Pantalla principal del SLAview

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

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

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

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

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

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

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

Configurando métricas SNMP en los dispositivos

Para implementar con éxito este procedimiento, los elementos de red que serán usado deben tener una community SNMP de lectura configurada.

Procedimiento 3.1. Pasos de configuración

1. Selecciona **Datos históricos** → **Dispositivos** → **Nuevo dispositivo** y rellena el formulario de acuerdo con las instrucciones de abajo:
 - a. Nombre y dirección de IP de gestión.
 - b. Versión SNMP y community como configurados en los elementos de red.
 - c. En el campo Mapeador, selecciona Interfaz y también CPU y, en caso de equipo Cisco, Memoria.
 - d. Clicka en el botón Guardar.

2. Espera en torno a 5 minutos para que el sistema descubra los elemento de interfaz de red, selecciona **Configuración** → **Perfiles** → **Objetos mapeados** , clics en el botón Asociación de objetos mapeados y rellena el formulario de acuerdo con las instrucciones de abajo:
 - a. Selecciona el tipo de perfil que corresponde al tipo de interfaz que deseas controlar. Ej.: para la interfaz serial Cisco selecciona la opción Serial-cisco.
 - b. Usa el filtro para seleccionar la interfaz. Ej: *Serial*.
 - c. Selecciona Interfaz en el campo tipo y clics en el botón Enviar.
 - d. Mueve la interfaz deseada a la caja de la derecha.
 - e. Usa la OID de filtro 1.3.6.1.2.1.2.2.1.7 = 1, marcando la opción Usar index de objeto mapeado. Esto filtrará las interfaces *ifAdminStatus up*.
 - f. Clics en Enviar y después Guardar.
3. Espera en torno a 10 minutos y selecciona **Datos históricos** → **Dispositivos** → **Dispositivo** . Después clics en el dispositivo creado y verifica los gráficos en las interfaces controlados.
4. Repite el mismo procedimiento para CPU y objetos de memoria si estás controlando elementos Cisco. En el paso 2, el tipo debe ser CPU o memoria.

Seguimiento de alarma

Procedimiento 3.2. Pasos de configuración

1. Selecciona **Alarmas** → **Perfiles** → Clics en el botón Nuevo.
2. Rellena el nombre del perfil y escoge la opción Objetos mapeados en el campo Tipos de objeto.
3. Selecciona las alarmas que quieres usar. Ej.: interfaz baja y utilización de banda alta.
4. Selecciona los objetos que quieres controlar. Ej: Router1FastEthernet0/1. Ahora, clics en el botón Guardar.
5. Selecciona **Sistema** → **Usuarios**. Clics en el botón Nuevo.
6. Rellena el nombre de perfil, selecciona los usuarios y después las alarmas que los usuarios serán capaces de recibir. Clics en el botón Guardar para guardar las alteraciones.

Capítulo 4. Generador de gráfico Telcomanager

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

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

Periodo

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

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

Gráfico diario

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

Gráfico semanal

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

Gráfico mensual

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

Gráfico trimestral

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

Gráfico anual

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

Gráfico bienal

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

Gráfico de cinco años

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

Gráfico personalizado

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

Recursos

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

Sugerencia

El sistema puede mostrar alertas en los gráficos cuando se excede el límite de licencia. Esta configuración se puede deshabilitar en Grafador.

Caja de estadísticas

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

Mostrar valor

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

Zoom vertical

Para habilitar este recurso, sigue el siguiente procedimiento:

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

Una curva

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

Modo relativo

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

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

Configuración de ejes

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

Administrar alarmas

Clica en esta opción en el menú Opciones del panel de control del gráfico para abrir una ventana donde puede configurar (editar y eliminar) las alarmas creadas por el gráfico.

Crear una alarma

Encontrarás esta opción al clicar con el botón derecho del ratón en el gráfico. Se abrirá una pantalla donde podrás crear alarmas. También se creará el perfil de alarma (si es necesario) y la alarma se asociará con el perfil de usuario.

Recolecta on-line

Encontrarás esta opción al clicar con el botón derecho del ratón en el gráfico. Se abrirá una nueva ventana en el navegador donde serás capaz de definir el tiempo de refresh e iniciar un polling online para el gráfico.

Asociar a Graph Set

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

Ejecutar suministro

Con el menú **Ejecutar suministro** en el panel de control, puede ejecutar los scripts de aprovisionamiento. Este icono solo está presente en el gráfico de objetos mapeados y cuando la CFGtool licencia.

Guardar imagen

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

Tipo de gráfico

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

Gráfico agregado

Clica en esta opción a través del menú popup del gráfico para abrir representaciones agregadas al gráfico. Existen dos opciones de gráficos: circular y barra. Estos gráficos pueden filtrarse por un periodo de un día.

Por ejemplo, si abres un gráfico redondo semanal y filtras de las 10:00h a las 17:00h, el gráfico redondo presentará los datos semanales para aquel periodo del día.

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

Sugerencia

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

Aproximar y alejar

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

Importante

Estas opciones solo son disponibles en gráficos del tipo lineal.

Exportar

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

Actualización automática

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

Sugerencia

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

Teclas

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

Tabla 4.1. Teclas

Tecla	Descripción
D	Transforma el gráfico para el modo derivativo.
I	Indica informaciones detalladas sobre el gráfico como resolución, curvas, samples y timesteps.
L	Relaciona el tiemestamp y el valor de cada punto de una curva.
N	Cambia el formato de las curvas del gráfico, una vez que todas ellas están empiladas.

Tecla	Descripción
P	Genera una curva de proyección que considera solo los puntos entre el intervalo limitado por las líneas señalizadas. Cuando mueves el ratón para abajo, el número de puntos disminuye, en caso contrario el número de puntos aumenta.
R	Ajusta el gráfico de forma que tenga la resolución máxima.
S	Guarda el gráfico como una imagen en el formato PNG.
W	Cambie la configuración de la curva para waas accell.
Z, Abre el popup de Violación de Proyección , una vez que la Proyección está activada.-	
-	Zoom out.
+	Zoom in.
LEFT	Mueve el gráfico para la izquierda.
RIGHT	Mueve el gráfico para la derecha.
*	Gráfico retorna a su tamaño normal.

Sugerencia

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

Capítulo 5. Datos históricos

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

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

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

Favoritos

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

Añadiendo objetos a favoritos

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

Eliminando objetos de los favoritos

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

Dashboards

Esta pestaña permite la creación de tableros personalizados, que ofrecen diferentes tipos de widgets, que contienen datos de variables de resumen o alarmas. El widget puede ser de informe, gráfico circular, gráfico en barras o gauge.

Cada usuario solo puede visualizar dashboards que se asociaron con su perfil de usuario. Además, solo es posible que el usuario visualice información de objetos en grupos que se asociaron con él perfil de usuario.

Los widgets de la variable de resumen brindan un Top 10 diario, semanal o mensual para la variable elegida. Es decir, se mostrarán los 10 objetos que tienen los valores más altos para la variable. Para widgets de este tipo de datos, las vistas de informe, gráfico circular y de gráfico en barras están disponibles.

Los widgets de alarma aportan la cantidad de objetos con alarma y la cantidad total de objetos asociados con la alarma. También se informa el porcentaje de objetos con alarma. Es posible filtrar la alarma en Alarmas haciendo clic en el widget. Para los widgets de este tipo de datos, solo están disponibles las vistas de indicadores.

Agregar nuevo dashboard


Accede a **Datos históricos** → **Dashboards**. Después, haz clic en **Nuevo dashboard**. Complete el formulario como se detalla a continuación:

Tabla 5.1. Nuevo formulario de dashboard

Campo	Descripción
Nombre	Nombre del ashboard
Descripción	Descripción del dashboard

Campo	Descripción
Perfiles de Usuario	Perfiles de usuario que pueden visualizar el dashboard

Sugerencia

Para abrir un dashboard en una nueva ventana, usa el ícono .


Agregar nuevo widget

Accede a cualquier dashboard y luego haga clic en el widget vacío para crear un nuevo widget. Complete el formulario como se detalla a continuación:

Tabla 5.2. Nuevo formulario de widget

Campo	Descripción
Título	Título del widget
Tipo de objeto	Elija si el tipo de objeto será Dispositivo o Objeto mapeado
Tipo de dato	Elija si el tipo de datos será la Variable de resumen o la Alarma
Variable de resumen	Elija una variable de resumen. Esta opción solo se mostrará si se seleccionan los tipos de datos de la Variable de resumen
Alarma	Elige una alarma Esta opción solo se mostrará si se seleccionan los tipos de datos de alarma
Período	Elige el período del widget entre 5, 15, 30 o 60 minutos. Esta opción solo está disponible si se seleccionan los tipos de datos de la variable de resumen
Tipo de widget	Elija un tipo de widget de widget entre Informe, Gráfico circular, Gráfico en barra o Gauge
Ancho	Elija el ancho del widget
Filtros	Filtre los resultados utilizando expresiones regulares. El contenido puede restringirse según los valores de los metadatos y los campos internos del sistema.

Sugerencia

Para editar el widget, haga clic en el icono .

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 5.1. 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 5.3. Formulario de nuevo grupo

Campo	Descripción
Nombre	Define un nombre para el grupo.
Descripción	Define una descripción para el grupo.
Resumen de grupo	Habilita el resumen de grupo para este grupo. Si el resumen de grupo está habilitada para el Usuario, se muestra el gráfico de grupo resumido.
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 opción está disponible solo cuando la Asociación automática está habilitada.
Servicio	Seleccione Sí para que el grupo pueda activar alarmas de servicio.
Dispositivos	Dispositivos que pertenecerán a este grupo.
Objetos mapeados	Objetos mapeados que pertenecerán a este grupo.
Perfiles de alarma	Asocia el grupo a un perfil de alarma. El grupo solo puede asociarse con un perfil de alarma si su resumen de grupo está habilitado.
Perfiles de Usuario	Perfiles de usuarios que tendrán acceso a este grupo.

3. Clicka en el botón **Guardar**.
4. Para añadir más grupos debajo de este grupo, clicka en el icono Grupos, selecciona Subgrupos en el área de selección del gráfico y repite los pasos de encima.

Para ver el Mapa del grupo, haga clic en el icono **Mapa** dentro del grupo que desea ver.

Añadir metadatos de grupos

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

Clicka 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, clicka en el botón **Borrar**.

Tabla 5.4. Campos de un metadato

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

Para asociar el metadato creado a un grupo, accede a la lista de grupos y clicka 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.

Carpetas de enlace

Las carpetas de enlace son usadas para crear grupos automáticos asociados a los objetos mapeados representando las conexiones en el sistema.

Para configurar los grupos formados por subgrupos pertenecientes al grupo de origen en la carpeta de enlace, el sistema comprobará si existen conexiones para cada uno de ellos y, en caso afirmativo, creará grupos para cada lado de la conexión con las interfaces que representan esta conexión.

Por ejemplo: un grupo 'S', posee dos subgrupos: 'A' y 'B'. 'A' posee un dispositivo 'Da' y 'B' posee el dispositivo 'Db'. La interfaz 'Ia' pertenece a 'Da' e la interfaz 'Ib' pertenece al 'Db'. 'Ia' y 'Ib' están conectadas. Una carpeta de enlace 'L' es criada con el grupo de origen 'S'. Dos grupos serán creados debajo de 'L': 'A' --> 'B' que poseen interfaz 'Ia' and 'B' --> 'A' que tienen la interfaz 'Ib'.

La visualización es restricta del mismo modo que grupos normales.

Procedimiento 5.2. Pasos de configuraciones

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

2. Clica en el icono Carpeta de enlace para abrir el formulario de configuración.
3. Clica en el botón **Nuevo** para definir una nueva carpeta de enlace y rellena el formulario de nueva carpeta de enlace.

Tabla 5.5. Formulario para nueva carpeta de enlace

Campo	Descripción
Prefijo	Prefijo para ser concatenado al nombre del grupo de origen.
Sufijo	Sufijo para ser concatenado al nombre del grupo de origen.
Crear subgrupo	Si sí, los grupos serán creados recursivamente. Si no, solo los grupos de root serán creados.
Grupo de destino	Grupo donde el enlace del grupo será creado.
Grupo de origen	Grupo para buscar conexiones.
Reglas	Reglas para filtrar que interfaces serán consideradas. Solo aplicado al nombre de interfaces.

4. Clica en el botón **Guardar**.
5. Los nuevos grupos serán creados tras la ejecución del agente de la carpeta de enlace. La ejecución del tiempo del agente puede ser configurada en parámetros del sistema.

Añadir metadatos de carpetas de enlace

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

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

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

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

Tabla 5.6. Campos de un metadato

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

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

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.

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

Procedimiento 5.3. Pasos de la configuración de los dispositivos

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

Tabla 5.7. 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	<p>Selecciona la versión SNMP. Los posibles valores son:</p> <p>SNMP v1 o SNMP v2c Especifica una community SNMP</p> <p>SNMP v3 Especifica el tipo de autenticación y sus parámetros</p>
Community SNMP	Rellena la community SNMP.

Campo	Descripción
Tipo de autenticación de SNMPv3	Tipo de autenticación. Los valores posibles son: authPriv, authNoPriv y noAuthNoPriv. Necesario para SNMPv3.
Nombre del usuario	Nombre del usuario. Necesario para SNMPv3.
Tipo de contraseña	Tipo de contraseña. Los valores posibles son: SHA-1 y MD5. Necesario para los tipos de autenticación authPriv y authNoPriv (SNMPv3).
Contraseña de autenticación	Contraseña de autenticación. Necesario para los tipos de autenticación authPriv y authNoPriv (SNMPv3).
Protocolo de Privacidad	Protocolo de Privacidad. Los valores posibles son: DES y AES. Necesario para los tipos de autenticación authPriv (SNMPv3).
Contraseña de privacidad	Contraseña de privacidad. Necesario para los tipos de autenticación authPriv (SNMPv3).
Utilizar configuración modelo de SNMP	Esta opción te deja definir los valores que pueden ser usados específicamente para este dispositivo. Los valores modelos están especificados en la configuración de los parámetros de los recolectores SNMP.
Considerar SysUpTime en la recolecta	Descarta la recolecta si el dispositivo no es permitido durante más de 5 minutos. Previene errores de cálculo.
SNMP Timeout	Tiempo límite en segundos para esperar una respuesta del paquete SNMP. Intervalo de valores 1-10.
Intentos SNMP	Número de nuevos intentos que serán permitidos al dispositivo si no responde a una consulta SNMP. Intervalo de valores 1-10.
Número de OIDs por paquete	Número de OIDs que serán enviadas en cada paquete SNMP. Intervalo de valores 1-100.
Tasa máxima de envío de paquetes (pps)	Número máximo de paquetes por segundo que un recolector SNMP enviará a cada dispositivo.
Ventana SNMP	Número de paquetes SNMP que serán enviados sin respuesta del dispositivo que está siendo polled.
Puerta SNMP	La puerta SNMP
Agentes	Esta opción permite que definas múltiples agentes SNMP en la misma dirección de IP y diferentes puertas. Ahora puedes especificar máscaras OID y la puerta SNMP para esta máscara. Esto significa que el recolector SNMP usará la puerta UDP especificada si la OID a ser

Campo	Descripción
	recolectada en este dispositivo corresponde a la máscara especificada. Ejemplo: <ul style="list-style-type: none"> • 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, 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) .

Campo	Descripción
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 recolecta por CALLview	Habilita la colección por CallView.
Perfil de voz	Seleccione el perfil de voz para recopilar datos de llamadas.
Habilitar colecta JMX	Seleccione Sí para habilitar la recopilación de estadísticas de Java Management Extensions o No para deshabilitar. Para realizar la recolección JMX es necesario que el Telco JMX Agent esté configurado en Sistema → Parámetros → Telcomanager JMX Agent .
Método de mapeo de topología	Selecciona el protocolo que será usado para el mapeo de topología. Las acciones disponibles son: CDP - Cisco Discovery Protocol, LLDP - Link Layer Discovery Protocol o ambos. Usando ambos métodos, el SLAview utilizará el protocolo SNMP para buscar informaciones de estos protocolos en las tablas MIB de los dispositivos comprobados.
Habilitar suministro	Habilitar suministro para configurar automáticamente las Cisco IP SLA probes, Telcomanager probes y exportación de Netflow.
Recolector	Asociación del dispositivo a un recolector remoto. Este campo está disponible solo cuando la arquitectura distribuida es habilitada.
Script de autenticación	Cuando el protocolo de conexión este configurado como Telnet , necesitas seleccionar un script de Inicio de sesión.

Campo	Descripción
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: Almacenamiento, Antena, Cámara, Enrutador, Estación, Firewall, Impresora, Inalámbrico, Otro, Punto de acceso, Servidor, Servidor Virtual, Servidor de Base de Datos, Switch o Telco Appliance. El tipo estándar es el Enrutador .
Script de exportación de configuración	Selecciona los scripts exportadores de configuración.
Dominio	Asociación de dominio del dispositivo.
Grupos	Clica en el botón Listar y selecciona los grupos deseados para este dispositivo en uno o más puntos en el grupo de jerarquía.
Mapeadores	Selecciona el mapeador deseado para mapear objetos, con interfaces y cpus en este dispositivo.(Ve la sección configuración de mapeadores.)
Perfiles del SLAview	Asocia el dispositivo a un Perfiles del SLAview.
Plantilla de Tiempo	Seleccione la plantilla de tiempo.

Creando un dispositivo utilizando el Asistente

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

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

Verificando objetos mapeados para el dispositivo

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

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

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

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

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

Importando archivos de dispositivo

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

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

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

Un archivo de dispositivo importado posee los siguientes campos:

Tabla 5.8. 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).

Campo	Descripción
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 Almacenamiento, Antena, Cámara, Enrutador, Estación, Firewall, Impresora, Inalámbrico, Otro, Punto de acceso, Servidor, Servidor Virtual, Servidor de Base de Datos, Switch o Telco Appliance.

Exportar datos

Haga clic en el botón **Exportar datos** para exportar la lista de objetos en formato CSV.

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**, clic en el ítem **Dispositivo** en el menú del árbol y clic 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, clic en el botón **Borrar**.

Tabla 5.9. 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 , Enum o SNMP .
OID	Este campo solo está disponible si el Tipo de dato es SNMP . Introduce una OID.
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 clic en el botón **Metadato** al lado del dispositivo que será configurado.

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

Importante

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

Informe de configuración de inventario

El Informe de configuración de inventario está destinado a agregar información de metadatos del sistema y dar cuenta de cada intersección de línea/columna de metadatos.

El informe está compuesto por niveles. Cada nivel tiene: nombre, línea y columna. Los campos de línea y columna corresponden a los metadatos del sistema.

Procedimiento 5.4. Pasos de la configuración de los Informes

1. Seleccione **Datos históricos** → **Dispositivos** → **Informe de inventario** .
2. Haga clic en el botón **Nuevo** para crear un informe y completar el formulario.

Tabla 5.10. Formulario de informe de inventario de configuración

Campo	Descripción
Nombre	Reportar nombre
Tipo	Tipo de metadatos: Device o Mapped objects .

3. Haga clic en el botón **Salvar**.
4. Una vez creado el informe, haga clic en **Editar** → **Nuevo** para crear los niveles del informe.

Tabla 5.11. Formulario de nivel de filtro

Campo	Descripción
Nombre	Nombre del filtro.

Campo	Descripción
Línea	Los metadatos que estarán representados por la línea.
Columnas	Los metadatos que estarán representados por la columna.
Nivel de filtro	Define el orden en el que se mostrará el filtro en el informe.

Importante

Los metadatos deben ser del tipo **Enum**, de lo contrario no aparecerán en la lista.

5. Haga clic en el botón **Salvar**.
6. Una vez que se crean el informe y sus niveles, puede ver el resultado haciendo clic en el nombre del informe en el menú de árbol o en el botón **Mostrar** en la pantalla **Informe de inventario de configuración**.
7. Cuando ejecuta el informe, se muestra el primer nivel. Al hacer clic en cualquier elemento de la tabla del informe (columna, fila o celda) el sistema mostrará el siguiente nivel, filtrando los resultados según el objeto seleccionado.

Probes

Probes son agentes activos que hacen mediciones en el desempeño de la red. Algunos proveedores soportan este tipo de agente, como la probe Cisco IP SLA, probes Juniper real-time performance (RTM), probes Telcomanager y muchas otras.

Las Probes son muy parecidas con objetos mapeados como interfaces y CPUs. La diferencia entre ellos es que el SLAview es capaz de configurar estos agentes en los dispositivos de red, ejecutando la configuración de scripts escritos por el usuario. Esto puede ser hecho por cualquier tipo de dispositivo que soporte protocolos SSH o TELNET para ejecutar esta configuración.

La figura de abajo muestra la relación entre el SLAview y las probes.

El sistema ejecuta los siguientes pasos para abrir una probe:

Procedimiento 5.5. Pasos de suministro de la probe del SLAview

1. SLAview configura una probe en un elemento de red utilizando un modelo de script o un nuevo script escrito por ti.
2. SLAview identifica la probe configurada utilizando un mapeador de probe que fue asociado al elemento de red configurado.
3. Los elementos de red ejecutan las mediciones de rendimiento de la probe en la red.
4. SLAview recolecta OIDs SNMP de acuerdo con los perfiles configurados para la probe.

Sugerencia

Si tu área es responsable por configurar las probes en la red, pero necesitas recolectar las mediciones utilizando el SLAview, puedes tratar la probe como un objeto más mapeado. Si es una probe Cisco, todo lo que tienes que hacer es asociar un mapeador al dispositivo donde las probes ya están configuradas y después asociarlas al perfil correcto para comprobar las probes que serán mapeadas.

Nuevas probes pueden ser creadas. Hay un asistente para la creación de probe que lo guiará y validará en cada paso de la creación.

Procedimiento 5.6. Configurando probes preexistentes

1. Selecciona **Datos históricos** → **Probes** → **Asistente** .
2. Rellena el formulario de acuerdo con las instrucciones de abajo para cada tipo de probe. Si decides ejecutar su script durante el asistente, la probe será creada en el sistema y preguntará si quieres asociarla perfiles.

Tabla 5.12. Telco ICMP/Jitter probe

Campo	Descripción
Nombre	Nombre de la probe.
Dispositivo	Selecciona el dispositivo donde la probe será configurada. Date cuenta de que el dispositivo debería haber sido añadido anteriormente al sistema.
Tipo de probe	Selecciona la probe Telco/ICMP Jitter .
Destination IP address	Ip de destino de la probe.
High latency discard (packets)	Cuántos de los paquetes mayores serán descartados de la estadística.
Low latency discard (packets)	Cuántos de los paquetes menores serán descartados de la estadística.
Number of packets	Número de paquetes de medición que serán enviados por la probe.
Packet interval (ms)	Intervalo entre la medición de los paquetes.
Packet size (bytes)	Tamaño del paquete.
Script de suministro	Selecciona el script Probe Telco ICMP Jitter .
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- Round-trip latency.
- Round-trip jitter.
- Round-trip packet loss.

Tabla 5.13. Telco HTTP probe

Campo	Descripción
Nombre	Nombre de la probe.
Dispositivo	Selecciona el dispositivo donde la probe será configurada. Date cuenta de que el dispositivo debería haber sido añadido anteriormente al sistema.

Campo	Descripción
Tipo de probe	Selecciona la probe Telco HTTP .
URL	Rellena la URL para ser probada.
Script de suministro	Selecciona el script Probe Telco HTTP .
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- HTTP round trip latency.
- Availability.

Tabla 5.14. Telco DNS probe

Campo	Descripción
Nombre	Nombre de la probe.
Dispositivo	Selecciona el dispositivo donde la probe será configurada. Date cuenta de que el dispositivo debería haber sido añadido anteriormente al sistema.
Tipo de probe	Selecciona la probe Telco DNS .
Destination IP	IP de destino de la probe.
URL	Rellena la URL para ser traducida.
Script de suministro	Selecciona el script Probe Telco DNS .
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- DNS round-trip latency answer.
- Availability.

Tabla 5.15. Telco SSH probe

Campo	Descripción
Nombre	Nombre de la probe.
Dispositivo	Selecciona el dispositivo donde la probe será configurada. Date cuenta de que el dispositivo debería haber sido añadido anteriormente al sistema.
Tipo de probe	Selecciona la probe Telco SSH .
Destination IP	IP de destino de la probe.
Port	Puerta TCP donde el servicio SSH se está ejecutando.
Script de suministro	Selecciona el script Probe Telco SSH .

Campo	Descripción
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- Round-trip SSH answer latency.
- Availability.

Tabla 5.16. Telco TCPConnect probe

Campo	Descripción
Nombre	Nombre de la Probe.
Dispositivo	Selecciona el dispositivo donde la probe será configurada. Date cuenta de que el dispositivo debería haber sido añadido anteriormente al sistema.
Tipo de probe	Selecciona la probe Telco TCPConnect .
Destination IP	IP de destino de la probe.
Port	Puerta TCP donde el servicio SSH se está ejecutando.
Script de suministro	Selecciona el script Probe Telco TCPConnect .
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- Round-trip answer latency for the TCP connection.
- Availability.

Tabla 5.17. Telco Twamp

Campo	Descripción
Nombre	Nombre de la Probe.
Dispositivo	Selecciona el dispositivo donde la probe será configurada. El dispositivo debe ser previamente añadido.
Tipo de probe	Selecciona la probe Telco Twamp .
Twamp light mode	Selecciona Sí para habilitar el modo TWAMP light.
Destination IP address	IP de destino de la probe.
Number of packets	Número de paquetes de medición que serán enviados por la probe.
Twamp interval (ms)	Intervalo de envío.
Twamp payload (bytes)	Payload, en bytes.

Campo	Descripción
Twamp port	Puerta del responder. El valor modelo es 862 .
Script de suministro	Selecciona el script Probe Telco Tm4_bold(Twamp) .
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- Round-trip time
- Send time
- Receive time
- Process time

Tabla 5.18. Cisco IP/SLA Jitter probe

Campo	Descripción
Nombre	Nombre de la probe.
Dispositivo	Selecciona el dispositivo donde la probe será configurada. Date cuenta de que el dispositivo debería haber sido añadido anteriormente al sistema.
Tipo de probe	Selecciona la probe IP/SLA Jitter .
Destination IP address	Dirección de IP de un dispositivo Cisco que soporta recursos de respuesta IP SLA.
Destination UDP port	Puerta UDP de destino para mediciones de paquetes.
Initial interval (s)	Intervalo inicial del dispositivo Cisco que esperará para iniciar después del boot de la probe. El uso de este parámetro es recomendado para evitar que las probes se ejecuten al mismo tiempo.
Interval between packets (ms)	Intervalo entre mediciones de paquetes.
Number of packets	Número de mediciones de paquetes que serán enviadas a cada momento que se ejecute la probe.
Origin IP address	Dirección de IP para ser usada como IP de origen para las mediciones de los paquetes.
Origin UDP port	Puerta UDP de origen para mediciones de paquetes.
Packet size (bytes)	Tamaño de cada medición de paquete.
ETIQUETA	Escoge una etiqueta.
Type of service (ToS)	Campo TOS para ser definido en las mediciones de los paquetes.

Campo	Descripción
VRF	Texto para identificar una VRF. Cuando este parámetro es usado, las mediciones de paquetes pasarán por la VRF especificada.
Script de suministro	Selecciona el script IP/SLA Jitter [ip sla monitor rtr] dependiendo de la sintaxis de la IP SLA del dispositivo.
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- One-way and round-trip latency.
- One-way and round-trip jitter.
- One-way and round-trip packet loss.
- Availability.

Sugerencia

Esta probe requiere que el dispositivo marcado sea un enrutador Cisco que soporte recursos de respuesta IP SLA. Para habilitar este recurso, solo escribe el comando **ip sla responder** o **rtr responder** en la línea de comando de la interfaz del dispositivo Cisco.

Tabla 5.19. Cisco IP/SLA ICMP Echo probe

Campo	Descripción
Nombre	Nombre de la probe.
Dispositivo	Selecciona un dispositivo donde la probe será configurada. Date cuenta de que el dispositivo debería haber sido añadido anteriormente al sistema.
Tipo de probe	Seleccione la probe SLA/ICMP Echo .
Destination IP address	Dirección de IP de un dispositivo Cisco que soporta recursos de respuesta IP SLA.
Origin IP address	Dirección de IP para ser usada como IP de origen para la medición de los paquetes.
Script de suministro	Selecciona el script IP/SLA ICMP Echo [ip sla monitor rtr]
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- Round-trip latency.
- Availability.

Tabla 5.20. Cisco IP/SLA Path Echo probe

Campo	Descripción
Nombre	Nombre de la probe.
Dispositivo	Selecciona el dispositivo donde la probe será configurada. Date cuenta de que el dispositivo debería haber sido añadido anteriormente al sistema.
Tipo de probe	Seleccione la probe SLA/Path Echo .
Destination IP address	Dirección de IP de un dispositivo Cisco que soporta recursos de respuesta IP SLA.
Origin IP address	Dirección de IP para ser usada como IP de origen para la medición de los paquetes.
Script de suministro	Selecciona el script Probe IP/SLA Path Echo [ip sla monitor rtr] dependiendo de la sintaxis del dispositivo IP SLA.
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- Round-trip latency.

Tabla 5.21. Cisco IP/SLA UDP Echo probe

Campo	Descripción
Nombre	Nombre de la probe.
Dispositivo	Selecciona el dispositivo donde la probe será configurada. Date cuenta de que el dispositivo debería haber sido añadido anteriormente al sistema.
Tipo de probe	Selecciona la probe SLA/UDP Echo .
Destination IP address	Dirección de IP del dispositivo objetivo.
Destination UDP port	Puerta UDP de destino para mediciones de paquetes.
Origin IP address	Dirección de IP para ser usada como origen para la medición de los paquetes.
Origin UDP port	Puerta UDP de origen para medición de paquetes.
Script de suministro	Selecciona el script Probe IP/SLA UDP Echo [ip sla monitor rtr] dependiendo de la sintaxis del dispositivo IP SLA.
Script de eliminación de probes	Escoge un script para eliminar la probe del dispositivo.

Métricas suministradas por esta probe:

- Round-trip latency.

- Availability.
3. Selecciona **Configuración** → **Perfiles** → **Objetos mapeados** y clicas en botón Asociar objetos mapeados para asociar la probe creada al perfil adecuado. Ej.: para Telco-DNS probes, usa el perfil Software/DNS y para IP/SLA UDP Jitter probe usa el perfil SLA/Jitter.

Tareas

La lista de tareas exhibe informaciones sobre los suministros de las probes.

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

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

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

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

Prerrequisitos

- El dispositivo donde las probes serán configuradas deben tener una CLI (command line interface) accesible por los protocolos SSH o Telnet.
- El agente de medida debe tener las variables de performance disponibles vía protocolo SNMP.
- La MIB del agente debe tener una OID cuyos valores son únicos e identifican cada instancia de probe. Por ejemplo, el nombre de la probe.
- La OID de encima debe configurarse a través de la interfaz de línea de comando del dispositivo, para que el mapeador creado sea capaz de unir la probe mapeada con el que fue suministrado.

Añadir metadatos de probes

Para acceder a la página de configuración de metadato, accede a **Datos históricos** → **Probes**, clicas en el ítem **Mapeador** en el menú del árbol y clicas en el botón **Metadato**.

Clicas 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, clicas en el botón **Borrar**.

Tabla 5.22. Campos de un metadato

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

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

Para asociar el metadato creado a una probe, accede a la lista de probes y clicas en el botón **Metadato** al lado de la probe que será configurada.

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

Informes

Modelos

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

Guardando

1. Abre el informe deseado y selecciona la opción Guardar modelo.
2. Rellena los campos de abajo:

Tabla 5.23. Forma del modelo

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

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

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

Programación

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

Opciones de programación

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

Sugerencia

Para programar un informe, debes guardarlo como modelo.

Sugerencia

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

Editando

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

Visualizando informes

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

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

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

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

Gestionando espacio de disco

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

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

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

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

Análisis de variable

El informe de análisis de variable proporciona estadísticas consolidadas para cualquier variable configurada en el sistema.

Sugerencia

Para saber como crear una variable, ve a la sección **Variables de resumen**.

Creando un nuevo informe

1. Accede a **Datos Históricos** → **Informes** → **Análisis de variable** .
2. Escoge **Nuevo informe de dispositivo** o **Nuevo informe de objeto mapeado** para tener un informe de perfil de dispositivo o un informe de perfil de objeto mapeado.
3. Selecciona los perfiles deseados y después clicas en las variables deseadas para cada función (Máx., Mín., Media, Suma, Desvío modelo, Porcentaje del límite y Porcentaje).
4. Rellena el formulario:

Tabla 5.24. Informe de Análisis de variable

Campo	Descripción
Generar informe Guardar modelo	Escoge Generar informe para solo una ejecución o Guardar modelo para guardar el informe como modelo.
Filtro de objeto	Filtra por objeto.
Filtro de ifAlias	Filtra por la OID SNMP ifAlias en caso de informes de objeto mapeado.
Exhibir ruta del grupo	Habilita esta opción para mostrar en el informe el grupo asociado.
Instante inicial	Instante inicial para selección de datos.
Instante final	Instante final para selección de datos.
Horario comercial	Si la opción "Día todo" está marcada, este campo es ignorado, en caso contrario, el dato es seleccionado dentro del intervalo estipulado para cada día.
Excluir fines de semana	Excluir periodo de fin de semana de los datos del informe.
Formato de salida	Opción disponible solo para informes que no son modelos. Una vez que el informe se torna un modelo, esta opción es ignorada.
Intervalo de exclusión	Añade una señalización y los valores de las variables que están configuradas dentro del intervalo serán ignorados del informe.

Campo	Descripción
Modelo de sustitución de variable	Añade rótulos a las variables.
Señalización	Puedes incluir una señalización para colorear una célula cuando el valor de una variable esté dentro de un determinado intervalo.
Grupos	Usa los botones disponibles para añadir o eliminar un grupo de la lista. Filtrará objetos situados debajo del grupo seleccionado en la jerarquía de grupo.
Agrupar resultados por grupos	Habilita esta opción para consolidar los resultados por grupo.
Usa fórmulas avanzadas	En lugar de utilizar funciones, puede crear fórmulas. Ejemplos: <ul style="list-style-type: none"> • <code>sum("Input traffic")/(8 * 1024 * 1024)</code> • <code>if((limit("Input traffic","max")== NaN), -1, 5)</code> • <code>if(max("Input traffic") > max("Output traffic"), max("Input traffic"),max("Output traffic"))</code>

Señalización

La opción señalización de informe es usada para colorear las células de los informes de Análisis de variable.

Cuando usas la señalización en un informe, el informe será coloreado de acuerdo con los límites de la configuración.

Ves a **Datos Históricos** → **Informes** → **Análisis de variable** → **Señalización** y clicas en el botón Nuevo para crear una nueva señalización.

Tabla 5.25. Señalización de Análisis de variable

Campo	Descripción
Nombre	Nombre de la señalización
Descripción	Campo de descripción.
Señalización de alarmas	Rellena los niveles de señalización. Ejemplo: <ul style="list-style-type: none"> • <code>40.00<=critical<=100.00 color red</code> • <code>20.00<=medium<40.00 color blue</code> • <code>5.00<=low<20.00 color gray</code>

Top N

Definiciones

El informe Top N suministra estadísticas consolidadas para cualquier métrica configurada en el sistema.

Un usuario será capaz solo de visualizar estadísticas para los objetos a los cuales tiene acceso.

Generando un nuevo informe

1. Accede a **Datos históricos** → **Informes** → **Top N**.
2. Escoge **Dispositivo u Objeto mapeados** para tener un informe de perfil de dispositivos o un informe de perfil de objeto mapeados.
3. Escoge el perfil deseado y después clicas en la métrica deseada para este perfil.
4. Rellena el formulario:

Tabla 5.26. Informe Top N

Campo	Descripción
Generar informe Guardar modelo	Escoge Generar informe para solo una ejecución o Guardar modelo para guardar el informe como modelo.
Objeto analizado	Automáticamente relleno con el tipo de perfil seleccionado.
Variable analizada	Automáticamente rellena con el nombre de la variable seleccionada.
Filtro de objeto	Filtra por objeto.
Fabricante	Filtra por el fabricante del objeto.
Tipo de fabricante	Filtra por el tipo de fabricante del objeto.
Filtro de ifAlias	Filtra por la OID ifAlias SNMP en caso de informes de interfaz.
Instante inicial	Instante inicial para selección de datos.
Instante final	Instante final para selección de datos.
Horario comercial	Exhibir porcentaje de ocupación de la banda, Exhibe el porcentaje de ocupación de la banda.
Formato de salida	Opción disponible solo para informes no-modelo. Una vez que el informe se torna un modelo, esta opción es ignorada.
Grupos	Usa los botones disponibles para añadir o eliminar un grupo de la lista. La lista filtrará objetos situados debajo del grupo seleccionado en la jerarquía de grupo.
Consolidando resultados por grupo	Habilita esta opción para consolidar los resultados por grupo.
Exhibir ruta del grupo	Habilita esta opción para mostrar en el informe el grupo asociado.

Syslog

Definiciones

Puedes configurar cualquier dispositivo para enviar mensajes Syslog al SLAview.

Los mensajes son recibidos por la puerta UDP 514.

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

Generando un nuevo informe

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

Tabla 5.27. Informe Syslog

Campos	Descripción
Inicio	Introduce el horario de inicio del periodo en el formato dd/mm/aaaa.
Fin	Introduce el horario final del periodo en el formato dd/mm/aaaa.
Mensaje	Filtra el mensaje syslog. Deja en blanco para tener todos los mensajes.
Prioridad	Selecciona el mensaje prioritario. Deja 0 para tener todas las prioridades.
Nivel	Selecciona el nivel de mensaje syslog. Escoge Todas para tener todos los mensajes.
Número de líneas	Escoge un límite de líneas para la salida del informe: 10000 o Ilimitado . En caso de que selecciones Ilimitado , el informe debe generarse en el formato CSV. Opción disponible solo para informes que no son modelo. Una vez que un informe se torna un modelo, esta opción es ignorada.
Formato de salida	Escoge el formato en que el informe se generará. Opción disponible solo para informes que no son modelo. Una vez que un informe se torna un modelo, esta opción es ignorada.
Filtros	Filtra los mensajes Syslog a partir de la Dirección IP de gestión , del Nombre o de un metadato del host. Usa expresiones regulares para filtrar los objetos. Al menos un campo de filtro debe rellenarse.

3. Clica en el botón Enviar.

Informe de Proyección

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

Configuración

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

Tabla 5.28. Formulario de configuración de proyección

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

Habilitado proyección para una curva gráfica

1. Accede a **Configuración** → **Perfiles** → **Objeto mapeado | Dispositivo** .
2. Clicka en el botón Gráfico para el perfil deseado.
3. Clicka en el botón Editando curvas para el gráfico deseado.
4. Clicka en el botón Editar para la curva deseado.
5. Clicka **Sí** en **Habilitar proyección** y escoge **Sí** en **Usar configuraciones modelo** o personaliza las configuraciones para esa curva.

Importante

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

Informes gráficos

1. Accede al gráfico que contiene la curva configurada por proyección, haga clic en la opción **Curvas de proyección**.
2. Seleccione la opción de **línea de tiempo**, para ver los valores de proyección en relación con la hora, o **Fecha y hora**, para mostrar el valor de proyección en relación a una fecha determinada.
3. La proyección se puede calcular en base al **media**, **máximo** o **percentil 95** del tráfico.

Generando un nuevo informe

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

Tabla 5.29. Formulario del informe de proyección

Campo	Descripción
Tipo de objeto	Selecciona un tipo de objeto.

Campo	Descripción
Perfil	Selecciona el perfil de objeto.
Curva	Selecciona la curva del gráfico.
Formato de salida	Opción disponible solo para no-modelo de informe. Una vez que el informe se torna un modelo, esta opción es ignorada.
Violación de límite Estimativa	<p data-bbox="906 464 1114 489">Violación de límite</p> <p data-bbox="1232 464 1427 1633">Si escoges esta opción, tendrás que seleccionar uno de los siguientes modos: Tasa o Límite del objeto. Seleccionando el modo Tasa, deberás introducir un valor entero y su unidad es bits por segundo (bps). El resultado será la fecha en que la tasa media excede el valor relleno. Seleccionando el modo Límite del objeto, deberás introducir un valor entero entre 0 y 100 y su unidad es %. El resultado será la fecha en que la tasa media excede el valor porcentual del límite que relleno. Por ejemplo, puedes descubrir cuando el límite de la interfaz va a explotar.</p> <p data-bbox="906 1665 1027 1690">Estimación</p> <p data-bbox="1232 1665 1427 1881">Si escoges esta opción, introducirás una fecha y un horario. El resultado será el valor de la curva</p>

Campo	Descripción
	en el momento relleno.
Filtro por dispositivo	Selecciona los dispositivos que serán analizados. En caso de que no selecciones ninguno, todos serán considerados.
Filtro por grupo	Selecciona los grupos que serán analizados. En caso de que no selecciones ninguno, todos serán considerados.
Entrada de datos	Es posible realizar una operación (Añadir o Sustraer) sobre los valores de la curva para calcular la proyección. Además puedes escoger el tipo de entrada (modo Absoluto o Relativo [%]). Basta seleccionar las opciones deseadas e introducir el valor, en bits/s.

- Después de rellenar el formulario, clic en **Enviar** para generar el informe.

Mapeo de IPs

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

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

Tabla 5.30. 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 con o horário final desejado.

Graph set

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

Definiciones

Creación

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

Tabla 5.31. Creación de graph set

Campo	Descripción
Nombre	Nombre del graphset.
Descripción	Descripción sobre el graphset.
Responsable	Nombre del usuario responsable del Graph Set.
Perfil de usuario	Perfil de usuario que tendrá acceso al Graph Set.
Tiempo entre diapositivas	Tiempo en segundos para cambiar las diapositivas utilizadas en la visualización NOC.
Exhibir en el NOC	Selecciona Sí para que el gráfico esté disponible en el NOC display.
Dimensiones	Dimensiones de la imagen.

Añadiendo gráficos

1. Accede a cualquier gráfico.
2. Clicka en el gráfico con el botón derecho del ratón.
3. Accede a la opción **Asociar al Graph Set** en el popup menú y selecciona el graph set deseado.
4. Las curvas no habilitadas durante la adición de gráficos no se representarán en el Graph Set.

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

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

Sugerencia

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

Visualizando un graph set


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

Editando un graph set

1. Clicka en **Datos históricos** → **Graph set**.
2. Escoge uno de los siguientes botones:
 - **Dependencias** para borrar el gráfico de un graph set.

- **Editar** para cambiar los campos de nombre y descripción del graphset.
- **Borrar** para borrar el graph set.

Generando gráficos para un graph set

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

Circuito

Un circuito es una conexión entre dos interfaces de dos dispositivos.

Procedimiento 5.7. Pasos de la configuración de los circuitos.

1. Seleccione **Datos históricos** → **Circuito** → **Circuito** .
2. Clica en el botón **Nuevo** y rellena el formulario de abajo.

Tabla 5.32. Formulario de nuevo circuito

Campo	Descripción
Nombre	Nombre del circuito.
Dispositivo A	Nombre del dispositivo A.
Mapeador A	Nombre del mapeador A.
Interfaz A	Nombre de interfaz A.
Dispositivo B	Nombre del dispositivo B.
Mapeador B	Nombre del mapeador B.
Interfaz B	Nombre de interfaz B.
Nombre de Metadatos	Este campo sólo está disponible si ya existe algún metadatos.

Al seleccionar un circuito, se mostrará el gráfico de cada interfaz.

Los circuitos también pueden ser descubiertos automáticamente por el sistema a través de los protocolos CDP y LLD.

Todo circuito se representa en los mapas en los que sus puntas forman parte.

Histórico de ruta

Definiciones

El Histórico de ruta permite la configuración de pruebas automáticas de traceroute. El usuario debe configurar el nombre de la prueba, una dirección IP o hostname y el intervalo de la prueba en minutos (en lo mínimo 5 minutos).

Creación

Accede a la ruta **Datos históricos** → **Histórico de ruta** → **Nueva prueba de ruta** .

Tabla 5.33. Creación de prueba de ruta

Campo	Descripción
Nombre	Nombre de la prueba.
Host	Dirección IP o hostname.
Intervalo	Intervalo de ejecución de las pruebas, en minutos.

Visualizando una prueba de ruta

1. Accede a la ruta **Datos históricos** → **Histórico de ruta**
2. Clica en el botón **Detalles** para exhibir todas las ejecuciones de una prueba.
3. Clica en el botón **Exhibir** para abrir las informaciones sobre la ejecución de la prueba.

También es posible visualizar las informaciones de las pruebas en la forma de gráficos. Para ello, clica en el botón **Visualizar gráficos**. Cada gráfico posee la información de un salto, informando las latencias medias verificada para el salto en cada ejecución de la prueba.

Capítulo 6. Configuración

Perfiles

Definiciones

Los perfiles de SLAview fueron proyectados para permitir que el usuario especifique que informaciones deben ser recolectadas y como la información debe ser procesada por el sistema. A continuación, los perfiles pueden ser usados por un grupo de dispositivos o de objetos mapeados.

Los perfiles permiten que especifiques variables de recolecta, fórmulas basadas en variables de recolecta (variables de resumen) y gráficos, que contienen curvas que están basadas en fórmulas de variables de resumen.

Después de que los perfiles estén configurados, pueden ser asociados a dispositivos o a objetos mapeados presentes en el sistema. Esta asociación puede ser manual o automática.

Recuerda que el SLAview ya tiene perfiles preconfigurados para los escenarios más comunes de seguimiento.

Tipos de perfil

El SLAview soporta 2 tipos de perfiles, que son perfiles de dispositivo y perfiles de objeto mapeado. La principal diferencia entre estos dos tipos está en el modo con que el recolector SNMP procesará las variables de recolecta configuradas para cada tipo.

Tipos

Perfiles de dispositivo	El sistema recolectará exactamente la OID especificada. Ejemplo: si quieres recolectar la OID sysUpTime de un dispositivo
Perfiles de objetos mapeados	El SLAview mapea la instancia del objeto que debe ser recolectado

Gestionando perfiles

Perfiles

- **Creando un perfil**

Clica en el botón Nuevo en la pantalla de configuración de perfil y especifica los parámetros siguientes:

Tabla 6.1. Formulario de perfil

Campo	Descripción
Nombre	Nombre del perfil.
Asociación automática	Selecciona Sí si los objetos deben ser automáticamente asociados al perfil. En este caso, las reglas apropiadas deben ser seleccionadas.

Campo	Descripción
Eliminación automática	Seleccione Sí si los objetos deben eliminarse automáticamente del perfil. Un objeto se eliminará automáticamente si las reglas del perfil ya no se cumplen.
VARIABLES DE RECOLECTA	Introduce las variables de recolecta que estarán en este perfil. Puedes configurarlas manualmente (SNMP), usar un script para ello (Telco Script), usar estadísticas predefinidas (ICMP) o usar un agente instalado en Windows (THA).
VARIABLES DE RESUMEN	Una variable de resumen es definida solo una vez y puede ser usada una vez en cada perfil de ese tipo. Este comportamiento permite la definición de diferentes fórmulas para la misma variable de resumen. Por ejemplo, la variable Utilización de CPU puede ser definida en un perfil denominado Cisco con una fórmula diferente de la de un perfil denominado Extreme .
Gráficos	La configuración de gráficos es extremadamente flexible. Un gráfico puede tener varias curvas y cada una de ellas basarse en fórmulas que pueden utilizar las variables de resumen.

Importante

Las variables de recolecta del perfil pueden ser cambiadas en cualquier momento, pero la eliminación de una OID también causará una eliminación en cascada de las variables de resumen y de las curvas relacionadas a esa variable de recolecta para el perfil y pérdida de datos históricos de las variables eliminadas.

Importante

En el caso de que algún perfil esté en rojo en la lista de perfiles significa que no hay respuesta SNMP.

Gestionando variables de recolecta

Para acceder a las variables de recolecta ya existentes, clic en el botón Recolecta en la pantalla de configuración de perfil.

Puedes crear una nueva recolecta clicando en el botón Nuevo.

Sugerencia

Recuerda que también es posible crear variables de recolecta a través del formulario del perfil.

Las variables pueden ser editadas a través del botón Editar y eliminadas por el botón Borrar:

1. Recolectar SNMP

- a. Selecciona la opción **SNMP**;
- b. Configura los campos **Nombre** y **OIDS**. Puedes rellenar estos campos manualmente o usar la herramienta MIB Browser (para ello, sigue los siguientes pasos).

- i. Clica en el botón Encontrar OID para llamar la herramienta MIB Browser.
 - ii. Escoge la MIB deseada y clica en el botón Seleccionar.
 - iii. Selecciona la OID deseada en el árbol de navegación de MIB.
 - iv. Clica en la OID y, en caso de que quieras probarla en un dispositivo preconfigurado, selecciona el dispositivo en la lista en el campo MIB Tester y clica en el botón SNMP WALK.
 - v. Clica en el botón Introducir para copiar los datos de la OID seleccionada para el formulario del perfil.
- c. Finalmente, clica en el botón Añadir en la ventana principal para confirmar la operación y la variable de recolecta SNMP será añadida al perfil.
2. **Recolecta Telco Script**
- a. Selecciona la opción **Telco Script**;
 - b. Rellena el campo **Nombre**;
 - c. Escoge el script de la recolecta que será usado. Para crear uno, ves a **Configuración** → **Scripts**.
 - d. Finalmente, clica en el botón Añadir para confirmar la operación.

3. **Recolecta ICMP**

- a. Selecciona la opción ICMP;
- b. Rellena el campo **Nombre**;
- c. Selecciona una de las opciones: **Jitter**, **Latencia** o **Pérdida de paquetes**;
- d. Finalmente, clica en el botón Añadir para confirmar la operación.

Sugerencia

Puedes configurar los parámetros de esta recolecta en **Sistema** → **Parámetros** → **ICMP** .

4. **Recolecta THA**

- a. Selecciona la opción THA;
- b. Rellena el campo **Nombre**;
- c. Selecciona una de las opciones: **Estatus del servicio**, **Performance counter** o **SQL counter**;
- d. Rellena el nombre de counter, cuando sea **Performance counter** o **SQL counter**;
- e. Rellena el nombre del servicio;
- f. Finalmente, clica en el botón Añadir para confirmar la operación.

Importante

Este tipo de recolecta solo funcionará en dispositivos con el agente Windows de Telcomanager instalado.

5. OID wildcards

Esta funcionalidad permite que sea realizada una operación sobre todos los valores retornados en la recolecta SNMP y se imprima el resultado de la operación como resultado de la recolecta.

Siguen, a continuación, las wildcards soportadas actualmente. Todas ellas, con excepción de **%INDEX%**, **%INDEX_POP_N%** y **%METADATA_<NAME>%**, deben ser añadidas al final de la OID.

Wildcards

%INDEX_WALK_MAX%	Esta wildcard buscará el valor máximo retornado en la operación SNMP_WALK ejecutada por el recolector SNMP.
%INDEX_WALK_MIN%	Esta wildcard buscará el valor mínimo retornado en la operación SNMP_WALK ejecutada por el recolector SNMP.
%INDEX_WALK_SUM%	Esta wildcard suministrará la suma de los valores retornados en la operación SNMP_WALK ejecutada por el recolector SNMP.
%INDEX_WALK_AVG%	Esta wildcard suministrará la media de los valores retornados en la operación SNMP_WALK ejecutada por el recolector SNMP.
%INDEX_WALK_COUNT%	Esta wildcard suministrará la cantidad de valores retornados en la operación SNMP_WALK ejecutada por el recolector SNMP.
%INDEX_WALK_LAST%	Esta wildcard buscará el valor del penúltimo índice retornado. Esto es muy útil para MIBs que retornan un histórico de los últimos N valores recolectados.
%INDEX%	Esta wildcard puede ser usada en cualquier posición en la OID. Esto hace que el recolector SNMP substituya el index de la OID en aquella posición en vez de anexar el índice en el final de la OID.
%INDEX_POP_N%	Esta wildcard puede ser usada en cualquier posición en la OID. El recolector SNMP toma el valor del OID definido en el campo sustitución la máscara con el índice del objeto mapeado, eliminando los N últimos decimales del índice. Si N es cero o mayor que el número de índice, el valor del índice se definirá a cero. EJ.: Para el OID 1.3.6.1.%INDEX_POP_2%.2.1.1.3 y un objeto con índice 1.2.3, la recolect se realizará en 1.3.6.1.1.2.1.1.3.
%METADATA_<NAME>%	Esta wildcard puede ser usada en cualquier posición en la OID. El colector SNMP toma el valor del metadato NAME y reemplaza en el wildcard.

Variables de resumen

Para acceder a las variables de resumen ya existentes, clicas en el botón Variables de resumen en la pantalla de configuración de perfil.

Puedes crear una nueva variable de resumen clicando en el botón Nuevo.

Sugerencia

Recuerda que también es posible crear variables de resumen a través del formulario del perfil.

Las variables pueden ser editadas a través del botón Editar y eliminadas por el botón Borrar:

1. Creando variables de resumen

Tabla 6.2. Variable de resumen

Campo	Descripción
Nombre	Define el nombre de la variable.
Unidad	Escoge una unidad. Ejemplo: pps, bps, volts.
Porcentaje	Campo utilizado para formatear informes. Selecciona esta opción para variables que retornan valores en porcentaje.
Por segundo	Campo utilizado para formatear informes. Selecciona esta opción para variables que retornan valores de tasa, como tráfico, por ejemplo.

Importante

¡No olvides clicar en el botón **Añadir!**

2. Fórmula de variables de resumen

En este paso, puedes ser capaz de definir fórmulas en notación infija utilizando las variables de recolecta configuradas en el perfil.

Selecciona las variables de recolecta y construye la fórmula con las funciones deseadas, siguiendo la notación infija. A continuación, clicla en el botón Añadir.

- **Definiciones**

La variable [delta_ts] se refiere al periodo entre cada SNMP polling, que se fija en 300 segundos. Esto quiere decir que representa el intervalo de tiempo.

La función [delta] se aplica a la OID que realiza la diferencia entre el valor recolectado en el momento actual y el valor recolectado anteriormente.

Estos campos [delta_ts] y [delta] se utilizan cuando la variable debe ser expresada con una tasa, como por ejemplo, la entrada de tráfico en una interfaz de red, para la que tenemos la siguiente fórmula:

```
((delta("ifHCInOctets") * 8) / $delta_ts$)
```

La función [prev] recupera el valor recolectado anteriormente para la OID. La siguiente fórmula demuestra la utilización de esta función:

```
(prev("ifHCInOctets") * 8)
```

En otro ejemplo, la disponibilidad de interfaz se expresa como un valor porcentual:

```
if(("ifOperStatus" == 1),100,0)
```

En la fórmula de encima, si la variable ifOperStatus es igual a 1, la fórmula retornará 100, en caso contrario retornará 0.

Después de terminar de editar la fórmula, clicas en el botón Guardar.

Gráficos

1. Creación de gráficos

Tabla 6.3. Gráfico

Campo	Descripción
Nombre	Descripción que aparecerá en el área del gráfico seleccionado.
Título	Descripción que aparecerá encima del gráfico.
Unidad	Descripción para el eje y del gráfico.

Importante

¡No olvides clicar en el botón **Añadir!**

2. Creando curvas para los gráficos

Al paso que vas añadiendo un gráfico al perfil, aparecerá en el formulario una sección para la creación de curvas para el gráfico.

Puedes añadir los gráficos que quieras y podrás configurar las curvas relativas a cada uno de ellos.

• **Tabla 6.4. Curva del gráfico**

Campo	Descripción
Rótulo	Nombre de la curva.
Tipo de línea	Los tipos de línea 1, 2 y 3 poseen diferentes niveles de espesura. Área rellenará el área abajo de la curva y Stack empilará las curvas.
Color	Escoge un color de la curva
Trazar la curva máxima	La curva máxima es trazada en gráficos semanales, mensuales y anuales. Para siempre trazar la curva máxima, el sistema considera la resolución mínima de datos disponibles, que son siempre datos de 5 minutos.
Habilitar proyección	Parámetros modelos de proyección. Accede a sección proyección para consejos sobre como configurar estos parámetros.
Fórmula	Formula una notación infija regular basada en el resumen de variables.

Importante

¡No te olvides de clicar en el botón **Añadir** y, a continuación, en **Guardar!**

Asociación de objetos

- **Asociando objetos a los perfiles**

SLAview soporta dos métodos de asociación de perfil, que son asociados manual y automático. Para el último caso, es necesario crear reglas de asociación.

Asociación de perfiles manuales

1. Clica en el botón **Asociaciones** (Objetos mapeados|Dispositivo) en la pantalla de configuración de perfil y luego en el botón **Asociar Objeto mapeado**. Rellena el formulario;

Tabla 6.5. Formulario de asociación de perfil

Campo	Descripción
Perfil	Selecciona el perfil que deseas asociar a los objetos.
Filtro	Puedes suministrar una string para filtrar los objetos. Tienes que usar expresiones regulares para filtrar.
Filtro de camino de grupo	Puedes suministrar un camino de grupo para filtrar objetos que estén asociados al grupo.
Tipo	Selecciona un tipo de objeto mapeado. Si es un perfil de dispositivo, este campo no estará presente.

2. Clica en el botón Enviar.
3. Los objetos disponibles aparecerán, a continuación, después mueve los objetos deseados a la caja de la derecha.

Haz uso del filtro de OID si quieres filtrar una condición SNMP. Por ejemplo, usa la expresión 1.3.6.1.2.1.2.2.1.7 = 1 y selecciona la opción **Usar index de objetos mapeados** para filtrar interfaces con el ifAdminStatus up.

4. Clica en el botón Enviar.
5. SLAview mostrará los resultados de la prueba para los objetos filtrados contra todos los OIDs del perfil. Si clicas en Guardar ahora, solo los objetos que respondan a todas las OIDs del perfil serán asociados.. Puedes seleccionar la opción **Forzar asociación** para los objetos que obtuvieron un error al responder al perfil, después estos también se asociarán.

Importante

Debes usar **Forzar asociación** con cautela, porque el SLAview intentará coleccionar las OIDs en objetos que no responden a ellas, lo que puede llevar a errores de recolecta.

Sugerencia

Usa **Forzar asociación** solo cuando sepas que el objeto comenzará a responder a las OIDs en un corto periodo de tiempo. En caso contrario, crea otro perfil sin las OIDs que no responden y usa este perfil en los objetos.

Asociación automática de perfiles

Este proceso permite a los operadores integrar fácilmente los elementos de red al SLAview, sin tener que preocuparse con configurar todas las asociaciones del perfil.

El proceso de asociación automática se ejecuta todos los días en dos momentos preconfigurados, que pueden ser ajustados en **Sistema** → **Parámetros** → **Agentes de asociación**

Procedimiento 6.1. Creando reglas

- Creando nuevas reglas para usar en los perfiles.

Procedimiento 6.2. Usando reglas en los perfiles

1. Clicka en el botón Editar para el perfil en la pantalla de configuración de perfil.
2. Selecciona **Sí** en la caja de selección **Asociación automática**.
3. Mueve las reglas de la caja de la izquierda a la caja de la derecha.
4. Clicka en el botón **Guardar**.

Importante

Todas las reglas son conectadas por un operador AND. Después, para que un objeto sea asociado a un perfil, debe obedecer a todas las reglas del perfil.

Procedimiento 6.3. Probando las reglas

1. Clicka en el botón Ejecutar en la pantalla de configuración de perfil para el perfil deseado.
2. Rellena el formulario de acuerdo con los dispositivos que deseas probar.
3. Clicka en Enviar para iniciar la asociación del agente on-demand.
4. Comprueba el archivo de agente log en **Sistema** → **Diagnósticos** → **Archivos de Log** → **profiled.log**, para ver si el agente está cerrado.
5. Clicka en el botón Dependencias para el perfil para comprobar si la Regla y las pruebas de SNMP polling están ok para los perfiles de objeto.
6. Si tienes errores en la columna SNMP, clicka en el botón Diagnóstico para comprobar que OIDs poseen errores.

Importante

Si el objeto no corresponde a las reglas de perfil, no aparecerá en este punto porque no fue asociado al perfil.

Comportamiento del sistema relacionado a los perfiles Automáticos

- La falta de respuesta SNMP para cualquier OID del perfil en un objeto en la primera prueba evitará el SNMP polling en aquel objeto hasta responder por esa OID en la próxima prueba. Los gráficos para aquel objeto indicarán el fallo.
- Si un objeto para de responder por una OID durante la operación normal del sistema, las OIDs que respondieron continuarán siendo recolectadas y el fallo será indicado en el gráfico del objeto.

- Si durante la operación normal del sistema un objeto falla por una regla, el SNMP polling para ese objeto será interrumpido.

Exportando Perfiles

La herramienta de exportación permite al usuario exportar todas las configuraciones del perfil del SLAview para un archivo y después importar de vuelta a las configuraciones. Este recurso es muy útil para importar perfiles predefinidos del equipo de consultores de Telcomanager.

1. Clicka **Configuración** → **Perfiles** → **Mostrar** .
2. Clicka en Exportar.

Sugerencia

Puedes exportar todos tus perfiles a un único archivo usando el botón **Exportar todos**

QoS

Definiciones

El modo de seguimiento de QoS fue específicamente desarrollado para trabajar con dispositivos que soportan la MIB CLASS-BASED-QoS del sistema Cisco, por tanto, solo funcionará para dispositivos que soportan esta MIB.

QoS puede ser controlado en otros sistemas, pero tendrán que ser mapeados a través del mapeador genérico del SLAview.

Utilizando un agente de mapeo específico, el SLAview es capaz de identificar todas las políticas de QoS aplicadas en esa interfaz, crear los perfiles apropiados para controlar estas políticas y ejecutar las asociaciones de perfil.

Habilitando el recurso de QoS

- Accede **Sistema** → **Parámetros** y habilita el QoS Cisco Profile, después el SLAview estará habilitado para crear los perfiles de QoS automáticamente.

Habilitando seguimiento de QoS en las interfaces

1. Accede **Configuración** → **QoS** y cree un nuevo grupo de **QoS** clicando en el botón Nuevo.
2. Selecciona las interfaces/reglas deseadas y los seguimientos y clicka en el botón Guardar.

Tabla 6.6. Formulario de Asistente de QoS

Campo	Descripción
Nombre	Nombre para identificar un Asistente de QoS.
Asociación automática	Selecciona Sí si los interfaces deben ser automáticamente asociados al perfil. En este caso, las reglas apropiadas deben ser seleccionadas. De lo contrario, seleccione las interfaces que se control.
Control	Seleccione QoS Monitoring.

Una vez creado el perfil, haga clic en el botón **Asociaciones** para ver las interfaces asociadas.

El proceso de asociación automática se ejecuta todos los días en dos momentos preconfigurados, que pueden ser ajustados en **Sistema** → **Parámetros** → **Agentes de asociación** → **Agente de asociación automática para perfiles de QoS**

La próxima vez que el proceso Cisco Policy Mapper y el proceso Cisco Auto QoS Profile se ejecuten, buscarán las políticas de QoS en la interfaz e intentarán crear los respectivos seguimientos.

Recolectoras

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

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

Tabla 6.7. Formulario de recolectoras

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

Importando archivos de recolectoras

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

Clica en el botón de importar y carga el archivo.

Un archivo de dispositivo importado posee los siguientes campos:

Tabla 6.8. Campos de archivos de recolectoras

Campo	Descripción
Nombre	Posible caracteres para el campo nombre.

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

Exportar datos

Haga clic en el botón **Exportar datos** para exportar la lista de objetos en formato CSV.

Añadir metadatos de recolectora

Para acceder a la página de configuración de metadato, accede a **Configuración** → **Recolectoras** y clic 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, clic en el botón **Borrar**.

Tabla 6.9. Campos de un metadato

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

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

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

Objetos

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

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

Importando archivos de objetos

1. Accede **Configuración** → **Objetos** y clic en el botón **Importar** para el tipo de objeto deseado.
2. Haz la descarga de un archivo formateado de acuerdo con las instrucciones en la pantalla.

3. Clica en el botón Añadir.
4. Ajusta las configuraciones y clica en el botón Guardar.

Mapeadores

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

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

Procedimiento 6.4. Creando un mapeador

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

Tabla 6.10. Formulario de Mapeador

Campo	Descripción
Nombre	Nombre del mapeador
Icono	Imagen que se mostrará próxima a los objetos descubiertos por este mapeador en el árbol del menú. Ve el paso 3 para instrucciones de personalización de esta imagen.
Tipo	Escoge SNMP , Telco script , Proceso o Servicio del Windows .
Script	Selecciona el script. Crea uno en la sección Scripts.
Eliminado automático	Si quieres que los objetos mapeados por este mapeador sean eliminados después de un cierto número de días consecutivos en que estén perdidos, selecciona Sí y rellena el número de días.
Incluir prefijo	Incluye el nombre del mapeador como prefijo para los objetos descubiertos por este mapeador.
Instancia de la OID utilizada como nombre de objeto	Marca esta opción si, en vez de rellenar el nombre del objeto con el valor de la OID, el mapeador debe rellenarlo con el valor de la instancia OID. Esta opción debe ser utilizada por objetos que no tengan un OID cuyo valor puede representarlos. Después puedes utilizar una OID estadística y un mapa de instancia de objetos con esta opción.
Interfaz de red	Marca esta opción si los objetos que serán descubiertos fueron interfaces de red. Esto hará que el mapeador busque propiedades de interfaz como ifAlias y ifSpeed.
Probe	Marca esta opción si el mapeador está hecho para descubrir probes, después las probes también

Campo	Descripción
	serán exhibidas en el menú Datos históricos → Probes .
Nombre	Nombre de la OID para ser usada para el mapeo de objetos.
OID	OID que será utilizada.
MIB	OID MIB.
Filtro por recolecta SNMP	Filtra por la respuesta de la recolectora SNMP.
Asociación de dispositivos	Habilita asociación de dispositivos automáticos al mapeador considerando las Reglas. Cuando está habilitado, el formulario mostrará la opción de eliminación automática que eliminará los dispositivos asociados cuando las condiciones no sean más conocidas.
Dispositivos	Selecciona los dispositivos que serán asociados al mapeador. En caso de que el tipo de mapeador sea Proceso , tras transportar el dispositivo para el lado derecho del filtro, clicas en él y, a continuación, en Listar procesos . Hecho esto, selecciona los procesos deseados.

Sugerencia

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

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

3. Configurando los iconos de mapeador.
 - a. Selecciona en el menú **Configuración** → **Mapeadores** y clicas en el botón Cambiar iconos.
 - b. Clicas en el botón Nuevo icono.
 - c. Rellena el nombre del mapeador y sube un icono para cada condición de objeto.
 - d. Clicas en el botón Enviar.

Mapeo cruzado de OIDs

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

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

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

1.3.6.1.4.1.9.9.109.1.1.1.1.2;1.3.6.1.2.1.47.1.1.1.1.7

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

Asociando dispositivos a los mapeadores

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

Exportando e importando mapeadores

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

Mantenimiento

Puedes crear un mantenimiento para suprimir las alarmas ICMP durante el mantenimiento de Windows en su infraestructura.

ICMP polling

El intervalo del ICMP polling del SLAview es flexible y puede ser configurado a través de los modelos de ICMP polling.

Procedimiento 6.5. Activando dispositivo de polling

1. Asocia el dispositivo a un perfil de alarma que posea la alarma **Sin respuesta ICMP**. (Ve en **Datos históricos** → **Alarmas**).
2. Ves a **Configuración** → **ICMP Polling** y crea un nuevo modelo de pooling donde irás a:
 - Definir los días y horas de la semana para el polling.
 - Definir el intervalo de polling.
 - Asociar los dispositivos que usarán este modelo.

Añadir metadatos de ICMP Polling

Para acceder a la página de configuración de metadato, accede a **Configuración** → **Rm4_bold(ICMP Polling)** y clicla 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, clicla en el botón **Borrar**.

Tabla 6.11. Campos de un metadato

Campo	Descripción
Nombre	Nombre del metadato.

Campo	Descripción
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 ICMP Polling, accede a la lista de modelos de ICMP Polling y clicas 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.

EPM (Extended Processing Module)

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

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

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

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

Tipos de probe

El objeto **Tipo de probe** está destinado a definir los campos que serán suministrados en el dispositivo remoto y también está disponible en el formulario de configuración de probe.

Procedimiento 6.6. Configurando nuevos tipos de probe

1. Selecciona **Configuración** → **Tipos de probe** → . Clicas en el botón Nuevo para definir un nuevo tipo.
2. Rellena el formulario de acuerdo con las siguientes instrucciones:

Tabla 6.12. Formulario de tipo de probe

Campo	Descripción
Nombre	Nombre del tipo de probe Ej.: Cisco/IP SLA jitter
Descripción	Texto descriptivo.

Campo	Descripción
Atributos	<p>Clica en el botón añadir para cada atributo necesario para configurar esta probe. Ej.: IP de destino, número de paquetes</p> <p>Nombre Texto identificando el atributo. Ej.: Ip de destino</p> <p>Código para suministro Texto para usarse en los scripts de suministro. Ex: ip_dst</p>

3. Crear un mapeador para mapear los objetos de probe

- Selecciona **Configuración** → **Mapeadores** y configura el mapeador con la OID que es única y rellena el campo de **Probe**. Ej.: Para Telco Probes la OID usada es tmTAPName, que representa el nombre de la probe.

4. Asociar un nuevo mapeador al dispositivo

- Cuando estás creando un nuevo mapeador en **Configuración** → **Mapeadores**, configure **Asociación de dispositivos** de acuerdo con tus necesidades. Puedes habilitar la Asociación Automática o la Eliminación Automática o seleccionar dispositivos específicos.
- Para comprobar la asociación, clica en Dependencias en el menú **Configuración** → **Mapeadores**.
- Ahora, cuando una nueva probe es suministrada en el dispositivo asociado, el sistema irá a descubrirla.

5. Crear un script de suministro

- Selecciona **Configuración** → **Script**. Clica en el botón Nuevo y crea un script para el nuevo tipo de probe usando los atributos de la sintaxis de script de suministro.

6. Crear un nuevo perfil

- Selecciona **Datos históricos** → **Probes** y crea una nueva probe utilizando el tipo de probe creado.
- Asocia el perfil a la probe en **Datos históricos** → **Perfiles**, botón Asociar objetos mapeados.

Añadir metadatos de tipos de probe

Para acceder a la página de configuración de metadato, accede a **Configuración** → **Tipos de Probe** 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 6.13. Campos de un metadato

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

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

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

Reglas

Creación de reglas

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

Tabla 6.14. 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 OIDs 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.

Campo	Descripción
	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.

Trap Receiver

SLAview es capaz de recibir, analizar y generar alarmas basadas en SNMPv1 y V2 traps.

Este módulo está compuesto por, lógica del trap receiver, alarma de trap e informes de trap recibidos.

Una trap es identificada por su OID. Cuando una trap es recibida y se tiene una trap receiver creada utilizando la misma OID, la lógica del trap receiver será evaluada para decidir si es necesario generar una incidencia de alarma. Esta incidencia será generada solo si hay alguna alarma utilizando la lógica del trap receiver.

Configuraciones del Trap Receiver

Selecciona **Configuración** → **Trap receiver**. Clica en Nuevo para crear un nuevo trap receiver.

Tabla 6.15. Configuración Trap Receiver

Columna	Descripción
Nombre	Nombre del trap receiver.
Descripción	Descripción sobre el trap receiver.
OID	OID para identificar la trap. Puedes clicar en Busca OID para navegar a través del MIB browser.
MIB	MIB que contiene la OID.
Identificar dispositivo por el origen	Escoge si el dispositivo generado por la trap será identificado por el origen (dirección de IP) o no. Si no, debes escoger una OID asociada al campo del dispositivo.
Identificación del dispositivo - OID	OID para identificar el dispositivo.
Identificación del dispositivo - Campo	Campos para identificación del dispositivo.

Clica en Guardar para crear el trap receiver.

Importante

La trap puede llevar cerca de 5 minutos para ser reconocida. Esto sucede porque este es el tiempo que el sistema necesita para actualizar las configuraciones.

Lógica del Trap Receiver

El trap receiver posee muchas lógicas asociadas a él. Cada lógica necesita ser asociada a una alarma (ve la sección Alarmas), para armarlo y desarmarlo.

Selecciona **Configuración** → **Trap receiver**.

Clica en lógica para listar las lógicas de un trap receiver de la lista.

Clica en Nuevo para crear una nueva lógica.

Tabla 6.16. Lógica Trap Receiver

Columna	Descripción
Nombre	Nombre de la lógica.
Descripción	Descripción sobre la lógica.
Fórmula	Ve la fórmula de la alarma.
Tipo de objeto	Escoge dispositivo u objetos mapeados. Si es seleccionado el Objeto mapeado , tienes que seleccionar un mapeador, una OID y un campo para identificar el objeto.
Mapeador	Mapeador para identificar el objeto mapeado.
OID	OID para identificar el objeto mapeado.
Campo	Campo para identificar el objeto.

Alarma de Trap

Ve la sección alarmas Alarmas.

Informe del Trap Receiver

Este informe lista informaciones sobre todas las traps recibidas por el sistema, usando filtros para generar el contenido.

Tabla 6.17. Informe del Trap Receiver

Columna	Descripción
Inicio	Trap recibida en el inicio.
Fin	Trap recibida en el final.
Origen	Origen de las traps. Por IP o hostname.
Varbind	Variable del Trap.
Formato de salida	HTML o CSV.
Número de líneas	Número de líneas en el informe.

Lógica de la fórmula del Trap Receiver

Las expresiones en el campo **Fórmula** son escritas en notación infija regular.

Debes construir las fórmulas utilizando las siguientes reglas:

- Usa paréntesis "(")" para precedencia de la operaciones.
- Usa los operadores lógicos AND y OR.
- Usa los operadores de comparación ==,<,>,<=,>= .

Procedimiento 6.7. Fórmula de entrada

1. Selecciona una variable encima de la caja de fórmulas y clics en Añadir para transportarla a la caja.
2. Edita la fórmula en la caja de fórmula para formar la expresión deseada.

Añadir metadatos de Trap Receiver

Para acceder a la página de configuración de metadato, accede a **Configuración** → **Trap receiver** y clics en el botón **Metadato**.

Clics 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, clics en el botón **Borrar**.

Tabla 6.18. 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 trap receiver clics en el botón **Metadato** al lado del trap receiver que será configurado.

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

Scripts

Puedes crear y ejecutar scripts de los tipos: **Acción de alarma**, **Mapeador**, **Recolector** y **Suministro y Mapeamiento 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, clics 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), clics en **Probar** 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:

SNMP

Comandos de gestión de SNMP.

Método `tmlSnmplib.snmpGet`: Ejecuta SNMP GET en el dispositivo.

- `tmlSnmplib.snmpGet(<target>, <oids>)`

Método `tmlSnmplib.snmpWalk`: Ejecuta SNMP WALK en el dispositivo.

- `tmlSnmplib.snmpWalk(<target>, <oids>)`

Método `tmlSnmplib.snmpSet`: Ejecuta SNMP SET en el dispositivo.

- `tmlSnmplib.snmpSet(<target>, <oids>)`

target: Define los parámetros y sus valores.

```
target = {
  Parámetro1 = Valor1,
  Parámetro2 = Valor2,
  ....
  ParámetroN = ValorN,
}
```

Tabla 6.19. Target

Parámetro	Descripción
host	Dirección IP del dispositivo.
community	Rellena la community SNMP. Necesario para las versiones v1 y v2c.
version	Selecciona la versión SNMP. Los posibles valores son: v1, v2c y v3.
timeout	Tiempo límite en segundos para esperar una respuesta del paquete SNMP.
retries	Número de nuevos intentos que serán permitidos al dispositivo si no responde a una consulta SNMP.
max_pps	Número de OIDs que serán enviadas en cada paquete SNMP.
max_per_packet	Número máximo de paquetes por segundo que un recolector SNMP enviará a cada dispositivo.

Parámetro	Descripción
window	Número de paquetes SNMP que serán enviados sin respuesta del dispositivo que está siendo polled.
port	La puerta SNMP
authentication_type	Tipo de autenticación. Los valores posibles son: authPriv, authNoPriv e noAuthNoPriv. Necesario para v3.
user_name	Nombre del usuario. Necesario para v3.
password_type	Tipo de contraseña. Los valores posibles son: SHA-1 y MD5. Necesario para los tipos de autenticación authPriv y authNoPriv (v3).
authentication_password	Contraseña de autenticación. Necesario para los tipos de autenticación authPriv y authNoPriv (v3).
privacy_protocol	Protocolo de Privacidad. Los valores posibles son: DES y AES. Necesario para los tipos de autenticación authPriv (v3).
privacy_password	Contraseña de privacidad. Necesario para los tipos de autenticación authPriv (v3).

oids: Define los OID.

```
oids = {[1] = 'OID1',
        [2] = 'OID2',
        ....
        [N] = 'OIDN',
}
```

Siendo **OIDN** el OID que el sistema recopilará.

----- Ejemplo -----

```
target = {
    host = '10.0.0.1'
    version = 'v3',
    timeout = '10',
    retries = 10,
    max_pps = 10,
    max_per_packet = 10,
    window = 10,
    port = 161,
    authentication_type = 'authPriv',
    user_name = 'User_name',
    password_type = 'SHA-1',
    authentication_password = '123456',
    privacy_protocol = 'DES',
    privacy_password = '123456'
```

```

}

oids = {
    [1] = "1.3.6.1.2.1.31.1.1.1.1",
    [2] = "1.3.6.1.2.1.2.2.1.2"
}

tmlSnmp.snmpWalk(target, oids)

```

ListMappedObj

Enumera los objetos mapeados que están activos.

Método tmlApi.listMappedObj: enumera los objetos.

- tmlApi.listMappedObj(<IP>,<Mapeador>)

Tabla 6.20. Parámetro

Parámetro	Descripción
<IP>	IP del dispositivo.
<Mapeador>	Nombre del Mapeador.

----- Ejemplo -----

```

h = params['ipaddr']

listMO= tmlApi.listMappedObj(h,'Interface')

tmlDebug vardump(listMO)

```

SSH

Se conecta a un servidor remoto a través de SSH.

Método tmlSSH.sshNew: Crea el objeto.

- ssh = tmlSSH.sshNew({host= <Host>,port= <port>,user=<user>,passwd=<passwd>,timeout=<timeout>})

Tabla 6.21. Parámetro

Parámetro	Descripción
<host>	IP del dispositivo.
<port>	Número de puerto.

Parámetro	Descripción
<user>	Nombre del usuario.
<passwd>	Contraseña de autenticación.
<timeout>	Tiempo límite en segundos para esperar una respuesta.

Método ssh:<comando>: Ejecutar la acción.

- ssh:<comando>([parámetro])

Tabla 6.22. Comando

Comando	Descripción
connect	Establece la conexión. No tiene parámetro.
send	Enviar comando Parámetro: acción/comando.
expect	Lee todo el contenido del búfer, luego verifica si el texto buscado está presente. Parámetro: texto buscado.
expectFast	Lee el contenido del búfer, si encuentra que el texto deja de leer. Parámetro: texto buscado.
read	Lee el contenido del búfer. No tiene parámetro.
setTimeout	Altera el timeout de la conexión. Parámetro: tiempo en segundos. Ej.: ssh:setTimeout('10').
disconnect	Desconecta. No tiene parámetro.

Socket (HTTP/HTTPS)

Ejecuta solicitud **HTTP/HTTPS**. Para ello, basta con indicar una URL y un método.

Los métodos válidos son **GET** y **POST** en caja alta.

Método tmlSocket.http: Ejecuta la solicitud HTTP.

- r = tmlSocket.http({url=<url>,method=<método>,params={<p1>,<p2>,....,<pn>}})

Método tmlSocket.https: Ejecuta la solicitud HTTPS.

- r = tmlSocket.https({url=<url>,method=<método>,params={<p1>,<p2>,....,<pn>}})

Tabla 6.23. Parámetros

Parámetros	Descripción
<url>	URL para realizar la solicitud. Por ejemplo: url='http://10.0.0.113/cgi-bin/index'.
<método>	Método para realizar la solicitud. Valores: 'GET' o 'POST'.
<pn>	Parámetros a enviar en la solicitud. Ej.: sysid='7'.

Método r.<comando>: Devuelve información de la solicitud.

- **r.content:** Devuelve el contenido de la página.
- **r.status:** Devuelve el código de retorno (Ej.: 200, 500, 404, etc.).

```
----- Ejemplo -----
r = tmlSocket.http({url='http://10.0.0.113/cgi-bin/index',
  method='GET',
  params={sysid='7'}})
--tmlDebug.log(r.content)
return toString(r.status)
-----
```

```
----- Ejemplo -----
url = 'https://www.telcomanager.com'
t = tmlSocket.https({url=url,method='GET',params={}})
r = string.sub(t.content,900,1200)
tmlDebug.log(t.status)
return r
-----
```

Telnet

Se conecta a un servidor remoto a través de Telnet.

Método `tmlTelnet.telnetNew`: Crea el objeto.

- `telnet = tmlTelnet.telnetNew({host= <Host>,port= <port>,timeout=<timeout>})`

Tabla 6.24. Parámetro

Parámetro	Descripción
<host>	IP del dispositivo.
<port>	Número de puerto.
<timeout>	Tiempo límite en segundos para esperar una respuesta.

Método `telnet:<comando>`: Ejecutar la acción.

- telnet:<comando>([parámetro])

Tabla 6.25. Comando

Comando	Descripción
connect	Establece la conexión. No tiene parámetro.
send	Enviar comando Parámetro: acción/comando.
expect	Lee todo el contenido del búfer, luego verifica si el texto buscado está presente. Parámetro: texto buscado.
expectFast	Lee el contenido del búfer, si encuentra que el texto deja de leer. Parámetro: texto buscado.
read	Lee el contenido del búfer. No tiene parámetro.
setTimeout	Altera el timeout de la conexión. Parámetro: tiempo en segundos. Ej.: telnet:setTimeout('10').
disconnect	Desconecta. No tiene parámetro.

THA

Proporciona información del Agente para Windows (THA).

Método tmlTHA.new: Crea el objeto.

- tha = tmlTHA.new({host= <host>,port= <port>})

Tabla 6.26. Parámetro

Parámetro	Descripción
<host>	IP del dispositivo de Windows.
<port>	Número de puerto.

Método sendCmd: Ejecute un comando THA.

- tha.sendCmd(<comando>, [parámetro])

Tabla 6.27. Comando

Comando	Descripción
hardware_monitor	Monitor de hardware. No tiene parámetro.
list_applications	Listado de aplicaciones. No tiene parámetro.
service_status	Estado del servicio Parámetro: nombre del servicio. El significado de cada número se puede ver en la página de microsoft [https://docs.microsoft.com/pt-br/dotnet/api/system.serviceprocess.servicecontrollerstatus?view=netframework-4.8].
start_service	Iniciar servicio parámetro: nombre del servicio.
stop_service	Detener el servicio. Parámetro: nombre del servicio.

Comando	Descripción
raw_counter	Analiza los datos de rendimiento que proporcionan las aplicaciones, los servicios y los controladores. Parámetro: path del contador deseado.

----- Ejemplo -----

```
tha = tmlTHA.thaNew({host='10.0.0.190', port=8888})
ret = tha:sendCmd('service_status', 'TelcoHostAgent' )
```

Otras funciones

- **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.
- **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

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

- abs
- clock
- difftime
- exp
- floor
- ipairs
- max
- min

- next
- pairs
- pow
- sqrt
- string.find
- string.sub
- 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']):

Validación de metadato

Los siguientes parámetros son exclusivos de los scripts de Validación de metadato.

- **params['metadata']**[<NOMBRE_DEL_METADATO>]['value']: Valor de metadatos actual (antes de editar), donde NOMBRE_DEL_METADATO es el nombre de los metadatos.
- **params['metadata']**[<NOMBRE_DEL_METADATO>]['new_value']: Valor de metadatos rellenado en el formulario, donde NOMBRE_DEL_METADATO es el nombre de los metadatos.

Parâmetros globais

- **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['obj'] [<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['obj'] [<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 autenticación.
- **params['passwd']**: Contraseña para autenticación.
- **params['enable_passwd']**: Contraseña de enable para autenticación.
- **params['protocol']**: Protocolo para conexión.
- **params['protocol_port']**: Puerto utilizado por el protocolo de 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']['startts']**: Inicio de alarma.
- **params['alarm']['endts']**: Fin 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['mitigation-block']**: IP del bloque mitigado.
- **params['mitigation-mask']**: Mascara de Bloque IP.
- **params['connection']**: Objeto de conexión a un dispositivo.
- **params['metadata'] [<NOMBRE_DEL_METADATO>]**: Devuelve el valor de los metadatos, donde NOMBRE_DEL_METADATO es el nombre de los metadatos.

- `params['user']['name']`: Nombre de usuario.
- `params['user']['username']`: Username.
- `params['user']['email']`: Correo electrónico del usuario.
- `params['user']['profile']`: Perfil de usuario.
- `params['user']['type']`: Tipo de acceso. Opciones: 'administrator', 'operator', 'configurator'.
- `params['action']`: Acción de script. El valor debe ser 'new' o 'edit'.
- `params['dev-config']`: Configuración probada del dispositivo a analizar.

Ejecutando scripts

Para ejecutar algún script ya creado, clicas en él en el menú a la izquierda. Puedes editarlo usando la caja de texto. Entonces, clicas en **Probar** y seleccionas 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 Acción de alarma

El script de Acción de alarma ejecuta una secuencia de comandos en el dispositivo y lo compara con las respuestas esperadas.

Este tipo de script puede asociarse con una alarma. Cuando la alarma está **ACTIVO**, el script se puede ejecutar en la pantalla de la Consola.

Los scripts de Acción de alarma están escritos en **Lua**.

Utilice el siguiente ejemplo para crear su script de Acción de alarma:

```
----- Inicio del 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('./open-ticket ' .. params['name'])
if(c:expect('#') == false) then
return nil
end

c:disconnect()

----- Fin del script -----

```

Script de Recolector

Creas un Script de recolector para realizar la Recolecta Telco Script.

Este tipo de script permite ejecutar operaciones matemáticas en los resultados de las recolectas. Esto hace posible formatear los valores que serán trazados en el gráfico.

Los scripts de recolecta pueden ser ejecutados en el modo **Simple** o **Avanzado**. Puedes alterar el modo en la esquina superior derecha de la pantalla.

Modo avanzado

En este modo, pueden recolectarse datos de un dispositivo y sus objetos mapeados en una única ejecución. Para ello, los scripts de recolecta necesitarán retornar una tabla. Esta necesita seguir la siguiente estructura:

- Primer nivel: Usa **'dev'** para variables de recolecta del dispositivo y **'mobj'** para variables de recolecta de objetos mapeados.
- Segundo nivel: Nombre del mapeador Este nivel es necesario solo si el primer nivel es **mobj'**.
- Tercer nivel: ifDescr del objeto mapeado. Este nivel es necesario solo si el primer nivel es **mobj'**.
- Cuarto nivel: Nombre de la variable de recolecta.

La tabla sigue, por tanto, el siguiente modelo:

```

result = {}
result['dev'] = {}
result['dev']['Total storage'] = storageTotal
result['dev']['Available storage'] = storageAvailable

result['mobj'] = {}
result['mobj']['Interface'] = {}
result['mobj']['Interface']['net0'] = {}
result['mobj']['Interface']['net0']['ifSpeed TCS'] = speed

-- "Total storage", "Available storage" e "ifSpeed TCS" são os nomes
  das variáveis de coleta
-- "Interface" é o nome do mapeador
-- "net0" é o ifDescr do objeto mapeado

```

Ve el ejemplo de un script en el modo avanzado a continuación:

```
----- Inicio del script -----

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

mobjjs = params['mobj']
-- mobjjs = { [mapper] = { [name] = { ['ifindex'] = ifIndex,
  ['description'] = ifAlias } } }

t = tmlSnmp.snmpGet(h,c,v,{[1] = '1.3.6.1.2.1.1.5.0'})

ret ={}
ret['dev'] = {'sysName' = t['1.3.6.1.2.1.1.5.0']}

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

descr = t['1.3.6.1.2.1.2.2.1.2']
speed = t['1.3.6.1.2.1.2.2.1.5']

ret['mobj'] = {'Interface' = {}}

for key,value in pairs(descr) do
  ret['mobj']['Interface'][value] = { ['ifDescr'] = value,
  ['ifSpeed'] = speed[key] }
end

return ret

----- Fin del script -----
```

Modo Simple

En este modo, los scripts necesitan retornar un valor.

Ve los ejemplos a continuación:

```
----- Inicio del script -----

srcaddr=nil
timeout=3000

n = tmlPing.pingNew({srcaddr=srcaddr,timeout=timeout,details=false})
```

```
-- 'details' é um parâmetro opcional

p = n:run({{ipaddr='10.0.0.99',nbpkts=10,interval=10,pktsize=64}})

tmlDebug vardump(p)

t = tmlSnmp.snmpGet('10.0.0.99','public','v2c',
  {[1] = '1.3.6.1.2.1.1.3.0'})

-- Valores serão salvos em t['1.3.6.1.2.1.1.3.0']

return t['1.3.6.1.2.1.1.3.0']
```

----- Fin del script -----

----- Inicio del script -----

```
db = tmlMsSql.msSqlNew({host=%HOST%,user=%USER%,passwd=%PASSWORD%,
  dbname=%DBNAME%})
rows = db.query(db,%QUERY%)

for i,row in pairs(rows) do
  value = row[%COL_NAME%]
done

-- DBNAME, QUERY e COL_NAME são strings
```

----- Fin del script -----

----- Inicio del script -----

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

t = tmlSnmp.snmpWalk(h,c,v,{[1] = '1.3.6.1.2.1.2.2.1.2'})

str=""

val = t['1.3.6.1.2.1.2.2.1.2']

for key,value in pairs(val) do
  str = str .. value .. "\n"
end
```



```

tmlDebug vardump(val)

return str

-- Cada valor é uma tabela com o índice retornado e seu valor
( ['idx'] = ['value'] )

----- Fin del script -----

----- Inicio del script -----

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

t = tmlSnmp.snmpGet2({host = h,community = c,
version = c, timeout = timeout,retries = retries,
max_pps = mpp, max_per_packet = mpps, window = w,
port = port},{[1] = '1.3.6.1.2.1.1.3.0'})

tmlDebug vardump(t['1.3.6.1.2.1.1.3.0'])

return t['1.3.6.1.2.1.1.3.0']

----- Fin del script -----

```

Script de Mapeador

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

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

- name
- description
- version
- index
- alias

- iftype
- speed
- metadata

Importante

Todos los campos retornados pueden ser una string.

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

```
----- Inicio del script -----

r = {}

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

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

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

tmlDebug vardump(ifDescr)

return r

----- Fin del script -----
```

Comprueba abajo el ejemplo anterior con uso de parámetros:

```
----- Inicio del script -----

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

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

ifDescr = t['1.3.6.1.2.1.2.2.1.2']
```

```

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

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

tmlDebug.vardump(ifDescr)

return r

----- Fin del script -----

```

Utilice el siguiente ejemplo para crear una script que complete los valores de metadatos de los objetos asignados.

```

----- Inicio del script -----

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

t = tmlSnmp.snmpWalk(h,c,v,{[1] = '1.3.6.1.2.1.2.2.1.2'})

ifDescr = t['1.3.6.1.2.1.2.2.1.2']
for key,value in pairs(ifDescr) do
    meta = {}
    meta['State'] = 'RJ'
    meta['Country'] = 'BR'
    r[key] = {[ 'name' ] = value,[ 'description' ] = value,
    [ 'version' ] = '1',[ 'index' ] = key, [ 'metadata' ] = meta}
end
tmlDebug.vardump(val)

return r

----- Fin del script -----

```

Observa algunos ejemplos más:

```

----- Inicio del script -----

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

```

```

v = params['snmp']['version']
timeout = params['snmp']['timeout']
retries = params['snmp']['retries']
mpp = params['snmp']['max_per_packet']
mpps = params['snmp']['max_pps']
w = params['snmp']['window']
port = params['snmp']['port']

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

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

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

tmlDebug.vardump(t['1.3.6.1.2.1.2.2.1.2'])

return r

----- Fin del script -----

----- Inicio del script -----

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

r = {}

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

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

return map

----- Fin del script -----

```

Script de Mapeamento de IPs

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

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

- name
- ipaddr

Importante

Todos los campos devueltos pueden ser una cadena.

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

```
----- Inicio del script -----  
  
r = {}  
  
r[1] = { ['name'] = 'name1', ['ipaddr'] = 'ipaddr1' }  
r[2] = { ['name'] = 'name2', ['ipaddr'] = 'ipaddr2' }  
r[3] = { ['name'] = 'name3', ['ipaddr'] = 'ipaddr3' }  
  
return r  
  
----- Fin del script -----
```

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**.

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 variable `m4_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.
- Los campos cerrados con el carácter \$ se obtienen del banco de datos basados en los códigos de suministro usados para configurar un tipo de probe. Son usado solo en la creación de probes.
- 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 6.28. 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..

Variables	Descripción
%current_collector_ip%	Dirección de IP del actual recolector en la arquitectura distribuida.

Script de validación de metadatos

Cree una secuencia de comandos personalizada que se pueda habilitar en la pantalla **Circuito**.

El script le dice si no se cumplió la condición, devolviendo un mensaje de error mientras edita los valores de los metadatos. De lo contrario, la operación devolverá un mensaje de éxito.

Utilice el siguiente ejemplo para crear su secuencia de comandos de validación de metadatos:

```

----- Inicio del script -----

if params['metadata']['NAME_OF_METADATA']['value'] == nil then;
  tmlDebug.log('empty value for metadata');
  return false;
end
return true

----- Fin del script -----

```

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 clics en el botón **Nuevo**.

Tabla 6.29. Formulario de Credencial de Dispositivo

Campo	Descripción
Nombre	Define el nombre de credencial.
Protocolo	Defina si la credencial será de AWSAPI , SNMP , SSH o 4_bold(Telnet) .
AWS key ID	Opción disponible solo para el protocolo AWSAPI . ID de clave de acceso.
AWS key secret	Opción disponible solo para el protocolo AWSAPI . Clave de acceso secreta.
Versión del SNMP	Selecciona la versión SNMP; Los posibles valores son:

Campo	Descripción
	SNMP v1 o SNMP v2c Especifica una community SNMP SNMP v3 Especifica el tipo de autenticación 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.
Asociación automática	Selecciona Sí para habilitar la asociación automática de dispositivos a este Credencial de Dispositivo considerando las Reglas de Asociación.
Dispositivos	Asocia los dispositivos que deben utilizar la credencial.

Importante

El proceso de asociación automática se ejecuta todos los días en dos momentos preconfigurados, que pueden ser ajustados en **Sistema** → **Parámetros** → **Agentes de asociación** → **Agente de asociación automática para credenciales de dispositivo** .

Añadir metadatos de credenciales de dispositivo

Para acceder a la página de configuración de metadato, accede **Configuración** → **Credencial de dispositivo**, clicas en el ítem **Credencial de dispositivo** en el menú del árbol y clicas en el botón **Metadato**.

Clicas 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, clicas en el botón **Borrar**.

Tabla 6.30. Campos de un metadato

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

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

Para asociar el metadato creado a una credencial, accede a la lista de credenciales y clicas 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.

Filtro de Syslog

Los filtros de Syslog pueden ser usados como Reglas de activación de alarmas del tipo **Syslog**.

Para crear un nuevo filtro, accede **Configuración** → **Filtro de syslog** → **Nuevo filtro de syslog** o **Configuración** → **Filtro de syslog** → **Filtro de syslog** y clicas en el botón **Nuevo**.

Tabla 6.31. Formulario de Filtro de Syslog

Campo	Descripción
Nombre	Rellena con el nombre del filtro.
Descripción	Rellena con la descripción del filtro;
Facilidad	Rellena con la Facilidad del Syslog.
Severidad	Rellena con la Severidad del Syslog.
Mensaje	Rellena con el mensaje del Syslog.

Añadir metadatos de filtro de Syslog

Para acceder a la página de configuración de metadato, accede a **Configuración** → **Filtro de syslog**, clicas en el ítem **Filtro de syslog** en el menú del árbol y clicas en el botón **Metadato**.

Clicas 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, clicas en el botón **Borrar**.

Tabla 6.32. Campos de un metadato

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

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

Para asociar el metadato creado a un perfil de Syslog, accede a la lista de filtros y clicas en el botón **Metadato** al lado del filtro que será configurado.

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

Plantilla de Tiempo

En esta pantalla, es posible crear plantillas de tiempo para la visualización de datos. Estas plantillas deben tener horario comercial y zonas horarias.

Cuando se muestran los gráficos de los dispositivos y sus objetos mapeados, esta configuración se verificará para mostrar los gráficos.

Tabla 6.33. Formulario de Filtro de preferencias locales.

Campo	Descripción
Nombre	Nombre Nombre de la plantilla.
Usar zona horaria predeterminada del sistema	SÍ para usar la zona horaria del sistema y NO para configurar la hora.
Huso horario	Zona horaria de plantilla, disponible cuando la opción NO está habilitada en el campo Usar zona horaria predeterminada del sistema .
Utiliza el horario comercial predeterminado del sistema	SÍ para usar los tiempos registrados en Preferencias locales y NO para definir los intervalos.
Horarios	Establezca las horas de inicio y finalización para la primera y segunda hora comercial. Disponible cuando la opción NO está habilitada en el campo Utiliza el horario comercial predeterminado del sistema .
Asociación automática	Seleccione SÍ si los dispositivos deben asociarse automáticamente con la Plantilla. En este caso, se deben seleccionar las reglas apropiadas.
Dispositivos Asociados	Seleccione los dispositivos que se asociarán con la plantilla. Para el campo de asociación automática marcado NO .
Reglas asociadas	Seleccione las reglas que deben asociarse con la plantilla. Para el campo de asociación automática marcado como SÍ .

Sugerencia

Los horarios para la ejecución de **asociaciones automáticas** se pueden configurar en: **Sistema** → **Parámetros** → **Agentes de asociación** → **Agente de asociación automática para plantillas de tiempo** ..

Capítulo 7. Herramientas

Discovery

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

Tabla 7.1. Parámetros del Discovery

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

Sugerencia


si se selecciona **Enviar correo electrónico con ips no registrados**, cuando un informe está listo, es enviado al correo electrónico de los usuarios. El servidor SMTP debe ser configurado, así como el correo electrónico de cada usuario en el formulario de configuración del usuario.

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


Exportar datos

Haga clic en el botón **Exportar datos** para exportar la lista de objetos en formato CSV.

Cuando el proceso termine, es posible añadir cualquiera de los hosts descubiertos como dispositivo.

Puedes seleccionar cada uno haciendo clic en el ícono  y 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**

Además, puede filtrar los resultados por IP descubiertas, ignoradas y reconocidas, simplemente haga clic en el icono  y seleccione la opción deseada.

En la pantalla principal de Discovery, se muestra el número de dispositivos descubiertos en la última ejecución del modelo. Los dispositivos descubiertos son todos aquellos que no están registrados en el sistema o en la lista de IP excluidas.

Para las Modelos con horarios, se mostrarán los botones de **Mostrar**, que muestran el resultado de la última ejecución, y el botón de **Histórico**, que muestra todos los resultados. Para las plantillas que no se han programado, puede ejecutar el descubrimiento haciendo clic en el botón **Rodar**.

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, clics en el botón Seleccionar en la lado derecho.

Software externo

Telcomanager Windows Collector

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

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

Telcomanager Host Agent

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

Este agente recolecta informaciones sobre los procesos que se están ejecutando. Será necesario para hacer recolectas del tipo THA.

Capítulo 8. Sistema

Registro de acceso

Acceso de usuario

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

Acceso simultáneo

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

Copia de Seguridad/Restaurar

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

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

Copia de seguridad local de configuración

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

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

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

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

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

Restauración local de configuración

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

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

Copia de seguridad Remota

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

Tabla 8.1. Copia de seguridad remota utilizando un servidor FTP

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

Tabla 8.2. Copia de seguridad remota utilizando un servidor S3

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

Restauración Remota

Selecciona un único sistema para ejecutar la restauración de los datos o clicla 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 autenticación Active Directory Kerberos.

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

Tabla 8.3. Formulario de Active directory

Campo	Descripción
Habilitar autenticación por el Active Directory	Cuando la opción Sí este seleccionada, el campo Autenticación 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 autenticación 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 **Autenticación local** activada, en el caso de que sea utilizado el control de acceso externo.

Agente de las carpetas de enlace

Esta configuración te permitirá elegir dos tiempos de ejecución en el mismo día para ejecutar el agente de las carpetas de enlace.

Agentes de asociación

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

Tabla 8.4. Formulario de agente de asociación automática

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

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

Agente de asociación automática de grupos

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

Agente de asociación automática de plantillas de tiempo

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

Agente de asociación automática de mapeadores

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

Agente de asociación automática para credenciales de dispositivo

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

Agente de asociación automática para perfiles de QoS

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

Perfil automático

Define dos horarios del día para que el agente de asociación del perfil automático se realice.

Perfil automático de alarma

Define dos horarios del día para que el agente de asociación del perfil automático de alarma se realice.

Alarmas

Tabla 8.5. Formulario de parámetros del Alarmas

Campo	Descripción
Período máximo de almacenamiento de eventos	Número de horas que la tabla de incidencias almacenará incidencias. Esta tabla se usa solo para niveles de depuración altos, ya que las incidencias no son utilizadas después de procesadas.
Período máximo de almacenamiento de alarmas	Después de este periodo, las alarmas se eliminarán.
Período máximo de almacenamiento de alarmas inactivas	Cuando la alarma se vuelve inactiva, estará disponible en el Alarmas consola por este período. Después de esto, la alarma puede ser visualizada en informe Alarmas.
Ventana de tiempo de recurrencia de alarma (minutos)	Es el intervalo de tiempo en el que, después del final de la alarma, puede volver a activarse y aumentará el número de recurrencias. Si la alarma

Campo	Descripción
	no está activa nuevamente al final de ese intervalo, el número de recurrencias volverá a cero. El número de recurrencias se puede ver en la pantalla de la consola en la columna RECURRENCIAS y al ver los detalles de la alarma. Si el campo tiene un valor de 0 (cero), el número de recurrencias siempre será cero.

Las incidencias de alarmas son generadas por los siguientes procesos:

- SlaSumCaching: genera incidencias para todas las alarmas configurables creadas con resumen de variables.
- ICMPAgent: genera incidencias para la alarma **Sin respuesta ICMP**.
- MIBget: genera incidencias para la alarma **Sin respuestaSNMP**.
- ObjectMapper: genera incidencias para la alarma **Objeto no encontrado**.

Atención

Puedes comprobar el ítem de **Configuración** en la sección **Sistema** → **Diagnósticos** → **Uso de disco** para comprobar si el banco de datos es muy grande, indicando que el sistema está generando muchas alarmas. Si este es el caso, puedes disminuir el periodo de almacenamiento o ayudar a las configuraciones de la alarma a generar menos alarmas.

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 disponible para reserva** mostrará el espacio que todavía puede ser distribuido.

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

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

Tabla 8.6. Formulario de almacenamiento de datos

Campo	Descripción
Iniciar proceso a partir de la ocupación en %	Cuando este valor se alcance, el proceso de limpieza se ejecutará de acuerdo con el tipo de ejecución configurada. Rellena un valor entre 1 y 85 .
Tipo de ejecución	Escoge si un agente funcionará a cada Intervalo de tiempo o en un Horario programado .
Intervalo de tiempo para ejecución (minutos)	Define el intervalo de tiempo, en minutos, para la ejecución del agente. El valor mínimo es 10 .
Horario de ejecución	Define el horario en el que se realice la ejecución del agente.

Campo	Descripción
Espacio disponible para los archivos SYSLOG	Almacenamiento dedicado para datos brutos de archivos SYSLOG.
Espacio disponible para los archivos de Informes programados	Almacenamiento dedicado a informes programados.
Trap receiver storage	Almacenamiento dedicado para archivos de Trap receiver.
Espacio disponible para archivos de captura	Almacenamiento dedicado a archivos de captura.
Limpiar datos históricos	Habilita la eliminación del datos históricos antiguos.
Limpiar alarmas	Habilita la eliminación del historial de alarmas antiguas.
Datos brutos del TRAFip	Área de almacenamiento destinada a los archivos de datos brutos del TRAFip. Este almacenamiento normalmente crece mucho más rápido que los datos resumidos. De esta forma, si los configuras con el mismo tamaño que los datos resumidos, vas a terminar con 10 veces menos datos históricos.
Datos resumidos del TRAFip	Almacenamiento dedicado para el TRAFip, datos procesados o TDB - Telco database. Este dato se usa para gráficos e informes TOPN.
Archivos de resumen remoto del TRAFip	Almacenamiento dedicado a los datos procesados del TRAFip enviados por los recolectores en un ambiente de arquitectura distribuida.
Datos de alteración de comportamiento del TRAFip	Almacenamiento dedicado para los datos de alteración de comportamiento, como datos de alarmas históricas, por ejemplo.
Datos brutos del SLAview	Almacenamiento dedicado para datos brutos del SLAview. Esto es, en general, de las recolectas SNMP de las OIDs.
Datos resumidos del SLAview	Almacenamiento dedicado para datos procesados del SLAview. Este dato se usa para gráficos e informes.
Archivos de resumen remoto SLAview	Almacenamiento dedicado a los datos procesados para los archivos de los datos SLAview enviados por los recolectores en un ambiente de arquitectura distribuida.
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.

Quando los campos **Datos brutos (MB)** y **Datos resumidos (MB)** están rellenos con '0' (cero), significa que el sistema está distribuyendo de manera automática el **Espacio disponible para reserva** 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 reserva** por 4. Así, tendrás el valor de cada espacio.

Atención

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

Arquitectura distribuida

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

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

Tabla 8.7. Formulario de los parámetros de la arquitectura distribuida

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

Aviso de Expiración

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

Tabla 8.8. Formulario de aviso de expiración

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

Copia de seguridad

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

BGP

Anuncie o quite rutas de sus tablas de enrutamiento

Tabla 8.9. Formulario BGP

Campo	Descripción
Habilitar BGP	Seleccione esta opción si desea anunciar o quitar una ruta.
Identificador BGP	Valor entero que identifica únicamente el emisor.
Número de AS local	Número del AS del emisor.
Número de AS del peer	Número del AS del receptor.
Ip del peer	IP del router del AS receptor.
Usar comunidad extendida	Seleccione Sí para que el usuario pueda habilitar el modo de comunidad extendida. [http://www.rfc-editor.org/rfc/rfc4360.html]
Comunidad BGP	Conjunto de etiquetas genéricas que se pueden utilizar para señalar varias directivas administrativas entre enrutadores BGP. Notación: <Administrador global>:<Administrador local> . Ejemplo: 65535:4294967295.

Una vez que se complete el formulario, el sistema le informará sobre el estado de la conexión:

- Idle: Ignorar todo.
- Connect: Intentando conectar.
- Active: Esperando una conexión.
- OpenSent: El paquete abierto ha sido enviado.
- OpenConfirm: Esperando keepalive o notificar.
- Established: Se ha establecido la conexión.

Circuito

Establezca el metadato deseado para crear una carpeta, generar nombres de circuitos y validar metadato.

Los datos se agrupan de acuerdo con el metadato elegido.

Tabla 8.10. 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 . Seleccione el script. Crea uno en la sección Scripts.
Metadatos para la agrupación	Seleccione el nombre del metadato que será el nombre de la carpeta.
Script de validación	Seleccionar script de validación de metadatos.

Cisco WAAS

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

Tabla 8.11. Formulario de Cisco WAAS

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

Recolector personalizado

Define el número de recolectas simultáneas permitidas.

Tabla 8.12. Formulario del recolector personalizado

Campo	Descripción
Número máximo de recolectas simultáneas	Escoge un valor entero mayor o igual a 50. El relleno modelo es de 10 recolectas.

Configuración de HTTPS

Configura el modo HTTPS (HyperText Transfer Protocol Secure).

Tabla 8.13. Formulario de HTTPS

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

Configuración del agente de captura

Configura el número permitido de agentes en ejecución simultánea.

Tabla 8.14. Formulario de configuración del agente de captura

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

Configuración regional

Tabla 8.15. 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

Configuraciones del trap receiver

Define la puerta que será oída para SNMP traps. La puerta modelo es **162**.

EPM

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

Tabla 8.16. 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!

Exportación

Syslog

Syslog es un mecanismo de seguimiento que envía mensajes cuando determinados eventos suceden. Están compuestos, básicamente, por la dirección de IP, por el timestamp y por el mensaje de log.

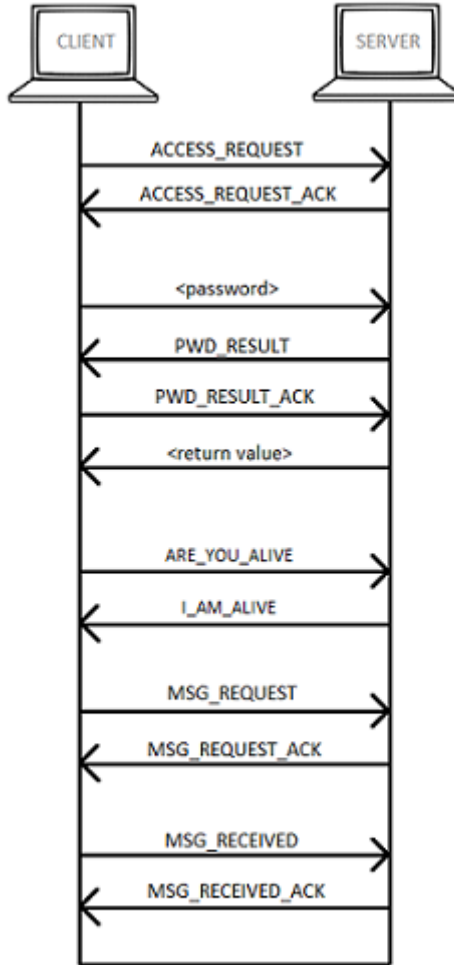
Debido al hecho de que estos mensajes Syslog son enviados por cada dispositivo de forma separada, este mecanismo proporciona informaciones más detalladas si las comparamos con las traps SNMP.

El TRAFip posee un agente exportador que envía estos mensajes Syslog de los dispositivos registrados en el sistema.

Es necesario que haya comunicación entre un host y el TRAFip para que estos mensajes Syslog sean recibidos por el host. Para configurar que hosts tendrán acceso a la exportación Syslog, clic en **Añadir** y especifica el host y la contraseña.

En el **Filtro por origen**, configurarás los dispositivos que serán oídos y que enviarán mensajes Syslog. Para que un dispositivo sea habilitado, selecciónalo y transpórtalo para el lado derecho del filtro usando el botón '>>>'.
>>>'

La imagen siguiente ilustra el protocolo de comunicación entre el cliente y el servidor:



Protocolo Syslog

Tabla 8.17. Protocolo Syslog

Mensaje	Descripción
ACCESS_REQUEST	Mensaje de solicitud de acceso por el cliente.
ACCESS_REQUEST_ACK	Configuración de entrega de mensaje enviada por el cliente.

Mensaje	Descripción
<password>	Contraseña configurada para el host en el campo Contraseña del formulario en Sistema → Parámetros → Exportación → Syslog .
PWD_RESULT	Autenticación de contraseña
PWD_RESULT_ACK	Configuración de entrega de mensaje enviada por el cliente.
<return value>	Es el valor de retorno de la autenticación. Si el host es autenticado, retorna 1. En caso contrario, la conexión es cerrada.
ARE_YOU_ALIVE	Verifica si el agente exportador está activo y ejecutando.
I_AM_ALIVE	Confirmación sobre si el agente exportador está activo y ejecutando.
MSG_REQUEST	El cliente envía un pedido para el envío de los mensajes.
MSG_REQUEST_ACK	Confirmación de entrega de mensaje enviada por el cliente.
MSG_RECEIVED	El cliente confirma que los mensajes fueron recibidos.
MSG_RECEIVED_ACK	Confirmación de entrega de mensaje enviada por el cliente.

Grafador

Ajuste de los parámetros del grafador.

Tabla 8.18. Formulario de parámetros del grafador

Campo	Descripción
¿Habilitar gráfico derivativo como modelo?	En el modo estándar, puntos de gráficos son conectados usando interpolación lineal. En el modo derivativo, se utiliza la interpolación por partes.
Habilitar actualización automática	Selecciona esta opción para tener todos los gráficos actualizados automáticamente. También puedes habilitar esta opción en tiempo de ejecución para cada gráfico.
Habilitar verificación de licencia	Seleccione sí para que aparezca una alerta en el gráfico si el usuario excede más del 10% del límite de la licencia de tráfico. La alerta se mostrará dentro de media hora después de la primera vez que el sistema excede el umbral.
Excluir fines de semana	Habilitando esta opción, los días del fin de semana se mostrarán con color más claro en los gráficos.
Intervalo de actualización	Intervalo de actualizaciones.
Horario comercial	Esta opción permite modificaciones en la visualización de los gráficos de acuerdo con

Campo	Descripción
	el horario comercial definido en Preferencias locales. Elija entre Sin acciones , Destacar horario comercial o Mostrar solo horario comercial .

Histórico de configuración

Selecciona el periodo de almacenamiento para diferentes áreas de configuración.

Tabla 8.19. 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 .

ICMP

Proceso de configuración de ICMP polling. El proceso responsable por el ICMP polling es el ICMPAgent.

El ICMP polling se ejecuta a cada minuto, pero para evitar pollings innecesarios, el sistema posee un proceso de amortecimiento. Este proceso causa el decaimiento de la frecuencia de polling con el tiempo y, en caso de que el elemento vuelva a responder, el proceso es interrumpido.

Tabla 8.20. Formulario de parámetros del proceso ICMP

Campo	Descripción
Número de fallos para activar amortecimiento	Después de este número de fallos consecutivos, el proceso de amortecimiento se iniciará.
Aumento del número de intervalos a cada fallo	Después de que el dispositivo sea colocado en modo de amortecimiento, este número es adicionado al número de intervalos entre polling cada vez que el dispositivo es polled.
Intervalo máximo permitido en el amortecimiento	Este es el número máximo de veces que el ICMPAgent saltará el polling de este dispositivo, incluso si está en modo de amortecimiento. Cuando esta condición es alcanzada, el ICMPAgent generará una incidencia para la alarma Maximum damping reached a cada minuto para cada dispositivo.

Campo	Descripción
Timeout ICMP (ms)	Timeout para el ICMP polling.
Prueba ICMP	Escoge Sí para verificar la conectividad de los equipos.
Nueva tentativa ICMP	Escoge Sí para rehacer la prueba de ICMP para los dispositivos que fallaron en la primera prueba.
Prueba TCP puerta 23	Escoge Sí para hacer una prueba de conexión TCP en la puerta 23 de los dispositivos. En caso de que el campo Prueba ICMP este configurado como Sí , la prueba será realizada solo en los dispositivos que fallaron en la primera prueba ICMP.
Prueba extendida	Asocia un metadato de dispositivo que contenga otros IPs para ser probados para un mismo dispositivo.
Número de paquetes	Define la cantidad de paquetes que serán enviados en la recolecta ICMP. El valor máximo es 10 .
Tamaño del paquete	Define el tamaño de los paquetes que serán enviados.
Intervalo entre paquetes (ms)	Define el intervalo, en milisegundos, entre el envío de los paquetes.
Número de pruebas simultáneas	Define cuantas pruebas podrán ser realizadas al mismo tiempo. En caso de que este campo sea configurado con el valor 0 (cero) , todas las pruebas deben ejecutarse simultáneamente.

Para más informaciones en el proceso de configuración del ICMP, ves a la sección configuración ICMP.

Importante

Por lo menos una de las pruebas (**Prueba ICMP** o **Prueba TCP puerta 23**) debe estar habilitada.

Inicio de sesión automático

Este recurso habilita la autenticación 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=<USUARIO>**.

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.

Mapa GIS

Es necesario registrar la llave **MapQuest AppKey** para visualizar mapas georreferenciados en el Mapview.

Escoge el plan que mejor responda a tus necesidades en: <https://developer.mapquest.com/plans>.

Mapeador de objetos

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

Tabla 8.21. Formulario de configuración de parámetros de mapeador de objetos

Campo	Descripción
Intervalo de ejecución del mapeador	Programa el intervalo entre las ejecuciones del mapeador.
Periodo máximo de almacenamiento del histórico de configuración	Programa el periodo de almacenamiento de logs a través de las configuraciones realizadas por el mapeador
Límite de mapeadores TCS simultáneos	Define un límite de ejecuciones simultáneas de mapeadores del tipo TCS. Rellena un valor entre 1 y 200 . La configuración de este parámetro puede afectar al rendimiento del sistema, así que se cuidadoso.
Número de recolectas simultáneas	Define un límite de ejecuciones simultáneas de mapeadores de jobs SNMP. La configuración de este parámetro puede afectar al rendimiento del sistema, así que se cuidadoso.
Número de procesos simultáneos	Define un límite de procesos simultáneos del mapeador. La configuración de este parámetro puede afectar al rendimiento del sistema, así que se cuidadoso.
Número de dispositivos en cada proceso	Define un límite de ejecuciones simultáneas de mapeadores del tipo TCS. Rellena un valor entre 1 y 200 . La configuración de este parámetro puede afectar al rendimiento del sistema, así que se cuidadoso.
Asignación de interfaz de netstream	Seleccione dispositivos que tengan los índices de interfaz en formato de 16 bits (equipo Huawei).

Mapeo de IPs

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

Tabla 8.22. 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.

Campo	Descripción
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.

Modo seguro

Al habilitar este modo, los usuarios quedan impedidos de realizar alteraciones en el sistema. Así, en el modo seguro, no será posible crear, editar o borrar objetos, ejecutar informes, scripts y agentes de asociación manual de mapeadores, perfiles del SLAview, perfiles de alarmas y grupos, y finalmente, generar archivos de copia de seguridad.

Además, algunas pestañas dejarán de exhibirse. Estas son:

- **Datos Históricos** → **Informes**;
- **Datos Históricos** → **Probes**;
- **Configuración** → **QoS**;
- **Configuración** → **Manutención**;
- **Configuración** → **ICMP Polling**;
- **Configuración** → **Tipos de probes**;
- **Configuración** → **Trap receiver**;
- **Configuración** → **Reglas**;
- **Herramientas** → **Discovery**;
- **Sistema** → **MIBs**;
- **Alarmas** → **Informes**.

Tabla 8.23. Formulario de modo seguro

Campo	Descripción
Habilitar	Selecciona Sí para habilitar el modo seguro e impedir que sean realizadas alteraciones en el sistema.

Importante

El permiso para alterar este parámetro debe ser habilitado en el formulario del usuario.

Importante

Estas restricciones no se aplican a la funcionalidad de Eagle Watcher.

Nivel de log

Escoge el nivel del ALARMDaemon: **Bajo**, **Medio** o **Alto**.

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

Personalización de interface

Puede personalizar la forma en que se mostrarán los dispositivos en el menú del árbol y en el título de los gráficos en **Datos históricos** → **Dispositivos** → **Dispositivo** .

Tabla 8.24. Formulario de personalización de interfaz

Campo	Descripción
Fórmula de nombre de dispositivo	Complete el campo con el nombre que desea que aparezca en el dispositivo en el menú del árbol. Verifique los Etiqueta que se pueden usar en este campo.
Listar interfaces por	Escoge Descripción o Rótulo .
Título modelo	Seleccione No para personalizar el título del gráfico.
Dispositivo	Complete el campo con el nombre que desea que aparezca en el título del gráfico del dispositivo. Verifique los Etiqueta que se pueden usar en este campo.
Interfaz	Complete el campo con el nombre que desea que aparezca en el título del gráfico de la interfaz. Verifique los Etiqueta que se pueden usar en este campo.

Las fórmulas tienen **Etiqueta** especiales que utilizan la información completada en los formularios de dispositivos e interfaces. Son los siguientes:

Etiqueta en el campo Fórmula del nombre del dispositivo (menú de árbol).

Tabla 8.25. Etiqueta en el campo Fórmula del nombre del dispositivo (menú de árbol).

Etiqueta	Descripción
%name%	Se refiere al nombre del dispositivo.
%ip_address%	Se refiere a la dirección de IP del dispositivo.
%custom_type%	Se refiere al valor del campo de tipo del dispositivo.
%custom_vendor%	Se refiere al fabricante del dispositivo.
%type%	Se refiere al tipo de dispositivo (Almacenamiento, Antena, Cámara, Enrutador, Estación, Firewall, Impresora, Inalámbrico, Otro, Punto de acceso, Servidor, Servidor Virtual, Servidor de Base de Datos, Switch o Telco Appliance).

Ejemplo: Dispositivo %name% - IP %ip_address% - Fabricante %custom_vendor%.

Etiqueta en el campo Dispositivo (Gráfico).

Tabla 8.26. Etiqueta en el campo Dispositivo (Gráfico).

Etiqueta	Descripción
%graph_title%	Se refiere al título del gráfico .
%name%	Se refiere al nombre del dispositivo.
%ip_address%	Se refiere a la dirección de IP del dispositivo.
%vendor%	Se refiere al Proveedor del dispositivo.
%type%	Se refiere al tipo de dispositivo (Almacenamiento, Antena, Cámara, Enrutador, Estación, Firewall, Impresora, Inalámbrico, Otro, Punto de acceso, Servidor, Servidor Virtual, Servidor de Base de Datos, Switch o Telco Appliance).
%metadata_{<NOMBRE_DE_METADATOS>}	Se refiere al valor de metadatos para la dispositivo .

Ejemplo: Dispositivo %name% - IP %ip_address% - Ubicación %metadata_{UF}%.

Etiqueta en el campo Interfaz (Gráfico).

Tabla 8.27. Etiqueta en el campo Interfaz (Gráfico).

Etiqueta	Descripción
%graph_title%	Se refiere al título del gráfico .
%name%	Se refiere al nombre del objeto.
%device_name%	Se refiere al nombre del dispositivo.
%ip_address%	Se refiere a la dirección de IP del dispositivo.
%ifdescr%	Se refiere al nombre del ifdescr .
%label%	Se refiere al nombre del etiqueta .
%ifalias%	Se refiere a ifalias .
%ifspeed%	Se refiere a ifspeed .
%rate%	Se refiere a la capacidad de la interfaz .
%mapper%	Se refiere al nombre del mapeador .
%metadata_{<NOMBRE_DE_METADATOS>}	Se refiere al valor de metadatos para la interfaz .

Ejemplo: Dispositivo %name% - Mapeador %mapper% - Ubicación %metadata_{UF}%.

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

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

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

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

Preferencias locales

Tabla 8.28. Formulario de preferencias locales

Campo	Descripción
Tamaño de la página en PDF	Tamaño de la página en los informes en PDF
Limitador de búsqueda	Rellena con un valor positivo entero para limitar tus búsquedas. El valor modelo es 2500.
Primer periodo del horario útil	Define los horarios inicial y final para el primer periodo de horario útil.
Segundo periodo del horario útil.	Define los horarios inicial y final para el segundo periodo de horario útil.

Proyección

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

QoS

Selecciona **Sí** para habilitar los procesos `ciscoPolicyMapper` y `qos_d`. También necesitas seleccionar el tiempo en el que estos procesos se ejecutarán.

El proceso `CiscoPolicyMapper` buscará todas las políticas de QoS en los dispositivos de red Cisco. El dispositivo necesita soportar la MIB `CLASS-BASED-QOS-MIB` y las políticas deben ser configuradas en las interfaces. Ves a la sección QoS.

Los procesos `qos_d` irán a trabajar con resultados del proceso `ciscoPolicyMapper` para crear perfiles `SLAview` necesarios para visualizar las estadísticas de QoS.

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 autenticación del `TRAFip/SLAview`.

Redundancia

Esta sección es utilizada para especificar las configuraciones de redundancia.

Activación

Tabla 8.29. 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.

Campo	Descripción
Tamaño máximo de histórico	Configura el tamaño máximo de histórico en MB. El tamaño de histórico mínimo es de 16MB.
Estado preferencial	Selecciona Maestro o Slave .

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

Conmutación

Tabla 8.30. 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.

Registro de acceso de usuarios

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

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

Tabla 8.31. 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.

Periodo de agregación del informe de alarma avanzada

Esta sección se refiere al informe avanzado de alarma.

Visualiza el inicio del periodo de agregación y configura los horarios iniciales y finales de los periodos.

Para más informaciones sobre la agregación, comprueba la sección Agregación de datos.

Importante

La alteración de los horarios iniciales y finales de los periodos supondrá el reinicio del periodo de agregación.

Formatear

Complete el campo para establecer el número de decimales para los informes.

Tabla 8.32. Formatear

Campo	Descripción
Número de decimales	Introduce un número entero. El máximo valor permitido es 6 .

Informes programados

Configura las características para los informes programados.

Tabla 8.33. Formulario de configuración de los informes programados

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

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

Tabla 8.34. Formulario de configuración del servidor FTP

Campo	Descripción
Servidor	Dirección de IP del servidor.
Directorio	Directorio en el servidor.
Usuario	Usuario a ser autenticado 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 8.35. Formulario de servidor SMPP

Campo	Descripción
Protocolo SMS	Escote la opción SMPP

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

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

Método URL(Uniform Resource Locator)

Este método debe usarse si tienes un gateway http.

SLAview ejecutará una operación http GET utilizando la URL suministrada.

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

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

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

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

SMTP

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

Tabla 8.36. Formulario de parámetros SMTP

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

Campo	Descripción
Remitente SMTP	Configura un remitente para el correo electrónico.

Puedes verificar las configuraciones SMTP antes de guardar: clics 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

Usa la OID sysUpTime para descartar resultados.	Si marcas esta opción, el proceso MIBget buscará la instancia sysUpTime.0 para el dispositivo y descartará todos los resultados si el valor de retorno de esta OID es menor que 300 segundos. Esta condición será considerada un reboot en el dispositivo y los contadores SNMP pueden ser inválidos.
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 Alarmas o traps auto generados por los TELCOMANAGER MIBS.

Tabla 8.37. 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 autenticación 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 autenticación 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 **Autenticación local** activada, en el caso de que sea utilizado el control de acceso externo.

Telcomanager Host Agent

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

Importante

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

- Llamada a procedimiento remoto (RPC)
- Registro remoto

Telcomanager JMX Agent

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

Tema

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

Tabla 8.38. 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 propio 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 8.39. Formulario de API de configuraciones

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

Datos brutos del TRAFip

Configura el acceso a los datos brutos del TRAFip.

Tabla 8.40. TRAFip's raw data form

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

Gest. de MIBs

Selecciona **System** → **MIBs**. En esta sección puedes subir los archivos de MIN y hacer la verificación de errores en ellas.

Usuarios

El sistema posee tres tipos de usuarios:

Tipos de usuario

Administrador	Tiene total acceso al sistema.
Configurador	Puede crear, borrar y editar cualquier objeto del sistema. No puede hacer cambios en las configuraciones del sistema.

Operador Solo puede visualizar el sistema de objetos comprobados e informes.

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

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

Editando usuarios

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

Tabla 8.41. Formulario de usuario

Campo	Descripción
Nombre de usuario	Inicio de usuario.
Nombre	Nombre de usuario.
Contraseña	Contraseña.
Confirmación de contraseña	Repite la contraseña.
Forzar cambio de contraseña	Si está habilitado, en su próximo inicio de sesión, el sistema le pedirá que cambie su 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 correos electrónicos cortos con alarmas. El sistema también puede enviar SMSs a través de integración con portal web. Para configurar el servidor SMS accede Sistema → Parámetros → Servidor SMS .
Autenticación vía token	Seleccione Sí para habilitar la autenticación de token. Este tipo de autenticación es necesaria para usar la aplicación móvil Telcomanager (Network Control).
Permiso para modo seguro	Esta opción está disponible solo para usuarios del tipo Administrador . Selecciona Sí para que el usuario tenga permiso para habilitar el modo seguro en Sistema → Parámetros → Modo seguro . Solo un usuario tendrá este poder.
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.
Autenticación local	Habilita autenticación basada en el Active Directory o TACACS. Para configurar el Active

Campo	Descripción
	Directory accede a Sistema → Parámetros → Active Directory y para configurar el TACACS accede a Sistema → Parámetros → TACACS .
Esconde objetos sin perfil	Esconde objetos mapeados que no están asociados al perfil de usuario.
Habilita informes de alarma avanzada	Habilita informes de alarmas avanzadas para ese usuario.
Tema	Selecciona el tema del usuario. Escoge el Tema Estándar en Sistema → Parámetros → Tema
Grupo de usuario	Asocia este usuario a un usuario del grupo de forma que se restrinja el número de accesos simultáneos al sistema con el grupo.
Idioma	Selecciona el idioma del usuario.
Perfil	Selecciona el perfil de usuario para restringir la alarma y el servicio de visualización de alarma y notificación.
Tipo	Tipos de usuario.
Menú	Usa la opción estándar para restringir al usuario a menús específicos.

Deshabilitar usuarios

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

Grupo de usuarios

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

Procedimiento 8.1. Gestionando grupos de usuarios

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

Tabla 8.42. 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.

Campo	Descripción
Usuarios	Especifica los usuarios que serán colocados en el grupo. Un usuario puede pertenecer solo a un grupo.

Perfiles de usuarios

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

Procedimiento 8.2. Gestionando perfiles de usuarios

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

Tabla 8.43. Formulario de usuario

Campo	Descripción
Nombre	Propiedades del perfil de usuario
Token do bot Telegram	Token obtenido tras crear un bot en el Telegram.
ID del chat Telegram	ID del chat en el que el bot está participando.
Eagle Watcher	Habilita Eagle Watcher. Para obtener más información, acceda al manual de Eagle Watcher.
Usuarios	Asocia los usuarios a un perfil.
Alarmas	Asocia un par de Perfil -> Alarma para este perfil.
Alarmas -> TRAFwatcher -> IP sospechosas	Habilite el envío de mensajes por Telegram y por correo electrónico a IP alarmadas en TRAFwatcher(TRAFwatcher → IPs Sospechosos). Seleccione la opción Traducir IP a subred para agregar el nombre de subred al contenido del mensaje.
Grupos	Selecciona los grupos a los cuales el usuario del perfil tendrá acceso.
Layer	Selecciona las layers a las cuales los usuarios del perfil tendrán acceso en el sistema FRONTlayer .
Alarmas de servicio	Asocia servicios de alarmas a este perfil.

Log de modo seguro

A través de este log es posible saber cuándo y cuál es el usuario que habilitó o deshabilitó el modo seguro en **Sistema** → **Parámetros** → **Modo seguro** .

Tabla 8.44. Formulario de Log de modo seguro

Campo	Descripción
Fecha inicial	Introduce el horario de inicio del periodo en el formato dd/mm/aaaa.

Campo	Descripción
Fecha final	Introduce el horario final del periodo en el formato dd/mm/aaaa.
Usuario	Filtro de usuario que realizó la alteración.

Alarma Consola

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

Tabla 8.45. Columnas Alarmas 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, clicla dos veces en la célula.
CAMINO	Muestra el primer camino de grupo del SLAview para el objeto.
RECURRENCIAS	Muestra el número de recurrencias de la alarma.
SISTEMA	Muestra el sistema de alarma.

Diagnósticos

Información de red

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

Pruebas de conexión

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

Captura de paquetes

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

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

Clica en Nuevo.

Tabla 8.46. 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.

SNMP

Usa este menú para iniciar el diagnóstico SNMP sobre todos los dispositivos configurados en el SLAview.

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.
ICMPAgent.log	proceso de log ICMP.
LinkCacheBuilder.log	Logs del proceso que crean la conexión automática en la aplicación MAPview.
mibcache.log	Logs sobre el proceso de recopilación de la MIB.
MIBget.log	Log de proceso de SNMP polling.
ObjectMapper.log	Log de proceso de mapeo de objeto SNMP.
qos_d.log	Logs del proceso de configuración de perfil del Cisco auto qos.
SlaSumCaching.log	Logs del proceso de resumen del SLAview.
SLAdiscover.log	Logs de los procesos que mapean las conexiones de red vía SNMP para la aplicación.
telco_logrotate.log	Logs del proceso de enrutamiento de log.

ALARMaction.log	Logs del proceso para enviar alarmas y traps, correos electrónicos y notificaciones sms.
ALARMDaemon.log	Logs que procesan incidencias y generan alarmas.
ciscoPolicyMapper.log	Logs del proceso que mapean las políticas de QoS para interfaces en la MIB Cisco Class Based QoS.
dbsync.log	Logs del proceso de sincronización del banco de datos para ambientes redundantes.
Standyd.log	Logs del proceso que controlan los estados de redundancia entre el aparato principal y el de copia de seguridad.
tmsync.log	Logs del proceso de sincronización del dispositivo principal para el de copia de seguridad en ambientes de redundancia.
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** .

Consulta de datos brutos del SLAview

Permite que los usuarios accedan exactamente a los valores recolectados por el recolector SNMP del SLAview.

Tabla 8.47. Consulta de datos brutos del SLAview - Paso 1

Columna	Descripción
Tipo de objeto	Escoge Dispositivo u Objetos mapeados.
Nombre	Nombre del objeto.

Clica en **Filtrar** para aplicar un filtro.

Tabla 8.48. Consulta de datos brutos del SLAview - Paso 2

Columna	Descripción
Objeto	Selecciona objetos filtrados.
Tiempo de inicio	Tiempo mínimo de recolecta.
Tiempo de fin	Tiempo máximo de recolecta.

Clica en **Generar informe**.

Plugins

Área de instalación de complementos adicionales en el sistema. Antes de instalar el complemento, haga clic en el botón de **Upload** o **Descarga**.

1. La acción de carga abrirá una ventana para que cargue el archivo.
2. La acción de descarga descargará el archivo al dispositivo.

Al final de la carga o descarga, será posible instalar la herramienta haciendo clic en el botón de **Instalar**

Una vez instalado, puede desinstalarlo o actualizarlo.

Importante

Solo el administrador puede acceder a esta pantalla.

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, tipo de licencia, la serie de datos históricos y el límite de bits/s o flow/s.

Capítulo 9. Alarmas

Informes

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

Informes eliminados

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

Tabla 9.1. Formulario de informe de alarmas eliminadas

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

Informes consolidados

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

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

Tabla 9.2. Formulario de alarmas consolidadas

Campo	Descripción
Filtro de alarma	Usa expresión regular y clicla 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, clic en cada encabezado de la columna.

Informes avanzados

Estos informes ofrecen flexibilidad para visualización de datos en diferentes formatos, utilizando tecnología de pivotante.

Importante

Este informe es procesado en una base diaria. por eso, cuando generas el informe, el día actual no está disponible.

Tabla 9.3. Formulario de informe avanzado de alarma

Campo	Descripción
Acción	Acción de la alarma.
Instante inicial	Día inicial. Este filtro trabajará en el momento inicial de la alarma.
Instante final	Último día. Este filtro trabajará en el momento final de la alarma.
Excluir fines de semana	Excluir periodo de fin de semana en el informe de datos.
Tipo	Tipo de objeto.
Fabricante	Filtra por el fabricante del objeto. Debes usar expresiones regulares para filtrar.
Tipo de fabricante	Filtra por el tipo de fabricante del objeto. Debes usar expresiones regulares para filtrar.
Día todo	Marca Sí para tener los datos agregados durante todo el día o marca No para tener los datos agregados dentro de los dos periodos configurados

Campo	Descripción
	en Sistema → Parámetros → Informes → Período de agregación del informe de alarma avanzado . Ej.: 9 a.m. a 12 p.m. y 13 p.m. a 18 p.m.
Todos los objetos	Marca Sí para incluir todos los objetos o marca No para incluir solo los objetos alarmados.
Formato de salida	Selecciona HTML, PDF o CSV. Opción disponible solo para informes que no son modelos. Si optas por guardar un modelo, está opción se ignora.
Alarmas	Selecciona las alarmas para este informe.
Grupos	Este campo puede ser usado para filtrar objetos asociados a algunos grupos de root.
Encabezamiento para columnas	Selecciona los ítems que serán posicionados en las columnas del informe.
Líneas de encabezamiento.	Selecciona los ítems que serán posicionados en las líneas del informe.
Agregación de datos	Ves a sección agregación de datos.

Agregación de datos

El campo agregación de datos se utiliza para definir las células de datos del informe. Los campos disponibles son:

- Funciones: función para ser aplicado a los datos. Las funciones disponible son:

Formulario de Agregación de Datos

Disponibilidad	Porcentaje de tiempo mientras la alarma no estuvo activa.
Frecuencia	Porcentaje de tiempo que la alarma estuvo activa.
Suma	Suma a ser aplicada a los periodos de alarma.
Media	Media a ser aplicada a los periodos de alarma.
Cantidad	Número de incidencias de alarmas.
Máximo	Tiempo máximo de incidencias de alarmas
Mínimo	Tiempo mínimo de incidencias de alarmas

- Elemento: Datos para ser aplicados a la función.
- Señalización de alarma: definición de límites para coloración de la célula. Ves a sección señalización de informes avanzados.

Señalización

La opción señalización de alarma es usada para colorear las células de los informes de alarma avanzados.

Cuando usas la señalización en un informe, el informe será coloreado de acuerdo con los límites de la configuración.

Ves a **Alarmas** → **Informes** → **Informes avanzados** → **Señalización** y clicas en el botón Nuevo para crear un nuevo informe de señalización.

Tabla 9.4. Informe de señalización de alarma avanzado

Campo	Descripción
Nombre	Señalización del nombre.
Descripción	Campo de descripción.
Señalización de alarmas	Rellena los niveles de señalización. Ejemplo: <ul style="list-style-type: none"> • 40.00<=critical<=100.00 color red • 20.00<=medium<40.00 color blue • 5.00<=low<20.00 color gray

Modelo de correo electrónico

Introducción

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

Tabla 9.5. 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, clicas en el botón **Preview**.

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

Tabla 9.6. Variables del correo electrónico

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

Variables	Descripción
\$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 Alarmas son personalizados y puedes configurar todos los que quieras.

Para gestionar los niveles de alarma, accede al menú **Alarmas** → **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 clicas en las flechas UP o DOWN localizadas en la esquina superior izquierda.

Añade un nuevo nivel de urgencia

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

Tabla 9.7. 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 Alarmas.
Color del plano de fondo	El color de plano de fondo que se mostrará en la consola Alarmas.
Color de texto	Color del texto que se mostrará en la consola Alarmas.
Aviso sonoro	Habilita el sonido de aviso para esta alarma. El sonido de aviso sonará en la consola del Alarmas, cuando esta función también este habilitada en la consola. Habilítala en Alarmas → 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 **Alarmas** → **Niveles de urgencia de alarma** y clicas 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, clicas en el botón **Borrar**.

Tabla 9.8. 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 un nivel de urgencia, accede a la lista de niveles y clicas 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

Sugerencia

Puede crear alarmas directamente desde el gráfico, simplemente haga clic derecho en el gráfico y luego en la opción **crear una alarma**.

Configuración de alarma fórmula

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

Tabla 9.9. Formulario de alarma fórmula

Campo	Descripción
Nombre	Texto descriptivo para la alarma. Ej.: alto tráfico, sin tráfico HTTP.
Tipo de objeto	Define si la alarma será de Dispositivo , Objeto mapeado u Grupos .
Tipo de alarma	Escoge Fórmula .
Niveles de alarma	Los niveles de alarma construyen una jerarquía de niveles, de modo que si se valida un nivel superior, no es necesario que se validen los siguientes. Cada

Campo	Descripción
	tipo de alarma Fórmula puede tener hasta 10 niveles de fórmula. Cada fórmula tendrá un nivel de urgencia asociado, teniendo prioridad la urgencia del nivel superior sobre los niveles inferiores.
Fórmula	Ves a la sección Fórmula de alarma fórmula.
Variable de resumen	Selecciona la variable de resumen y clicas en Añadir variable .
Varbind	Campo de texto libre que puede ser usado para reconocer las alarmas que son encaminadas como traps.
Descripción	Campo de texto libre que puede usarse para describir las alarmas que son encaminadas como traps.
Correo electrónico	Ves a la sección de acciones.
Dispositivo móvil	Ves a la sección de acciones.
Trap	Ves a la sección de acciones.
Script de acción	Ves a la sección de acciones.
Script	Selecciona un script de Acción de alarma para ser ejecutado.
Enviar correo electrónico después de (minutos)	Ves a la sección de acciones.
Enviar mensajes de dispositivo móvil después de (minutos)	Ves a la sección de acciones.
Enviar trap después de (minutos)	Ves a la sección de acciones.
Ejecutar script de acción tras (minutos)	Ves a la sección de acciones.
Deshabilitar trap para la alarma eliminada	Si la opción "No" es seleccionada, la trap será enviada y la condición de eliminada será indicada en ella. La opción "Sí" evitará que la trap sea enviada.
Deshabilitar mensajes de dispositivo móvil para la alarma eliminada	Si la opción "No" es seleccionada, los mensajes de dispositivo móvil serán enviados y las condiciones de eliminados serán indicadas en ellos. La opción "Sí" después de que los mensajes de dispositivo móvil sean enviados.
Deshabilitar correo electrónico para la alarma eliminada	Si la opción "No" es seleccionada, el correo electrónico será enviado y la condición de eliminado será indicada en él. La opción "Sí" evitará que el correo electrónico sea enviado.
Deshabilitar script de acción para alarma suprimida	Selecciona "Sí" para impedir que el script de Acción de alarma suceda cuando la alarma este eliminada.
Incidencias consecutivas para armar	Escoge el número de incidencias consecutivas de la fórmula de alarma que debe disparar la alarma. No utilizado en alarmas de Trap.
No incidencias consecutivas para desarmar	Escoge el número de no-incidencias consecutivas de la fórmula de alarma que debe desarmar la alarma. No utilizado en alarmas de Trap.

Campo	Descripción
Nivel de urgencia	Selecciona el nivel para la alarma.
Acción de alarma	Asociar los scripts de Acción de alarma que se pueden ejecutar en la pantalla de la consola cuando la alarma está ACTIVO .
Perfil de alarma	Selecciona los perfiles de alarma a los cuales debe pertenecer.

Fórmula de alarma fórmula

Las expresiones en el campo **Fórmula** son escrita en notación infija regular.

Debes escribir las fórmulas siguiendo las siguientes reglas:

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

Procedimiento 9.1. Fórmula de entrada

1. Selecciona las variables y clicla en el botón Añadir variable para transportarla a la caja de fórmula.
2. Edite la fórmula en la caja de fórmula para formar la expresión deseada.

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

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

Observa el ejemplo:

```
((("Input traffic"/"Speed")>=0.9) or (("Output traffic"/"Speed")>=0.9))
and (weekday > 1 and weekday < 7 and time > 09:00)
```

En el ejemplo de encima, la alarma se disparará si el tráfico de entrada o de salida supera el 90% de la utilización y el día de la semana está entre domingo y sábado después de las 9h.

También es posible establecer la alarma metadatos de dispositivos o de objetos mapeados, dependiendo del tipo de objeto de la alarma.

La sintaxis es la siguiente: **this.object.metadata("<nombre_del_metadato>")**.

Observa el ejemplo a continuación:

```
"Perda de pacote" > this.object.metadata("Limite de perda de pacote")
```

Vamos a suponer que la fórmula del ejemplo anterior fue configurada en una alarma con tipo de objeto **Dispositivo**. El metadato de dispositivo "Límite de pérdida de paquete" fue configurado con el valor 5 para un dispositivo X y con el valor 10 para un dispositivo Y. Así, en caso de que la pérdida de paquete del dispositivo X es mayor que 5, la alarma será activada. Análogicamente, si la pérdida de paquete del dispositivo X es mayor que 10, la alarma será disparada para este objeto.

Fórmula de alarmas de grupo

Hay dos tipos de fórmulas para alarmas de grupo: fórmulas de **servicio** o fórmulas basadas en **variables de resumen**.

No está permitido usar ambos tipos de fórmulas en la misma alarma.

Variable de Resumen

Las fórmulas de las alarmas de grupo siguen la misma notación y reglas descritas en la sección anterior. El único cambio es la necesidad de usar un prefijo de tipo de objeto antes del nombre de la variable. Si la variable es de tipo de dispositivo, debe usar el prefijo "D:" antes del nombre de la variable, si el tipo es Objeto asignado, debe usar el prefijo "M:" antes del nombre de la variable.

Procedimiento 9.2. Fórmula de entrada

1. Selecciona las variables y clics en el botón Añadir variable para transportarla a la caja de fórmula.
2. Edite la fórmula en la caja de fórmula para formar la expresión deseada.

Ejemplo 1:

```
(( "M:Input traffic" / "M:Speed" ) >= 0.9) or (( "M:Output traffic" / "M:Speed" ) >= 0.9)
```

En el ejemplo de encima, la alarma se disparará si el tráfico de entrada o de salida supera el 90% de la utilización.

Ejemplo 2:

```
("D:CPU Utilization" > 75)
```

Servicio

Comprueba si tus objetos están alarmados.

En la pantalla de la consola, las alarmas activas que pertenecen a la fórmula se mostrarán cuando se expanda la alarma de servicio.

La sintaxis es la siguiente: `checkAlarms([OPCIÓN],[TIPO_DE_OBJETO],["A1", "A2", "A3", ..., "An"])`

Tabla 9.10. OPCIÓN

OPCIÓN	Descripción
none	Alarma si ningún objeto está alarmado por alguna alarma en la lista.

OPCIÓN	Descripción
any	Alarma si algún objeto está alarmado por alguna alarma en la lista.
partial	Alarma si algún objeto, pero no todos, está alarmado por cualquier alarma en la lista.
all	Alarma si todos los objetos están alarmados por cualquier alarma en la lista.

Tabla 9.11. TIPO_DE_OBJETO

TIPO_DE_OBJETO	Descripción
device	Dispositivo.
mapobj	objeto mapeado.

An a **An** es una lista de nombres de alarmas para verificar sus objetos.

Ejemplo:

```
checkAlarms(any,device,["High temperature","High memory usage"])
```

La alarma anterior se activará si algún objeto es alarmante para cualquiera de las alarmas de la lista (High temperature o High memory usage).

Importante

Para alarmar a un grupo utilizando fórmulas de tipo **Servicio**, es necesario que el grupo tenga habilitado el campo Servicio.

Importante

Para poder usar alarmas para un grupo, es necesario habilitar el resumen del grupo para ello.

Configuración de las alarmas de cambio de comportamiento (Alarmas Históricas)

Las KPIs (Key Performance Indicators) usan cambios de comportamiento de la alarma para las que es posible estabilizar un comportamiento. El principio de la operación de este recurso es estabilizar este comportamiento para cada hora del día y, si la superficie de KPI sufre un cambio repentino durante la hora corriente, el sistema alarmará esta condición.

Lo que debes tener en mente es que algunas variables no son adecuadas para este tipo de análisis. Por ejemplo, el tráfico de interfaz para interfaces cuyo tráfico es esporádico.

Por ello debes usar este recurso para las variables donde el comportamiento es **previsible**.

Buenos ejemplos de uso de este recurso son:

- Interfaces de red con alto volumen de tráfico.
- Uso de CPU para enrutadores con carga significativa.
- Número de conexiones en un servidor web con carga significativa.

Malos ejemplos de uso de este recurso son:

- Red o servidor con errores en general.
- Interfaces de red con tráfico bajo o con volumen imprevisible.

Configuración

Esta alarma está basada en un análisis de tendencias que es ejecutada durante un periodo configurado por el usuario, para cada alarma. La alarma siempre es aplicada al resumen de variables y tiene un factor de tolerancia que irá a ayudar a su perfeccionamiento.

Tabla 9.12. Formulario de cambio de comportamiento

Campo	Descripción
Nombre	Texto descriptivo para la alarma. Ej.: alto tráfico, ningún tráfico HTTP.
Tipo de objeto	Escoge el tipo de objeto deseado para alarmar: Dispositivo , Objeto mapeado u Grupos .
Tipo de alarma	Escoge Alteración de comportamiento .
Variable	Selecciona la variable de resumen y clicla en el botón Añadir variable .
Horario de activación	Ves a sección activación de fórmulas de alarma.
Histórico mínimo (días)	Mínima cantidad de días necesarios para rellenar el periodo de análisis.
Histórico máximo (días)	Máxima cantidad de días permitidos para rellenar el periodo de análisis.
Número de violaciones consecutivas (días)	Ves a la sección Número de violaciones consecutivas.
Factor de tolerancia superior	Ves a la sección Factor de tolerancia.
Factor de tolerancia inferior	Ves a la sección Factor de tolerancia.
Periodo de alarma (minutos)	Ves a la sección Periodo de alarma.
Modo de activación	Define qué factores de tolerancia se considerarán para activar la alarma. Elija entre Ambos , Superior o Inferior .
Valor de protección (%)	Considera un valor mínimo para el umbral que es añadido a los valores esperados.
Proyección basada en el valor medio	Selecciona Sí para que la proyección de los valores máximos y mínimos sea calculada basándose en el valor medio.
Deshabilitar tendencias negativas	Selecciona Sí para que no sean consideradas tendencias negativas para la proyección.
Correo electrónico	Ves a la sección de acciones.
Dispositivo móvil	Ves a la sección de acciones.
Trap	Ves a la sección de acciones.
Script de acción	Ves a la sección de acciones.
Script	Selecciona un script de Acción de alarma para ser ejecutado.

Campo	Descripción
Enviar correo electrónico después de (minutos)	Ves a la sección de acciones.
Enviar mensajes de dispositivo móvil después de (minutos)	Ves a la sección de acciones.
Enviar trap después de (minutos)	Ves a la sección de acciones.
Ejecutar script de acción tras (minutos)	Ves a la sección de acciones.
Deshabilitar trap para la alarma eliminada	Si la opción no es seleccionada, la trap será enviada y la condición de eliminada será indicada en la trap. La opción Sí evitará que la trap sea enviada.
Deshabilitar sms para alarma eliminada	Si la condición no es seleccionada, el sms será enviado y la condición de eliminado será indicada en el sms. La opción Sí evitará que el sms sea enviado.
Deshabilitar el correo electrónico para la alarma eliminada	Si la opción no es seleccionada, el correo electrónico será enviado y la condición de eliminado será indicado en el correo electrónico. La opción Sí evitará que el correo electrónico sea enviado.
Deshabilitar script de acción para alarma suprimida	Selecciona "Sí" para impedir que el script de Acción de alarma suceda cuando la alarma este eliminada.
Incidencias consecutivas para armar	Escoge el número de incidencias consecutivas de la fórmula de alarma que debe disparar la alarma. No utilizado en alarmas de Trap.
No incidencias consecutivas para desarmar	Escoge el número de no-incidencias consecutivas de la fórmula de alarma que debe desarmar la alarma. No utilizado en alarmas de Trap.
Nivel de urgencia	Selecciona el nivel para la alarma.
Acción de alarma	Asociar los scripts de Acción de alarma que se pueden ejecutar en la pantalla de la consola cuando la alarma está ACTIVO .
Perfil de alarma	Selecciona los perfiles de alarma a los cuales debe pertenecer.

Fórmulas de horario de activación

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

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

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

Para restringir la incidencia de alarmas, puedes usar las variables **weekday** y **time** con los operadores definidos. Los valores para weekday deben estar entre 1 (domingo) y 7 (sábado). Para las variables **time**, debes usar HH:MM.

Ejemplo:

1. Rellena el campo **Variable** con: "Tráfico de entrada"
2. Rellena el campo **Varbind** con: > 300000

3. Rellena el campo **Fórmula del horario de activación** con: `weekday > 1 and weekday < 7 and time > 09:00`

Esta alarma se disparará si el tráfico de entrada supera 300000 bps y el día de la semana está entre domingo y sábado después de las 9h.

Número de violaciones consecutivas

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

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

Factor de tolerancia

Este factor es medido en el valor de desvío modelo y es usado para comparar el valor esperado con el valor actual.

El cálculo a seguir se ejecutará para determinar si el valor observado determina un cambio de comportamiento:

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

Onde

N é o fator de tolerância

SD é o desvio padrão da curva

AV é o valor médio para a atual meia-hora

EV é o valor médio esperado para a atual meia-hora

Como se muestra en el gráfico a continuación, el sistema calcula el valor de la media para cada media hora del día.

Una vez que el SLAview posee los valores disponibles para calcular el valor de la media para la media hora actual, este valor es calculado y comparado con el valor esperado, como descrito anteriormente.

En la imagen a continuación, puedes ver el algoritmo que el SLAview utiliza para estimar valores futuros para cada media hora del día. Básicamente ejecuta una aproximación para la función de primer grado usando variables históricas y si los valores futuros actuales caen entre estas funciones, considerando el factor de tolerancia, la alarma es encendida.

Periodo de alarma

El SLAview mostrará una muestra cada 30 minutos o a cada 5 minutos.

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

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

Acciones

Cada vez que el sistema del SLAview procesa un polling de SNMP de 5 minutos, todas las fórmulas de alarma son evaluadas y si se muestran verdaderas, se generarán las incidencias. La alarma se disparará para una condición de alarma solo si el número de incidencias consecutivas límite es superado.

La excepción del comportamiento anterior es el ICMP polling, donde el polling puede suceder cada minuto.

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

Campos de acción

Incidencias consecutivas para armar	Esto representa el número de veces consecutivas en las que el límite es superado.
No incidencias consecutivas para desarmar	Esto representa el número de veces consecutivas en las que el límite no es superado.

Tipos de acciones

Correo electrónico	Correo electrónico enviado al usuario. El servidor SMTP del SLAview debe ser configurado, así como el correo electrónico de cada usuario en el formulario de configuración del usuario. El correo electrónico será enviado después del número de minutos definido en el campo Enviar correo electrónico después de (minutos) , comenzando desde el horario de activación.
Dispositivo móvil (SMS)	Mensajes más cortos que los enviados por correo electrónico. Esta alarma puede ser enviada a un correo electrónico por el gateway de SMS si el campo de SMS está configurado en el siguiente formato: 88888888@operador.com. Si el SMS es un número de teléfono, los protocolos SMPP o HTTP también pueden ser usados para enviar el mensaje. Para hacer esto, necesitas configurar el siguiente ítem: Sistema → Parámetros → Servidor SMS .
Dispositivo móvil (Telegram)	Un mensaje será enviado a un chat del Telegram por un bot. Para configurar esta funcionalidad, debes crear un bot en el Telegram, para hacerlo, una vez en el Telegram, inicia una conversación como el usuario @BotFather. Escoge la opción/newbot y sigue las instrucciones para finalizar la creación del bot. Al terminar anota el token del bot Telegram. Crea un grupo en Telegram y asocia el bot. El grupo debe tener al menos 3 miembros. Accede al formulario de perfil de usuarios, rellena el campo "Token del bot Telegram" y clicas en Validar. Si todo va bien, el campo "ID del chat Telegram" será automáticamente relleno. El mensaje será enviado después de los segundos definidos en el campo Enviar mensaje después de , iniciando por el tiempo de activación de la alarma.
Trap	Una trap se enviará para cada alarma. La trap debe ser interpretada usando la MIB TELCOMANAGER-ALARMANAGER-MIB.my, que está disponible en la lista de mib del SLAview. También debes configurar el servidor para enviar las traps en Sistema → Parámetros . La trap será enviada después del número

de minutos definido en el campo **Enviar trap después de (minutos)**, comenzando desde el horario de activación.

Script de acción

Un Acción de alarma será ejecutado en caso de que la alarma sea activada. La ejecución sucederá cuando se pase el número de minutos configurados en el campo **Ejecutar script de acción tras (minutos)**

Gráfico de alarma de cambio de comportamiento

Una vez que configures una alarma de cambio de comportamiento, un nuevo icono de gráfico, con el subtítulo **Cambio de comportamiento**, estará disponible para todos los objetos que están asociados a aquella alarma.

Este gráfico está disponible para cada alarma configurada para aquel objeto y contiene tres curvas. Una curva es el valor de la media para las variables de resumen y las otras dos curvas son los límites superior e inferior para la generación de la incidencia de alarma.

Configuración de alarmas syslog

Tabla 9.13. Formulario de alarma syslog

Campo	Descripción
Nombre	Texto descriptivo para la alarma.
Tipo de alarma	Escoge Syslog .
Correo electrónico	Ves a la sección de acciones.
Dispositivo móvil	Ves a la sección de acciones.
Trap	Ves a la sección de acciones.
Enviar correo electrónico después de (minutos)	Ves a la sección de acciones.
Script	Selecciona un script de Acción de alarma para ser ejecutado.
Enviar mensajes de dispositivo móvil después de (minutos)	Ves a la sección de acciones.
Enviar trap después de (minutos)	Ves a la sección de acciones.
Ejecutar script de acción tras (minutos)	Ves a la sección de acciones.
Deshabilitar trap para la alarma eliminada	Si la opción "No" es seleccionada, la trap será enviada y la condición de eliminada será indicada en ella. La opción "Sí" evitará que la trap sea enviada.
Deshabilitar 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 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 script de acción para alarma suprimida	Selecciona "Sí" para impedir que el script de Acción de alarma suceda cuando la alarma este eliminada.
Nivel de urgencia	Selecciona el nivel para la alarma.

Campo	Descripción
Filtro de syslog de activación	Selecciona un Filtro de Syslog para activar la alarma
Desactivar por	Escoge Horario o Syslog .
Tiempo de desactivación	Selecciona el horario para desactivar la alarma.
Filtro de syslog de desactivación	Selecciona un Filtro de Syslog para desactivar la alarma
Acción de alarma	Asociar los scripts de Acción de alarma que se pueden ejecutar en la pantalla de la consola cuando la alarma está ACTIVO .
Perfil de alarma del dispositivo	Selecciona los perfiles de alarma a los cuales debe pertenecer.

Gestión de eliminación de alarmas.

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

Para eliminar, sigue el siguiente procedimiento:

1. Ves a la guía **Alarmas** → **Alarmas** y clicas en el botón Alarmas eliminadas.
2. Rellena los campos del filtro de esta forma para seleccionar las alarmas/objetos deseados y clicas en el botón Filtro.
3. Selecciona las alarmas/objetos de la lista.
4. Rellena el campo razón de eliminación si lo deseas.
5. Clicas en el botón Guardar para eliminar las alarmas/objetos seleccionados.

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

Importante

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

Importante

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

Añadiendo metadatos de alarma

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

Clicas 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, clicas en el botón **Borrar**.

Tabla 9.14. 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 clicas 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.

Pueden ser automatizados utilizando las mismas reglas de resumen de perfiles. Define los horarios para la ejecución automática en: **Sistema** → **Parámetros** → **Agentes de asociación** → **Perfil automático de alarma** .

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

Tabla 9.15. Formulario de perfil de alarma

Campo	Descripción
Nombre	Texto descriptivo para un perfil de alarma.
Tipo de objeto	Escoge un tipo de objeto de acuerdo con el objeto que debe ser controlado: Dispositivo u Objeto Mapeado .
Tipo de asociación de objeto	Escoge Manual para asociar manualmente o Automático para usar una regla para asociar.
Alarma de dispositivo	Este campo aparece cuando el Tipo de objeto es Dispositivo . Selecciona las alarmas deseadas para pertenecer al perfil.
Alarma de objeto mapeado	Este campo aparece cuando el Tipo de objeto es Objeto mapeado . Selecciona las alarmas deseadas para pertenecer al perfil.
Dispositivos	Este campo aparece cuando el Tipo de objeto es Dispositivo y el Tipo de asociación de objeto es Manual . Selecciona los dispositivos que serán controlados.
Objetos mapeados	Este campo aparece cuando el Tipo de objeto es Objeto mapeado y el Tipo de asociación de objeto es Manual . Selecciona los objetos mapeados que serán controlados.

Campo	Descripción
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.

Importante

Cuando un objeto o una alarma es asociada, el sistema comprueba si las alarmas son compatibles con los objetos. Si no son compatibles, la configuración no es permitida. Un objeto es compatible con una alarma si tiene todas las variables de resumen de la fórmula de alarma.

Añadiendo metadatos de perfil de alarma

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

Tabla 9.16. 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 clicas en el botón **Metadato** al lado del perfil de la alarma que será configurada.

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

Alarmas de servicio

Introducción

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

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

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

Creando una nueva Alarma de Servicio.

1. Selecciona **Alarmas** → **Alarmas de servicio**. Clica en el botón nuevo para definir un nuevo tipo.
2. Rellena el formulario de acuerdo con las siguientes instrucciones:

Tabla 9.17. Formulario de alarmas de servicio

Campo	Descripción
Nombre	Nombre de la alarma de servicio
Varbind	Variable de una trap para ser enviada cuando la alarma sea activada.
Fórmula	Fórmula de alarma de servicio. La fórmula es construida usando los siguientes campos: Objeto, Nombre y Alarma
Objeto	Tipo de objeto con el que la alarma de servicio está relacionada. Es usado para construir la fórmula.
Nombre	Nombre de objeto escogido en el campo "Objeto". Es utilizado para construir la fórmula.
Alarma	Alarma que será asociada al objeto escogido en los campos "Objeto" y "Nombre". Para aprender más sobre alarmas lee la sección: Alarmas Alarmas.
Correo electrónico	Un correo electrónico será enviado a los usuarios.
Enviar correo electrónico después de	Atraso, en minutos, para enviar un correo electrónico a los usuarios.
Dispositivo móvil	Un SMS y/o un mensaje para un chat Telegram serán enviados.
Enviar SMS y/o mensaje Telegram después de	Atraso, en minutos, para enviar un mensaje de dispositivo móvil a los usuario
Trap	Una Trap será enviada cuando la alarma sea activada.
Enviar trap después de	Atraso, en minutos, para enviar una Trap.
Ejecutar script de acción tras	Atraso, en minutos, para ejecutar script de acción.

Fórmula

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

Añadiendo metadatos de alarmas de servicio

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

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

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

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

mm4_table(ES,Campos de un metadato) mm4_thead(Campo,Descripción) mm4_trow(Nombre,Nombre del metadato.) mm4_trow(Descripción,Descripción del metadato.) mm4_trow(Tipo de dato,Escoge si el metadato será del tipo **Texto**, **Entero** o **Enum**.) mm4_tlastrow(Valores,Este campo solo está disponible si el **Tipo de dato** es **Enum**. Introduce una lista de valores, separándolos por punto y coma (;).)

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

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

Consola

Introducción

El aplicativo Alarmas 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.
- Grupo de usuarios para recibir alarmas.
- Interfaz gráfica para crear alarmas y fórmulas personalizadas.
- Las alarmas pueden emitir sonidos.
- Perfiles de alarma para facilitar la asociación de alarmas a los objetos gestionados.
- Reconocimiento de alarmas y comentarios.
- Eliminación de alarmas para evitar correos electrónicos, mensajes de dispositivo móvil y traps para alarmas repetidas.

Operación de Consola

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

Autenticación

Un usuario debe estar autenticado para acceder al Alarmas.

Control de acceso

Cada usuario recibirá alarmas sobre objetos de acuerdo con las asociaciones de jerarquía del grupo y de las alarmas configuradas en el perfil de usuarios.

Consola

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

Puedes configurar las columnas en **Sistema** → **Usuarios** → **Alarm consola** o haciendo clic en el botón |||.

La consola posee las siguientes columnas:

Tabla 9.18. Alarmas 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 Reconocer 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	Comentarios de la Alarma
CAMINO	Muestra el primer camino de grupo del SLAview para el objeto.
RECURRENCIAS	Muestra el número de recurrencias de la alarma. Para configurar la ventana de tiempo de repetición de alarma, acceda a la pantalla Alarms (Sistema → Parámetros → Alarmas).
SISTEMA	Muestra el sistema de alarma.

Menú de contexto

Haga clic derecho en la alarma deseada para mostrar el menú contextual. Mostrará las siguientes opciones:

Tabla 9.19. Menú de contexto

Columna	Descripción
Suprimir alarmas [S]	Suprime cualquier alarma. Para obtener más información, consulte la sección Suprimir alarmas.
Restablecer alarmas [S]	Elimina la clase Suprimido. Solo disponible para alarmas suprimidas .
Reconocer alarmas [A]	Reconocer alarmas. Para obtener más información, consulte la sección Reconocer alarmas.

Columna	Descripción
Liberar alarmas [A]	Elimina la clase Reconocer, volviendo a la clase anterior. La alarma puede ser liberada por el operador solo por un usuario administrador . Opción disponible para alarmas reconocidas .
Reconocer y comentar alarmas [M]	Reconocer y comentar la alarma. Para obtener más información, consulte la sección Reconocer alarmas.
Comentarios de la Alarma [C]	Opción para escribir un comentario sobre la alarma. Disponible solo si la alarma es Reconocida por el usuario activo.
Registro de eventos [E]	Lista de eventos (cambios) de la alarma seleccionada.
Abrir gráficos [O]	Abrir los gráficos de objetos.
Localizar en el mapa [L]	Abre el mapa que contiene los objetos de alarma. Opción disponible para SLAview SISTEMA y alarmas de grupo .
Informe de datos brutos [R]	Abre el informe de datos brutos. Opción disponible para alarmas de TIPO de Subred .
Informe de tráfico sospechoso [T]	Abre el informe de tráfico sospechoso. Opción disponible para las alarmas del SISTEMA TRAFwatcher .
Eliminar [D]	El Alarmas 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 → Alarmas .
[Diagnósticos] Ping [P]	Pruebas de conexión (Ping). Opción disponible para alarmas de TIPO de Objeto mapeado o Dispositivo .
[Diagnósticos] Traceroute [U]	Pruebas de conexión (Traceroute). Opción disponible para alarmas de TIPO de Objeto mapeado o Dispositivo .
[Diagnósticos] Verificador SNMP [N]	Verificador SNMP. Opción disponible para alarmas de TIPO de Objeto mapeado o Dispositivo .
[Acción] Script de acción de alarma	Haga clic en el botón [Acción] <NOMBRE_ALARMA> para ejecutar el Script de acción de alarma asociado con la alarma.

Las acciones se pueden realizar haciendo clic en la opción del menú contextual o utilizando las teclas de acceso directo.

Suprimir alarmas [S]

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

los correos electrónicos, mensajes de dispositivo móvil y traps. Puedes configurar el comportamiento deseado en este campo en configuración de alarma. Puedes comprobar las operaciones de eliminación de log ejecutadas por los usuarios en informe de alarmas eliminados. Puedes gestionar la lista de eliminación de alarma/objeto en **Alarmas** → **Alarmas** → **Eliminación de alarmas** .

Reconocimiento de alarma [A]


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

Nuevo pestaña


Haga clic en el ícono + para crear nuevas pestañas.

Las pestañas son para que pueda filtrar las alarmas que se mostrarán de acuerdo con el nombre, sistema, objeto y clase.

Cambiar el modo de visualización

Haga clic en el símbolo  para cambiar el modo de visualización. Los modos disponibles son: cuadros o pestañas.

Administrar pestañas

Haga clic en el  para crear, editar, eliminar y abrir las guías.

Habilitar aviso sonoro


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

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

Recargar

El Alarmas sincroniza tus alarmas con el banco de datos del sistema cada 2 minutos. Esta sincronización puede accionarse inmediatamente haciendo clic en el botón Recargar.

Mostrar/Ocultar columnas

Haga clic en  icono para configurar qué columnas se muestran.

Filtro de alarma

Filtra las alarmas.

Detalles de alarma

Clica con el botón derecho del ratón para mostrar los Detalles de alarma. Se mostrará la siguiente información de alarma: Nombre, Nivel de urgencia, Estado de alarma, Hora de Inicial, Hora de Final, Trap, Usuario, Comentarios de la Alarma y otra información de objeto.

Haga clic en el icono junto al número de repeticiones para ver más detalles de las horas de alarma. Para configurar la ventana de tiempo de repetición de alarma, acceda a la pantalla **Alarms (Sistema → Parámetros → Alarmas)**.

Alarmas de servicio

Las alarmas de servicio se pueden ampliar haciendo clic en el botón >.

Las alarmas activas que pertenecen a la fórmula de alarma de servicio se mostrarán como elementos secundarios de la alarma de servicio.

Sugerencia

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

Capítulo 10. Eagle Watcher

Configuración

Esta pestaña muestra la lista de perfiles de usuario que tienen Eagle Watcher habilitado.

Seleccione la opción **Sí** en el campo Eagle Watcher en el formulario **Perfil de usuario** para habilitar Eagle watcher.

El acceso a Eagle Watcher se bloqueará para los usuarios de tipo **Operador** que no tengan Eagle Watcher habilitado en su **Perfil de usuario**.

Haga clic en el botón **Configuración** para abrir la pantalla **Configuración**. En esta pantalla es posible Añadir, editar y eliminar **Vistas**. Los usuarios de tipo **Operador** no tienen acceso a esta pantalla.

Haga clic en el botón **Abrir** para abrir Eagle Watcher con la vista de este perfil de usuario.

Importante

Esta pestaña solo es visible para los usuarios que tienen una **LICENCIA** con Eagle Watcher habilitado.

Importante

Esta pestaña solo es visible para los usuarios del tipo **Configurador** o **Administrador**.

Capítulo 11. NOC display

NOC Display

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

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

Capítulo 12. MapView

Introducción

La herramienta Mapview trabaja junto con el SLAview y traza una representación gráfica de la estructura de los grupos del SLAview.

Los mapas del Mapview son jerárquicos, así como el SLAview. Además, los subgrupos o dispositivos dentro del grupo son representados como iconos gráficos y mudan de color basados en las alarmas.

El Mapview también traza conexiones entre estos elementos, identificando las conexiones basadas en protocolos CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol) y IP, donde las interfaces en la misma subred de 30 bits son consideradas conectadas.

Tipos de conexiones

Principales recursos

- Aplicativo en HTML5 con interfaz gráfica.
- Topología de red jerárquica.
- Fácil navegación con el ratón e interacción por todo el mapa.
- Integración con el Alarmas, lo que permite el filtro de alarma clicando en cualquier objeto del mapa, posibilitando el aislamiento de un problema.
- El mismo elemento de red puede ser asociado a múltiples mapas, habilitando diferentes visiones topológicas de la red.
- Control de acceso basado en el usuario.
- Imagen de fondo configurable.
- Enlace de conexión automática entre elementos de red.
- Tamaño y posiciones editables para cada elemento del mapa.
- Visualización de mapas georreferenciados.

Operación

Navegación en el mapa

Los mapas del Mapview reflejan la estructura de los grupos jerárquicos del sistema SLAview. Puedes navegar a través de esta jerarquía clicando en cada icono con el botón derecho del ratón y abriéndolo.

También puedes navegar en el enlace jerárquico clicando en los enlaces de mapas con el botón derecho del ratón.

Filtro

Puede buscar en el mapa los objetos que desea seleccionar.

Filtro de alarma para el mapa

Este filtro puede accionarse para cualquier mapa. Está localizado debajo de los subtítulos de color del mapa.

Para usar este filtro debes seguir los pasos siguientes:

1. Selecciona el botón Exhibir localizado en la parte inferior de cualquier mapa. En este momento, la ventana de Filtro de Alarma aparecerá.
2. Selecciona las alarmas que deseas filtrar y después sitúalas en la caja de la derecha del Filtro de Alarma.
3. Selecciona la opción **Incluir alarmas** para que estas alarmas aparezcan en el mapa o la opción **Excluir alarmas** para excluirlas del mapa.
4. Clica en el botón OK para aplicar este filtro al mapa en cuestión.

Para deshabilitar este filtro, clica en Limpiar filtro.

Filtro de alarma de objeto

Este filtro puede accionarse para cualquier objeto de cualquier mapa. Al clicar con el botón derecho del ratón en un objeto en el Mapview, se mostrarán opciones como **Filtrar alarmas en el Alarmas** y **Filtrar excluyendo alarmas del Alarmas**.

Ambas opciones abrirán la consola de alarmas, la diferencia es que **Filtrar alarmas en el Alarmas** mostrará solo las alarmas de objeto relacionadas jerárquicamente con ella y **Filtrar excluyendo alarmas del Alarmas** mostrará todas las alarmas **excepto** las del objeto seleccionado y de los objetos relacionados jerárquicamente con ella.

Sugerencia

El filtro de alarma de objeto puede trabajar junto con el filtro de alarma para el mapa. Esta funcionalidad es interesante cuando necesitas comprobar las alarmas referentes a solo un determinado dispositivo o grupo y no a sus objetos subordinados, por ejemplo. En esta situación, la consola de alarmas exhibirá **Filtro habilitado**.

Datos detallados

Haga doble clic en el icono del dispositivo para mostrar una tabla con la siguiente información en sus interfaces:

- Mapeador.
- Nombre.
- Descripción.
- Velocidad.

- IP.
- Alarmas activas.

Haga doble clic en el icono del link para mostrar una tabla con la siguiente información:

- Nombre.
- Mapeador.
- Objeto mapeado.
- Alarmas activas.
- Método de mapeo de topología.

Guardando el mapa

Puedes guardar los siguientes atributos del mapa:

- Posición de tamaño de cada objeto del mapa.
- Posición de tamaño de la fuente para cada objeto del mapa.
- Tamaño de la ventana del mapa.

Para ejecutar esta operación clic en el menú **Configuración** → **Guardar Mapa**.

Cambiando el modo de visualización

Es posible visualizar un mapa georreferenciado usando el menú **Visualización** → **Visualizar como GIS** o el atajo **T**. En él, los objetos están dispuestos de acuerdo con sus latitudes y longitudes.

En caso de dispositivos, la localización geográfica es configurada en el formulario del propio dispositivo en los campos **Latitud** y **Longitud**. Ya los grupos de dispositivos son situados a partir de una media de las localizaciones de los dispositivos pertenecientes al grupo.

Para volver al modo normal de visualización, basta usar nuevamente el atajo **T** o el menú **Visualización** → **Visualizar como imagen**.

Importante

Para visualizar el gráfico de este modo, es necesario registrar una llave suministrada por el MapQuest. Registra esta llave en **Sistema** → **Parámetros** → **Mapa GIS**.

Layout en grid

Para aplicar el layout en grid a los elementos del mapa, clic en el menú **Herramientas** → **Layout en grid**.

Creando y eliminando conexiones

Para crear una conexión entre dos objetos del mapa, clic en los dos objetos con el botón **SHIFT** presionado y clic en el menú **Editar** → **Crear enlaces**.

Para eliminar la conexión, selecciona los dos objetos y clic en el menú **Editar** → **Eliminar enlace** **O** haga clic con el botón derecho en la conexión manual y luego haga clic en **Remover enlace**.

Estilo de conexión

Seleccione la opción **Editar** → **Enlace directo** (o tecla D) para que los enlaces seleccionados estén representados por una línea directa.

Seleccione la opción **Editar** → **Enlace ortogonal** (o tecla O) para que los enlaces seleccionados estén representados por una conexión ortogonal..

Para cambiar el estilo de más de un enlace al mismo tiempo, haga clic directamente en los enlaces deseados mientras presiona la **SHIFT** o haga clic en **Editar** → **Seleccionar todos los enlaces** (tecla A).

Seleccionando objetos

Puedes seleccionar un objeto clicando en él.

Puede seleccionar un área manteniendo presionado el botón **CTRL** mientras arrastra el mouse.

Puede seleccionar más de un objeto haciendo clic en ellos con el botón **SHIFT** presionado.

Para seleccionar todos los objetos simultáneamente, clic en el menú **Editar** → **Seleccionar todos** o utiliza el atajo (A).

Alineando objetos

Puedes alinear automáticamente objetos preseleccionados, accediendo al menú **Herramientas** y escogiendo el alineamiento deseado.

Editando las propiedades del objeto del mapa

Puedes aumentar el tamaño de un objeto seleccionándolo y arrastrando el cuadrado de cambio de tamaño o seleccionándolo y, a continuación, accediendo al menú **Editar** → **Aumentar objetos** o usando el atajo **P**. Para disminuirlo, clic **Editar** o utiliza el atajo (M).

Para editar varios objetos simultáneamente, selecciónalos arrastrando el ratón entorno de ellos y después escoge una de las opciones de encima. Para guardar los cambios es necesario que guardes el mapa.

Editando las propiedades del texto del mapa

Puedes aumentar el tamaño del texto de un objeto seleccionándolo y, a continuación, accediendo al menú **Editar** → **Aumentar fuente** o usando el atajo **F**. Para disminuirlo, clic **Editar** o utiliza el atajo (N).

Para revertir las alteraciones y hacer el texto del objeto volver a su tamaño original, clic en el menú **Editar** → **Tamaño original**. Estate atento al seleccionar esta opción, ya que el tamaño del icono también será alterado.

El texto está situado encima del objeto por configuración estándar, pero puedes alterar esta posición a través del menú **Texto**. Escoge una de las opciones: **Encima**, **Debajo** o **A la derecha** y guarda el mapa.

Cambiando la imagen de fondo

Para abrir el Gestor de Imágenes, clic en **Configuración** → **Imágenes de Mapas**.

Para hacer upload de una nueva imagen en el sistema, rellena el **Nombre del Archivo**, carga la imagen y clic en **Añadir Imagen**.

Puedes visualizarla a través del botón **Visualizar** y borrarla usando el botón **Borrar**.

Para cargar una imagen de fondo para el mapa, clic en la caja de selección a la izquierda de la imagen y cierra el popup.

Sugerencia

Para que la imagen se guarde como fondo de mapa, es necesario guardar el mapa en **Configuración** → **Guardar Mapa**.

Zoom in/out

Clica con el botón derecho del ratón en el área seleccionada del mapa para seleccionar las opciones **Aproximar/Alejar**. La opción **Estado Inicial** vuelve al zoom inicial.

También puedes usar el menú Visualización para seleccionar estas opciones.

También puede arrastrar el cursor del mouse para variar el nivel de zoom.

Ajustar la pantalla

Clica en el botón derecho del ratón en una área vacía del mapa y escoge la opción **Ajustar la pantalla** o usa el atajo **W**.

Esta funcionalidad también puede accederse a través del menú **Visualización**.

Habilitar cambio de tamaño de la imagen

Usando el menú **Visualización** → **Habilitar cambio de tamaño de la imagen** o el atajo **B**, es posible cambiar el tamaño de la imagen de fondo haciendo clic en el cuadrado de cambio de tamaño y luego arrastrando el mouse con el botón presionado.

Haga clic en menú **Visualización** → **Establecer tamaño de la imagen** para desactivar la opción de cambio de tamaño.

Adición de texto y formas geométricas

A través de iconos en el menú de Mapview, puede agregar textos predefinidos y formas geométricas al mapa. Las formas geométricas disponibles son cuadriláteros, círculos y elipses.

Es posible elegir diferentes propiedades para las formas geométricas, como: texto, ancho, altura, diámetro, anchura del trazo, tamaño de letra, color y relleno. Las propiedades del objeto se pueden editar en cualquier momento haciendo clic con el botón derecho del ratón sobre él y eligiendo la opción Propiedades. Para guardar los objetos agregados, es necesario que guarde el mapa en **Configuración** → **Guardar Mapa**.

Capítulo 13. Metadato

Introducción

La herramienta Metadato trabaja junto con los objetos del sistema.

Los **objetos** se pueden asociar a un **metadato** durante su creación o edición.

Creación de un metadato

Para acceder a la página de configuración de metadatos, acceda a la pantalla de configuración del objeto y haga clic en el botón **Metadato**.

Haga clic en el botón (nuevo) para crear un metadatos. Puede ser del tipo **Texto**, **Entero** o **Enum**.

Puede cambiar el metadato cuando desee usar el botón **Editar** y comprobar el historial de cambios mediante el botón **Histórico**.

Para quitar un metadato, haga clic en el botón **Eliminar**.

Tabla 13.1. Formulario de un nuevo metadato

Campo	Descripción
Nombre	Nombre del metadato.
Descripción	Descripción del metadato.
Tipo de dato	Seleccione si el metadato será del tipo Texto , Entero o Enum .
Valores	Este campo sólo está disponible si el Tipo de dato es Enum . Entre una lista de valores, separándolos por punto y coma (;).
Relleno obligatorio	Seleccione SÍ para que sea obligatorio el relleno del campo referente al metadato cuando un objeto es creado o editado.
Mostrar en la lista de objetos	Seleccione SÍ para mostrar el metadato en la pantalla de configuración del objeto.

Para asociar el metadato creado a un objeto, acceda a la lista del objeto y haga clic en el botón **Editar** junto al objeto que se va a configurar.

Capítulo 14. 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 15. Glosario

Siglas

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

Tabla 15.1. 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 Application Services.
WAN	Red de larga distancia. Del inglés, Wide Area Network.