Manual SLAview

Manual SLAview

Índice

Lista de Tabelas

Prefácio

Público alvo

Este manual é designado aos administradores de rede, consultores de rede e parceiros da Telcomanager.

Para entender completamente este manual, o leitor deve ter conhecimento intermediário sobre gerenciamento de redes, protocolo TCP/IP e protocolo SNMP.

Convenções utilizadas neste manual

Este documento utiliza as seguintes convenções:

Tabela 1. Convenções do manual

Item	**Convenções**
Selecionando um item do menu	**Menu → Submenu → Item do menu**
Comandos, botões e palavras-chave	Fonte em **negrito**

Capítulo 1. Introdução

Sobre

SLAview é um gerenciador de sistema de rede focado em análise de performance.

As principais tecnologias utilizadas são protocolo SNMP, protocolo ICMP e Cisco SLA Probes, Telcomanager Software Probes e algoritmos de análise comportamental.

Principais recursos

- Monitoramento de qualquer dispositivo da rede usando protocolos SNMP v1, v2c e v3.
- Acesso a todos os recursos do sistema através de um web browser.
- Visões hierárquicas.
- Captura e relatório de Syslog.
- Plataforma multi-tenant, que fornece isolamento do ambiente do usuário.
- Criação de fórmulas, permitindo que o usuário defina suas próprias KPIs (Key Performance Indicators).
- Alarme de análise de comportamento em qualquer KPI monitorada.
- Arquitetura escalável. O sistema pode crescer no número de elementos coletados pelo uso de appliances coletores remotos e no número de usuários e relatórios suportados pelo meio da implantação de EPMs (Expanded Processing Modules), que são appliances responsáveis por realizar o compartilhamento de carga com o sistema central.
- Alta disponibilidade pode ser oferecida pelo uso de soluções redundantes, em que dois appliances trabalham em HOT-STANDBY.
- Relatórios de projeção.
- Todos os relatórios podem ser salvos como templates, agendados e exportados em formato PDF, HTML e CSV.
- Polling de SNMP online com 10 segundos de intervalo, clicando em qualquer gráfico.
- Exportação de imagem de gráfico em massa.
- Flexibilidade na criação de gráficos.
- Gráfico em HTML5 interativo, com recursos como zoom vertical e horizontal, auto-escala e gráficos agregados.
- Descoberta de objetos SNMP.
- Banco de dados de alta performance para dados históricos armazenados.
- Relatórios Top N para todos os elementos monitorados.
- Relatórios de alarmes avançados que permitem agregação de dados através da técnica de pivoteamento.

- Polling, consolidação e perfis de gráfico.
- Associação de perfis automáticos, facilitando as tarefas administrativas diárias.
- Ferramenta MAP nomeada MAPview, com topologia de recurso de mapeamento e navegação de interface intuitiva.
- Ferramenta ALARMmanager, que permite que os usuários configurem alarmes como uma fórmula com as métricas monitoradas para cada objeto. Os alarmes podem ser visualizados em um console ou enviados por email, SMS e traps SNMP.
- Agente de auto QoS (Quality of Service) desenvolvido para MIB Cisco Class Based QoS

Requisitos mínimos

Estes requisitos são para os computadores que irão acessar o sistema pelo web browser.

Hardware

- Processador Pentium 2 400 MHZ ou superior.
- 128 MB de memória RAM.

Navegador

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

Capítulo 2. Conceitos básicos

SNMP Polling, sumarização e gráficos

A principal tecnologia empregada no sistema do SLAview é o protocolo SNMP (Simple Network Management Protocol).

O SLAview é capaz de realizar o monitoramento de qualquer equipamento que rode o agente SNMP ou apenas responda ao ping de consulta.

O protocolo SNMP trabalha com a MIB (Management Information Base) do equipamento. A MIB é um banco de dados que pode ser consultado para fornecer informação de configuração e performance. O agente SNMP controla o acesso à MIB e responde às consultas ao seu banco de dados.

O sistema SLAview possui um processo de polling muito flexível. Ele pode mapear instâncias de uma ampla variedade de objetos nos arquivos de MIB, como interfaces de rede, processadores, unidades de armazenamento e muitos outros. O mapeamento de objetos é definido pelo usuário e irá se referir a eles como objetos monitorados ou mapeados. Uma vez que os mapeamentos foram realizados, as instâncias dos objetos encontrados podem ser associadas à perfis onde as OIDs que são usadas no processo de polling foram definidas.

O sistema fornece perfis, onde o usuário pode definir fórmulas de sumarização baseadas nas OIDs, que são, na verdade, as métricas ou KPIs que devem ser monitoradas.

Os gráficos também são definidos nos perfis e as curvas são fórmulas baseadas na sumarização de variáveis pré-definidas.

Alarmes

Os alarmes são definidos como fórmulas baseadas na sumarização de variáveis. Você pode definir fórmulas livremente usando a notação infixa.

Capítulo 3. Guia rápido de inicialização

Acessando a interface web

Uma vez que o servidor SLAview é acessado, digitando seu endereço ip no navegador, escolha o sistema SLAview clicando no ícone localizado no canto superior direito da janela.

O acesso inicial no sistema pode ser feito utilizando o usuário **telco_adm** e a senha **sysoper**. Neste ponto, é recomendada uma mudança de senha.

Se a autenticação for bem sucedida, uma tela semelhante a que encontra-se abaixo é mostrada ao usuário.

A sessão pode ser encerrada a qualquer momento clicando no ícone de **Logout** no canto direito superior da janela.

Tela principal do SLAview

A tela principal do sistema é dividida nas seguintes áreas:

Área 1: Menu árvore. Usada para navegar pelos objetos do sistema e configuração dos itens.

Área 2: Display de dados. Usado para mostrar gráficos, relatórios e formas de configuração.

Área 3: Menu principal. Usado para selecionar todos os recursos do sistema.

Área 4: Seleção de gráfico. Usado para selecionar gráficos e propriedades dos objetos.

Área 5: Painel de controle. Usado para acessar as ferramentas dos gráficos.

Área 6: Cabeçalho. Usado para indicar qual usuário está logado, qual está deslogado e trocar entre os sistemas TRAFip e SLAview.

Configurando métricas SNMP nos dispositivos

Para uma implementação de sucesso deste procedimento, os elementos de rede que serão usados devem ter uma community SNMP de leitura configurada.

Procedimento 3.1. Passos de configuração

1. Selecione **Dados históricos** → **Dispositivos** → **Novo dispositivo** e preencha o formulário de acordo com as instruções abaixo:
   a. Nome e endereço de IP de gerenciamento.
   b. Versão SNMP e community como configurados nos elementos de rede.
   c. No campo Mapeador, selecione Interface e também CPU e, em caso de equipamento Cisco, Memória.
   d. Clique no botão Salvar.
2. Espere em torno de 5 minutos para o sistema descobrir os elemento de interface de rede, selecione **Configuração** → **Perfis** → **Objetos mapeados** ,clique no botão Associção de objetos mapeados e preencha o formulário de acordo com as instruções abaixo:
   a. Selecione o tipo de perfil que corresponda ao tipo de interface que você deseja monitorar. Ex: para interface serial Cisco selecione a opção Serial-cisco.
   b. Use o filtro para selecionar a interface. Ex: *Serial*.
   c. Selecione Interface no campo tipo e clique no botão Enviar.
   d. Mova a interface desejada para a caixa da direita.
   e. Use a OID de filtro 1.3.6.1.2.1.2.2.1.7 = 1, marcando a opção Usar index de objeto mapeado. Isto irá filtrar as interfaces *ifAdminStatus up*.
   f. Clique em Enviar e depois Salvar.
3. Espere em torno de 10 minutos e selecione **Dados históricos** → **Dispositivos** → **Dispositivo** . Depois clique no dispositivo criado e verifique os gráficos nas interfaces monitoradas.
4. Repita o mesmo procedimento para CPU e objetos de memória se você estiver monitorando elementos Cisco. No passo 2, o tipo deve ser CPU ou memória.

Monitoramento de alarme

Procedimento 3.2. Passos de configuração

1. Selecione **ALARMmanager** → **Perfis** → Clique no botão Novo.

2. Preencha o nome do perfil e escolha a opção Objetos mapeados no campo Tipos de objeto.

3. Selecione os alarmes que você quer usar. Ex: interface baixa e utilização de banda alta.

4. Selecione os objetos que você quer monitorar. Ex: Router1FastEthernet0/1. Agora, clique no botão Salvar.

5. Selecione **Sistema** → **Usuários**. Clique no botão Novo.

6. Preencha o nome de perfil, selecione os usuários e depois os alarmes que os usuários serão capazes de receber. Clique no botão Salvar para salvar as alterações.

Capítulo 4. Gerador de gráfico Telcomanager

O menu Dados históricos será utilizado para visualizar todos os gráficos do sistema. Abaixo deste menu estão os objetos monitorados do sistema, como dispositivos e interfaces. Quando você clica em um ícone de objeto, seus gráficos serão mostrados na área de seleção de gráficos. Quando você clica em um ícone nesta área, o Telcographer é carregado na área de display de dados.

O Telcographer é um gerador de gráfico altamente interativo escrito em HTML5. As funções desta aplicação serão explicadas abaixo.

Período

O gráfico lê informações do Banco de Dados da Telco, onde todas as informações são gravadas em uma resolução de 5 minutos.

A informação da resolução de 5 minutos está disponível para todo o período de gravação para cada objeto monitorado.

Gráfico diário

Neste período, a informação é apresentada com o maior nível de detalhes. O período de tempo é de 24 horas. Possui uma amostra para cada 5 minutos e 288 amostras no total.

Gráfico semanal

Cada amostra é um valor médio de 6 amostras de 5 minutos, que corresponde a 30 minutos. O período de tempo é de 7 dias com 336 amostras. A curva de máximo é obtida calculando o valor máximo para cada 6 amostras de 5 minutos.

Gráfico mensal

Cada amostra é um valor médio de 24 amostras de 5 minutos, que corresponde a 2 horas. O período de tempo é de 30 dias com 360 amostras. A curva de máximo é obtida calculando o valor máximo para cada 24 amostras 5 minutos.

Gráfico trimestral

Cada amostra é um valor médio de 72 amostras de 5 minutos, que corresponde a 6 horas. O período de tempo é de 90 dias com 360 amostras. A curva de máximo é obtida calculando o valor máximo para cada 72 amostras de 5 minutos.

Gráfico anual

Cada amostra é um valor médio de 288 amostras de 5 minutos, que corresponde a um dia. O período de tempo é de 364 dias com 364 amostras. A curva de máximo é obtida calculando o valor máximo para cada 288 amostras de 5 minutos.

Gráfico bienal

Cada amostra é um valor médio de 576 amostras de 5 minutos, que correspondem a dois dias. O período de tempo é de 728 dias com 364 amostras. A curva de máximo é obtida calculando o valor máximo para cada 576 amostras de 5 minutos.

Gráfico de cinco anos

Cada amostra é um valor médio de 1440 amostras de 5 minutos, que correspondem a 5 dias. O período de tempo é 1820 dias com 364 amostras. A curva de máximo é obtida calculando o valor máximo para cada 1440 amostras de 5 minutos.

Gráfico customizado

Você pode escolher um período customizado para o seu gráfico. Para isso, selecione o período **Personalizado** e defina as datas e horários de início de fim.

Recursos

O Telcographer possui diversos recursos que podem ser acessados através do painel de controle acima do gráfico. Alguns deles podem ser acessados também clicando com o botão direito do mouse em qualquer ponto do gráfico.

Caixa de estatísticas

Ao movimentar o mouse sobre uma curva na legenda do gráfico, será mostrada uma caixa de estatísticas com as seguintes informações: Mínimo, Máximo, Média, Total e Desvio padrão da curva.

Mostrar valor

Este recurso irá fazer com que o ponteiro do mouse mostre os eixos x e y para a posição do ponteiro.

Zoom vertical

Para usar este recurso, siga os passos abaixo:

1. Selecione a opção no menu Opções do painel de controle do gráfico.
2. Pressione e segure o botão do mouse na posição inicial y desejada.
3. Enquanto estiver segurando o botão, mova o cursor do mouse para a posição final y desejada e solte o botão do mouse.

Uma curva

Clique nesta opção no menu Opções do painel de controle do gráfico e depois clique em uma das curvas na legenda. Esta ação irá fazer com que seja mostrado no gráfico apenas a curva selecionada.

Modo relativo

Clique nesta opção no menu Opções do painel de controle do gráfico para mostrar cada curva no gráfico relacionada com as outras curvas. Isso significa que, para cada amostra, o somatório dos dados representa 100%.

Este modo funciona apenas se todas as curvas do gráfico estiverem empilhadas.

Configuração de eixos

Clique nesta opção no menu Opções do painel de controle do gráfico para abrir a janela na qual será possível selecionar as curvas que irão aparecer utilizando a escala direita ou esquerda do eixo x.

Coleta on-line

Você encontrará essa opção ao clicar com o botão direito do mouse no gráfico. Ela vai abrir uma nova janela no navegador onde você será capaz de definir o tempo de refresh e iniciar um polling online para o gráfico.

Associar a Graph Set

Clique com o botão direito do mouse e depois nesta opção para abrir uma caixa onde você será capaz de associar o gráfico a um graphset criado anteriormente.

Salvar imagem

O ícone **Salvar imagem** no painel de controle do gráfico irá salvar o gráfico como uma imagem jpeg.

Tipo de gráfico

Através do menu **Tipo de gráfico** no painel de controle, você pode escolher o tipo de visualização do gráfico: em linha, pizza ou barra.

Gráfico agregado

Clique nesta opção através do menu popup do gráfico para abrir representações agregadas do gráfico. Existem duas opções de gráficos: pizza e barra. Estes gráficos podem ser filtrados por um período do dia. Por exemplo, se você abrir um gráfico em pizza de um gráfico semanal e filtrar das 10:00h às 17:00h, o gráfico em pizza irá representar os dados semanais para aquele período do dia.

Mesmo se você não habilitar o filtro, você pode configurar o período do gráfico usando o campo **Horário útil**. Quando este campo está configurado com **1 dia**, aparece um outro campo: **Últimas horas**, que refere-se às horas que serão consideradas no gráfico. Por exemplo, quando este campo está configurado com o valor 1, isso significa que o gráfico está considerando apenas a última hora. O valor máximo que pode ser configurado é o **24**, que representa as últimas 24 horas.

Dica

Para retirar alguma curva do gráfico, basta clicar nela na legenda.

Aproximar e afastar

Utilize essas funções no menu do popup do gráfico para dar zoom in ou zoom out, respectivamente, na escala do tempo. Por exemplo, utilizando isto em um gráfico anual, é possível dar um zoom in no gráfico diário em um dia particular.

Importante

Essas opções apenas são disponíveis em gráficos do tipo linha.

Exportar

Clique no gráfico com o botão direito do mouse e acesse esta opção. Os dados do gráfico podem ser exportados nos formatos HTML, CSV ou TSV.

Atualização automática

Selecione esta opção para o gráfico ser atualizado automaticamente a cada 5 minutos. Esta opção deve ser previamente habilitada em **Sistema** → **Parâmetros** → **Grafador** , onde você também pode confirar o intervalo de atualização.

Dica

Os gráficos em **Pacotes/s** (pps) e **Bit/s** (bps) possuem uma curva para configuração de sample não aplicada. Logo, para verificar a informação desta curva, passe o mouse sobre a legenda com o nome "**No sample total**".

Teclas

Algumas teclas do seu teclado possuem funcionalidades especiais. Veja abaixo quais são elas e suas descrições.

Tabela 4.1. Teclas

Tecla	Descrição
D	Transforma o gráfico para o modo derivativo.
I	Indica informações detalhadas sobre o gráfico como resolução, curvas, samples e timestamps.
L	Relaciona o timestamp e o valor de cada ponto de uma curva.
N	Muda o formato das curvas do gráfico, uma vez que todas elas estejam empilhadas.
P	Gera uma curva de projeção que considera apenas os pontos entre o intervalo limitado pelas linhas sinalizadas. Quando você move o mouse para baixo, o número de pontos diminui, caso contrário, o número de pontos aumenta.
R	Ajusta o gráfico de forma que ele tenha a resolução máxima.
S	Salva o gráfico como uma imagem no formato PNG.
W	Muda a configuração da curva para waas accell.
Z	Abre o popup de **Violação de Projeção**, uma vez que a Projeção está ativada.
-	Zoom out.
+	Zoom in.
LEFT	Desloca o gráfico para esquerda.
RIGHT	Desloca o gráfico para direita.
*	Gráfico retorna ao seu tamanho normal.

Dica

Você pode converter o tempo em timestamp para data usando o comando **ts2date** na CLI.

Capítulo 5. Dados históricos

Este capítulo descreve os elementos da guia de dados históricos.

Abaixo desta guia você pode acessar todos os dados processados pelos objetos monitorados.

Os dados podem ser acessados através de gráficos e relatórios.

Favoritos

Usando este recurso, cada usuário pode configurar os objetos de interesse para acesso rápido.

Adicionando objetos aos favoritos

Para adicionar objetos aos seus favoritos, simplesmente clique no ícone da estrela dourada mostrado como primeiro elemento da área do gráfico selecionada para o objeto desejado.

Removendo objetos dos favoritos

Para remover objetos dos seus favoritos, simplesmente clique no ícone da estrela dourada como primeiro elemento da área do gráfico selecionada para o objeto desejado.

Grupos

Os grupos são usados para organizar objetos. Os grupos são hierárquicos e podem ter quantos níveis forem necessários.

Grupos podem ser utilizados para restringir acesso do usuário aos objetos monitorados. Ao associar o usuário a um ou mais nós na hierarquia do grupo, o usuário é restrito aos objetos associados a estes grupos ou para grupos abaixo desta hierarquia. Esta associação é realizada quando você configura o usuário

Objetos podem ser associados a grupos manualmente ou automaticamente. Durante a configuração, quando associado manualmente, o formulário de grupos irá mostrar Dispositivos e Objetos mapeados para serem associados. Caso contrário, quando associado automaticamente, o formulário de grupos irá mostrar as regras de associação ao grupo. Estas regras irão ser associadas às condições de associação aos grupos.

Objetos podem ser removidos do grupo automaticamente quando eles não atenderem mais as regras de associação. Esta opção está apenas disponível quando o grupo possui associação automática habilitada. Remoção automática do grupo pode ser configurada em configuração de grupo.

Importante

Se qualquer objeto do grupo retornar um valor NaN, o valor exibido no gráfico do grupo é NaN. A lógica utilizada é A + B + C + NaN = NaN

Procedimento 5.1. Passos de configuração

1. Selecione **Dados históricos** → **Grupos**.
2. Clique no ícone Grupos para abrir o formulário de configuração de grupos. Este formulário permite que você crie grupos raiz, edite os grupos já existentes e crie grupos abaixo do grupo raiz.
3. Clique no botão **Novo** para definir um novo grupo e preencha o formulário.

Table 5.1. Formulário de novo grupo

Campo	Descrição
Nome	Nome de grupo
Grupo superior	O grupo raiz em relação a este. Se nenhum grupo raizt é selecionado, esse grupo será um grupo raiz no sistema.
Associação automática	Associação automática de objeto a este grupo considerando Regras. Quando habilitado, o formulário irá mostrar uma opção para auto remoção de objetos.
Dispositivos	Dispositivos que irão ser colocados nesse grupo.
Objeto mapeado	Objetos mapeados que serão colocados neste grupo.

4. Clique no botão **Salvar**.
5. Para adicionar mais grupos abaixo desse grupo, clique no ícone grupos e depois no ícone Subgrupos localizado na área de seleção do gráfico e repita os passos acima.

Pastas de enlace

As pastas de enlace são usadas para criar grupos automáticos associados aos objetos mapeados representando as conexões no sistema.

Para configurar os grupos formados por subgrupos pertencentes ao grupo de origem na pasta de enlace, o sistema irá checar se existem conexões para cada um e, em caso afirmativo, irá criar grupos para cada lado da conexão com as interfaces que representam essa conexão.

Por exemplo: um grupo 'S', possui dois subgrupos: 'A' e 'B'. 'A' possui o dispositivo 'Da' e 'B' possui o dispositivo 'Db'. A interface 'Ia' pertence a 'Da' e a interface 'Ib' pertence ao 'Db'. 'Ia' e 'Ib' estão conectadas. Uma pasta de enlace 'L' é criada com o grupo de origem 'S'. Dois grupos serão criados abaixo de 'L': 'A' --> 'B' que possuem interface 'Ia' and 'B' --> 'A' que tem a interface 'Ib'.

A visualização é restrita do mesmo jeito que grupos normais.

Procedimento 5.2. Passos de configuraçãos

1. Selecione **Dados históricos** → **Grupos**.
2. Clique no ícone Pasta de enlace para abrir o formulário de configuração.
3. Clique no botão **Novo** para definir uma nova pasta de enlace e preencha a o formulário de nova pasta de enlace.

Table 5.2. Formulário para nova pasta de enlace

Campo	Descrição
Prefixo	Prefixo para ser concatenado ao nome do grupo de origem.
Sufixo	Sufixo para ser concatenado ao nome do grupo de origem.

Campo	Descrição
Criar subgrupo	Se sim, os grupos serão criados recursivamente. Se não, apenas os grupos de root serão criados.
Grupo de destino	Grupo onde o link do grupo será criado.
Grupo de origem	Grupo para buscar conexões.
Regras	Regras para filtrar quais interfaces serão consideradas. Apenas aplicado a nome de interfaces.

4. Clique no botão **Salvar**.

5. Os novos grupos serão criados após a execução do agente da pasta de enlace. A execução do tempo do agente pode ser configurada em parâmetros do sistema.

Dispositivos

Um dispositivo é qualquer elemento de rede que possua um endereço de IP e suporte para protocolos SNMP e ICMP.

Para mapear física e logicamente os dispositivos como interfaces, cpus e outros, o sistema possui um processo de mapeamento que roda periodicamente e mapeia (veja a seção: Configuração de mapeadores). Existe um mapeador pré-configurado para mapear interfaces de dispositivos que usam a OID ifDescr para executar esta tarefa.

Procedimento 5.3. Passos da configuração dos dispositivos

1. Selecione **Dados históricos** → **Dispositivos** → **Dispositivo** .

2. Clique no botão **Novo** e preencha o formulário abaixo.

Tabela 5.3. Formulário de novo dispositivo

Campo	Descrição
Nome	Nome do dispositivo.
Descrição	Descrição do dispositivo.
Endereço IP de gerência	Endereço de IP do dispositivo. Este endereço de IP deve responder às consultas SNMP para o monitoramento SNMP e às requisições ICMP echo para monitoramento ICMP.
Tipo	Tipo do dispositivo, o usuário pode usar este campo para categorizar livremente todos os dispositivos configurados.
Fabricante	Nome do fabricante do dispositivo.
Latitude	Coordenada geográfica, no formato de graus decimais (DD, na sigla em inglês), usada para que o dispositivo seja localizado em mapas georreferenciados. Exemplo: -22.9035.
Longitude	Coordenada geográfica, no formato de graus decimais (DD, na sigla em inglês), usada para

Campo	Descrição
	que o dispositivo seja localizado em mapas georreferenciados. Exemplo: -43.2096.
Credencial de SNMP	Escolha uma credencial de SNMP.
Versão do SNMP	Selecione a versão SNMP. Os possíveis valores são: SNMP v1 ou SNMP v2c — Especifica uma community SNMP SNMP v3 — Especifica o tipo de autenticação e seus parâmetros
Community SNMP	Preencha a community SNMP.
Utilizar configuração padrão de SNMP	Esta opção deixa você definir valores que podem ser usados especificamente para este dispositivo. Os valores padrões são especificados na configuração dos parâmetros dos coletores SNMP.
Considerar SysUpTime na coleta	Descarta a coleta se o dispositivo não é permitido por mais de 5 minutos. Previne erros de cálculo.
SNMP Timeout	Tempo limite em segundos para esperar por uma resposta de pacote SNMP. Intervalo de valores: 1-10.
Tentativas SNMP	Número de novas tentativas que serão permitidas para o dispositivo se ele não responder a uma consulta SNMP. Intervalo de valores: 1-10.
Número de OIDs por pacote	Número de OIDs que serão enviadas em cada pacotes SNMP. Intervalo de valores: 1-100.
Taxa máxima de envio de pacotes (pps)	Número máximo de pacotes por segundo que uma coletora SNMP irá enviar para cada dispositivo.
Janela SNMP	Número de pacotes SNMP que serão enviados sem resposta do dispositivo que está sendo polled.
Porta SNMP	A porta SNMP.
Agentes	Esta opção permite que você defina múltiplos agentes SNMP no mesmo endereço de IP e diferentes portas. Agora você pode especificar máscaras OID e a porta SNMP para esta máscara. Isto significa que o coletor SNMP usará a porta UDP especificada se a OID a ser coletada neste dispositivo corresponder à máscara especificada. Exemplo:

Campo	Descrição
	• Prefixo OID .1.3.4.6.9.9.1.2.* Porta SNMP: 163 • Prefixo OID .1.3.4.6.9.9.1.3.* Porta SNMP: 164
Credencial de conexão	Escolha uma credencial de conexão.
Protocolo de conexão	Escolha entre **SSH** ou **Telnet**.
Porta SSH	Quando o **Protocolo de conexão** é SSH, entre com a porta SSH. O valor padrão é **22**.
Porta Telnet	Quando o **Protocolo de conexão** é Telnet, entre com a porta Telnet. O valor padrão é **23**.
Usuário	Usuário para ser usado para acessar o dispositivo. Esta string está disponível como um campo livre %username% para scripts de provisionamento.
Senha do usuário	Senha a ser usada para acessar o dispositivo. Esta string está disponível como um campo livre %passwd% para scripts de provisionamento.
Senha de enable	Senha de enable é usada para acessar o dispositivo. Esta string está disponível como um campo livre %enable_passwd% para scripts de provisionamento.
Habilitar coleta pelo TRAFip	Habilita a coleta pelo TRAFip.
Endereços IP do Netflow exporter	Preencha o endereço de IP que o netflow exporter irá usar para enviar fluxos. Ao lado deste campo, tem um ícone de lupa. Clique nele para preencher automaticamente usando como base o Endereço de IP do dispositivo.
Configuração de sampling rate	Pode ser setada manualmente ou baseada em um fluxo.
Netflow sampling rate	Se você está exportando fluxos, escolha se considerará uma taxa manual configurada ou se detectará a taxa dos registros de fluxos.
Habilitar coleta pelo SLAview	Habilita a coleta pelo SLAview.
Perfis automáticos	Selecione esta opção para habilitar o uso desse dispositivo e seus objetos mapeados em perfis automáticos. A associação só irá ocorrer se o dispositivo ou seus objetos corresponderem às regras de perfil. (Veja a seção de configuração de perfil) .
Habilitar gerência de configuração	Habilita a gerência de configuração pelo CFGtool.
Modo de exportação de configuração	Selecione **Ativo** para exportar a configuração periodicamente de acordo com o tempo configurado em **Sistema** → **Parâmetros** → **Gerência de configuração** . Para exportar a

Campo	Descrição
	configuração usando filtro de trap, selecione **Passivo**.
Método de mapeamento de topologia	Selecione o protocolo que será usado para o mapeamento de topologia. As opções disponíveis são: CDP - Cisco Discovery Protocol, LLDP - Link Layer Discovery Protocol ou ambos. Usando ambos os métodos, o SLAview utilizará o protocolo SNMP para buscar informações destes protocolos nas tabelas MIB dos dispositivos monitorados.
Habilitar provisionamento	Habilitar provisionamento para configurar automaticamente as Cisco IP SLA probes, Telcomanager probes e exportação de Netflow.
Coletor	Associação do dispositivo a um coletor remoto. Este campo está disponível apenas quando a arquitetura distribuída é habilitada.
Script de autenticação	Quando o protocolo de conexão estiver configurado como **Telnet**, você precisa selecionar um script de Login.
Script para provisionamento	Preencha esta opção para provisionamento de Netflow em sistemas com arquitetura distribuída e configuração de probes. Este script será usado para reconfigurar exportação de Netflow para um coletor de backup se o coletor falhar.
Templates de polling	Escolha um template do polling ICMP para o dispositivo. O template de polling permite que você configure os tempos específicos para capturar os dispositivos e medir a disponibilidade deles.
Tipo de dispositivo	Campo usado para escolher um ícone para representar o dispositivo graficamente nos Mapas. É possível escolher entre: Câmera, Firewall, Roteador, Servidor, Switch ou Sem Fio. O tipo padrão é o **Roteador**.
Script de exportação de configuração	Selecione os scripts exportadores de configuração dos tipos running e startup.
Domínio	Associação de domínio do dispositivo.
Grupos	Clique no botão de **Listar** e selecione os grupos desejados para este dispositivo em um ou mais pontos no grupo de hirarquia.
Mapeadores	Selecione o mapeador desejado para mapear objetos, como interfaces e cpus neste dispositivo.(Veja a seção configuração de mapeadores.)
Perfis de alarme	Associa o dispositivo a um perfil de alarme.

Criando um dispositivo utilizando o Assistente

Existe um assistente para criação de um dispositivo que irá guiá-lo e validará cada passo.

1. Selecione **Dados Históricos** → **Dispositivos** → **Assistente** .
2. Preencha os campos de acordo com a tabela acima.
3. Durante a criação, você é capaz de testar a conectividade do equipamento, mapear os objetos do dispositivo e testar os objetos associados aos perfis, por exemplo.
4. Depois disso, você pode visualizar e salvar seu novo dispositivo.

Verificando objetos mapeados para o dispositivo

Clique no ícone de objetos mapeados no menu lateral em árvore para ver todos os objetos mapeados do sistema. Acessando o formulário de cada um, você pode habilitar projeção e adicionar uma descrição para o objeto. Além disso, você pode associá-lo a um perfil e/ou um perfil de alarme.

Também é possível checar o histórico de configuração e deletar o objeto usando, respectivamente, os botões **Histórico** e **Apagar**.

Existe um filtro no topo da página com opções para selecionar objetos localizados e não localizados. Objetos não localizados são objetos mapeados que não foram localizados por um mapeador do dispositivo. Ex: um módulo de interface que foi removido por um roteador irá levar esta interface a um estado de não localizado.

Na área do menu em árvore, abaixo de cada dispositivo, o sistema mostra os seus respectivos objetos mapeados. A cor dos ícones indica as seguintes condições:

Ícone verde	O objeto tem um perfil associado a ele.
Ícone sem cor	O objeto não tem um perfil associado a ele.
Ícone vermelho piscando	O objeto não foi localizado pelo mapeador de processos do objeto.

Importar arquivos de dispositivo

Para importar um arquivo de dispositivo, acesse **Dados históricos** → **Dispositivos**.

Clique no item **Dispositivos** na árvore de menu.

Clique no botão **Importar** e carregue o arquivo.

Um arquivo de dispositivos importados tem os seguintes campos:

Tabela 5.4. Campos do arquivo de dispositivo

Campo	Descrição
Nome	Possíveis caracteres para o campo de nome.

Campo	Descrição
Descrição	Possíveis caracteres para o campo de descrição (opcional).
Endereço IP de gerência	Endereço de IP. Ex.: 10.0.0.1
Versão SNMP	Tipo **1** para versão 1, **2c** para versão 2 e **3** para versão 3.
Community SNMP	Possíveis caracteres para Community SNMP.
Protocolo de conexão	Escreva **SSH** ou **TELNET**.
Usuário	Possíveis caracteres para campo de nome (opcional).
Senha de usuário	Possíveis caracteres para campo de senha (opcional).
Senha de enable	Possíveis caracteres para campo de senha (opcional).
Habilitar coleta pelo TRAFip	SIM para habilitar e NÃO para desabilitar a coleta pelo TRAFip.
Endereço IP do Netflow exporters	Lista de endereço IP separada por vírgula. Ex.: 10.0.0.1,10.0.0.2
Configuração de sampling rate	Terá o valor 0 para manual e o valor 1 para fluxo.
Netflow sampling rate	Valor inteiro maior que 0.
Habilitar coleta pelo SLAview	SIM para habilitar e NÃO para desabilitar a coleta pelo SLAview.
Perfil automático	Selecione **SIM** para habilitar o uso deste dispositivo e seus objetos em um perfil automático.
Tipo de dispositivo	Campo usado para escolher um ícone para representar graficamente o dispositivo nos mapas. Escolha Câmera, Firewall, Roteador, Servidor, Switch ou Sem Fio.

Importante

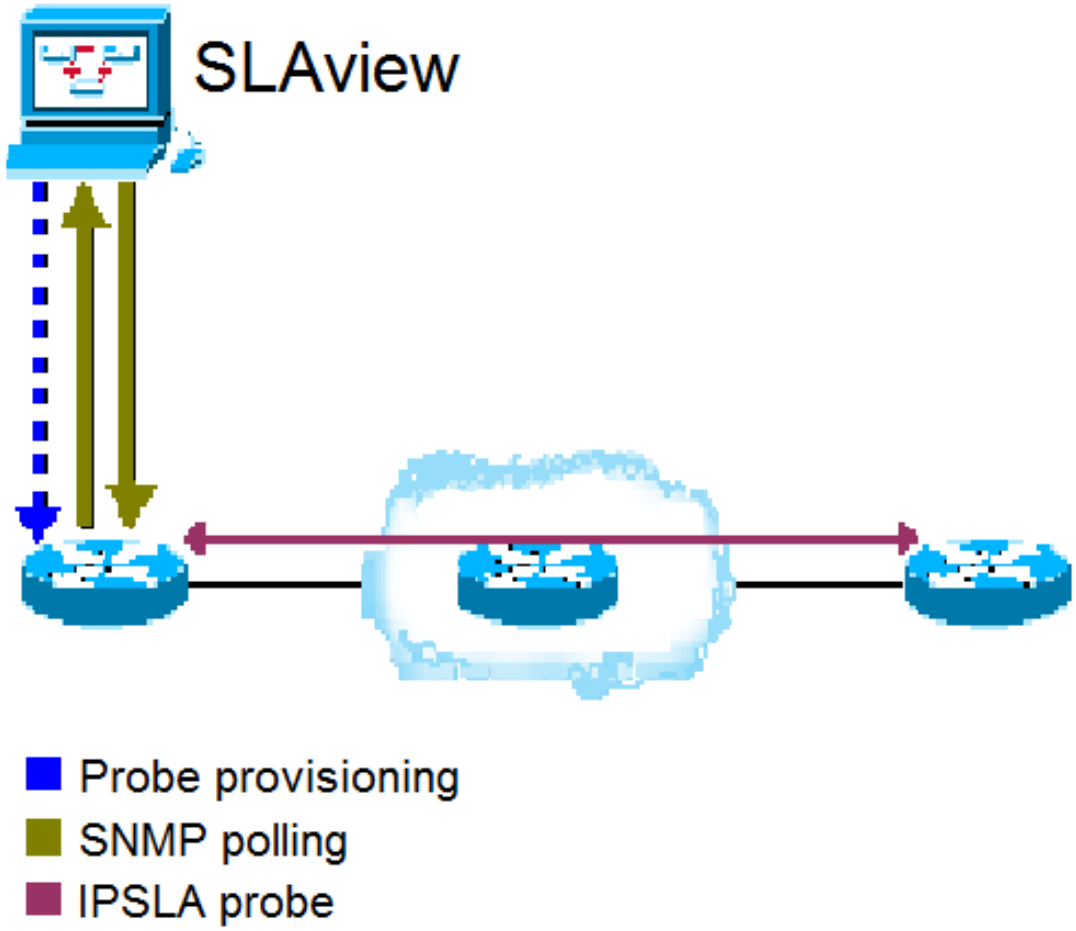
Se o ícone do dispositivo ficar vermelho, significa que todos os exportadores estão indisponíveis.

Probes

Probes são agentes ativos que fazem medições no desempenho da rede. Alguns fornecedores suportam este tipo de agente, como a probe Cisco IP SLA, probes Juniper real-time performance (RTM), probes Telcomanager e muitas outras.

Probes são muito parecidas com objetos mapeados como interfaces e CPUs. A diferença entre eles é que o SLAview é capaz de configurar estes agentes nos dispositivos de rede, executando a configuração de scripts escritos pelo usuário. Isso pode ser feito por qualquer tipo de dispositivo que suporte protocolos SSH ou TELNET para executar esta configuração.

A figura abaixo mostra a relação entre o SLAview e as probes. O sistema executa os seguintes passos para abrir uma probe:



Provisionamento da probe IPSLA

Procedimento 5.4. Passos de provisionamento da probe do SLAview

1. SLAview configura uma probe em um elemento de rede utilizando um template de script ou um novo script escrito por você.

2. SLAview identifica a probe configurada utilizando um mapeador de probe que foi associado ao elemento de rede configurado.

3. Os elementos de rede executam as medições de performance da probe na rede.

4. SLAview coleta OIDs SNMP de acordo com os perfis configurados para a probe.

> **Dica**
>
> Se sua área é responsável por configurar as probes na rede, mas você precisa coletar as medições utilizando o SLAview, você pode tratar a probe como mais um objeto mapeado. Se for uma probe Cisco, tudo que você tem que fazer é associar um mapeador ao dispositivo onde as probes já estão configuradas e depois associá-las ao perfil correto para monitorar as probes que serão mapeadas.

Novas probes podem ser criadas. Há um assistente de criação de probe que irá guiá-lo e validará cada passo da criação.

Procedimento 5.5. Configurando probes pré-existentes

1. Selecione **Dados históricos** → **Probes** → **Assistente** .

2. Preencha o formulário de acordo com as instruções abaixo para cada tipo de probe. Se você escolher rodar seu script durante o assistente, a probe será criada no sistema e será perguntando se você quer associar perfis a ela.

Table 5.5. Telco ICMP/Jitter probe

Campo	Descrição
Nome	Nome da probe.
Dispositivo	Selecione o dispositivo onde a probe será configurada. Veja que o dispositivo deveria ter sido adicionado anteriormente ao sistema.
Tipo de probe	Selecione a probe **Telco/ICMP Jitter**.
Versão do IP	Selecione IPV4 ou IPv6.
Ip de destino	Ip de destino da probe.
Número de pacotes	Número de pacotes de medição a serem enviados pela probe.
Intervalo de pacotes	Intervalo entre a medição dos pacotes.
Tamanho do pacote	Tamanho do pacote medido.
Script de provisionamento	Selecione o script **Probe Telco ICMP Jitter**.
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.

Métricas fornecidas por esta probe:

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

Table 5.6. Telco HTTP probe

Campo	Descrição
Nome	Nome da probe.
Dispositivo	Selecione o dispositivo onde a probe será configurada. Veja que o dispositivo deveria ter sido adicionado anteriormente ao sistema.
Tipo de probe	Selecione a probe **Telco HTTP**.
URL	Preencha a URL para ser testada.
Script de provisionamento	Selecione o script **Probe Telco HTTP**.
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.

Métricas fornecidas por esta probe:

- HTTP round trip latency.
- Availability.

Table 5.7. Telco DNS probe

Campo	Descrição
Nome	Nome da probe.
Dispositivo	Selecione o dispositivo onde a probe será configurada. Veja que o dispositivo deveria ter sido adicionado anteriormente ao sistema.
Tipo de probe	Selecione a probe **Telco DNS**.
Versão do IP	Selecione IPV4 ou IPv6.
Ip de destino	IP de destino da probe.
URL	Preencha a URL para ser traduzida.
Script de provisionamento	Selecione o script **Probe Telco DNS**.
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.

Métricas fornecidas por esta probe:

- DNS round-trip latency answer.
- Availability.

Table 5.8. Telco SSH probe

Campo	Descrição
Nome	Nome da probe.
Dispositivo	Selecione o dispositivo onde a probe será configurada. Veja que o dispositivo deveria ter sido adicionado anteriormente ao sistema.
Tipo de probe	Selecione a probe **Telco SSH**.
Versão do IP	Selecione IPV4 ou IPv6.
Ip de destino	IP de destino da probe.
Porta	Porta TCP onde o serviço SSH está rodando.
Script de provisionamento	Selecione o script **Probe Telco SSH**.
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.

Métricas fornecidas por esta probe:

- Round-trip SSH answer latency.
- Availability.

Table 5.9. Telco TCPConnect probe

Campo	Descrição
Nome	Nome da Probe.
Dispositivo	Selecione o dispositivo onde a probe será configurada. Veja que o dispositivo deveria ter sido adicionado anteriormente ao sistema.
Tipo de probe	Selecione a probe **Telco TCPConnect**.
Versão do IP	Selecione IPV4 ou IPv6.
Ip de destino	IP de destino da probe.
Porta	Porta TCP onde o serviço SSH está rodando.
Script de provisionamento	Selecione o script **Probe Telco TCPConnect**.
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.

Métricas fornecidas por esta probe:

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

Table 5.10. Telco TWAMP probe

Campo	Descrição
Nome	Nome da Probe.
Dispositivo	Selecione o dispositivo onde a probe será configurada. O dispositivo deve ser previamente adicionado.
Tipo de probe	Selecione a probe **Telco Twamp**.
Modo Twamp light	Selecione **Sim** para habilitar o modo TWAMP light.
Versão do IP	Selecione IPV4 ou IPv6.
Endereço de IP de destino	IP de destino da probe.
Número de pacotes	Número de pacotes de medição a serem enviados pela probe.
Intervalo Twamp	Intervalo de envio.
Payload Twamp	Payload, em bytes.
Porta Twamp	Porta do responder. O valor padrão é **862**.
Script de provisionamento	Selecione o script **Probe Telco Twamp**.
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.

Métricas fornecidas por esta probe:

- Round-trip time

- Send time
- Receive time
- Process time

Table 5.11. Cisco IP/SLA Jitter probe

Campo	Descrição
Nome	Nome da probe.
Dispositivo	Selecione o dispositivo onde a probe será configurada. Veja que o dispositivo deveria ter sido adicionado anteriormente ao sistema.
Tipo de probe	Selecione a probe **IP/SLA Jitter**.
Versão do IP	Selecione IPV4 ou IPv6.
Endereço de IP de destino	Endereço de IP de um dispositivo Cisco que suporta recursos de resposta IP SLA.
Porta UDP de destino	Porta UDP de destino para medições de pacotes.
Intervalo inicial [segundos]	Intervalo inicial do dispositivo Cisco que irá esperar para iniciar depois do boot da probe. O uso deste parâmetro é recomendado para evitar que as probes rodem ao mesmo tempo.
Intervalo entre pacotes [milisegundos]	Intervalo entre medições de pacotes.
Número de pacotes	Número de medições de pacotes que serão enviadas a cada momento que a probe rodar.
Endereço de IP de origem	Endereço de IP para ser usado como IP de origem para as medições dos pacotes.
Porta UDP de origem	Porta UDP de origem para medições de pacotes.
Tamanho do pacote	Tamanho de cada medição de pacote.
TAG	Escolha uma tag.
Tipo de serviço (ToS)	Campo TOS para ser definido nas medições dos pacotes.
VRF	Texto para identificar uma VRF. Quando este parâmetro é usado, as medições de pacotes irão passar pela VRF especificada.
Script de provisionamento	Selecione o script **IP/SLA Jitter [ip sla monitor | rtr]** dependendo da sintaxe da IP SLA do dispositivo.
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.

Métricas fornecidas por esta probe:

- One-way and round-trip latency.
- One-way and round-trip jitter.

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

> **Dica**
> Esta probe requer que dispositivo marcado seja um roteador Cisco que suporte recursos de resposta IP SLA. Para habilitar este recurso, apenas digite o comando **ip sla responder** ou **rtr responder** na linha de comando da interface do dispositivo Cisco.

Table 5.12. Cisco IP/SLA ICMP Echo probe

Campo	Descrição
Nome	Nome da probe.
Dispositivo	Selecione um dispositivo onde a probe será configurada. Veja que o dispositivo deveria ter sido adicionado ao sistema anteriormente.
Tipo de probe	Selecione a probe **SLA/ICMP Echo**.
Versão do IP	Selecione IPV4 ou IPv6.
Endereço de IP de destino	Endereço de IP de um dispositivo Cisco que suporta resposta de recursos IP SLA.
Endereço de IP de origem	Endereço de IP a ser usado como IP de origem para medição de pacotes.
Script de provisionamento	Selecione o script **IP/SLA ICMP Echo** [ip sla monitor | rtr]
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.
Versão do IP	Selecione IPV4 ou IPv6.
Endereço de IP de destino	Endereço de IP de um dispositivo Cisco que suporta resposta de recursos IP SLA.
Endereço de IP de origem	Endereço de IP a ser usado como IP de origem para medição de pacotes.

Métricas fornecidas por esta probe:

- Round-trip latency.
- Availability.

Table 5.13. Cisco IP/SLA Path Echo probe

Campo	Descrição
Nome	Nome da probe.
Dispositivo	Selecione o dispositivo onde a probe será configurada. Veja que o dispositivo deveria ter sido adicionado ao sistema anteriormente.
Tipo de probe	Selecione a probe **SLA/Path Echo**.
Versão do IP	Selecione IPV4 ou IPv6.

Campo	Descrição
Endereço de IP de destino	Endereço de IP de um dispositivo Cisco que suporta resposta de recursos IP SLA.
Endereço de IP de origem	Endereço de IP a ser usado como IP de origem para medição de pacotes.
Script de provisionamento	Selecione o script **Probe IP/SLA Path Echo [ip sla monitor | rtr]** dependendo da sintaxe do dipositivo IP SLA.
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.

Métricas fornecidas por esta probe:

- Round-trip latency.

Table 5.14. Cisco IP/SLA UDP Echo probe

Campo	Descrição
Nome	Nome da probe.
Dispositivo	Selecione o dispositivo onde a probe será configurada. Veja que o dispositivo deveria ter sido adicionado ao sistema anteriormente.
Tipo de probe	Selecione a probe **SLA/UDP Echo**.
Versão do IP	Selecione IPV4 ou IPv6.
Endereço IP de destino	Endereço de IP do dispositivo alvo.
Porta UDP de destino	Porta UDP de destino para medição de pacotes.
Endereço IP de origem	Endereço de IP para ser usado como origem para medição de pacotes.
Porta UDP de origem	Porta UDP de origem para medição de pacotes.
Script de provisionamento	Selecione o script **Probe IP/SLA UDP Echo [ip sla monitor | rtr]** dependendo da sintaxe do dispositivo IP SLA.
Script de remoção de probes	Escolha um script para remover a probe do dispositivo.

Métricas fornecidas por esta probe:

- Round-trip latency.
- Availability.

3. Selecione **Configuração** → **Perfis** → **Objetos mapeados** e clique no botão Associar objetos mapeados para associar a probe criada ao perfil adequado. Ex: para Telco-DNS probes, use o perfil Software/DNS e para IP/SLA UDP Jitter probe use o perfil SLA/Jitter.

Tarefas

A lista de tarefas exibe informações a respeito dos provisionamentos de probes.

As tarefas são mostradas de acordo com a data e a hora de execução.

Usando o botão **Script**, é possível ver mais detalhes a respeito do script, como seu nome, o modo de execução e o conteúdo do script.

Já o botão **Exibir** mostra detalhes do provisionamento, como o status e o dispositivo. O resultado do provisionamento pode ser visto clicando novamente no botão **Exibir**.

As tarefas podem ser deletadas a qualquer momento através do botão **Remover**.

Pré-requisitos

- O dispositivo onde as probes serão configuradas devem ter uma CLI (command line interface) acessível pelos protocolos SSH ou Telnet.
- O agente de medida deve ter as variáveis de performance disponíveis via protocolo SNMP.
- A MIB do agente deve ter uma OID cujos valores são únicos e identificam cada instância de probe. Por exemplo, o nome da probe.
- A OID acima deve ser configurada através da interface de linha de comando do dispositivo, para que o mapeador criado seja capaz de unir a probe mapeada com a que foi provisionada.

Relatórios

Templates

Para a maioria dos relatórios disponíveis no sistema, você tem a opção de salvá-los como template.

Salvando

1. Abra o relatório desejado e selecione a opção Salvar template.
2. Preencha os campos abaixo:

Tabela 5.15. Forma do template

Campos	Valores
Nome	Nome do relatório.
Permissão de escrita	Selecione quem pode alterar este relatório. Esta opção de grupos é baseada no grupo de usuários.
Permissão de leitura	Selecione quem pode ler este relatório. Esta opção de grupos é baseada nos grupos de usuários.
Enviar relatório por e-mail	Enviar por e-mail.
Formato do anexo	Escolha o formato desejado: PDF or CSV.

3. Preencha os outros campos de relatório e clique no botão de Enviar.

Depois de executar os passos acima, o relatório salvo estará disponível em **Lista de template** para cada tipo de relatório.

Agendamento

1. Abra a lista de template para o relatório criado ou crie um novo relatório.
2. Selecione a opção Agendar template.
3. Selecione a opção de agendamento apropriada.

Opções de agendamento

- Uma execução: o início e fim de tempo dos dados serão o início e fim do tempo dos relatórios.
- Diário: os dados terão início à 00:00 h e fim às 23:59 h do dia anterior
- Semanal: os dados terão início no Domingo à 00:00 h e fim no Sábado da semana anterior às 23:59 h.
- Mensal: os dados terão início no dia 01 à 00:00 h e fim no último dia do mês anterior às 23:59 h.

Dica

Para agendar um relatório, você deve salvá-lo como template.

Dica

Quando um relatório está pronto, ele é enviado para o e-mail dos usuários. O servidor SMTP deve ser configurado, bem como o email para cada usuário no formulário de configuração do usuário.

Editando

Após o template estar salvo, um botão de **Editar** aparecerá na lista de template e pode ser usado para mudar os parâmetros do relatório.

Visualizando relatórios

Depois do sistema rodar um template, um novo relatório é gerado.

Todas as instâncias do relatório podem ser acessadas através do botão Detalhes para cada template.

Para visualizar uma instância do relatório, siga o procedimento abaixo:

1. Clique no botão **Detalhes** para o template desejado.
2. Escolha o formato de saída desejado, entre HTML, CSV e PDF.
3. Clique no botão **Mostrar** para a instância de relatório desejada.

Gerenciando espaço de disco

O espaço total disponível e atualmente usado pelos templates de relatório é listado abaixo da lista de template.

O sistema tem uma área de armazenamento reservada que é compartilhada por todos os relatórios.

Você pode aumentar ou diminuir este espaço indo em **Sistema** → **Parâmetros** → **Armazenamento de dados** .

Você pode deletar relatórios gerados clicando no botão Detalhes na lista de template, para o template desejado.

Análise de variável

O relatório de análise de variável disponibiliza estatísticas consolidadas para qualquer variável configurada no sistema.

Dica

Para saber como criar uma variável, cheque a seção **Variáveis de sumarização**.

Criando um novo relatório

1. Acesse **Dados Históricos** → **Relatórios** → **Análise de variável** .
2. Escolha **Novo relatório de dispositivo** ou **Novo relatório de objeto mapeado** para ter um relatório de perfil de dispositivo ou um relatório de perfil de objeto mapeado.
3. Selecione os perfis desejados e então clique nas variáveis desejadas para cada função (Max, Min, Média, Soma, Desvio padrão, Percentual do limite e Percentil).
4. Preencha o formulário:

Tabela 5.16. Relatório Análise de variável

Campo	Descrição
Gerar relatório | Salvar template	Escolha **Gerar relatório** para apenas uma execução ou **Salvar template** para salvar o relatório como template.
Filtro de objeto	Filtra por objeto.
Filtro de ifAlias	Filtra pela OID SNMP ifAlias em caso de relatórios de objeto mapeado.
Exibir caminho do grupo	Habilite essa opção para mostrar no relatório o grupo associado.
Instante inicial	Instante inicial para seleção de dados.
Instante final	Instante final para seleção de dados.
Horário útil	Se a opção "Dia todo" estiver marcada, este campo é ignorado, caso contrário os dados são selecionados dentro do intervalo estipulado para cada dia.
Excluir fins-de-semana	Exclui período de fim de semana dos dados do relatório.
Formato de saída	Opção disponível apenas para relatórios que não são templates. Uma vez que o relatório se torna um template, esta opção é ignorada.
Intervalo de exclusão	Adicione uma sinalização e os valores das variáveis que estão dentro do intervalo nela configurado serão ignorados do relatório.
Padrão de substituição de variável	Adicione rótulos às variáveis.

Campo	Descrição
Sinalização	Você pode incluir uma sinalização para colorir uma célula quando o valor de uma variável estiver dentro de um determinado intervalo.
Grupos	Use os botões disponíveis para adicionar ou remover um grupo da lista. Ela irá filtrar objetos abaixo do grupo selecionado na hierarquia de grupo.
Agrupar resultados por grupos	Habilite esta opção para consolidar os resultados por grupo.

Sinalização

A opção sinalização de relatório é usada para colorir as células do relatório Análise de variável.

Quando você usa a sinalização em um relatório, o relatório irá ser colorido de acordo com os limites da configuração.

Vá em **Dados Históricos** → **Relatórios** → **Análise de variável** → **Sinalização** e clique no botão Novo para criar uma nova sinalização.

Tabela 5.17. Sinalização de Análise de variável

Campo	Descrição
Nome	Nome da sinalização.
Descrição	Campo de descrição.
Sinalização de alarmes	Preencha os níveis de sinalização. Exemplo: • 40.00<=critical<=100.00 color red • 20.00<=medium<40.00 color blue • 5.00<=low<20.00 color gray

Top N

Definições

O relatório Top N fornece estatísticas consolidadas para qualquer métrica configurada no sistema.

Um usuário será capaz apenas de visualizar estatísticas para os objetos aos quais tem acesso.

Gerando um novo relatório

1. Acesse **Dados históricos** → **Relatórios** → **Top N** .
2. Escolha **Dispositivo** ou **Objetos mapeados** para ter um relatório de perfil de dispositivos ou um relatório de perfil de objetos mapeados.
3. Escolha o perfil desejado e depois clique na métrica desejada para este perfil.

4. Preencha o formulário:

Tabela 5.18. Relatório Top N

Campo	Descrição
Gerar relatório | Salvar template	Escolha **Gerar relatório** para apenas uma execução ou **Salvar template** para salvar o relatório como template.
Objeto analisado	Automaticamente preenchido com o tipo de perfil selecionado.
Variável analisada	Automaticamente preenchida com o nome da variável selecionada.
Filtro de objeto	Filtra por objeto.
Fabricante	Filtra pelo fabricante do objeto.
Tipo de fabricante	Filtra por tipo de fabricante do objeto.
Filtro de ifAlias	Filtra pela OID ifAlias SNMP, em caso de relatórios de interface.
Instante inicial	Instante inicial para seleção de dados.
Instante final	Instante final para seleção de dados.
Horário útil	Se a opção "Dia todo" estiver marcada, este campo é ignorado, caso contrário os dados são selecionados dentro do intervalo estipulado para cada dia.
Excluir fins-de-semana	Exclui período de fim de semana do relatório de dados.
Todos os perfis	Procure a métrica para todos os objetos que estão sendo monitorados, não apenas para este perfil.
Use percentil	Use percentil para computar resultados dos relatórios.
Exibir percentual de ocupação da banda	Exibe o percentual de ocupação da banda.
Formato de saída	Opção disponível apenas para relatórios não-template. Uma vez que o relatório se torna um template, esta opção é ignorada.
Grupos	Use os botões disponíveis para adicionar ou remover grupo da lista. A lista irá filtrar objetos abaixo do grupo selecionado neste grupo de hierarquia.
Consolidando resultados por grupo	Habilite esta opção para consolidar os resultados por grupo.

Relatório de Projeção

Uma vez que este recurso está ativado, o sistema é capaz de prever o comportamento de qualquer curva de um gráfico e informar a violação de data de um determinado limiar, ou, dada a data, informar o valor da curva.

Configuração

Acesse **Sistema** → **Parâmetros** → **Projeção**

Tabela 5.19. Formulário de configuração de projeção

Campo	Descrição
Graus de liberdade	A ordem polinomial a ser usada. Atualmente, apenas a primeira ordem polinomial é suportada.
Amostragem	Configura a amostragem por dia, semana ou mês para o processo de projeção.
Histórico	Configura o número de amostras que serão analisadas. Ex: Se você escolher o valor **6** para histórico e **semana** para amostragem, o sistema irá analisar 6 semanas atrás para prever a projeção.
Intervalo	Se a opção **Dia todo** estiver marcada, este campo é ignorado. Caso contrário, a projeção vai considerar apenas o intervalo configurado para cada dia.

Habilitando projeção para uma curva gráfica

1. Acesse **Configuração** → **Perfis** → **Objeto mapeado | Dispositivo** .
2. Clique no botão Gráfico para o perfil desejado.
3. Clique no botão Editando curvas para o gráfico desejado.
4. Clique no botão Editar para a curva desejada.
5. Clique **Sim** em **Habilitar projeção** e escolha **Sim** em **Usar configurações padrão** ou customize as configurações para aquela curva.

Importante

Os relatórios de projeção estarão disponíveis um dia depois de habilitar o recurso, uma vez que o processo de projeção roda em uma base diária.

Relatórios gráficos

1. Acesse o gráfico que contém a curva configurada por projeção, clique com o botão direito nele e selecione a opção **Violação de projeção**.
2. Selecione a curva desejada na caixa de popup, insira um valor para ele e clique OK para ter a taxa de crescimento e a data de violação.

Gerando um novo relatório

1. Acesse **Dados históricos** → **Relatórios** → **Projeção** → **Novo relatório** .
2. Preencha o formulário:

Tabela 5.20. Formulário do relatório de projeção

Campo	Descrição
Tipo de objeto	Selecione o tipo de objeto.
Perfil	Selecione o perfil de objeto.
Curva	Selecione a curva do gráfico.
Formato de saída	Opção disponível apenas para não-template de relatório. Uma vez que o relatório se torna um template, essa opção é ignorada.
Limite de violação | Estimativa	Escolhendo **Limite de violação**, você entrará com um valor e o SLAview irá retornar a data de violação desse valor. Se você escolher **Estimativa**, você entrará com uma data e um horário e o SLAview irá retornar o valor da curva nesse momento.
Filtro	Filtra objetos. Você tem que usar expressões regulares para filtrar.
Filtro por dispositivo	Selecione os dispositivos a serem processados ou todos se nenhum for selecionado.
Filtro por grupo	Selecione os grupos a serem processados ou todos se nenhum for selecionado.
Entrada de dados	É possível realizar uma operação (**Adição** ou **Subtração**) sobre os valores da curva para calcular a projeção. Você ainda pode escolher o tipo de entrada (modo **Absoluto** ou **Relativo [%]**). Basta selecionar as opções desejadas e entrar com o valor, em bits/s.

3. Depois de preencher o formulário, clique em **Enviar** para gerar o relatório.

Graph set

O graph set é um relatório gráfico onde você pode visualizar múltiplos gráficos em modo grid na área de visualização dos dados.

Definições

Usuários dos tipos **Operador** e **Configurador** são capazes de gerenciar apenas seus próprios graph sets.

Usuários **administradores** são capazes de visualizar, editar e deletar todos os graph sets, mas não podem criar um graph set para um usuário específico.

Criação

Acesse o caminho **Dados históricos** → **Graph set** → **Novo graph set** .

Tabela 5.21. Criação de graph set

Campo	Descrição
Nome	Nome do graphset.
Descrição	Descrição sobre o graphset.
Tempo entre slides	Tempo em segundos para mudar os slides utilizados na visualização NOC.
Exibir no NOC	Selecione **Sim** para o gráfico estar disponível no NOC display.
Salvar em	Caminho para salvar uma imagem do graphset. Exemplo: C:\Users\Telco\Images
Dimensões	Dimensões da imagem salva.

Adicionando gráficos

1. Acesse qualquer gráfico.
2. Clique no gráfico com o botão direito do mouse.
3. Acesse a opção **Associar a Graph Set** no popup menu e selecione o graph set desejado.

Há uma outra maneira de adicionar gráficos ao graph set. Ela torna possível a adição de gráficos dos tipos barra e pizza. Siga o procedimento abaixo:

1. Acesse o graph set;
2. Clique no símbolo **+**;
3. Preencha os campos (tipo de objeto, objetos, gráficos, tipo de gráfico e período);
4. Clique em **Inserir gráfico**.

Dica

Para desassociar um gráfico, basta clicar no símbolo **X** ao lado dele.

Visualizando um graph set

1. Acesse o caminho **Dados históricos** → **Graph Set**
2. Clique no ícone para o Graph Set desejado que está na árvore do menu.

Editando um graph set

1. Clique em **Dados históricos** → **Graph set**.
2. Escolha um dos seguintes botões:
   - **Dependências** para deletar gráfico de um graph set.
   - **Editar** para mudar os campos de nome e descrição do graphset.

- **Deletar** para apagar o graph set.

Gerando gráficos para um graph set

1. Acesse o graph set;
2. Clique no símbolo ⚙;
3. Selecione uma das opções:
   - **Visualizar gráficos** para configurar o tempo de início para os gráficos mostrados na tela.
   - **Salvar imagens** para gerar e salvar cada gráfico como uma imagem no formato PNG.
4. Preencha os campos:
   - **Início dos dados**: Momento de início do gráfico;
   - **Salvar em**: Caminho para salvar uma imagem do graph set. Exemplo: C:\Users\Telco\Images;
   - **Dimensões**: Dimensões da imagem a ser salva.
5. Clique no botão **Gerar gráficos**.

NOC Display

O NOC display é um modo de visualização de Graph sets. Nele, todos os graph sets habilitados pelo usuário alternam-se automaticamente após um período previamente configurado em cada graph set.

Este recurso é de grande utilidade quando o operador deve checar todos os gráficos do graph set constantemente.

Capítulo 6. Configuração

Perfis

Definições

Os perfis de SLAview foram projetados para permitir que o usuário especifique quais informações devem ser coletadas e como a informação deve ser processada pelo sistema. Em seguida, os perfis podem ser usados por um grupo de dispositivos ou de objetos mapeados.

Os perfis permitem que você especifique variáveis de coleta, fórmulas baseadas em variáveis de coleta (variáveis de sumarização) e gráficos, que contém curvas que são baseadas em fórmulas de variáveis de sumarização.

Depois que os perfis estão configurados, eles podem ser associados a dispositivos ou a objetos mapeados presentes no sistema. Essa associação pode ser manual ou automática.

Mantenha em mente que o SLAview já tem perfis pré-configurados para os cenários mais comuns de monitoramento.

Tipos de perfil

O SLAview suporta 2 tipos de perfis, que são perfis de dispositivo e perfis de objeto mapeado. A principal diferença entre esses dois tipos está no modo com que o coletor SNMP irá processar as variáveis de coleta configuradas para cada tipo.

Tipos

Perfis de dispositivo	O sistema irá coletar exatamente a OID especificada. Exemplo: se você quiser coletar a OID sysUpTime de um dispositivo, então você deve configurar a OID 1.3.6.1.2.1.1.3.0, e NÃO a 1.3.6.1.2.1.1.3. Isso quer dizer que o SLAview irá coletar a instância 0 da OID sysUpTime.
Perfis de objetos mapeados	O Slaview mapeia a instância do objeto que deve ser coletado, assim, quando o SNMP polling ocorre, o valor da instância é anexada à OID. Exemplo: para coletar a OID ifInOctets para uma interface, você deve configurar apenas a OID 1.3.6.1.2.1.2.2.1.10.

Gerenciando perfis

Perfis

- **Criando um perfil**

  Clique no botão Novo na tela de configuração de perfil e especifique os parâmetros abaixo:

  Tabela 6.1. Formulário de perfil

Campo	Descrição
Nome	Nome do perfil.

Campo	Descrição
Associação automática	Selecione **Sim** se os objetos devem ser automaticamente associados ao perfil. Neste caso, as regras apropriadas devem ser selecionadas.
Variáveis de coleta	Entre com as variáveis de coleta que estarão neste perfil. Você pode configurá-las manualmente (SNMP), usar um script para isso (TCS), usar estatísticas pré-definidas (ICMP) ou usar um agente instalado no Windows (THA).
Variáveis de sumarização	Uma variável de sumarização é definida apenas uma vez e pode ser usada uma vez em cada perfil daquele tipo. Este comportamento permite a definição de diferentes fórmulas para a mesma variável de sumarização. Por exemplo, a variável **Utilização de CPU** pode ser definida em um perfil denominado **Cisco** com uma fórmula diferente da de um perfil denominado **Extreme**.
Gráficos	A configuração de gráficos é extremamente flexível. Um gráfico pode ter várias curvas e cada curva baseia-se em fórmulas que podem utilizar as variáveis de sumarização.

Importante

As variáveis de coleta do perfil podem ser mudadas a qualquer momento, mas a remoção de uma OID também causará uma remoção em cascata das variáveis de sumarização e das curvas relacionadas àquela variável de coleta para o perfil e perda de dados históricos das variáveis removidas.

Importante

No caso de algum perfil estar na cor vermelha na lista de perfis, isso quer dizer que não está havendo resposta SNMP.

Gerenciando variáveis de coleta

Para acessar as variáveis de coleta já existentes, clique no botão Coleta na tela de configuração de perfil.

Você pode criar uma nova variável de coleta clicando no botão Novo.

Dica

Lembre-se que também é possível criar variáveis de coleta através do formulário do perfil.

As variáveis podem ser editadas através do botão Editar e removidas através do botão Remover.

1. **Coleta SNMP**

   a. Selecione a opção **SNMP**;

   b. Configure os campos **Nome** e **OIDs**. Você pode preencher esses campos manualmente ou usar a ferramente MIB Browser (para esta, siga os passos a seguir).

      i. Clique no botão Encontrar OID para chamar a ferramenta MIB Browser.

ii. Escolha a MIB desejada e clique no botão Selecionar.

iii. Selecione a OID desejada na árvore de navegação de MIB.

iv. Clique na OID e, em caso de querer testá-la em um dispositivo pré-configurado, selecione o dispositivo na lista no campo MIB Tester e clique no botão SNMP WALK.

v. Clique no botão Inserir para copiar os dados da OID selecionada para o formulário do perfil.

c. Finalmente, clique no botão Adicionar na janela principal para confirmar a operação e a variável de coleta SNMP estará adicionada ao perfil.

2. **Coleta TCS**

a. Selecione a opção **TCS**;

b. Preencha o campo **Nome**;

c. Escolha o script de coleta a ser usado. Para criar um, vá em **Configuração** → **Scripts**.

d. Finalmente, clique no botão Adicionar para confirmar a operação.

3. **Coleta ICMP**

a. Selecione a opção **ICMP**;

b. Preencha o campo **Nome**;

c. Selecione uma das opções: **Jitter**, **Latência** ou **Perda de pacotes**;

d. Finalmente, clique no botão Adicionar para confirmar a operação.

Dica

Você pode configurar os parâmetros dessa coleta em **Sistema** → **Parâmetros** → **ICMP** .

4. **Coleta THA**

a. Selecione a opção **THA**;

b. Preencha o campo **Nome**;

c. Selecione uma das opções: **Status do serviço**, **Performance counter** ou **SQL counter**;

d. Preencha o nome do counter, quando for **Performance counter** ou **SQL counter**;

e. Preencha o nome do serviço;

f. Finalmente, clique no botão Adicionar para confirmar a operação.

Importante

Este tipo de coleta só funcionará em dispositivos com o agente Windows da Telcomanager instalado.

5. **OID wildcards**

   Esta funcionalidade permite que seja realizada uma operação sobre todos os valores retornados na coleta SNMP e imprima o resultado da operação como resultado da coleta.

   Seguem, abaixo, as wildcards suportadas atualmente. Todas elas, com exceção da **%INDEX%**, devem ser anexadas ao final da OID.

Wildcards

%INDEX_WALK_MAX%	Esta wildcard irá buscar o valor máximo retornado na operação SNMP_WALK executada pelo coletor SNMP.
%INDEX_WALK_MIN%	Esta wildcard irá buscar o valor mínimo retornado na operação SNMP_WALK executada pelo coletor SNMP.
%INDEX_WALK_AVG%	Esta wildcard irá fornecer a média dos valores retornados na operação SNMP_WALK executada pelo coletor SNMP.
%INDEX_WALK_COUNT%	Esta wildcard irá fornecer a quantidade de valores retornados na operação SNMP_WALK executada pelo coletor SNMP.
%INDEX_WALK_LAST%	Esta wildcard irá buscar o valor do penúltimo índice retornado. Isto é muito útil para MIBs que retornam um histórico dos últimos N valores coletados.
%INDEX%	Esta wildcard é a **única** que pode ser usada em qualquer posição na OID. Isto faz com que o coletor SNMP substitua o index da OID naquela posição ao invés de anexar o índice no final da OID.

Variáveis de sumarização

Para acessar as variáveis de sumarização já existentes, clique no botão Variáveis de sumarização na tela de configuração de perfil.

Você pode criar uma nova variável de sumarização clicando no botão Novo.

Dica

Lembre-se que também é possível criar variáveis de sumarização através do formulário do perfil.

As variáveis podem ser editadas através do botão Editar e removidas através do botão Remover.

1. **Criando variáveis de sumarização**

Tabela 6.2. Variável de sumarização

Campo	Descrição
Nome	Defina o nome da variável.
Unidade	Escolha uma unidade. Exemplo: pps, bps, volts.
Percentual	Campo utilizado para formatação de relatórios. Selecione essa opção para variáveis que retornam valores em percentual.

Campo	Descrição
Por segundo	Campo utilizado para formatação de relatórios. Selecione essa opção para variáveis que retornam valores de taxa, como tráfego, por exemplo.

Importante

Não se esqueça de clicar no botão **Adicionar**!

2. **Fórmula de variável de sumarização**

Neste passo, você será capaz de definir fórmulas em notação infixa utilizando as variáveis de coleta configuradas no perfil.

Selecione as variáveis de coleta e construa a fórmula com as funções desejadas, seguindo a notação infixa. Em seguida, clique no botão Adicionar.

- **Definições**

  A variável [delta_ts] é referente ao período entre cada SNMP polling, que é fixado em 300 segundos. Isto é, ela representa o intervalo de tempo.

  A função [delta] é aplicada à OID que realiza a diferença entre o valor coletado no momento atual e o valor coletado anteriormente.

  Estes campos [delta_ts] e [delta] são utilizados quando a variável deve ser expressada como uma taxa, como, por exemplo, a entrada de tráfego em uma interface de rede, para a qual temos a seguinte fórmula:

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

  Em outro exemplo, a disponibilidade da interface é expressa como um valor percentual:

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

  Na fórmula acima, se a variável ifOperStatus é igual a 1, a fórmula retornará 100, caso contrário retornará 0.

  Depois de você terminar de editar a fórmula, clique no botão Salvar.

Gráficos

1. **Criação de gráficos**

Tabela 6.3. Gráfico

Campo	Descrição
Nome	Descrição que irá aparecer na área do gráfico selecionada.
Título	Descrição que irá aparecer acima do gráfico.
Unidade	Descrição para o eixo y do gráfico.

Importante

Não se esqueça de clicar no botão **Adicionar**!

2. **Criando curvas para os gráficos**

   Ao passo que você adiciona um gráfico ao perfil, aparecerá no formulário uma seção para a criação de curvas para o gráfico.

   Você pode adicionar quantos gráficos quiser e poderá configurar as curvas relativas à cada um deles.

   - **Tabela 6.4. Curva do gráfico**

Campo	Descrição
Rótulo	Nome da curva.
Tipo de linha	Os tipos de linha 1, 2 e 3 possuem diferentes níveis de espessura. Área irá preencher a área abaixo da curva e Stack irá empilhar as curvas.
Cor	Escolha a cor da curva.
Plotar a curva máxima	A curva máxima é plotada em gráficos semanais, mensais e anuais. Para sempre plotar a curva máxima, o sistema considera a resolução mínima de dados disponíveis, que são sempre os dados de 5 minutos.
Habilitar projeção	Parâmetros padrões da projeção. Acesse a seção de projeção para dicas de como configurar estes parâmetros.
Fórmula	Fórmula em notação infixa regular baseada na sumarização de variáveis.

Importante
Não se esqueça de clicar no botão **Adicionar** e, em seguida, em **Salvar**!

Associação de objetos

- **Associando objetos aos perfis**

  SLAview suporta dois métodos de associação de perfil, que são associações manual e automática. Para o último caso, é necessário criar regras de associação.

Associação de perfis manuais

1. Clique no botão Associar (Objetos mapeados|Dispositivo) na tela de configuração de perfil e preencha o formulário:

   Tabela 6.5. Formulário de associação de perfil

Campo	Descrição
Perfil	Selecione o perfil que você deseja associar aos objetos.
Filtro	Você pode fornecer uma string para filtrar os objetos. Você tem que usar expressões regulares para filtrar.

Campo	Descrição
Tipo	Selecione o tipo de objeto mapeado. Se for um perfil de dispositivo, este campo não estará presente.

2. Clique no botão Enviar.

3. Os objetos disponíveis irão aparecer, em seguida, depois mova os objetos desejados para a caixa da direita

   Faça uso do filtro de OID se você quiser filtrar uma condição SNMP. Por exemplo, use a expressão 1.3.6.1.2.1.2.2.1.7 = 1 e selecione a opção **Usar index de objetos mapeados** para filtrar inerfaces com o ifAdminStatus up.

4. Clique no botão Enviar.

5. SLAview irá mostrar os resultados do teste para os objetos filtrados contra todos as OIDs do perfil. Se você clicar em Salvar agora, apenas os objetos que respondem a todas as OIDs do perfil serão associados. Você pode selecionar a opção **Forçar associação** para os objetos que obtiveram erro ao responder ao perfil, logo eles também serão associados.

Importante

Você deve usar o **Forçar associação** com cautela, porque o SLAview irá tentar coletar as OIDs em objetos que não respondem a elas, o que pode levar a erros de coleta.

Dica

Use a opção **Forçar associação** apenas quando você souber que o objeto irá começar a responder às OIDs em um curto período de tempo. Caso contrário, crie outro perfil sem as OIDs que não respondem e use este perfil nos objetos.

Associação automática de perfis

Este processo habilita operadores a integrar facilmente os elementos de rede ao SLAview, sem ter que se preocupar com configurar todas as associações do perfil.

O processo de associação automática roda todo dia em dois momentos pré-configurados, que podem ser ajustados em **Sistema** → **Parâmetros** → **Agentes de associação**

Procedimento 6.1. Criando regras

- Criando novas regras para usar nos perfis.

Procedimento 6.2. Usando regras nos perfis

1. Clique no botão Editar para o perfil na tela de configuração de perfil.

2. Selecione **Sim** na caixa de seleção **Associação automática**.

3. Mova as regras da caixa da esquerda para caixa da direita.

4. Clique no botão **Salvar**.

Importante

Todas as regras são conectadas por um operador AND. Logo, para um objeto ser associado a um perfil, ele deve obedecer a todas as regras do perfil.

Procedimento 6.3. Testando as regras

1. Clique no botão Executar na tela de configuração de perfil para o perfil desejado.
2. Preencha o formulário de acordo com os dispositivos os quais você deseja testar.
3. Clique em Enviar para iniciar a associação do agente on-demand.
4. Cheque o aquivo de agente log em **Sistema** → **Diagnósticos** → **Arquivos de Log** → **profiled.log** , para ver se o agente está encerrado.
5. Clique no botão Dependências para o perfil para checar se a Regra e os testes de SNMP polling estão ok para os perfis de objeto.
6. Se você tiver erros na coluna SNMP, clique no botão Diagnóstico para checar que OIDs possuem erros.

Importante

Se o objeto não corresponder as regras de perfil, ele não irá aparecer neste ponto porque não foi associado ao perfil.

Comportamento do sistema relacionado aos perfis Automáticos

- A falta de resposta SNMP para qualquer OID do perfil em um objeto no primeiro teste irá evitar o SNMP polling naquele objeto até responder por aquela OID no próximo teste. Os gráficos para aquele objeto irão indicar a falha.
- Se um objeto parar de responder por uma OID durante a operação normal do sistema,as OIDs que responderam irão continuar a ser coletadas e a falha será indicada no gráfico do objeto.
- Se durante a operação normal do sistema um objeto falhar por uma regra, o SNMP polling para aquele objeto será interrompido.

Exportando Perfis

A ferramenta de exportação habilita o usuário a exportar todas as configurações de perfil do SLAview para um arquivo e depois importar de volta as configurações. Este recurso é muito útil para importar perfis pré-definidos da equipe de consultores da Telcomanager.

1. Clique **Configuração** → **Perfis** → **Mostrar** .
2. Clique em Exportar.

Dica

Você pode exportar todos os seus perfis para um único arquivo usando o botão **Exportar todos**.

QoS

Definições

O módulo de monitoramento de QoS foi especificamente desenvolvido para trabalhar com dispositivos que suportam a MIB CLASS-BASED-QoS dos sistema Cisco, portanto, ele só vai funcionar para dispositivos que suportam essa MIB.

Qos pode ser monitorado em outros sistemas, mas eles terão que ser mapeados através do mapeador genérico do SLAview.

Utilizando um agente de mapeamento específico, o SLAview é capaz de identificar todas as políticas de QoS aplicadas naquela interface, criar os perfis apropriados para monitorar essas políticas e executar as associações de perfil.

Habilitando o recurso de QoS

- Acesse **Sistema** → **Parâmetros** → **QoS** e habilite o QoS Cisco Profile, logo o SLAview estará habilitado a criar os perfis de QoS automaticamente.

Habilitando monitoramento de QoS nas interfaces

1. Acesse **Configuração** → **QoS** e crie um novo grupo de **QoS** clicando no botão Novo.

2. Selecione as interfaces desejadas e os monitoramentos e clique no botão Salvar.

A próxima vez que o processo Cisco Policy Mapper e o processo Cisco Auto QoS Profile rodarem, eles irão buscar por políticas de QoS na interface e tentarão criar os respectivos monitoramentos.

Importante
O processo mencionado é executado a toda hora.

Coletoras

Esta seção deve ser usada se você estiver implantando o sistema do modo de arquitetura distribuída.

Para mais detalhes de implantação de arquitetura distribuída consulte a seção de arquitetura distribuída.

Tabela 6.6. Formulário de coletoras

Campo	Descrição
Nome	Nome para identificar um appliance coletor.
Chave	Preencha uma chave com string. Esta string deve ser igual ao campo **chave de coletor** no menu **Sistema** → **Parâmetros** → **Arquitetura distribuída** no appliance coletor.
Endereço de IP	Endereço de IP que o coletar irá usar para acessar o appliance central.
IP do exportador	Endereço de IP usado pelo coletor para receber fluxos do roteador. Este endereço de IP é usado em caso de querer que o sistema reconfigure automaticamente a exportação de netflow no roteador se um appliance coletor falhar.
Senha	Esta senha deve corresponder ao campo **senha** no menu **Sistema** → **Parâmetros** → **Arquitetura distribuída** no appliance coletor.
Coletora de backup	Coletora que irá ser o backup para esta coletora em caso de falha.
Dispositivos	Dispositivos que esta coletora irá coletar.

Importando arquivos de coletoras

Para importar um arquivo de coletoras, acesse **Configuração** → **Coletoras**.

Clique no botão de importar e carregue o arquivo.

Um arquivo de dispositivo importado possui os seguintes campos:

Tabela 6.7. Campos de arquivos de coletoras

Campo	Descrição
Nome	Possíveis caracteres para o campo nome.
Chave	Caracteres alfanuméricos.
Endereço de IP	Endereço de IP. Ex.: 10.0.0.1
Senha	Possíveis caracteres para campo de senha.

Objetos

Nesta tela você pode acessar cada forma de configuração de objeto e os objetos já configurados.

Para alguns tipos de objetos, você tem a opção de fazer um upload de um arquivo de configuração para configurar vários objetos.

Importando arquivos de objetos

1. Acesse **Configuração** → **Objetos** e clique no botão Importar para o tipo de objeto desejado.
2. Faça o upload de um arquivo formatado de acordo com as instruções na tela.
3. Clique no botão Adicionar.
4. Ajuste as configurações e clique no botão Salvar.

Mapeadores

Mapeadores são usados para descobrir objetos relacionados utilizando o protocolo SNMP ou por scripts. Exemplos daqueles objetos são: interface de rede, processadores, bancos de memória, unidades de storage, probes e outros.

Mapeadores podem ter dispositivos associados automaticamente a eles, considerando Regras que devem ser selecionadas como condição

Procedimento 6.4. Criando um mapeador

1. Selecione **Configuração** → **Mapeadores**.
2. Clique no botão Novo item e preencha o formulário como detalhado abaixo:

Tabela 6.8. Formulário de Mapeador

Campo	Descrição
Nome	Nome do mapeador

Campo	Descrição
Ícone	Imagem que será mostrada próxima aos objetos descobertos por este mapeador na árvore do menu. Veja o passo 3 para instruções de customização dessa imagem.
Tipo	Escolha SNMP ou TCS.
Script	Selecione o script. Crie um na seção Scripts.
Remoção automática	Se você quer que os objetos mapeados por este mapeador sejam removidos depois de um certo número de dias consecutivos que eles estão perdidos, selecione **Sim** e preencha o número de dias.
Incluir prefixo	Inclui o nome do mapeador como prefixo para os objetos descobertos por este mapeador.
Instância da OID usada como nome de objeto	Marque esta opção se, ao invés de preencher o nome do objeto com o valor da OID, o mapeador deve preenchê-lo com o valor da instância da OID. Esta opção deve ser utilizada por objetos que não tenham uma OID cujo valor pode representá-los. Logo você pode utilizar uma OID estatística e um mapa de instância de objetos com esta opção.
Interface de rede	Marque esta opção se os objetos que serão descobertos forem interfaces de rede. Isto fará com que o mapeador busque propriedades de interface como ifAlias e ifSpeed.
Probe	Marque esta opção se o mapeador é feito para descobrir probes, logo as probes também serão exibidas no menu **Dados históricos** → **Probes**.
Nome	Nome da OID a ser usada para o mapeamento de objetos.
OID	OID que será utilizada.
MIB	OID MIB.
Filtro por coletora SNMP	Filtra pela resposta da coletora SNMP.
Associação de dispositivos	Habilita associação de dispositivos automáticos ao mapeador considerando as Regras. Quando habilitado, o formulário irá mostrar a opção remoção automática que irá remover os dispositivos associados quando as condições não forem mais conhecidas.
Dispositivos	Selecione os dipositivos associados ao mapeador.

Dica

Abaixo da seção Configuração de Mapeamento, você deve especificar a OID (Object Identifier) de uma MIB (Management Information Base) onde o sistema pode achar nome

de instâncias únicas como valores retornados, logo o objeto pode ser identificado. Esta OID pode ser carregada utilizando a ferramenta MIB Browse clicando no botão procurar OID.

Use o botão Encontrar OID para pesquisar a MIB e preencher os últimos campos do formulário.

3. Configurando os ícones de mapeador.

   a. Selecione no menu **Configuração** → **Mapeadores** e clique no botão Mudar ícones.

   b. Clique no botão Novo ícone.

   c. Preencha o nome do mapeador e faça um upload de um ícone para cada condição de objeto.

   d. Clique no botão Enviar.

Mapeamento cruzado de OIDs

Este recurso permite que você crie um mapeador especificando 2 OIDs. O mapeador irá encontrar o valor para a primeira OID e depois usará como index para achar o valor da segunda OID.

Logo, o mapeador irá mapear o index da primeira OID com o valor da segunda OID.

Este mapeador pode ser usado, por exemplo, para mapear CPUs Cisco, onde você pode especificar as seguintes 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

A primeira OID é a cpmCPUTotalPhysicalIndex do CISCO-PROCESS-MIB e a segunda é a entPhysicalName do ENTITY-MIB, onde você pode achar o nome de cada CPU.

Associando dispositivos aos mapeadores

Depois de configurar um novo mapeador, você deve associá-lo a um dispositivo onde o objeto deve ser descoberto. Esta associação pode ser feita em cada configuração de dispositivo ou clicando no botão Associação de dispositivos na lista de mapeadores.

Exportando e importando mapeadores

O botão **Exportar** exporta toda configuração do mapeador para um arquivo. Para importar essa configuração de volta, você pode utilizar o botão **Importar** e então fazer download desse arquivo.

Manutenção

Você pode criar uma manutenção para suprimir os alarmes ICMP durante a manutenção do Windows na sua infraestrutura.

ICMP polling

O intervalo do ICMP polling do SLAview é flexível e pode ser configurado através dos templates de ICMP polling.

Procedimento 6.5. Ativando dispositivo de polling

1. Associe o dispositivo a um perfil de alarme que possua o alarme **Sem resposta ICMP**. (Veja em **Dados históricos** → **ALARMmanager** → **Perfis**) .
2. Vá para **Configuração** → **ICMP Polling** e crie um novo template de pooling onde você irá:
   - Definir os dias e horas da semana para o polling.
   - Definir o intervalo de polling.
   - Associar os dispositivos que irão usar este template.

EPM (Extended Processing Module)

EPM é outra aplicação em adição ao já existente instalado no cliente. É um módulo extendido da solução de monitoramento.

Necessita ser habilitado em **Sistema** → **Parâmetros** → **EPM** .

EPM é uma solução escalável para os vários usuários acessando o sistema pela interface web, visualizando gráficos e relatório de dados sumarizados. Os dados sumarizados são replicados para as máquinas EPM realizando um acesso de dados mais rápido e dados redundantes.

1. Clique **Configuração** → **EPM**.
2. Clique em Novo para criar uma nova entrada EPM.
3. Preencha os campos nome e endereço IP.
4. Selecione status administrativo.
5. Clique em Salvar.

Tipos de probe

O objeto **Tipo de probe** é destinado a definir os campos que serão provisionados no dispositivo remoto e também está disponível no formulário de configuração de probe.

Procedimento 6.6. Configurando novos tipos de probe

1. Selecione **Configuração** → **Tipos de probe**. Clique no botão Novo para definir um novo tipo.
2. Preencha o formulário de acordo com as instruções abaixo:

Tabela 6.9. Formulário de tipo de probe

Campo	Descrição
Nome	Nome do tipo de probe. Ex: Cisco/IP SLA jitter
Descrição	Texto descritivo.
Atributos	Clique no botão adicionar para cada atributo necessário para configurar esta probe. Ex: IP de destino, número de pacotes

Campo	Descrição	
	Nome	Texto identificando o atributo. Ex: Ip de destino
	Código para provisionamento	Texto para ser usado nos scripts de provisionamento. Ex: ip_dst

3. **Criar um mapeador para mapear os objetos de probe**

   - Selecione **Configuração** → **Mapeadores** e configure o mapeador com a OID que é única e preencha o campo de **Probe**. Ex: Para Telco Probes a OID usada é tmTAPName, que representa o nome da probe.

4. **Associar um novo mapeador ao dispositivo**

   - Quando você está criando um novo mapeador em **Configuração** → **Mapeadores**, configure **Associação de dispositivos** de acordo com suas necessidades. Você pode habilitar a Associação Automática ou a Remoção Automática ou selecionar dispositivos específicos.
   - Para checar a associação, clique em Dependências no menu **Configuração** → **Mapeadores**.
   - Agora, quando uma nova probe é provisionada no dispositivo associado, o sistema irá descobri-la.

5. **Criar um script de provisionamento**

   - Selecione **Configuração** → **Script**. Clique no botão Novo e crie um script para o novo tipo de probe usando os atributos da sintaxe de script de provisionamento.

6. **Criar um novo perfil**

   - Selecione **Dados históricos** → **Probes** → **Assistente** e crie uma nova probe utilizando o tipo de probe criado.
   - Associe o perfil à probe em **Dados históricos** → **Perfis** → **Objetos mapeados** , botão Associar objetos mapeados.

Regras

Criação de regras

1. Selecione **Configuração** → **Regras** e selecione o tipo de regra, se é dispositivo ou objeto mapeado.
2. Clique no botão Novo para criar uma nova regra e preencha o formulário:

Tabela 6.10. Perfil automático de regras

Campo	Descrição
Nome	Nome da regra.
Descrição	Descrição da regra.
Filtro por campos da base de dados	Filtro baseado nos campos da base de dados. Por exemplo, o campo **Nome** refere-se ao nome do objeto e o campo **Mapeador** (somente para regras de objeto mapeado) refere-se ao nome do mapeador.
Filtro por coleta SNMP	Filtra baseado nas OIDs que serão monitoradas quando as regras forem testadas. Selecione a opção **Usar índice de objeto mapeado** quando usando OIDs que devem ser testadas contra objetos mapeados, como, por exemplo, ifConnectorPresent.

Filtro 'No Response'

O filtro de verificação de resposta, que está localizado no 'Filtro por coleta SNMP', consiste em validar um objeto no caso de retornar uma mensagem específica de erro.

Para utilizá-lo, você deve escolher o operador 'No Response' no filtro. No campo 'valor' você deve utilizar um desses valores:

- $nosuchobject$ - É utilizado para validar a resposta 'Sem tal objeto' de um objeto.
- $nosuchinstance$ - É utilizado para validar a resposta 'Sem tal instância' de um objeto.

Trap Receiver

SLAview é capaz de receber, analisar e gerar alarmes baseados em SNMPv1 e V2 traps.

Este módulo é composto por, lógica do trap receiver, alarme de trap e relatórios de trap recebidos.

Uma trap é identificada pela sua OID. Quando uma trap é recebida e se tem uma trap receiver criada utilizando a mesma OID, a lógica do trap receiver será avaliada para decidir se é necessário gerar uma ocorrência de alarme. Esta ocorrência irá apenas ser gerada se tiver algum alarme utilizando a lógica do trap receiver.

Configuração do Trap Receiver

Selecione **Configuração** → **Trap receiver**. Clique em Novo para criar um novo trap receiver.

Tabela 6.11. Configuração Trap Receiver

Coluna	Descrição
Nome	Nome do trap receiver.
Descrição	Descrição sobre o trap receiver.
OID	OID para identificar a trap. Você pode clicar em Busca OID para navegar através do MIB browser.

Coluna	Descrição
MIB	MIB que contém a OID.
Identificar dispositivo pela origem	Escolha se o dispositivo gerado pela trap será identificado pela origem (endereço de IP) ou não. Se não for, você deve escolher uma OID associada ao campo do dispositivo.
Identificação do dispositivo - OID	OID para identificar o dispositivo.
Identificação do dispositivo - Campo	Campos para identificação do dispositivo.

Clique em Salvar para criar o trap receiver.

Importante

A trap pode levar em torno de 5 minutos para ser reconhecida. Isto acontece porque este é o tempo que o sistema precisa para atualizar as configurações.

Lógica do Trap Receiver

O trap receiver possui muitas lógicas associadas a ele. Cada lógica precisa ser associada a um alarme (veja na seção ALARMmanager), para armá-lo e desarmá-lo.

Selecione **Configuração** → **Trap receiver**.

Clique em lógica para listar as lógicas de um trap receiver da lista.

Clique em Novo para criar uma nova lógica.

Tabela 6.12. Lógica Trap Receiver

Coluna	Descrição
Nome	Nome da lógica.
Descrição	Descrição sobre a lógica.
Fórmula	Veja a fórmula do alarme.
Tipo de objeto	Escolha dispositivo ou objeto mapeado. Se for selecionado **Objeto mapeado**, você tem que selecionar um mapeador, uma OID e um campo para identificar o objeto.
Mapeador	Mapeador para identificar o objeto mapeado.
OID	OID para identificar o objeto mapeado.
Campo	Campo para identificar o objeto.

Alarme de Trap

Veja a seção de alarmes ALARMmanager.

Relatório de Trap Receiver

Este relatório lista informações sobre todas as traps recebidas pelo sistema, usando filtros para gerar o conteúdo.

Tabela 6.13. Relatório de Trap Receiver

Coluna	Descrição
Início	Trap recebida no começo.
Fim	Trap recebida no final.
Origem	Origem das traps. Por IP ou hostname.
Varbind	Variável do Trap.
Formato de saída	HTML ou CSV.
Número de linhas	Número de linhas no relatório.

Lógica da fórmula do Trap Receiver

As expressões no campo **Fórmula** são escritas em notação infixa regular.

Você deve construir as fórmulas utilizando as seguintes regras:

- Use parênteses "( )" para precedência das operações.
- Use os operadores lógicos AND e OR.
- Use os operadores de comparação ==,<,>,<=,>= .

Procedimento 6.7. Fórmula de entrada

1. Selecione uma variável acima da caixa de fórmulas e clique em Adicionar para transportá-la para a caixa.
2. Edite a fórmula na caixa de fórmula para formar a expressão desejada.

Scripts

Você pode criar e executar scripts dos tipos: **Mapeador**, **Coletor** e **Provisionamento**.

Os tipos de scripts aparecerão numa caixa de seleção no menu lateral à esquerda da página. Ao selecionar um deles, serão listados os scripts já existentes para este tipo.

Criando scripts

Para criar um novo script, clique no sinal de +. A caixa de texto virá com um exemplo do tipo de script selecionado. Edite a caixa de texto e, após isso, selecione o modo de execução (**Lua**, **Send/Expect** ou **Texto**, dependendo do tipo de script), clique em **Rodar** e selecione o objeto em que o script será executado.

> **Dica**
> Você pode salvar ou remover um script a qualquer momento utilizando os ícones que encontram-se acima da caixa de texto.

Funções

O sistema fornece algumas funções para dar mais poder aos scripts:

- **tmlSnmp.snmpGet**: Executa SNMP GET no dispositivo.
- **tmlSnmp.snmpGet2**: Executa SNMP GET no dispositivo quando a configuração SNMP não é a padrão.

- **tmlSnmp.snmpWalk**: Executa SNMP WALK no dispositivo.
- **tmlSnmp.snmpWalk2**: Executa SNMP WALK no dispositivo quando a configuração SNMP não é a padrão.
- **tmlSSH.sshNew**: Conecta-se a um servidor remoto através de SSH.
- **tmlTelnet.telnetNew**: Conecta-se a um servidor remoto através de Telnet.
- **tmlUtils.removeTerminalEscape**: Remove caracteres de terminais.
- **tmlDebug.log**: Imprime o log na aba **Debug** do **Resultado**.
- **tmlDebug.vardump**: Imprime o log da variável na aba **Debug** do **Resultado**.
- **tmlJson:encode**: Converte uma tabela em Lua para um JSON em texto livre.
- **tmlJson:decode**: Converte um JSON em texto livre em uma tabela em Lua.
- **tmlPing.pingNew**: Envia pacotes através do protocolo ICMP.

As funções em Lua permitidas no scripts são as seguintes:

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

Variáveis

Também existem variáveis que estão disponíveis em todos os scripts e são preenchidas de acordo com o objeto relacionado.

Elas são armazenadas na tabela params (params['variable_name']):

- **params['ipaddr']**: Endereço IP.
- **params['name']**: Nome do dispositivo.
- **params['description']**: Descrição do dispositivo.
- **params['type']**: Tipo do dispositivo.
- **params['snmp']['community']**: Comunidade SNMP do dispositivo.
- **params['snmp']['version']**: Versão SNMP do dispositivo.
- **params['snmp']['timeout']**: SNMP Timeout do dispositivo.
- **params['snmp']['retries']**: Novas tentativas SNMP do dispositivo.
- **params['snmp']['max_per_packet']**: Número de OIDs por pacote.
- **params['snmp']['max_pps']**: Taxa máxima de envio de pacotes (pps).
- **params['snmp']['window']**: Janela SNMP do dispositivo.
- **params['snmp']['port']**: Porta SNMP do dispositivo.
- **params['ifindex']**: ifIndex do objeto mapeado.
- **params['ifdescr']**: Descrição do objeto mapeado.
- **params['username']**: Nome do usuário para autenticação.
- **params['passwd']**: Senha para autenticação.
- **params['enable_passwd']**: Senha de enable para autenticação.
- **params['protocol']**: Protocolo para conexão.
- **params['alarm']['active']**: Status do alarme. Retorna **true** ou **false**.
- **params['alarm']['name']**: Nome do alarme.
- **params['alarm']['urgency']**: Nível de urgência do alarme.
- **params['alarm']['object']['name']**: Nome do objeto alarmado.
- **params['alarm']['object']['description']**: Descrição do objeto alarmado.
- **params['alarm']['object']['type']**: Em alarmes de dispositivo, é o tipo do dispositivo alarmado.
- **params['alarm']['object']['manufacturer']**: Em alarmes de dispositivo, é o fabricante do dispositivo alarmado.
- **params['alarm']['object']['device']['name']**: Em alarmes de objeto mapeado, é o nome do dispositivo ao qual o objeto mapeado alarmado pertence.
- **params['alarm']['object']['device']['description']**: Em alarmes de objeto mapeado, é a descrição do dispositivo ao qual o objeto mapeado alarmado pertence.
- **params['alarm']['object']['device']['type']**: Em alarmes de objeto mapeado, é o tipo do dispositivo ao qual o objeto mapeado alarmado pertence.

- **params['alarm']['object']['device']['manufacturer']**: Em alarmes de objeto mapeado, é o fabricante do dispositivo ao qual o objeto mapeado alarmado pertence.
- **params['blackhole']['ipaddr']**: Anúncio ou remoção do IP em blackhole.

Executando scripts

Para executar algum script já criado, clique nele no menu à esquerda. Você pode editá-lo usando a caixa de texto. Então, clique em **Rodar** e selecione o objeto em que o script será executado.

Além disso, é possível acompanhar os detalhes da última execução usando a aba **Resultado** disposta no final da página.

Dica

É possível salvar as alterações realizadas no script clicando no ícone de salvar, que encontra-se acima da caixa de texto.

Script de Coletor

Crie um Script de coletor para realizar a Coleta TCS.

Este tipo de script permite executar operações matemáticas nos resultados das coletas. Isto torna possível a formatação de valores que serão plotados no gráfico.

Use os exemplos a seguir para criar scripts de coleta em Lua:

```
---------------------- início do 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']

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


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

t = tmlSnmp.snmpWalk('10.0.0.99','public','v2c',
```

```
{[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'] )
```

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

Confira abaixo o exemplo anterior com uso de parâmetros:

----------------------- início do 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'] )
```

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

Observe mais um exemplo:

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

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


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'])

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

Script de Mapeador

Crie um script de mapeador personalizado para mapear um dispositivo usando Mapeador TCS.

O script tem que retornar uma tabela. Cada entrada nesta tabela é formada por outra tabela, que tem as seguintes entradas:

- name
- description
- version
- index

Importante

Todos os campos retornados podem ser uma string.

Use os exemplos a seguir para criar seus scripts de mapeador personalizado:

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

res = {}

res[1] = {['name'] = 'mapper_test',['description'] = 'Interface1',
['version'] = '1',['index'] = '1.3.6.1.2.1.1.3.0'}

return res
```

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


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

r = {}
t = tmlSnmp.snmpWalk('10.0.0.99','public','v2c',
{[1] = '1.3.6.1.2.1.2.2.1.2'})

val = t['1.3.6.1.2.1.2.2.1.2']

for key,value in pairs(val) do
 r[key] = {['name'] = value,['description'] = value,
 ['version'] = '1',['index'] = key}
end

return r

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

Confira abaixo o exemplo anterior com uso de parâmetros:

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

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

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

val = t['1.3.6.1.2.1.2.2.1.2']

for key,value in pairs(val) do
 r[key] = {['name'] = value,['description'] = value,
 ['version'] = '1',['index'] = key}

end

return r

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

Observe mais um exemplo:

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

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

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

val = t['1.3.6.1.2.1.2.2.1.2']

for key,value in pairs(val) do
 r[key] = {['name'] = value,['description'] = value,
 ['version'] = '1',['index'] = key}

tmlDebug.vardump(t['1.3.6.1.2.1.2.2.1.2'])

return r

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

Script de Provisionamento

O script de provisionamento executa uma sequência de perguntas e respostas esperadas pelo dispositivo.

Esse tipo de script pode ser criado de três modos: **Texto**, **Lua** e **Send/Expect**.

Modo Texto

Neste modo, o script será constituído, basicamente, por todos os comandos que são executados em um dispositivo.

Modo Lua

Neste formato, é possível tornar o provisionamento mais personalizado através da programação.

Ele terá como padrão a variável **params['connection']**, que é o objeto de conexão ao dispositivo que está sendo provisionado.

Modo Send/Expect

Este modo é o mais utilizado para provisionamento. Veja abaixo o script de Probe IP/SLA ICMP Echo [ip sla monitor] escrito neste modo e, a seguir, a descrição do mesmo:

```
  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
```

- Os campos **send** são os comandos para serem executados no dispositivo.
- Os campos **expect** são strings esperadas pelo dispositivo.
- Os campos **abort** são usados para inserir uma string que irá causar o encerramento do script se recebido pelo dispositivo. O texto inserido depois do caracter **;** irá trabalhar da mesma forma que o campo esperado.
- Os campos encerrados com o caractere **$** são obtidos do banco de dados baseados nos códigos de provisionamento usados para configurar um tipo de probe. Eles são usados apena sna criação de probes.
- Quando os campos são encerrados com o caractere **%**, eles podem ser caracterizados como wildcards especiais. Veja a lista das wildcards suportadas na próxima seção.

Wildcards

Tabela 6.14. Lista de wildcards

Variáveis	Descrição
%username%	Campo de usuário do formulário de configuração do dispositivo.
%passwd%	Campos de senha de usuário do formulário de configuração do dispositivo.
%enable_passwd%	Habilitar campo de senha do formulário de configuração do dispositivo.
%probe_index%	Index SNMP da probe.
%probe_name%	Campo de nome do formulário de configuração de probe.
%collector_ip%	Endereço de IP do novo coletor quando o atual coletor está abaixo na arquitetura distribuída.
%current_collector_ip%	Endereço de IP do atual coletor na arquitetura distribuída.

Credencial de dispositivo

Muitos dispositivos utilizam as mesmas configurações de SNMP e de acesso remoto.

É possível configurar estes parâmetros em uma credencial e depois associá-la aos dispositivos que possuem a mesma configuração.

Para criar uma nova credencial, acesse **Configuração** → **Credencial de dispositivo** → **Nova credencial de dispositivo** ou **Configuração** → **Credencial de dispositivo** → **Credencial de dispositivo** e clique no botão **Novo**.

Tabela 6.15. Formulário de Credencial de dispositivo

Campo	**Descrição**
Nome	Defina o nome da credencial.
Protocolo	Defina se a credencial será de **SNMP**, **SSH** ou **Telnet**.
Versão do SNMP	Selecione a versão SNMP. Os possíveis valores são: SNMP v1 ou SNMP v2c — Especifica uma community SNMP SNMP v3 — Especifica o tipo de autenticação e seus parâmetros
Community SNMP	Preencha a community SNMP.
Porta SSH	Preencha a porta SSH. O valor padrão é **22**.
Porta Telnet	Preencha a porta Telnet. O valor padrão é **23**.
Usuário	Usuário para ser usado para acessar o dispositivo. Esta string está disponível como um campo livre %username% para scripts de provisionamento.
Senha do usuário	Senha do usuário que irá acessar o dispositivo. Esta string está disponível como um campo livre %passwd% para scripts de provisionamento.
Senha de enable	Senha de enable é a usada para acessar o dispositivo. Esta string está disponível como um campo livre %enable_passwd% para scripts de provisionamento.
Dispositivos	Associe os dispositivos que devem utilizar a credencial.

Filtro de Syslog

Os filtros de Syslog podem ser usados como Regras de ativação de alarmes do tipo **Syslog**.

Para criar um novo filtro de Syslog, acesse **Configuração** → **Filtro de syslog** → **Novo filtro de syslog** ou **Configuração** → **Filtro de syslog** → **Filtro de syslog** e clique no botão **Novo**.

Tabela 6.16. Formulário de Filtro de Syslog

Campo	Descrição
Nome	Preencha com o nome do filtro.
Descrição	Preencha com a descrição do filtro.
Facilidade	Preencha com a Facilidade do Syslog.
Severidade	Preencha com a Severidade do Syslog.
Mensagem	Preencha com a mensagem do Syslog.

Capítulo 7. Ferramentas

MIB Browser

Você pode explorar todas as MIBs instaladas no sistema utilizando o MIB browser. Estes elementos estão listados na tela com filtros aplicados.

Se você quer explorar uma MIB, clique no botão Selecionar no lado direito.

Software externo

Telcomanager Windows Collector

Faça o download do executável **Telcomanager Windows Collector** para instalar o coletor de Netflow para Windows.

Ele encaminha todos os pacotes de Netflow recebidos por uma máquina Windows para um appliance com TRAFip.

Telcomanager Host Agent

Faça o download do executável **Telcomanager Host Agent** (THA) para instalar este agente no Windows.

Este agente coleta informações acerca dos processos rodando. Ele será necessário para fazer coletas do tipo THA.

Discovery

O recurso Discovery é usado para descobrir todos os hosts que estão sendo usados numa rede. Preencha o campo IP/Máscara e clique em Executar para iniciar a função discovery.

Quando o processo termina, o sistema irá mostrar uma lista com todos os hosts descobertos.

Capítulo 8. Sistema

Registro de acesso

Acesso de usuário

Esta opção mostra um relatório sumarizado por dia contendo o registro de acesso de usuários. Cada linha do relatório é um link para um relatório diário detalhado.

Acesso simultâneo

Este relatório mostra o número de usuários que estão logados no sistema para cada grupo de usuário.

Backup/Restore

Você pode executar backup e restore de todos os dados do sistema de qualquer servidor ftp ou um simples arquivo download/upload com todas as configurações do sistema.

Vá em **Sistema** → **Backup/Restore** para trabalhar com as seguintes opções de backup/restore:

Backup local de configuração

Clique neste ícone para mostrar todos os arquivos de backup de configuração.

Você pode criar um novo arquivo clicando no botão Criar novo.

O botão Configurar é usado para selecionar o número de arquivos a serem mantidos.

Clique no botão Download para fazer o download de um arquivo de configuração para o seu desktop.

O botão Copiar para Restore é usado para copiar o arquivo de configuração para a área de restore para que ele possa ser restaurado.

Restore local de configuração

Esta opção é usada para restaurar um arquivo de backup. Fazendo isto, todas as configurações atuais do sistema serão substituídas pelas definições contidas no arquivo restaurado.

Para executar uma restauração do sistema, você deve fazer upload do arquivo de configuração da sua máquina local ou copiar um arquivo de backup antigo disponível no sistema e depois clicar no botão Restore para aquele arquivo.

Backup remoto

Esta opção pode ser usada para salvar os arquivos de configuração e dados históricos do sistema em um servidor de backup remoto.

Tabela 8.1. Formulário de backup remoto

Campo	Descrição
Versão do IP	Escolha se é IPv4 ou IPv6.
Servidor de backup	Endereço de IP do servidor de backup.
Diretório de backup	Diretório no servidor de backup.
Usuário	Usuário para ser autenticado no servidor de backup.
Senha do usuário	Senha.
Protocolo utilizado no backup	Protocolo a ser usado nos backups.
Porta utilizada pelo protocolo	Número da porta.
Tamanho do servidor (GB)	Tamanho do servidor em Gigabytes.
Ativar backup	Selecione **Sim** para ativar o recurso de backup.
Hora para realizar o backup	Selecione o instante do dia para a execução dos backups.

Restore remoto

Selecione um único sistema para executar restore de dados ou clique Requisitar restore completo para buscar dados de todos os sistemas.

Importante

- O servidor ftp deve estar online, já que os dados serão buscados nele.
- Apenas execute esta operação em uma instalação de um TRAFip ou SLAview novos e vazios, já que todos os dados serão substituídos.

Situação da restauração

Esta opção irá mostrar o status de restauração uma vez que for solicitada uma operação de restauração remota.

Parâmetros

Esta seção é usada para configurar vários parâmetros do sistema que são usados por diferentes processos.

Active directory

Esta opção possibilitará que os usuários loguem no TRAFip usando o método de autenticação Active Directory Kerberos.

Para um usuário ser autenticado por esse método, é preciso que o TRAFip esteja configurado.

Tabela 8.2. Formulário de Active directory

Campo	Descrição
Habilitar autenticação pelo Active Directory	Uma vez que a opção **Sim** estiver selecionada, o campo **Autenticação local** aparecerá no formulário de usuário.

Campo	Descrição
Servidor	Digite o endereço do servidor Active Directory. Exemplo: kerberos.example.com
Domínio	Digite o domínio do Active Directory. Exemplo: ATHENAS.MIT.EDU

Quando este método está ativado, não existe autenticação local, ou seja, qualquer usuário que não seja do tipo **Administrador** loga pelo TACACS.

Importante

O usuário **Administrador** tem a opção de escolher logar localmente ou não, entretanto, recomenda-se que haja sempre uma conta de **Administrador** com **Autenticação local** ativada, caso seja utilizado controle de acesso externo.

Agente das pastas de enlace

Esta configuração permitirá você escolher dois tempos de execução no mesmo dia para executar o agente das pastas de enlace.

Agentes de associação

Agente de associação automática de grupos

Configure os períodos desejados para que a associação automática de grupos seja executada. Isso acontecerá duas vezes ao dia.

Tabela 8.3. Formulário de agente de associação automática de grupos

Campo	Descrição
Primeiro horário de execução	Escolha o horário para a primeira execução acontecer.
Segundo horário de execução	Escolha o horário para a primeira execução acontecer.

Agente de associação automática de mapeadores

Configure os períodos desejados para que a associação automática de mapeadores seja executada. Isso acontecerá em dois momentos do dia.

Tabela 8.4. Formulário de agente de associação automática de mapeadores

Campo	Descrição
Primeiro horário de execução	Escolha o horário para a primeira execução acontecer.
Segundo horário de execução	Escolha o horário para a primeira execução acontecer.

Perfil automático

Defina dois horários do dia para que o agente de associação do perfil automático rode.

Perfil automático de alarme

Defina dois horários do dia para que o agente de associação do perfil automático de alarme rode.

ALARMmanager

Tabela 8.5. Formulário de parâmetros do ALARMmanager

Campo	Descrição
Período máximo de armazenamento de eventos	Número de horas que a tabela de ocorrências irá armazenar ocorrências. Esta tabela é usada apenas para níveis de depuração altos, uma vez que as ocorrências não são utilizadas depois de processadas.
Período máximo de armazenamento de alarmes	Depois desse período, os alarmes serão deletados.
Período máximo de armazenamento de alarmes inativos	Uma vez que o alarme se torna inativo, ele estará disponível no ALARMmanager console por este período. Depois disto, o alarme pode ser visualizado em relatório ALARMmanager.

Ocorrências de alarmes são geradas pelos seguintes processos:

- SlaSumCaching: gera ocorrências para todos os alarmes configuráveis criados com sumarização de variáveis.
- ICMPAgent: gera ocorrências para o alarme **Sem resposta ICMP**.
- MIBget: gera ocorrências para o alarme **Sem resposta SNMP**.
- ObjectMapper: gera ocorrências para o alarme **Objeto não encontrado**.

Cuidado

Você pode checar o item de **Configuração** na seção **Sistema** → **Diagnósticos** → **Uso de disco** para checar se o banco de dados é muito grande, indicando que o sistema está gerando muitos alarmes. Se este for o caso, você pode diminuir o período de armazenamento ou ajudar as configurações do alarme para gerar menos alarmes.

Armazenamento de dados

Nesta área, você deve configurar o armazenamento de espaço que deveria ser alocado para cada tipo de dado do sistema.

O campo **Espaço de distribuição disponível** irá mostrar o espaço que ainda pode ser distribuído.

Para checar quanto espaço cada área está consumindo, você deve fazer login no sistema desejado (TRAFip, SLAview ou CFGtool) e acessar **Sistema** → **Diagnósticos** → **Armazenamento de dados** . O item do banco de dados TDB corresponde aos dados sumarizados para cada tipo de sistema.

Você pode realizar a redistribuição de espaço de armazenamento entre diferentes áreas a qualquer momento.

Tabela 8.6. Formulário de armazenamento de dados

Campo	Descrição
Iniciar processo a partir da ocupação em %	Quando este valor for atingido, o processo de limpeza será executado de acordo com o tipo de execução configurado. Preencha um valor entre **1** e **85**.
Tipo de execução	Escolha se o agente rodará a cada **Intervalo de tempo** ou num **Horário agendado**.
Intervalo de tempo para execução (minutos)	Defina o intervalo de tempo, em minutos, para a execução do agente. O valor mínimo é **10**.
Horário de execução	Defina o horário em que a execução do agente acontecerá.
Espaço disponível para os arquivos de SYSLOG	Armazenamento dedicado para dados brutos de arquivos SYSLOG.
Espaço disponível para os arquivos de Relatórios agendados	Armazenamento dedicado para relatórios agendados.
Trap receiver storage	Armazenamento dedicado para arquivos de Trap receiver.
Espaço disponível para arquivos de captura	Armazenamento dedicado para arquivos de captura.
Dados brutos do TRAFip	Área de armazenamento destinada aos arquivos de dados brutos do TRAFip. Este armazenamento normalmente cresce muito mais rápido que os dados sumarizados. Dessa forma, se você configurar com o mesmo tamanho dos dados sumarizados, você terminará com 10 vezes menos dados históricos.
Dados sumarizados do TRAFip	Armazenamento dedicado para o TRAFip, dados processados ou TDB - Telco database. Este dado é usado para gráficos e relatórios TOPN.
Arquivos de sumarização remota do TRAFip	Armazenamento dedicado para os dados processados do TRAFip enviados pelos coletores num ambiente de arquitetura distribuída.
Dados de alteração de comportamento do TRAFip	Armazenamento dedicado para os dados de alteração de comportamento, como dados de alarmes históricos, por exemplo.
Dados brutos do SLAview	Armazenamento dedicado para dados brutos do SLAview. Isto é, em geral, das coletas SNMP das OIDs.
Dados sumarizados do SLAview	Armazenamento dedicado para dados processados pelo SLAview. Este dado é usado para gráficos e relatórios.
Arquivos de sumarização remota SLAview	Armazenamento dedicado para os dados processados para os arquivos dos dados SLAview enviados pelos coletores em um ambiente de arquitetura distribuída.
Dados de alteração de comportamento do SLAview	Armazenamento dedicado para os dados de alteração de comportamento, como dados de alarmes históricos, por exemplo.

Campo	Descrição
Dados de versões do CFGtool	Armazenamento dedicado para versões de configurações dos dispositivos. Mesmo que este valor seja ultrapassado, os dados de versão de dispositivos com apenas uma versão não serão excluídos.

Quando os campos **Dados brutos (MB)** e **Dados sumarizados (MB)** estão preenchidos com '**0**' (zero), isso significa que o sistema está distribuindo de maneira automática o **Espaço disponível para distribuição** entre os **Dados brutos do TRAFip**, **Dados brutos do SLAview**, **Dados sumarizados do TRAFip** e **Dados sumarizados do SLAview**.

Você pode configurar manualmente esses valores, mas não se esqueça que os dados brutos tendem a crescer muito mais rápido do que os dados sumarizados. Para redistribuir os espaços, divida o valor de **Espaço disponível para distribuição** por 4. Assim, você terá o valor de cada espaço.

Cuidado

Se você reduzir o espaço de armazenamento de qualquer uma dessas áreas, a próxima vez que o coletor de lixo for executado, ele limpará os dados para adequar o espaço de armazenamento.

Arquitetura distribuída

Estes parâmetros devem ser usados se você desejar rodar o sistema no modo de arquitetura distribuída.

Para mais detalhes da arquitetura distribuída vá à seção arquitetura distribuída.

Tabela 8.7. Formulário dos parâmetros da arquitetura distribuída

Campo	Descrição
Número máximo de falhas consecutivas do coletor	Este número representa quandas vezes o nó da central irá esperar os arquivos processados de um nó do coletor enquanto este nó é considerado desativado. Esta checagem é realizada a cada 5 minutos por um processo de controle para os sistemas TRAFip e SLAView. Depois que o coletor está definido como desabilitado pelo nó central, o coletor de backup, se estiver definido, irá substituir as operações com os coletores defeituosos.
Habilitar arquitetura distribuída	Selecione esta opção se o appliance será parte de um sistema de arquitetura distribuída.
É coletora?	Marque **Sim** nesta opção se o appliance terá o papel de coletora no sistema. Caso contrário este appliance será considerado um nó central.
Chave do coletor	Preencha com uma string de identificação para identificar este coletor no nó central.
Versão do IP	Escolha se é IPv4 ou IPv6.
IP da consolidadora	Preencha com o endereço IP do appliance para ser usado como nó central.
Senha	Senha usada para autenticação.

Aviso de Expiração

Configure quantos dias antes da expiração da licença você será lembrado a respeito dela.

Tabela 8.8. Formulário de aviso de expiração

Campo	Descrição
Alertar expiração faltando	Defina um valor entre 10 e 30.

Backup

- Dados: Parâmetros para executar backup remoto. Veja a seção backup remoto.
- Configuração: configure o número de antigas configurações de backup de arquivos para manter no sistema.

Cisco WAAS

Cisco WAAS (Wide Area Application Services) é uma ferramenta desenvolvida pela Cisco que é capaz de acelerar as aplicações da mesma.

Tabela 8.9. Formulário de Cisco WAAS

Campo	Descrição
Habilitar monitoramento ao Cisco WAAS	Escolha **Yes** ou **Não**.

Coletor personalizado

Defina o número de coletas simultâneas permitidas.

Tabela 8.10. Formulário do coletor personalizado

Campo	Descrição
Número máximo de coletas simultâneas	Escolha um valor inteiro menor ou igual a 50. O preenchimento padrão é de 10 coletas.

Configuração de HTTPS

Configure o modo HTTPS (HyperText Transfer Protocol Secure).

Tabela 8.11. Formulário de HTTPS

Campo	Descrição
Habilitar https	Escolha **Sim** e o servidor será reiniciado no modo HTTPS.
Certificado	Importe o certificado https.

Configuração do agente de captura

Configure o número permitido de agentes em execução simultânea.

Tabela 8.12. Formulário de configuração do agente de captura

Campo	Descrição
Número de agentes em execução simultânea	Entre com um inteiro menor ou igual a 10. O valor padrão é **3**.

Configuração regional

Tabela 8.13. Formulário de configuração regional

Campo	Descrição
Separador de decimal	Separador decimal para relatórios do sistema.
Linguagem do sistema	Escolha a linguagem padrão do sistema. Cada usuário pode definir sua própria configuração de idioma em configuração do usuário.
Número de casas decimais nos arquivos de exportação	Configuração usada para formatar campos de números nos relatórios exportados.
Separador de arquivo CSV	Separador para relatórios CSV.

Configurações do trap receiver

Defina a porta que será ouvida para SNMP traps. A porta padrão é **162**.

EPM

EPM (Extended Processing Module) é outra aplicação em adição à já instalada no equipamento. É um módulo estendido da solução de monitoramento.

Tabela 8.14. Formulário EPM

Campo	Descrição
Habilitar EPM	Selecione esta opção se você desejar habilitar o módulo de solução de monitoramento.
É EPM?	Marque **Sim** nesta opção se esta aplicação for utilizada como EPM.

Importante

Mudando esta configuração você irá perder todos os seus dados históricos, logo, tenha cuidado!

Exportação

Syslog

Syslog é um mecanismo de monitoramento que envia mensagens quando determinados eventos acontecem. Elas são compostas, basicamente, pelo endereço de IP, pelo timestamp e pela mensagem de log.

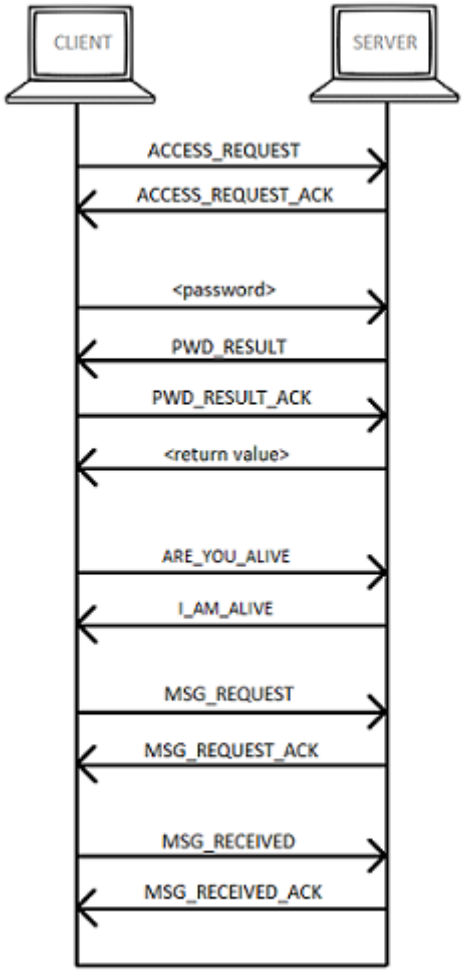
Devido ao fato de as mensagens Syslog serem enviadas de cada dispositivo separadamente, esse mecanismo disponibiliza informações mais detalhadas ao ser comparado às traps SNMP.

O TRAFip dispõe de um agente exportador que envia essas mensagens Syslog dos dispositivos cadastrados no sistema.

É necessário que haja comunicação entre um host e o TRAFip para que essas mensagens Syslog sejam recebidas pelo host. Para configurar quais hosts terão acesso à exportação Syslog, clique em **Adicionar** e especifique o host e a senha.

No **Filtro por origem**, você configurará os dispositivos que serão ouvidos e enviarão mensagens Syslog. Para que um dispositivo seja habilitado, selecione-o e transporte-o para o lado direito do filtro usando o botão '>>>'.

A imagem a seguir ilustra o protocolo de comunicação entre o cliente e o servidor:



Protocolo Syslog

Tabela 8.15. Protocolo Syslog

Mensagem	**Descrição**
ACCESS_REQUEST	Mensagem de solicitação de acesso pelo cliente.
ACCCESS_REQUEST_ACK	Confirmação de entrega da mensagem enviada pelo cliente.

Mensagem	Descrição
<password>	Senha configurada para o host no campo **Senha** do formulário em **Sistema** → **Parâmetros** → **Exportação** → **Syslog** .
PWD_RESULT	Autenticação de senha.
PWD_RESULT_ACK	Confirmação de entrega da mensagem enviada pelo cliente.
<return value>	É o valor de retorno da autenticação. Se o host for autenticado, retorna 1. Caso contrário, a conexão é fechada.
ARE_YOU_ALIVE	Verifica se o agente exportador está ativo e rodando.
I_AM_ALIVE	Confirmação sobre o agente exportador estar ativo e rodando.
MSG_REQUEST	Cliente envia um pedido para o envio das mensagens.
MSG_REQUEST_ACK	Confirmação de entrega da mensagem enviada pelo cliente.
MSG_RECEIVED	Cliente confirma que as mensagens foram recebidas.
MSG_RECEIVED_ACK	Confirmação de entrega da mensagem enviada pelo cliente.

Grafador

Ajuste dos parâmetros do grafador

Tabela 8.16. Formulário de parâmetros do grafador

Campo	Descrição
Habilitar gráfico derivativo como padrão?	No modo padrão, pontos de gráficos são conectados usando interpolação linear. No modo derivativo, a interpolação por partes é utilizada.
Habilitar atualização automática	Selecione esta opção para ter todos os gráficos atualizados automaticamente. Você também pode habilitar esta opção em tempo de execução para cada gráfico.
Mostrar horário comercial	Habilitando essa opção, o horário comercial definido em Preferências locais será mostrado nos gráficos.
Excluir fins-de-semana	Habilitando essa opção, os dias do fim de semana serão mostrados com cor mais clara nos gráficos.
Intervalo de atualização	Intervalo entre as atualizações.

Histórico de configuração

Selecione o período de armazenamento para diferentes áreas de configuração.

Tabela 8.17. Parâmetros de históricos de configuração

Campo	Descrição
Período máximo de armazenamento de histórico de configuração	Isto inclui todas as mudanças de configuração, exceto para o usuário relacionado às operações. Este dado será mostrado em **Sistema → Diagnósticos → Logs de configuração** .
Período máximo de armazenamento de histórico de configuração de usuários	Isto é específico para operações de usuário. Estes dados podem ser mostrados em **Sistema → Diagnósticos → Logs de configuração** selecionando a opção usuário no campo **Tipo de objeto**.
Período máximo de armazenamento de estatísticas de sumarização	Isto é relacionado apenas ao processo de sumarização. Esta estatística pode ser checada em **Sistema → Diagnósticos → Sumarizador** .

Integridade de segurança

Selecione o período de tempo em que o alarme de Integridade de Segurança permanecerá ativo.

Tabela 8.18. Integridade de Segurança

Parâmetro	Descrição
Limite de modificação(segundos)	Período de tempo em que o alarme de modificação de arquivos permanecerá alarmado.
Limite de alteração(segundos)	Período de tempo em que o alarme de ausência de arquivos permanecerá alarmado.

ICMP

Processo de configuração ICMP polling. O processo responsável pelo ICMP polling é o ICMPAgent

O ICMP polling roda a cada minuto, mas para evitar pollings desnecessários, o sistema possui um sistema de amortecimento que causa o decaimento do polling de frequência com o tempo e ele irá voltar ao normal se o elemento voltar a responder novamente.

Tabela 8.19. Formulário de parâmetros do processo ICMP

Campo	Descrição
Número de falhas para ativar amortecimento	Depois desse número de falhas consecutivas, o processo de amortecimento irá iniciar.
Aumento do número de intervalos a cada falha	Depois que o dispositivo é colocado em modo de amortecimento, este número é adicionado ao número de intervalos entre polling cada vez que o dispositivo é polled.
Intervalo máximo permitido no amortecimento	Este é o número máximo de vezes que o ICMPAgent irá pular o polling desse dispositivo, mesmo que em modo de amortecimento. Quando essa condição é alcançada, o ICMPagent irá gerar uma ocorrência

Campo	Descrição
	para o alarme **Maximum damping reached** a cada minuto para cada dispositivo.
Timeout ICMP (ms)	Timeout para o ICMP polling.
Número de pacotes	Defina a quantidade de pacotes que será enviada na coleta ICMP. O valor máximo é **10**.
Tamanho do pacote	Defina o tamanho dos pacotes a serem enviados.
Intervalo entre pacotes (ms)	Defina o intervalo, em milisegundos, entre o envio dos pacotes.
Número de testes simultâneos	Defina quantos testes poderão ser realizados ao mesmo tempo. Caso este campo seja configurado com o valor **0 (zero)**, todos os testes devem rodar simultaneamente.

Para mais informações no processo de configuração do ICMP, vá à seção configuração ICMP.

Login automático

Este recurso habilita a autenticação bypass para requisições URL vindas de outro sistema.

Para habilitar este recurso, siga o procedimento abaixo:

1. Vá até **Sistema → Parâmetros → Login automático** .
2. Selecione sim na opção **Habilitar login automático**.
3. Preencha a URL no formato requerido, que é a página cujas requisições serão originadas.
4. No seu servidor web, preencha a seguinte URL: http://TelcoApplianceIP.

Logotipo

Escolha um arquivo de imagem do seu Desktop e faça o upload, logo a imagem será mostrada no canto direito superior.

Lembre que a imagem deve estar com altura fixada em 43 pixels e largura variável de 20 à 200 pixels.

Mapa GIS

É necessário cadastrar a chave **MapQuest AppKey** para visualizar mapas georreferenciados no Mapview.

Escolha o plano que melhor atenda às suas necessidades em: https://developer.mapquest.com/plans .

Mapeador de objetos

Para mais detalhes sobre mapeamento de objetos vá à seção configuração de mapeadores.

Tabela 8.20. Formulário de configuração de parâmetros de mapeador de objetos

Campo	Descrição
Intervalo de execução do mapeador	Programe o intervalo entre as execuções do mapeador.

Campo	Descrição
Período máximo de armazenamento do histórico de configuração	Programe o período de armazenamento de logs pelas configurações realizadas pelo mapeador
Limite de mapeadores TCS simultâneos	Defina um limite de execuções simultâneas de mapeadores do tipo TCS. Preencha um valor entre **1** e **200**. A configuração deste parâmetro poderá afetar a performance do sistema, então seja cuidadoso.

Nível de log

Escolha o nível do ALARMDaemon: **Baixo**, **Médio** or **Alto**.

Este nível determinará a quantidade de detalhes no log do alarme.

Personalização de interface

Você pode customizar a maneira como os dispositivos serão mostrados no menu em árvore em **Dados históricos** → **Dispositivos** → **Dispositivo** .

Para isso, basta preencher o campo **Fórmula de nome de dispositivo** com o que você deseja que apareça no menu.

A fórmula possui tags especiais que utilizam as informações preenchidas nos formulários dos dispositivos. São as seguintes:

Tabela 8.21. Fórmula de nome de dispositivo

Tag	Descrição
%n	Refere-se ao **nome** do dispositivo.
%a	Refere-se ao **endereço de IP** do dispositivo.
%t	Refere-se ao **tipo** do dispositivo.
%m	Refere-se ao **fabricante** do dispositivo.
%d	Refere-se ao **tipo de dispositivo** (Câmera, Firewall, Roteador, Servidor, Switch ou Sem fio).

Preferências locais

Tabela 8.22. Formulário de preferências locais

Campo	Descrição
Tamanho da página em PDF	Tamanho da página nos relatórios em PDF.
Limitador de pesquisa	Preencha com um valor positivo inteiro para limitar suas pesquisas. O valor padrão é 2500.
Primeiro período do horário comercial	Defina os horários inicial e final para o primeiro período do horário comercial.
Segundo período do horário comercial	Defina os horários inicial e final para o segundo período do horário comercial.

Projeção

Configuração de padrão de parâmetros para projeção. Vá à seção projeção para dicas em como configurar estes parâmetros.

QoS

Selecione **Sim** para habilitar os processos ciscoPolicyMapper e qos_d. Você também precisa selecionar o tempo que esses processos irão rodar.

O processo CiscoPolicyMapper irá buscar todas as políticas de QoS nos dispositivos de rede Cisco. O dispositivo precisa suportar a MIB CLASS-BASED-QOS-MIB e as políticas devem ser configuradas nas interfaces. Veja na seção QoS.

Os processos qos_d irão trabalhar com resultados do processo ciscoPolicyMapper para criar perfis SLAview necessários para visualizar as estatísticas de QoS.

Redirecionamento de login

Preencha o campo **página de destino após login** para ser redirecionado a outro sistema após o login. No sistema redirecionado, você será capaz de acessar todos os objetos sem autenticação do TRAFip/SLAview.

Redundância

Esta seção é utilizada para especificar as configurações de redundância.

Tabela 8.23. Configurações de redundância

Campo	Descrição
Habilitar redundância	Escolha Sim.
Versão do IP	Escolha se é IPv4 ou IPv6.
IP de sincronização local	Preencha com o endereço de IP configurado para a interface diretamente conectada a outro appliance.
IP de sincronização remota	Preencha com o endereço de IP configurado para o appliance remoto.
Tamanho máximo de histórico	Configure o tamanho máximo de histórico em MB. O tamanho de histórico mínimo é de 16MB.
Interfaces	Selecione a interface que irá compartilhar os endereços de IP entra os dois appliances. Use a tecla **CTRL** para selecionar múltiplas interfaces. Pelo menos uma interface deve ser reservada para possuir um endereço de IP exclusivo para fins de gerenciamento. Uma interface deve ser usada para a conexão back-to-back e outras podem ser usadas para compartilhar IPs.
Estado preferencial	Selecione **Mestre** ou **Slave**.

Vá à seção redundância para detalhes de habilitação deste recurso.

Registros de acesso de usuários

O sistema oferece uma ferramenta que disponibiliza um relatório sumarizado diário contendo registro de acesso de usuários. Para mais informações a respeito disso, consulte a seção **Registro de acesso**.

Você pode configurar o tempo máximo em que esses registros ficarão no sistema.

Tabela 8.24. Formulário de registros de acesso de usuários

Campo	Descrição
Período máximo de armazenamento dos registros de acessos de usuários (meses)	Escolha um valor menor ou igual a 36. O valor padrão é **12**, ou seja, o equivalente a 1 ano.

Relatórios

Essa seção permite fazer configurações avançadas dos relatórios.

Período de agregação do relatório de alarme avançado

Essa seção é referente ao relatório avançado de alarme.

Visualize o início do período de agregação e configure os horários iniciais e finais dos períodos.

Para mais informações a respeito da agregação, cheque a seção Agregação de dados.

> **Importante**
> A alteração dos horários iniciais e finais dos períodos acarretará no reinicialização do período de agregação.

Relatórios agendados

Configure as características que os relatórios agendados possuirão.

Tabela 8.25. Formulário de configuração dos relatórios agendados

Campo	Descrição
Tempo de atualização da página de espera (segundos)	Entre com um inteiro.
Tempo Máximo de Execução (minutos)	Entre com um inteiro.
Número Máximo de Processos Simultâneos	Entre com um inteiro.
Prefixo do assunto do e-mail	Defina um prefixo para o assunto do e-mail.
Hostname para link do email	Configure um hostname para o e-mail.

Servidor SMS

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

Use este método se o seu operador móvel disponibilizar uma conta SMPP.

Tabela 8.26. Formulário de servidor SMPP

Campo	Descrição
Protocolo SMS	Escolha a opção SMPP
Host	Host SMPP.
Porta	Porta SMPP.
Sistema ID	Sistema ID SMPP.
Tipo de sistema	Tipo de sistema SMPP.
Senha	Senha SMPP.
URL	Veja a seção de URL.
Número de telefone de origem	Número de telefone que será mostrado como chamada SMS.

SMSs podem ser enviadas utilizando métodos distintos. Ambos podem ser configurados por este formulário.

Método URL(Uniform Resource Locator)

Este método deve ser usado se você tiver um gateway http.

SLAview irá executar uma operação http GET utilizando a URL fornecida.

Você deve usar as wildcars $CELLPHONE$ e MSG na URL.

A wildcard $CELPHONE$ será substituída pelo campo wildcard SMS que você preencheu no formulário de configuração do usuário.

A wildcard MSG será substituída por uma mensagem de alarme, que contém as seguintes informações:

- Nome do alarme.
- Nível de urgência do alarme.
- Estado do alarme.
- Data e horário que o alarme mudou de estado.
- Variável de alarme.

SMTP

Preencha este formulário com os parâmetros SMTP para enviar emails.

Tabela 8.27. Formulário de parâmetros SMTP

Campo	Descrição
Servidor SMTP	Configure o servidor SMTP. A porta usada pelo servidor SMTP pode ser alterada neste campo. Siga o exemplo: smtp.server.com:port
Usuário SMTP	Entre com o email.

Campo	Descrição
Senha SMTP	Entre com a senha. Se o servidor SMTP não solicitar autenticação este campo pode ser deixado em branco.
Remetente SMTP	Configura um remetente para o email.

Você pode verificar as configurações SMTP antes de salvar: clique em **Teste SMTP** e entre com o endereço de email para o teste.

SNMP

Coletor SNMP

Estes parâmetros serão usados para todos os processos que executam SNMP polling. Estas são configurações padrões, mas elas podem ser ajustadas a nível do dispositivo.

Para uma referência de todos os processos do sistema, vá para seção arquivos de log.

Parâmetros SNMP

Use a OID sysUpTime para descartar resultados.	Se você marcar esta opção, o processo MIBget irá buscar a instância sysUpTime.0 para o dispositivo e descartar todos os resultados se o valor de retorno desta OID for menor que 300 segundos. Esta condição será considerada um reboot no dispositivo e os contadores SNMP podem ser inválidos.
SNMP Timeout	Tempo limite em segundos que a coletora irá esperar por um pacote de resposta SNMP. Intervalo de valores: 1-10.
Novas tentativas SNMP	Número de tentativas que serão permitidas ao dispositivo se ele não responder a uma consulta SNMP. Intervalo de valores: 1-10.
Número de OIDs por pacote	Número de OIDs que a coletora irá enviar em cada pacote SNMP. Intervalo de valores: 1-100.
Taxa máxima de envio por pacote	Número máximo de pacotes por segundo que um coletor SNMP irá enviar para cada dispositivo.
Janela SNMP	Número de pacotes SNMP que serão enviados sem resposta do dispositivo que está sendo sondado.
Porta SNMP	Porta TCP padrão para conectar com o agente SNMP.
Ignorar interfaces	Preencha a expressão para ignorar estas interfaces.
Interfaces high counter	Preencha a expressão para usar, nestas interfaces, o contador de OID mais alto(ifHCInOctets e ifHCOutOctets).
Interfaces SecRate	Preencha a expressão para usar a sec rate OIDs (IfHCIn1SecRate and IfHCOut1SecRate) nestas interfaces.

Trap SNMP

Preencha os campos abaixo para especificar os hosts que irão receber os traps. Estes traps podem ser alarmes de ALARMmanager ou traps auto gerados pelas TELCOMANAGER MIBS.

Tabela 8.28. Campos de TRAP

Campo	Descrição
Hosts para enviar Traps	Endereços de IP dos hosts. Ex: 10.0.0.1,10.0.0.2.
Comunidade para enviar Traps	Comunidades SNMP dos hosts de trap.

TACACS

Habilita o método de autenticação TACACS+. Até dois servidores podem ser configurados para Redundância.

O nome de usuário e senha para cada usuário deve ser configurado no sistema, exatamente como o servidor TACACS.

Quando este método está ativado, não existe autenticação local, ou seja, qualquer usuário que não seja do tipo **Administrador** loga pelo TACACS.

Importante

O usuário **Administrador** tem a opção de escolher logar localmente ou não, entretanto, recomenda-se que haja sempre uma conta de **Administrador** com **Autenticação local** ativada, caso seja utilizado controle de acesso externo.

Tema

Nesta seção, você pode ver o tema padrão do sistema.

Tabela 8.29. Configuração do tema

Campo	Descrição
Tema padrão	Escolha o tema padrão para o sistema: Dark, Green & Yellow ou Telcomanager.

Dica

Perceba que cada usuário pode definir seu próprio tema em configuração de usuário.

Verificação de versão do sistema

Todo dia entre 2h e 3h da manhã, ocorre uma verificação de versão do sistema para checar se há uma nova build disponível. Uma vez que exista, o usuário será informado.

Web Services

API de Configurações

Tabela 8.30. Formulário de API de configurações

Campo	Descrição
Hosts com acesso permitido à API de configurações	Configure os hosts que são habilitados para acessas a API de configurações.

Campo	Descrição
Nome de usuário utilizado pela API de configurações	Digite o usuário.

Dados brutos do TRAFip

Configure o acesso aos dados brutos do TRAFip.

Tabela 8.31. TRAFip's raw data form

Campo	Descrição
IP com permissão de acesso	Digite o IP.
Senha	Digite a senha.

Geren. de MIBs

Selecione **System** → **MIBs**. Nesta seção você pode fazer o upload de arquivos de MIB e fazer a verificação de erros nelas.

Usuários

O sistema possui três tipos de usuários:

Tipos de usuário

Administrador — Tem total acesso ao sistema.

Configurador — Pode criar, remover e editar qualquer objeto do sistema. Não pode fazer mudanças nas configurações do sistema.

Operador — Pode apenas visualizar o sistema de objetos monitorados e relatórios.

Quando você associa grupos a usuários, você irá restringir a visualização desse usuário a objeto com hierarquia de grupos.

Usuários também podem ser limitados aos menus que eles irão acessar e ao número de usuários simultâneos que irão acessar o sistema.

Editando usuários

1. Selecione **Sistema** → **Usuários** → **Lista de usuários** .
2. Clique nos botões Novo ou Editar e preencha o formulário abaixo:

Tabela 8.32. Formulário de usuário

Campo	Descrição
Nome de usuário	Login de usuário.
Nome	Nome de usuário.

Campo	Descrição
Senha	Senha.
Confirmação de senha	Repita a senha.
E-mail	E-mail para enviar alarmes e quando um relatório agendado estiver disponível. Você deve configurar o servidor SMTP.
SMS	Número de celular para enviar alarmes utilizando o protocolo SNMP ou celular@teste.com para enviar emails curtos com alarmes. O sistema também pode enviar SMSs através de integração com portal web. Para configurar o servidor SMS acesse **Sistema** → **Parâmetros** → **Servidor SMS** .
Habilitar favoritos	Habilita o recurso Favoritos.
Usar gráfico compacto	Compacte os gráficos para que caibam na mesma página ou visualize-os no tamanho normal.
Autenticação local	Habilita autenticação baseada no Active Directory ou TACACS. Para configurar o Active Directory acesse **Sistema** → **Parâmetros** → **Active Directory** e para configurar o TACACS acesse **Sistema** → **Parâmetros** → **TACACS** .
Esconde objetos sem perfil	Esconde objetos mapeados que não estão associados ao perfil de usuário.
Habilita relatórios de alarme avançado	Habilita relatórios de alarmes avançados para aquele usuário.
Tema	Selecione o tema do usuário. Escolha o Tema Padrão em **Sistema** → **Parâmetros** → **Tema**
Grupo de usuário	Associa este usuário a um usuário de grupo de forma a restringir o número de acessos simultâneos ao sistema com o grupo.
Idioma	Selecione o idioma do usuário.
Perfil	Selecione o perfil de usuário para restringir o alarme e serviço de visualização de alarme e notificação.
Tipo	Tipo de usuário.
Menu	Use a opção padrão para restringir o usuário a menus específicos.
Grupos	Selecione os grupos aos quais o usuário irá possuir acesso. Esta opção irá limitar o usuário ao próprio grupo e aos grupos abaixo do nível de hierarquia dele.

Grupos de usuários

Os grupos de usuários são usados para gerenciar quantos usuários podem estar logados simultaneamente ao sistema.

Procedimento 8.1. Gerenciando grupos de usuários

1. Selecione **Sistema → Usuários → Grupos de usuários** .
2. Clique nos botões Novo ou Editar e preencha o formulário abaixo:

Tabela 8.33. Formulário de usuário

Campo	Descrição
Nome	Nome do grupo de usuários.
Descrição	Descrição do grupo de usuário.
Limitar o número de acessos simultâneos	Selecione um número entre 1 e 255. Este será o limite de acessos simultâneos no sistema com os usuários deste grupo.
Usuários	Especifica os usuários que irão ser colocados no grupo. Um usuário pode pertencer apenas a um grupo.

Perfis de usuários

Os perfis de usuários são usados para associar alarmes aos usuários.

Procedimento 8.2. Gerenciando perfis de usuários

1. Selecione **Sistema → Usuários → Perfis de usuários** .
2. Clique nos botões Novo ou Editar e preencha o formulário abaixo:

Tabela 8.34. Formulário de usuário

Campo	Descrição
Nome	Nome do perfil de usuário.
Token do bot Telegram	Token obtido após criar um bot no Telegram.
ID do chat Telegram	ID do chat no qual o bot está participando.
Usuários	Associa os usuários a um perfil.
Perfis -> Alarmes	Associa um par de Perfil -> Alarme para este perfil.
Alarmes de serviço	Associa serviços de alarmes a este perfil.

Alarme Console

Você pode selecionar as colunas que serão mostradas no ALARMmanager console. Além disso, você é habilitado a configurar a ordem em que as colunas aparecerão. Para isso, basta clicar e arrastar as linhas.

Tabela 8.35. Colunas ALARMmanager console

Coluna	Descrição
INÍCIO	Tempo da primeira ocorrência.

Coluna	Descrição
TÉRMINO	Tempo da última ocorrência. Mostra ATIVO se o alarme não terminou.
USUÁRIO	Usuário que programou o alarme.
TIPO	Tipo de objeto, pode ser dispositivo ou objeto mapeado.
OBJETO	Nome do objeto.
DESCRIÇÃO	Descrição do objeto.
IFALIAS	Se o objeto for uma interface, mostra sua ifAlias.
ESTADO	Estado do alarme, pode ser ativado ou desativado.
ALARME	Nome do alarme.
NÍVEL	O nível para o alarme definido em configuração de nível.
TRAP	Sim se foi gerado por um trap e não qualquer outro caso.
COMENTÁRIOS	Comentários do operador. Para inserir um comentário, clique duas vezes na célula.

Diagnósticos

Informações de rede

Mostra a data e a hora do sistema, interfaces de rede e gateway padrão.

Testes de conectividade

Testes como ping, nslookup e traceroute para testar a conectividade entre o appliance e os elementos de rede.

Captura de pacotes

Usando essa ferramenta, você pode analisar os pacotes que estão passando pelas interfaces do appliance.

Clique em **Sistema** → **Diagnósticos** → **Captura de pacotes** .

Clique em Novo.

Tabela 8.36. Captura de pacotes

Coluna	Descrição
Interface de rede	Escolha a interface a ser analisada.
Tamanho máximo do arquivo	Escolha o tamanho máximo do arquivo onde o resultado da análise será registrado.
Quantidade máxima de pacotes	Preencha o número máximo de pacotes a serem analisados. Preencha 0 se quiser que não tenha limites.

Coluna	Descrição
Porta	Filtra portas para analisar. Digite * para todas as portas ou vírgula para valores separados.
Excluir porta	Exclui portas para analisar. Digite * para todas as portas ou vírgula para valores separados.
Host	Escolha um host para filtrar ou selecione **Todos** para todos os hosts.

Clique Enviar para iniciar a captura e depois Voltar para voltar à lista de arquivos de captura.

Se você desejar encerrar a captura, clique Parar. Um botão de Download irá aparecer e você pode fazer o download do arquivo capturado.

Objetos

Mostra o número de objetos e perfis configurados.

SNMP

Use este menu para iniciar o diagnóstico SNMP sobre todos os dispostivios configurados no SLAview.

Sumarizador

Esta seção mostra o tempo que o processo sumarizador leva para rodar pelo último dia.

Ao implantar o sistema em arquitetura distribuída, o tempo para enviar os arquivos sumarizados de todos os coletores também será mostrado.

Importante

O processo de sumarização roda a cada cinco minutos, logo o tempo do processo rodar deve ser menor que cinco minutos para uma boa performance do sistema.

Uso de disco

Mostra informação sobre o uso de armazenamento das áreas.

Logs do sistema	Logs do sistema operacional.
Logs SLAview	Logs do SLAview.
Logs TRAFip	Logs TRAFip.
SLAview Banco de dados TDB	Uso de armazenamento para o banco de dados SLAview Telco, que é usado para segurar os dados sumarizados do SLAview.
TRAFip Banco de dados TDB	Uso de armazenamento para o banco de dados TRAFip Telco, que é usado para segurar os dados sumarizados do TRAFip.
TRAFip dados brutos	Armazenamento usado para os dados brutos do TRAFip.
SLAview dados brutos	Armazenamento usado para os dados brutos do SLAview.

Detalhe dos dados brutos	Armazenamento dos dados brutos por dia para o sistema que você está logado.

Arquivos de Log

Nesta área você pode visualizar os arquivos de log do sistema. Abaixo, uma lista de arquivos.

Arquivos de LOG

createMark.log	Logs do processo de update da versão.
backupgen.log	Configuração de backup diário de processos de logs.
dbackupArchive.log	Logs de processo remoto de backup.
ICMPAgent.log	processo de log ICMP.
LinkCacheBuilder.log	Logs do processo que criam a conexão automática na aplicação MAPview.
mibcache.log	Logs sobre o processo de compilação da MIB.
MIBget.log	Log de processo de SNMP polling.
ObjectMapper.log	Log de processo de mapeamento de objeto SNMP.
qos_d.log	Logs do processo de configuração de perfil do Cisco auto qos.
SlaSumCaching.log	Logs do processo de sumarização do SLAview.
SLAdiscover.log	Logs dos processos que mapeiam as conexões de rede via SNMP para a aplicação.
telco_logrotate.log	Logs do processo de roteamento de log.
ALARMaction.log	Logs do processo de enviar alarmes e traps, e-mails e notificações sms.
ALARMDaemon.log	Logs que processam ocorrências e geram alarmes.
ciscoPolicyMapper.log	Logs do processo que mapeiam as políticas de QoS para interfaces na MIB Cisco Class Based QoS.
dbsync.log	Logs do processo de sincronização do banco de dados para ambientes redundantes.
Standyd.log	Logs do processo que controlam os estados de redundância entre o aparelho principal e o de backup.
tmsync.log	Logs do processo de sincronização do dispositivo principal para o de backup em ambientes de redundância.
Gc*	Logs do processo do coletor de lixo.

Logs de configuração

Esta opção disponibiliza os logs da configuração do sistema.

Estes logs são mantidos por um período definido em **Sistema** → **Parâmetros** → **Histórico de configuração** → **Período máximo de armazenamento de histórico de configuração** .

Consulta de dados brutos do SLAview

Permite que os usuários acessem exatamente os valores coletados pelo coletor SNMP do SLAview.

Tabela 8.37. Consulta de dados brutos do SLAview - Passo 1

Coluna	Descrição
Tipo de objeto	Escolha Dispositivo ou Objetos mapeados.
Nome	Nome do objeto.

Clique em **Filtrar** para aplicar um filtro.

Tabela 8.38. Consulta de dados brutos do SLAview - Passo 2

Coluna	Descrição
Objeto	Selecione objetos filtrados.
Tempo de início	Tempo mínimo de coleta.
Tempo de fim	Tempo máximo de coleta.

Clique em **Gerar relatório**.

Imagens de mapa

Abra o menu **Sistema** → **Imagens de mapa** para fazer o upload de uma imagem de fundo para ser usada nos mapas do **Mapview**.

Para fazer o upload de uma nova imagem, clique em Escolher arquivo e depois no botão Adicionar.

Uma vez que foi feito o upload da imagem, clique aqui para saber como usar as imagens.

Fuso horário

Este menu é usado para configurar o fuso horário correto para o servidor. Existem 4 fusos pré-definidos: **Brasília**, **Acre**, **Fernando de Noronha** e **Amazônia**. Você pode selecionar um deles ou fazer o upload de um novo fuso.

Este procedimento é usualmente necessário se existem modificações de dados durante o dia.

Suporte

Esta opção pode ser usada para estabilizar uma conexão segura para os servidores de suporte da internet da Telcomanager.

Uma vez que a conexão é estabelecida, você pode contactar o time de suporte da Telcomanager com o código de serviço.

Dica

Se seu código de serviço não funcionar, tente entrar com um diferente código de serviço.

Sobre

Esta seção lista a versão que está atualmente instalada e as opções de licença.

Você também pode chegar o número de dispositivos existentes, a série de dados históricos e o limite bits/s ou flow/s.

Capítulo 9. ALARMmanager

Relatórios

Para acessar os relatórios ALARMmanager, vá até **ALARMmanager → Relatórios**

Relatórios suprimidos

Este relatório fornece os logs de todas as operações de supressão realizadas pelos usuários.

Tabela 9.1. Formulário de relatório de alarmes suprimidos

Campo	Descrição
Formato de saída	Selecione um dos formatos para o relatório: HTML, CSV ou PDF.
Tipo de objeto	O tipo de objeto para o alarme.
Instante inicial	O instante inicial para o relatório.
Instante final	O instante final para o relatório.
Operação	Filtro para operação de supressão.
Filtro de usuário	Filtra pelo usuário que executou a operação.
Filtro de objeto	Filtra pelo objeto em que a operação foi executada.
Filtro de alarme	Filtra pelo alarme em que a operação foi executada.

Relatórios consolidados

Este relatório disponibiliza uma visão de todos os eventos de alarme de maneira detalhada ou resumida.

Este relatório pode ser salvo como um template. Para instruções em como trabalhar com templates de relatório, vá à seção templates neste manual.

Tabela 9.2. Formulário de alarmes consolidados

Campo	Descrição
Filtro de alarme	Use expressão regular e clique no botão Filtrar para selecionar o alarme desejado.
Filtro de objeto	Use expressão regular para filtrar os objetos desejados.
Fabricante	Filtrar pelo fabricante do objeto. Você tem que usar expressão regular para filtrar.
Tipo de fabricante	Filtrar pelo tipo de fabricante. Você tem que usar expressão regular para filtrar.
Tipo de objeto analisado	Tipo do objeto.
Filtro ifAlias	Filtra baseado na interface OID ifAlias. Você deve usar expressão regular para filtrar.
Instante inicial	Período inicial de análise.

Campo	Descrição
Instante final	Período final de análise.
Período	Se a opção **Dia todo** estiver marcada, este campo é ignorado, ao contrário, o dado é selecionado com aquele intervalo para cada dia.
Excluir fins-de-semana	Excluir período de fins-de-semana do relatório de dados.
Somente ativos	Mostra apenas os alarmes ativos.
Consolidado	Esta opção irá sumarizar todas as ocorrências de alarme para cada objeto.
Somente gerados por trap	Mostra apenas alarmes gerados por traps **link down**.
Formato de saída	Selecione um dos formatos para o relatório: HTML, PDF ou CSV.
Grupos	Este campo pode ser usado para filtrar objetos associados a apenas alguns grupos de root.

Dica

Para ordenar os resultados do relatório, clique em cada cabeçalho da coluna.

Relatórios avançados

Estes relatórios fornecem flexibilidade para visualização de dados em diferentes formatos, utilizando tecnologia de pivoteamento.

Importante

Este relatório é processado em uma base diária, logo, quando você gera o relatório, o dia atual não estará disponível.

Tabela 9.3. Formulário de relatório avançado de alarme

Campo	Descrição
Ação	Ação do alarme.
Instante inicial	Dia inicial. Este filtro irá trabalhar no momento inicial do alarme.
Instante final	Último dia. Este filtro irá trabalhar no momento final do alarme.
Excluir fins-de-semana	Exclui período do fim de semana do relatório de dados.
Tipo	Tipo de objeto.
Fabricante	Filtra pelo fabricante do objeto. Você deve usar expressões regulares para filtrar.
Tipo de fabricante	Filtra pelo tipo de fabricante do objeto. Você deve usar expressões regulares para filtrar.
Dia todo	Marque **Sim** para ter os dados agregados durante o dia todo ou marque **Não** para ter os dados agregados dentro dos dois períodos configurados em **Sistema** → **Parâmetros** → **Relatórios** → **Período de**

Campo	Descrição
	agregação do relatório de alarme avançado . Ex.: 9 a.m. às 12 p.m. e 13 p.m. às 18 p.m.
Todos os objetos	Marque **Sim** para incluir todos os objetos ou marque **Não** para incluir apenas os objetos alarmados.
Formato de saída	Selecione HTML, PDF ou CSV. Opção disponível apenas para relatórios que não são templates. Se você optar por salvar template, esta opção é ignorada.
Alarmes	Selecione os alarmes para o relatório.
Grupos	Este campo pode ser usado para filtrar objetos associados para alguns grupos de root.
Cabeçalho para colunas	Selecione os itens que serão posicionados nas colunas do relatório.
Linhas do cabeçalho	Selecione os itens que serão posicionadas nas linhas do relatório.
Agregação de dados	Veja a seção agregação de dados.

Agregação de dados

O campo agregação de dados é utilizado para definir as células de dados do relatório. Os campos disponíveis são:

- Funções: função para ser aplicada aos dados. As funções disponíveis são:

Formulário de Agregação de Dados

Disponibilidade	Percentual de tempo enquanto o alarme não ficou ativo.
Frequência	Percentual de tempo que o alarme está ativo.
Soma	Soma a ser aplicada aos períodos de alarme.
Média	Média a ser aplicada aos períodos de alarme.
Quantidade	Número de ocorrências de alarmes.
Máximo	Tempo máximo de ocorrências de alarmes.
Mínimo	Tempo mínimo de ocorrências de alarmes.

- Elemento: Dado para ser aplicado à função.
- Sinalização de alarme: definição de limites para coloração da célula. Veja a seção sinalização de relatórios avançados.

Sinalização

A opção sinalização de alarme é usada para colorir as células dos relatórios de alarme avançados.

Quando você usa a sinalização em um relatório, o relatório irá ser colorido de acordo com os limites da configuração.

Vá para **ALARMmanager** → **Relatórios** → **Relatórios avançados** → **Sinalização** e clique no botão Novo para criar um novo relatório de sinalização.

Tabela 9.4. Relatório de sinalização de alarme avançado

Campo	Descrição
Nome	Sinalização do nome.
Descrição	Campo de descrição.
Sinalização de alarmes	Preencha os níveis de sinalização. Exemplo: • 40.00<=critical<=100.00 color red • 20.00<=medium<40.00 color blue • 5.00<=low<20.00 color gray

Template de Email

Introdução

Você pode selecionar o formato de e-mail do ALARMmanager e escolher se você deseja utilizar o template padrão ou personalizá-lo.

Tabela 9.5. Template de Email

Campo	Descrição
Habilitar template de e-mail padrão	Selecione **Não** para customizar o template de email.
Conteúdo de e-mail	Você pode escolher o formato de e-mail que você irá receber (HTML ou Txt).

Customizando o e-mail

Quando você está editando seu template de e-mail, é possível restaurar o padrão apenas clicando no padrão **Restaurar template padrão**.

Se o conteúdo de e-mail está em formato HTML, você pode ter uma pré-visualização antes de salvar o novo template. Para fazer isto, clique no botão **Preview**.

Você terá as seguintes palavras chave entre '**$**' e você pode substituí-las para sua configuração de alarme:

Tabela 9.6. Variáveis de e-mail

Variáveis	Descrição
$date$	Data de ativação/desativação do alarme.
$objtype$	Tipo do objeto: Objeto mapeado ou Device. Alarme de serviço não possui tipo de objeto.
$object$	Nome do objeto.
$path$	Exibe o caminho para o objeto no SLAview.
$alarm$	Nome do alarme.

Variáveis	Descrição
$action$	Estado do alarme: ativado ou desativado.
$level$	Nível de urgência do alarme.
$formula$	Fórmula do alarme.
$varbind$	Varbind.
$suppressed$	Indica se o alarme foi suprimido.
$color$	Variável para ser usada no e-mail HTML. Verde para desativado e vermelho para ativado.

Níveis de urgência de alarme

Os níveis de urgência na aplicação ALARMmanager são customizáveis e você pode configurar quantos quiser.

Para gerenciar os níveis de alarme, acesse o menu **ALARMmanager** → **Níveis de urgência de alarme**.

Aqui você possui uma lista de níveis pré-configurados. Você pode editar níveis e adicionar outros.

Mudando o nível de prioridade da urgência

Para mudar o nível de prioridade de urgência, selecione o nível desejado e clique nas setas UP ou DOWN localizadas no canto superior esquerdo.

Adicionando um novo nível de urgência

Para adicionar um nível de urgência, clique no botão Novo e preencha o formulário.

Tabela 9.7. Formulário de nível de urgência de alarme

Campo	Descrição
Rótulo	Defina uma legenda para o nível de urgência. Ela será mostrada em uma coluna do ALARMmanager console.
Cor do plano de fundo	A cor do plano de fundo que será mostrada no ALARMmanager console.
Cor do texto	Cor do texto que será mostrado no ALARMmanager console.
Aviso sonoro	Habilita som de aviso para este alarme. O som de aviso irá ser tocado pelo Java ALARMmanager Console se esta função também estiver habilitada no console. Para habilitá-la, acesse **ALARMmanager** → **Console** → **botão ALARMmanager** → **Ferramentas**
Alarmes	Selecione os alarmes que irão receber esta prioridade.
Alarmes de serviço	Selecione os alarmes de serviço que irão receber esta prioridade.

Alarmes

Configuração de alarmes padrão

Este tipo de alarme é usado para análise de tráfego imediata, quando não tem condições possíveis para determinar a fórmula. Use este alarme para manter controle sobre as condições de contorno que necessitam de tratamento quando detectadas.

Tabela 9.8. Formulário de alarme padrão

Campo	Descrição
Nome	Texto descritivo para o alarme. Ex.: alto tráfego, sem tráfego HTTP.
Tipo de objeto	Defina se o alarme será de **Dispositivo** ou **Objeto mapeado**.
Tipo de alarme	Escolha **Padrão**.
Fórmula	Veja a seção Fórmula de alarmes padrão.
Variável de sumarização	Selecione a variável de sumarização e clique em **Adicionar variável**.
Varbind	Campo de texto livre que pode ser usado para reconhecer os alarmes que são encaminhados como traps.
Email	Veja a seção de ações.
Dispositivo móvel	Veja a seção de ações.
Trap	Veja a seção de ações.
Provisionamento	Veja a seção de ações.
Script de provisionamento	Selecione um script de provisionamento para ser executado.
Enviar email após (minutos)	Veja a seção de ações.
Enviar mensagens de dispositivo móvel após (minutos)	Veja a seção de ações.
Enviar trap após (minutos)	Veja a seção de ações.
Executar provisionamento após (minutos)	Veja a seção de ações.
Desabilitar trap para alarme suprimido	Se a opção "Não" é selecionada, a trap será enviada e a condição de supressão será indicada nela. A opção "Sim" irá prevenir que a trap seja enviada.
Desabilitar mensagens de dispositivo móvel para alarme suprimido	Se a opção "Não" é selecionada, as mensagens de dispositivo móvel serão enviadas e as condições de supressão serão indicadas nele. A opção "Sim" irá prevenir que as mensagens de dispositivo móvel sejam enviadas.
Desabilitar email para alarme suprimido	Se a opção "Não" é selecionada, o email será enviado e a condição de supressão será indicada nele. A opção "Sim" irá prevenir que o email seja enviado.

Campo	Descrição
Desabilitar provisionamento para alarme suprimido	Selecione "Sim" para impedir que o provisionamento aconteça quando um alarme estiver suprimido.
Ocorrências consecutivas para armar	Escolha o número de ocorrências consecutivas da fórmula de alarme que deve disparar o alarme. Não utilizado em alarmes de Trap.
Não ocorrências consecutivas para desarmar	Escolha o número de não-ocorrências consecutivas da fórmula de alarme que deve desarmar o alarme. Não utilizado em alarmes de Trap.
Nível de urgência	Selecione o nível para o alarme.
Perfil de alarme	Selecione os perfis de alarme aos quais ele deve pertencer.

Fórmula de alarmes padrão

As expressões no campo **Fórmula** são escritas em notação infixa regular.

Você deve escrever as fórmulas seguindo as regras a seguir:

- Use parênteses "()" para precedência da operação.
- Use os operadores lógicos AND e OR.
- Use os operadores de comparação ==,!=,<,>,<=,>=.
- Use os símbolos *,-,+ e / para executar as operações.

Procedimento 9.1. Fórmula de entrada

1. Selecione as variáveis e clique on botão Adicionar variável para transportá-las para a caixa de fórmula.
2. Edite a fórmula na caixa de fórmula para formar a expressão desejada.

Exemplo 1:

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

Os alarmes anteriores serão disparados se o tráfego de entrada ou saída ultrapassar 90% da utilização.

Configuração dos alarmes de mudança de comportamento (Alarmes Históricos)

Mudanças de comportamento do alarme são usadas pelas KPIs (Key Performance Indicators) para as quais é possível estabilizar um comportamento. O princípio da operação deste recurso é estabilizar este comportamento para cada hora do dia e, se a superfície de KPI sofrer uma mudança repentina durante a hora corrente, o sistema irá alarmar esta condição.

O que você deve manter em mente é que algumas variáveis não são adequadas para este tipo de análise. Por exemplo, tráfego de interface para interfaces cujo tráfego é esporádico.

Logo, você deve usar este recurso para as variáveis onde o comportamento é **previsível**.

Bons exemplos do uso deste recurso são:

- Interfaces de rede com alto volume de tráfego.
- Uso de CPU para roteadores com carga significativa.
- Número de conexões em um servidor web com carga significativa.

Exemplos ruins do uso deste recurso são:

- Rede ou servidor com erros em geral.
- Interfaces de rede com tráfego baixo ou com volume imprevisível.

Configuração

Este alarme é baseado em uma análise de tendências que é executada durante um período configurado pelo usuário, para cada alarme. O alarme sempre é aplicado à sumarização de variáveis e tem um fator de tolerância que irá ajudar o seu aperfeiçoamento.

Tabela 9.9. Formulário de mudança de comportamento

Campo	Descrição
Nome	Texto descritivo para o alarme. Ex.: alto tráfego, nenhum tráfego HTTP.
Tipo de objeto	Escolha o tipo de objeto desejado para alarmar: **Dispositivo** ou **Objeto mapeado**.
Tipo de alarme	Escolha **Histórico**.
Variável	Selecione a variável de sumarização e clique no botão **Adicionar variável**.
Horário de ativação	Veja a seção ativação de fórmulas de alarme.
Histórico mínimo (dias)	Mínima quantidade de dias necessários para preencher o período de análise.
Histórico máximo (dias)	Máxima quantidade de dias permitida para preencher o período de análise.
Número de violações consecutivas (dias)	Veja a seção Número de violações consecutivas.
Fator de tolerância	Veja a seção Fator de tolerância.
Período de alarme (minutos)	Veja a seção Período de alarme.
Email	Veja a seção de ações.
Dispositivo móvel	Veja a seção de ações.
Trap	Veja a seção de ações.
Provisionamento	Veja a seção de ações.
Enviar email após (minutos)	Veja a seção de ações.
Enviar mensagens dispositivo móvel após (minutos)	Veja a seção de ações.
Enviar trap após (minutos)	Veja a seção de ações.
Executar provisionamento após (minutos)	Veja a seção de ações.
Desabilitar trap para alarme suprimido	Se a opção não é selecionada, o trap será enviado e a condição de supressão será indicada na trap. A opção **Sim** irá prevenir que a trap seja enviada.

Campo	Descrição
Desabilitar sms para alarme suprimido	Se a condição não é selecionada, o sms será enviado e a condição de supressão será indicada no sms. A opção **Sim** irá prevenir que o sms seja enviado.
Desabilitar e-mail para alarme suprimido	Se a opção não é selecionada, o e-mail será enviado e a condição de supressão será indicada no e-mail. A opção sim irá previnir que o e-mail seja enviado.
Desabilitar provisionamento para alarme suprimido	Selecione "Sim" para impedir que o provisionamento aconteça quando um alarme estiver suprimido.
Ocorrências consecutivas para armar	Escolha o número de ocorrências consecutivas da fórmula de alarme que deve disparar o alarme. Não utilizado em alarmes de Trap.
Não ocorrências consecutivas para desarmar	Escolha o número de não-ocorrências consecutivas da fórmula de alarme que deve desarmar o alarme. Não utilizado em alarmes de Trap.
Nível de urgência	Selecione o nível para o alarme.
Perfil de alarme	Selecione os perfis de alarme aos quais ele deve pertencer.

Fórmulas de horário de ativação

Este campo é usado apenas para alarmes históricos. Ele define quando uma ocorrência de alarme deve ser gerada.

As variáveis utilizadas são weekday e time. Existem duas variáveis que podem ser usadas: **everyday**, para disparar o alarme todo dia da semana e **everytime**, para disparar o alarme todo tempo do dia.

Se você deseja definir quando uma ocorrência de alarme deve ser gerada, você pode usar as variáveis **weekday** e **time** com os operadores definidos. Os valores para weekday devem estar entre 1 (domingo) e 7 (sábado). Para as variáveis **time**, você deve usar HH:MM.

Exemplo:

1. Preencha o campo **Variável** com: "Tráfego de entrada"
2. Preencha o campo **Varbind** com: > 300000
3. Preencha o campo **Fórmula do horário de ativação** com: weekday > 1 and weekday < 7

Este alarme será disparado se o tráfego de entrada ultrapassar 300000 bps e os dias da semana estiverem entre domingo e sábado.

Número de violações consecutivas

A violação das amostras será considerada se elas acontecerem consecutivamente e o número de violações for acima do parâmetro especificado, ao contrário elas serão descartadas da computação do comportamento.

Por exemplo, suponha que você tenha uma mudança de comportamento no alarme para um tráfego de interface e que em algum momento o tráfego era 500MB +- 300MB e o tráfego detectado era 3GB. Esta amostra não será usada na computação comportamental e o tráfego esperado para o dia seguinte continuará sendo 500MB. Esta amostra será apenas utilizada se tiverem N amostras consecutivas violadas, o que caracteriza um novo comportamento.

Fator de tolerância

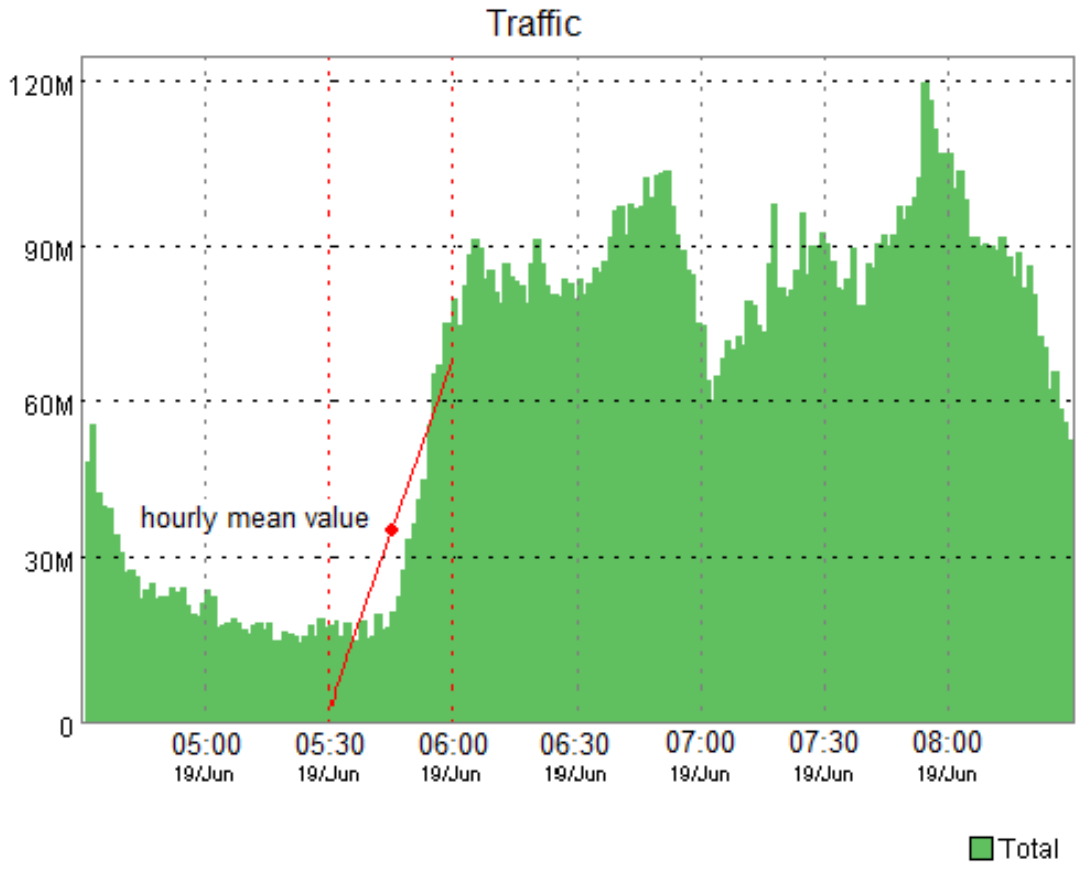
Este fator é medido no valor de desvio padrão e é usado para comparar o valor esperado com o valor atual.

O cálculo a seguir será executado para determinar se o valor observado determina uma mudança de comportamento:

```
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 mostrado no gráfico a seguir, o sistema calcula o valor da média para cada meia hora do dia.

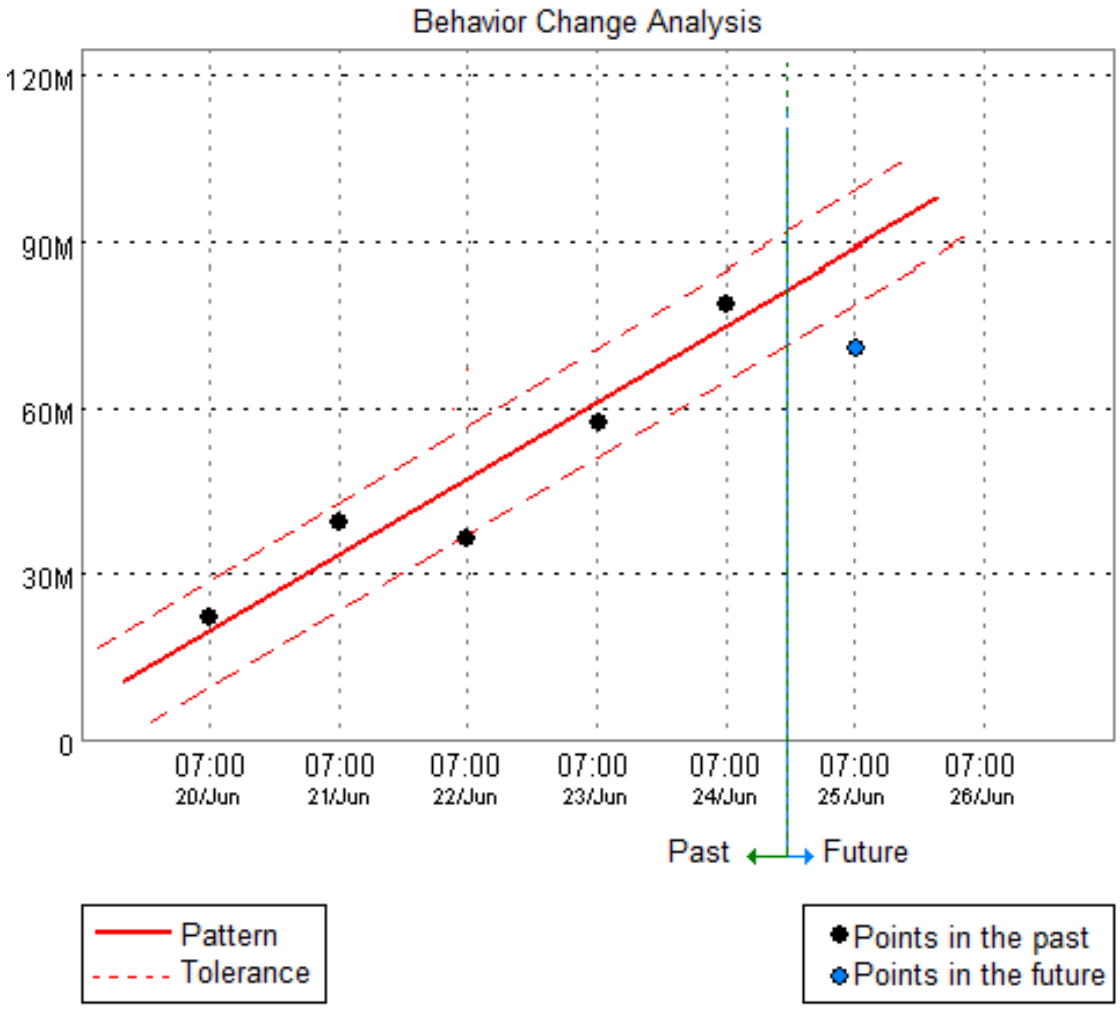


Behavior change mean value

Uma vez que o SLAview possua os valores disponíveis para calcular o valor da média para a meia hora atual, este valor é calculado e comparado ao valor esperado, como descrito anteriormente.

Na imagem a seguir, você pode ver o algoritmo que o SLAview utiliza para estimar valores futuros para cada meia hora do dia. Ele basicamente executa uma aproximação para a função de primeiro grau usando

variável histórica e se o os valores futuros atuais cairem entre essas funções, considerando o fator de tolerância, o alarme será ligado.



Behavior change trend analysis

Período de alarme

SLAview irá mostrar uma amostra a cada 30 minutos ou a cada 5 minutos.

Quando o período de alarme é configurado como 5 minutos, o sistema irá mostrar o valor da média para cada 5 minutos e irá comparar com o valor esperado, mas ele não será salvo se tiver uma mudança no comportamento.

Quando o período de alarme é configurado como 30 minutos, o sistema irá mostrar o valor da média para cada meia hora e determinará se o valor observado representa uma mudança no comportamento.

Ações

Cada momento que o sistema do SLAview processa um polling de SNMP de 5 minutos, todas as fórmulas de alarme são avaliadas e, se elas retornarem verdadeiro, ocorrências serão geradas. O alarme irá disparar para uma condição de alarme apenas se o número de ocorrências consecutivas limite for ultrapassado.

A exceção do comportamento anterior é o ICMP polling, onde o polling pode tomar lugar a cada minuto.

Quando você marca uma ação para um alarme, você tem que preencher alguns campos:

Campos de ação

Ocorrências consecutivas para armar	Isto representa o número de vezes consecutivas em que o limite é ultrapassado.
Não ocorrências consecutivas para desarmar	Isto representa o número de vezes consecutivas em que o limite não é ultrapassado.

Tipos de ações

Email	Email será enviado ao usuário. O servidor SMTP do SLAview deve ser configurado, bem como o email de cada usuário no formulário de configuração do usuário. O email será enviado após o número de minutos definido no campo **Enviar email após (minutos)**, começando do horário de ativação.
Dispositivo móvel(SMS)	Mensagens mais curtas que as enviadas por email. Este alarme pode ser enviado para um email pelo gateway de SMS se o campo de SMS estiver configurado no seguinte formato: 88888888@operador.com. Se o SMS é um número de telefone, os protocolos SMPP ou HTTP também podem ser usados para enviar a mensagem. Para fazer isto, você precisa configurar o seguinte item: **Sistema** → **Parâmetros** → **Servidor SMS** .
Dispositivo móvel(Telegram)	Uma mensagem será enviada para um chat do Telegram por um bot. Para configurar esta funcionalidade , você deve criar um bot no Telegram, para fazê-lo, uma vez no Telegram, inicie uma conversa com o usuário @BotFather. Escolha a opção /newbot e siga as instruções para finalizar a criação do bot. Ao terminar anote o token do bot Telegram. Associe o bot ao chat no qual as mensagens serão enviadas. Acesse o formulário de perfil de usuários, preencha o campo "Token do bot Telegram" e clique em Validar. Se tudo correr bem, o campo "ID do chat Telegram" será automaticamente preenchido. A mensagem será enviada após os segundos definidos no campo **Enviar mensagem após**, iniciando pelo tempo de ativação do alarme.
Trap	Uma trap será enviada para cada alarme. A trap deve ser interpretada usando a MIB TELCOMANAGER-ALARMMANAGER-MIB.my, que está disponível na lista de mib no SLAview. Você deve configurar o servidor para enviar traps em **Sistema** → **Parâmetros** → **SNMP** → **SNMP trap** . A trap será enviada depois do número de minutos definido no campo **Enviar trap após (minutos)**, começando do horário de ativação.
Provisionamento	Um script de provisionamento será executado caso o alarme seja ativado. A execução acontecerá assim que passar o número de minutos configurado no campo **Executar provisionamento após (minutos)**, começando do horário de ativação.

Gráfico de alarme de mudança de comportamento

Uma vez que você configura um alarme de mudança de comportamento, um novo ícone de gráfico, com uma legenda **Mudança de comportamento**, estará disponível para todos objetos que estão associados àquele alarme.

Este gráfico está disponível para cada alarme configurado para aquele objeto e contém três curvas. Uma curva é o valor da média para as variáveis de sumarização e as outras duas curvas são os limites superior e inferior para a geração da ocorrência de alarme.

Configuração de alarmes syslog

Tabela 9.10. Formulário de alarme syslog

Campo	Descrição
Nome	Texto descritivo para o alarme.
Tipo de alarme	Escolha **Syslog**.
Email	Veja a seção de ações.
Dispositivo móvel	Veja a seção de ações.
Trap	Veja a seção de ações.
Provisionamento	Veja a seção de ações.
Script de provisionamento	Selecione um script de provisionamento para ser executado.
Enviar email após (minutos)	Veja a seção de ações.
Enviar mensagens de dispositivo móvel após (minutos)	Veja a seção de ações.
Enviar trap após (minutos)	Veja a seção de ações.
Executar provisionamento após (minutos)	Veja a seção de ações.
Desabilitar trap para alarme suprimido	Se a opção "Não" é selecionada, a trap será enviada e a condição de supressão será indicada nela. A opção "Sim" irá prevenir que a trap seja enviada.
Desabilitar sms para alarme suprimido	Se a opção "Não" é selecionada, o sms será enviado e a condição de supressão será indicada nele. A opção "Sim" irá prevenir que o sms seja enviado.
Desabilitar email para alarme suprimido	Se a opção "Não" é selecionada, o email será enviado e a condição de supressão será indicada nele. A opção "Sim" irá prevenir que o email seja enviado.
Desabilitar provisionamento para alarme suprimido	Selecione "Sim" para impedir que o provisionamento aconteça quando um alarme estiver suprimido.
Nível de urgência	Selecione o nível para o alarme.
Filtro de syslog de ativação	Selecione um Filtro de Syslog para ativar o alarme.
Desativar por	Escolha **Horário** ou **Syslog**.
Tempo de desativação	Selecione o horário para desativar o alarme.

Campo	Descrição
Filtro de syslog de desativação	Selecione um Filtro de Syslog para desativar o alarme.
Perfil de alarme do dispositivo	Selecione os perfis de alarme aos quais ele deve pertencer.

Gerenciamento de supressão de alarmes

Nesta seção você irá aprender como gerenciar todas as tuplas de alarme/objeto as quais o usuário possui acesso.

Para suprimir, siga o procedimento abaixo:

1. Vá para guia **ALARMmanager** → **Alarmes** e clique no botão Alarmes suprimidos.
2. Preencha os campos do filtro desta forma para selecionar os alarmes/objetos desejados e clique no botãoFiltro.
3. Selecione os alarmes/objetos da lista.
4. Preencha o campo razão de supressão se desejado.
5. Clique no botão Salvarpara suprimir os alarmes/objetos selecionados.

Para tirar a supressão dos alarmes, siga o mesmo procedimento, mas deselecione os alarmes/objetos desejados.

Importante

Perceba que se o alarme já está suprimido, ele não será suprimido novamente e o mesmo acontece à ação de desuprimir.

Importante

Alarmes suprimidos podem ser considerados para colorir o mapa usando a flag "Considerar suprimido" no MapView. Se um alarme suprimido é inativado por um momento e depois fica ativo, ele é marcado como suprimido.

Perfis

Perfis são usados para juntar alarmes e objetos monitorados.

Perfis de alarme podem ser automatizados utilizando as mesmas regras para sumarização de perfis. Defina os horários para a execução automática em: **Sistema** → **Parâmetros** → **Agentes de associação** → **Perfil automático de alarme** .

Procedimento 9.2. Gerenciando perfis de alarme

1. Vá para **ALARMmanager** → **Perfis**.
2. Clique no botão Novo ou selecione um perfil e clique no botão Editar.
3. Depois de definir um nome, escolha o tipo de objeto de acordo com o objeto que deve ser monitorado: Dispositivo ou Objeto Mapeado.
4. O próximo passo é definir o tipo de associação de objeto: manual ou automática.

5. Associe os alarmes ao perfil.

6. Finalmente, associe os objetos que devem ser monitorados. Na associação manual, clique no objeto respectivo e arraste da caixa da esquerda para a da direita. Na associação automática você terá que clicar na regra de associação e arrastar da caixa da esquerda para a da direita. Veja a seção Regras.

Importante

Quando um objeto ou um alarme é associado, o sistema chega se os alarmes são compatíveis aos objetos. Se eles não forem compatíveis, a configuração não é permitida. Um objeto é compatível com um alarme se ele tem todas as variáveis de sumarização da fórmula de alarme.

Alarmes de serviço

Introdução

O recurso de alarmes de serviço permite que você junte alarme de diferentes objetos em uma única fórmula. Agora o TRAFip pode disparar o alarme sob condições mais sofisticadas.

Você será capaz de criar, por exemplo, os seguintes alarmes:

- Um alarme que é ativo quando um link de WAN tem uma alta latência e também possui um baixo tráfego.
- Um alarme para lhe dizer quando ambos o primário e os links de backup de locação irão falhar.

Criando um novo Alarme de Serviço

1. Selecione **ALARMmanager** → **Alarmes de serviço**. Clique no botão novo para definir um novo tipo.

2. Preencha o formulário de acordo com as instruções abaixo:

Tabela 9.11. Formulário de alarmes de serviço

Campo	Descrição
Nome	Nome do alarme de serviço.
Varbind	Variável de uma trap para ser enviada quando o alarme se tornar ativo.
Fórmula	Fórmula de alarme de serviço. A fórmula é construída usando os seguintes campos: Objeto, Nome e Alarme
Objeto	Tipo de objeto ao qual o alarme de serviço está relacionado. É usado para construir a fórmula.
Nome	Nome do objeto escolhido no campo "Objeto". É utilizado para construir a fórmula.
Alarme	Alarme que será associado ao objeto escolhido nos campos "Objeto" e "Nome". Para aprender mais sobre alarmes leia a seção: AlarmManager Alarmes.
E-mail	Um e-mail será enviando aos usuários.
Enviar e-mail após	Atraso, em minutos, para enviar um e-mail aos usuários.

Campo	Descrição
Dispositivo móvel	Um SMS e/ou uma mensagem para um chat Telegram serão enviados..
Enviar SMS e/ou mensagem Telegram após	Atraso, em minutos, para enviar uma mensagem de dispositivo móvel aos usuários.
Trap	Uma Trap será enviada quando o alarme se tornar ativo.
Enviar trap após	Atraso, em minutos, para enviar uma Trap.

Fórmula

Nas fórmulas você pode usar os operadores lógicos OR, AND, NOT e XOR para construir fórmulas mais complexas.

Console

Introdução

A aplicação ALARMmanager trabalha de forma integrada entre os sistemas e é capaz de gerar alarmes baseados em fórmulas.

Ela também possui os seguintes recursos:

- Interface gráfica em HTML5.
- Alarme através de email, mensagens de dispositivo móvel e traps.
- Grupo de usuários para receber alarmes.
- Interface gráfica para criar alarmes e fórmulas customizadas.
- Alarmes podem emitir sons.
- Perfis de alarme para facilitar a associação de alarmes aos objetos gerenciados.
- Reconhecimento de alarmes e comentários.
- Supressão de alarmes para evitar emails, mensagens de dispositivo móvel e traps para alarmes repetidos.

Operação de Console

Para acessar o console operacional de alarme, vá em **ALARMmanager** → **Console**

Autenticação

Um usuário deve estar autenticado para acessar o ALARMmanager.

Controle de acesso

Cada usuário irá receber alarmes sobre objetos de acordo com as associações da hierarquia do grupo e aos alarmes configurados a ele em perfil de usuários.

Console

O console do ALARMmanager irá mostrar todos os alarmes que estão ativos e também inativos que ainda não foram inativos pelo parâmetro de período de armazenamento do ALARMmanager. Os alarmes que você poderá visualizar dependerão da permissão que o seu usuário possui.

Você pode configurar as colunas em **Sistema** → **Usuários** → **Alarm console** .

O console possui as seguintes colunas:

Tabela 9.12. ALARMmanager console

Coluna	Descrição
INÍCIO	O momento da primeira ocorrência.
TÉRMINO	O momento da última ocorrência. Mostra ATIVO se o alarme ainda não terminou.
USUÁRIO	Usuário que programou o alarme.
TIPO	Tipo de objeto, pode ser dispositivo ou objeto mapeado.
OBJETO	Nome do objeto.
DESCRIÇÃO	Se o objeto é uma interface, mostra seu ifAlias.
CAMINHO	Mostra o primeiro caminho para o objeto nos grupos SLAview.
ESTADO	Estado do alarme, pode ser ativo ou inativo.
ALARME	Nome do alarme.
NÍVEL	O nível do alarme definido na configuração de nível.
TRAP	Sim se foi gerado por um trap e não caso contrário.
COMENTÁRIOS	Comentário pelo operador. Para inserir um comentário, clique duas vezes naquela célula.

Reconhecimento de alarme

Uma vez que o alarme é reconhecido, a linha de alarme mostra o nome de usuário que executou a operação e sua informação também pode ser vista em relatórios de alarmes consolidados. Depois de reconhecer um alarme, você é capaz de inserir comentários para o alarme.

Para reconhecimento de alarme, clique com o botão direito nele e depois selecione a opção Reconhecer alarmes no menu. O alarme é depois mostrado na tabela de alarmes reconhecidos para todos os operadores.

Para múltiplos reconhecimentos de uma vez, selecione com o botão esquerdo do mouse e depois clique com o botão direito na lista para mostrar o menu.

O alarme pode ser liberado do operador apenas pelo usuário administrador. Para isso, o administrador deve selecionar o alarme de reconhecimento na lista e selecionar a opção de alarme Liberar alarmes no menu.

Supressão de alarme

O mecanismo de supressão de alarme permite que você suprima qualquer tupla de alarme/objeto, desde que o alarme já esteja configurado para aquele objeto. A supressão também desabilitará os e-mails, mensagens

de dispositivo móvel e traps para o alarme/objeto ou indicará esta condição nos e-mails, mensagens de dispositivo móvel e traps. Você deve configurar o comportamento desejado neste campo em configuração de alarme.

Para suprimir um alarme siga o procedimento abaixo:

1. Selecione o alarme desejado com o botão esquerdo do mouse. Para escolher mais de um alarme, segure a tecla CTRL e selecione os alarmes com o botão esquerdo do mouse.
2. Clique com o botão direito do mouse para mostrar o popup menu. Clique na opção Suprimir alarmes no popup menu.
3. Preencha a caixa de texto com a razão de supressão. Você também pode deixá-la em branco.
4. Clique no botão Confirmar.

Você pode checar as operações de supressão de log executadas pelos usuários em relatório de alarmes suprimidos.

Você pode gerenciar a lista de supressão de alarme/objeto em **ALARMmanager** → **Alarmes** → **Supressão de alarmes** .

Comentário de alarmes

Para inserir comentários para um alarme, primeiramente você precisa reconhecê-lo.

Para inserir um comentário, siga o procedimento abaixo:

1. Clique na tabela "Reconhecidos".
2. Dê um duplo clique na coluna COMENTÁRIOS para o alarme.
3. Preencha a caixa de texto na janela Comentários de Alarme e clique no botão Confirmar.

Habilitar som para um alarme

O som do alarme irá funcionar se tiver um ativo, não reconhecido, Critical ou Major no ALARMmanager console.

Selecione a opção **ALARMmanager** → **Console** → **Habilitar aviso sonoro** .

Sincronização de alarme

O ALARMmanager sincroniza seus alarmes com o banco de dados do sistema a cada 2 minutos. Esta sincronização pode ser acionada imediatamente no menu **ALARMmanager** → **Console** → **Sincronizar alarmes** .

Excluindo alarmes

O ALARMmanager deleta automaticamente os alarmes que tenham terminado, mas você será capaz de visualizá-los depois no console até que o armazenamento máximo de alarmes inativos tenha passado. Para configurar este parâmetro vá ao menu **Sistema** → **Parâmetros** → **ALARMmanager** .

O operador pode deletar os alarmes a qualquer momento se ele estiver no estado inativo, selecionando os alarmes com o botão direito no mouse e clicando na opção Apagar no popup menu.

Abrir gráficos

Selecione uma linha de alarme e clique no botão Abrir gráficos para abrir os gráficos do objeto.

Filtro de alarme

Este filtro pode ser acionado de qualquer objeto em qualquer mapa. Isto irá filtrar os alarmes dos objetos e também dos objetos relacionados a ele hierarquicamente.

Cheque esta seção para instruções de como usar este filtro.

Localizando objeto nos mapas

Selecione uma linha de alarme no console e depois clique no botão Localizar no MapView para abrir o mapa que contém os objetos de alarme.

Capítulo 10. MapView

Introdução

A ferramenta Mapview trabalha junto com o SLAview e plota uma representação gráfica da estrutura dos grupos do SLAview.

Os mapas do Mapview são hierárquicos, assim como o SLAview. Além disso, subgrupos ou dispositivos dentro do grupo são representados como ícones gráficos e mudam de cor baseados em alarmes.

O Mapview também plota conexões entre esses elementos, identificando as conexões baseadas no tabelas SNMP CDP (Cisco Discovery Protocol), tabelas SNMP LLDP (Link Layer Discovery Protocol) e tabelas SNMP IP, onde interfaces na mesma subrede de 30 bits são consideradas conectadas.

Principais recursos

- Aplicativo em HTML5 com interface gráfica.
- Topologia de rede hierárquica.
- Fácil navegação com o mouse e interação por todo o mapa.
- Integração com o ALARMmanager, o que permite a filtragem de alarme clicando em qualquer objeto do mapa, possibilitando a isolação de um problema.
- O mesmo elemento de rede pode ser associado a múltiplos mapas, habilitando diferentes visões topológicas da rede.
- Controle de acesso baseado no usuário.
- Imagem de fundo configurável.
- Link de conexão automática entre elementos de rede.
- Tamanho e posições editáveis para cada elemento do mapa.
- Visualização de mapas georreferenciados.

Operação

Navegação no mapa

Os mapas do Mapview refletem a estrutura dos grupos hierárquicos do sistema SLAview. Você pode navegar através daquela hierarquia clicando em cada ícone com o botão direito do mouse e o abrindo.

Você também pode navegar no link hierárquico clicando nos links de mapas com o botão direito do mouse.

Filtro de alarme para o mapa

Este filtro pode ser acionado de qualquer mapa. Ele está localizado abaixo das legendas de cor do mapa.

Para usar este filtro você deve seguir os passos abaixo:

1. Selecione o botão Exibir localizado na parte inferior de qualquer mapa. Neste momento, a janela de Filtro de Alarme irá aparecer.

2. Selecione os alarmes que você deseja filtrar e depois os posicione na caixa da direita da janela de Filtro de Alarme.

3. Selecione a opção **Incluir alarmes** para ter aqueles alarmes aparecendo no mapa ou a opção **Excluir alarmes** para excluí-los do mapa.

4. Clique no botão OK para ter este filtro aplicado ao mapa em questão.

Para desabilitar este filtro, clique em Limpar filtro.

Filtro de alarme de objeto

Este filtro pode ser acionado em qualquer objeto de qualquer mapa. Ao clicar com o botão direito do mouse em um objeto no Mapview, serão mostradas opções como **Filtrar alarmes no ALARMmanager** e **Filtrar excluindo alarmes do ALARMmanager**.

Ambas as opções abrirão o console de alarmes, a diferença é que **Filtrar alarmes no ALARMmanager** irá mostrar apenas os alarmes do objeto selecionado e dos objetos relacionados hierarquicamente a ele e **Filtrar excluindo alarmes do ALARMmanager** irá mostrar todos os alarmes **exceto** os do objeto selecionado e dos objetos relacionados hierarquicamente a ele.

Dica

O filtro de alarme de objeto pode trabalhar juntamente com o filtro de alarme para o mapa. Essa funcionalidade é interessante quando você precisa checar os alarmes referentes apenas a um determinado dispositivo ou grupo e não de seus objetos subordinados, por exemplo. Nesta situação, o console de alarmes exibirá **Filtro habilitado**.

Salvando o mapa

Você pode salvar os seguintes atributos do mapa:

- Posição e tamanho de cada objeto do mapa.
- Tamanho da fonte para cada objeto do mapa.
- Tamanho da janela do mapa.

Para executar esta operação clique no menu **Arquivo → Salvar Mapa**.

Mudando o modo de visualização

É possível visualizar um mapa georreferenciado usando o menu **Visualização → Visualizar como GIS** ou o atalho **T**. Nele, os objetos são dispostos de acordo com suas latitudes e longitudes.

No caso de dispositivos, a localização geográfica é configurada no formulário do próprio dispositivo nos campos **Latitude** e **Longitude**. Já os grupos de dispositivos são posicionados a partir de uma média das localizações dos dispositivos pertencentes ao grupo.

Para voltar ao modo normal de visualização, basta usar novamente o atalho **T** ou o menu **Visualização → Visualizar como imagem**.

Importante

Para visualizar o gráfico neste modo, é necessário cadastrar uma chave fornecida pelo MapQuest. Cadastre esta chave em **Sistema** → **Parâmetros** → **Mapa GIS** .

Layout em grid

Para aplicar o layout em grid aos elementos do mapa, clique no menu **Ferramentas** → **Layout em grid**.

Criando e removendo conexões

Para criar uma conexão entre dois objetos do mapa, clique nos dois objetos com o botão SHIFT pressionado e clique no menu **Editar** → **Criar enlaces**.

Para remover a conexão, selecione os dois objetos e clique no menu **Editar** → **Remover enlace**.

Editando as propriedades do objeto do mapa

Para editar vários objetos simultaneamente, selecione-os arrastando o mouse em torno deles e depois clique nas opções no menu Editar e clique na área do mapa para ver as mudanças. Para salvar as mudanças é necessário que você salve o mapa.

Mudando imagem de fundo

Para definir uma imagem para o mapa, clique na opção **Editar** → **Imagens de Mapas** e escolha um mapa.

Para fazer upload de uma nova imagem no sistema, vá em **Sistema** → **Imagens de mapa**.

Zoom in/out

Clique com o botão direito do mouse na área selecionada do mapa para selecionar as opções Aproximar/ Afastar. A opção **Estado Inicial** volta para o zoom inicial.

Estender imagem

Usando o menu **Visualização** → **Estender imagem** ou o atalho **B**, é possível estender a imagem de fundo do MAPview de acordo com o tamanho da janela.

Para voltar ao modo padrão, onde o tamanho da imagem de fundo não se altera, basta usar novamente o atalho **T** ou o menu **Visualização** → **Manter o tamanho da imagem**.

Capítulo 11. Recursos habilitados com licença

Redundância

A solução de redundância te habilita a implantar dois appliances idênticos trabalhando em modo HOT-STANDBY.

Importante

Essa funcionalidade só funcionará se os dois appliances estiverem na mesma versão.

Dica

É aconselhável que os appliances tenham as mesmas configurações de hardware. Caso haja diferenças, o sistema mostrará um aviso.

Conceitos

- Quando este recurso é habilitado, o sistema trabalha com duas máquinas idênticas em HOT-STANDBY realizando a sincronização dos dados e observando cada um dos estados a todo momento.
- Um protocolo de comunicação roda entre os dois servidores e, se uma falha é detectada em um dos servidores, o outro irá agir como o servidor ativo - se ele já não estiver - e a trap tmTSRedundancyStateChangeTrap será enviada. Esta trap é documentada na MIB TELCOMANAGER-TELCOSYSTEM-MIB.
- Ambos appliances compartilham o mesmo endereço IP, que é usado para enviar fluxos dos roteadores. Este endereço de IP é ativo apenas no servidor ATIVO e quando mudam de estado, o endereço MAC da interface irá migrar para o servidor ATIVO.

Habilitando a redundância

1. Usando dois appliances Telcomanager idênticos com a opção de licença de redundância habilitada, faça uma conexão back-to-back usando a mesma interface em cada dispositivo e configure um endereço de IP não-válido entre aquelas interfaces, usando CLI (command line interface) em cada dispositivo.
2. Na CLI, configure o endereço de IP que será compartilhado entre dois servidores apenas no servidor ativo.
3. Vá ao menu **Sistema** → **Parâmetros** → **Redundância** e preencha o formulário de ambos os dispositivos.
4. Espere 20 minutos para verificar o estado de cada servidor em **Sistema** → **Diagnósticos** → **Informação de rede** .

Arquitetura distribuída

Conceitos

A arquitetura distribuída deve ser usada para dimensionar a capacidade do sistema para coletar fluxos de IP e dados SNMP e para processar os dados brutos, uma vez que essas tarefas são designadas ao appliance coletor.

Pré-requisitos

- Todas as máquinas envolvidas devem ter o mesmo acesso SNMP para todos os dispositivos monitorados.
- Os fluxos de IP devem ser exportados para os appliances coletores.
- Deve possuir largura de banda suficiente para transferir os arquivos de sumarização entre os appliances coletores e appliance central. Mantenha em mente que um coletor requer em torno de 64 Kbps de largura de banda para monitorar 1000 interfaces com 10 variáveis de sumarização em cada interface.
- As portas TCP 22 e 3306 devem estar disponíveis entre o appliance coletor e o central. A porta 22 é usada para transferir arquivos no protocolo SSH e a 3306 é utilizada para emitir consulta do banco de dados para o appliance central.

Implantação

1. No appliance central, vá em **Sistema** → **Parâmetros** → **Arquitetura distribuída** e preencha o formulário.
2. No appliance coletor, vá em **Sistema** → **Parâmetros** → **Arquitetura distribuída** .
3. No appliance central, vá em **Configuração** → **Coletoras** e preencha o formulário.
4. Espere em torno de 20 minutos e vá ao menu **Configuração** → **Coletoras**, para checar se as coletoras listadas estão com o menu em status **ON**.