Manual TRAFwatcher

Manual TRAFwatcher

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 e protocolo TCP/IP.

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

TRAFwatcher é um módulo que atua juntamente com o TRAFip para ajudar na detecção de ameaças na sua rede.

Principais recursos

- Suporte para NetFlow, jFlow, sFlow, IPFIX e Huawei netstream.
- Acesso a todos os recursos do sistema através de um web browser.
- Alta disponibilidade pode ser oferecida pelo uso de soluções redundantes, em que dois appliances trabalham em HOT-STANDBY.
- 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.
- Banco de dados de alta performance para dados históricos armazenados.
- Perfis de ameaça que podem ser associados à subredes para que endereços IPs dentro delas sejam alarmados caso os limites definidos sejam ultrapassados.
- Criação de scripts para anunciar endereços IPs suspeitos em blackhole.

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. 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.

Painel de Controle

Esta aba mostra os limites e um resumo dos IPs que tiveram tráfego suspeito detectado no momento para cada subrede.

Limites

Para cada subrede, será mostrada uma tabela contendo os limites, os valores máximos, as médias e as distâncias percentuais entre as médias e os valores máximos de **Bytes de origem**, **Bytes de destino**, **Fluxos de origem**, **Fluxos de destino**, **Pacotes de origem**, **Pacotes de destino**, **IP Flood de origem** e **IP Flood de destino**.

Se a subrede estiver usando o limite automático, aparecerá um **(auto)** ao lado dos valores dos limites.

A distância percentual do valor máximo para a média é calculada da seguinte forma:

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

Resumo das últimas ameaças

São mostrados os IPs (origem ou destino), a duração do ataque, o tipo de ataque detectado, o tipo do limite que foi ultrapassado, o valor do limite e o valor que foi observado no tráfego.

Clicando no botão **Adicionar à lista de exclusão**, o IP passará a ser excluído da análise de tráfego suspeito.

Para rodar o script de **Blackhole** manualmente, clique no ícone mostrado na coluna **Blackhole**.

Para obter estatísticas detalhadas e consolidadas para cada fluxo, gere um **relatórios de dados brutos** clicando no ícone  .

Importante

Só aparecerão nesta tela as subredes que usam limite automático ou que estão associadas a algum Perfil de Ameaça.

Subredes

Os objetos de subredes permitem a análise de blocos IP.

Definições

- **Tráfego de destino da subrede**: composto pelo somatório de todos os fluxos em que o endereço de IP de destino pertence ao bloco de IP de subrede.

- **Tráfego de origem da subrede**: composto pelo somatório de todos os fluxos em que o endereço de IP de origem pertence ao bloco de IP da subrede.
- **Tráfego absoluto da subrede**: composto pelo somatório de todos os fluxos em que o endereço de IP de origem ou destino pertence ao bloco de IP de subrede.
- **Tráfego absoluto externo da subrede**: composto pelo somatório de todos os fluxos em que o endereço de IP pertence ao bloco de IP da subrede, porém ou o endereço IP de origem ou de destino pertencem a uma subrede desconhecida.

Configuração

Para gerenciar o sistema de subredes, acesse **Dados Históricos** → **Subredes**.

Clique no item de menu da árvore **Subredes** para ter a lista de subredes configuradas.

Para adicionar uma nova subrede, clique no botão **Novo** e preencha o formulário.

Tabela 2.1. Formulário de nova subrede

Campos	**Descrição**
Nome	Nome da subrede.
Descrição	Descrição de subrede.
Blocos de endereço IP	Subredes podem ter mais que uma faixa de endereços. Ex: 10.0.0.0/24, 10.0.1.0/24, 2001:db8:abcd:2000::/64, 2001:cdba:9abc:5678::/64.
Tráfego limite (bps)	Este valor será plotado no gráfico do objeto como uma linha pontilhada vermelha.
Threshold do Fator de Atividade de origem	Limite do **Fator de Atividade** de origem.
Threshold do Fator de Atividade de destino	Limite do **Fator de Atividade** de destino.
Habilitar projeção	Use os parâmetros padrão de projeção ou defina-os.
Habilitar TRAFWatcher	Selecione **Sim** para habilitar a Análise de Ameaças pelo TRAFwatcher.
Usar limite automático	Selecione **Sim** para que o sistema calcule os limites automaticamente de acordo com o tipo do **Fator de tolerância**. Se você selecionar **Não**, a detecção de ameaças será realizada a partir dos limites configurados manualmente no **Perfil de ameaça**.
Fator de tolerância	Este campo só está disponível quando o campo **Usar limite automático** for **Sim**. O fator **Extremo** é mais tolerante às ameaças, ou seja, os thresholds serão maiores caso essa opção seja selecionada. Para uma avaliação moderada de ameaças, selecione **Moderado**.
Perfil de ameaça	Este campo só está disponível quando o campo **Usar limite automático** for **Não**. Selecione o perfil de ameaça para esta subrede para ser usado na Análise de ameaças ou deixe em branco.

Campos	Descrição
Perfil de alarme	Associação de perfil de alarme.

Dica

Você pode habilitar o TRAFwatcher para várias subredes simultaneamente. Para isso, na lista de todas as subredes, selecione as que você deseja habilitar para o TRAFwatcher e clique no botão **Habilitar TRAFwatcher**.

Importar arquivos de subredes

Para importar um arquivo de subrede, acesse **Dados históricos** → **Subredes**.

Clique no item **Subredes** no menu da árvore.

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

Uma subrede importada possui os seguintes campos:

Tabela 2.2. Campos de um arquivo de subrede

Campo	Descrição
Nome	Nome da subrede.
Descrição	Descrição da subrede (opcional).
Blocos de endereço IP	Subredes podem ter mais que uma faixa de endereços. Formato de entrada: IP1/Máscara1,IP2/Máscara2 (IP/32 no caso de usar um IP único). Ex: 10.0.0.1/32,10.0.1.0/24
Tráfego limite (bps)	Preencha com valores inteiros maiores ou iguais a 0.
Habilitar TRAFwatcher	Preencha com **YES** ou **NO**.

Adicionar metadados de subredes

Para acessar a página de configuração de metadado, acesse **Dados históricos** → **Subredes**, clique no item **Subredes** no menu da árvore e clique no botão **Metadado**.

Clique no botão **Novo** para criar um novo metadado. Ele pode ser do tipo **Texto**, **Inteiro** ou **Enum**.

Você pode alterar o metadado quando desejar usando o botão **Editar** e verificar o histórico de alterações através do botão **Histórico**.

Para remover um metadado, clique no botão **Apagar**.

Tabela 2.3. Campos de um metadado

Campo	Descrição
Nome	Nome do metadado.
Descrição	Descrição do metadado.
Tipo de dado	Escolha se o metadado será do tipo **Texto**, **Inteiro** ou **Enum**.

Campo	Descrição
Valores	Este campo só é disponível se o **Tipo de dado** for **Enum**. Entre com uma lista de valores, separando-os por ponto e vírgula (;).

Para associar o metadado criado à uma subrede, acesse a lista de subredes e clique no botão **Metadado** ao lado da subrede que será configurada.

Após, preencha os metadados de acordo com o tipo. Você pode preencher todos eles ou apenas os que desejar.

Estatísticas

Ao acessar uma subrede através do menu lateral, o display de dados mostrará suas estatísticas para cada 5 minutos.

São mostrados os valores de **Média** e **Máximo** dos bytes, pacotes, fluxos e IP Flood de origem e de destino.

No topo da página, são exibidos os valores mais altos registrados.

Importante
É necessário que a subrede esteja associada a um Perfil de Ameaça para que estes valores sejam obtidos.

Importante
A subrede que ultrapassar o limite definido no perfil de ameaça associado a ela, terá sua célula destacada na cor vermelha.

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 2.4. 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.

Campos	Valores
Enviar relatório para servidor FTP	Enviar para o servidor FTP.
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: Pode ser **Imediata** ou **Agendada**. Os instantes inicial e final dos dados serão configurados no próprio formulário.
- Diário: Defina um **Horário de Execução** e todo dia, neste horário, será executado um relatório com período de 1 dia. Se a opção **Considerar dia da execução** estiver marcada, o dia de execução será considerado neste período.
- Semanal: Defina um **Dia da semana** e um horário para que o relatório seja executado. Os dados terão início no Domingo às 00h e fim no Sábado da semana anterior às 23h59min. Se a opção **Considerar dia da execução** estiver marcada, a semana do dia de execução será considerada neste período.
- Mensal: Defina um **Dia de execução** e um horário para que o relatório seja executado. Os dados terão início no dia 01 às 00h e fim no último dia do mês anterior às 23h59min. Se a opção **Considerar dia da execução** estiver marcada, o mês do dia de execução será considerado neste período.

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 Ameaças

O relatório de análise de ameaças fornece informações detalhadas a respeito de tráfegos suspeitos, mostrando IPs de origem e de destino, quando o fluxo começou e quando terminou. Além disso, mostra qual parâmetro do perfil de ameaça foi ultrapassado: Bytes/s, Pacotes/s, Fluxos/s ou Endereços IP/s.

Para gerar um novo relatório, acesse **Dados Históricos** → **Relatórios** → **Análise de Ameaças** .

O formulário já estará preenchido, mas você poderá editá-lo. Então, clique no botão **Enviar**.

Tabela 2.5. Relatório de Análise de Ameaças

Campo	Descrição
Instante inicial	Preencha com o horário do início do período.
Instante final	Preencha com o horário do fim do período.
Filtro por subrede	Selecione **Nenhum** para não filtrar por Subrede ou selecione a subrede desejada.
Número de linhas	Estabeleça um limite de linhas para a saída do relatório.
Tipo de Ataque	Você pode escolher entre **Alto fluxo de dados entre dois IPs**, **Alto fluxo de dados entre dois IPs (Porta 0)**, **Amplificação de DNS**, **Amplificação de NTP**, **Amplificação de SNMP**, **ICMP Flood**, **IP Flood** e **Syn flood**.

Dica

Você pode gerar **relatórios de dados brutos** para obter estatísticas detalhadas e consolidadas para cada fluxo. Para isso, basta clicar no ícone que aparece ao lado de cada endereço IP.

Lista de IPs em blackhole

Esta aba mostra os endereços IP que foram anunciados em blackhole manualmente ou automaticamente.

Para cada IP, será mostrado uma tabela contendo o horário que o IP teve o tráfego suspeito detectado, o horário que foi anunciado em blackhole e o horário em que foi removido de blackhole.

Acessando **Sistema** → **Parâmetros** → **Análise de Ameaças** você pode configurar o período máximo, em minutos, em que os endereços IP continuarão sendo exibidos na lista após sua remoção do blackhole.

Removendo endereços IPs da lista de blackhole

Para remover endereços IPs do blackhole manualmente, clique no ícone mostrado na coluna **Executar script de remoção**.

Capítulo 3. Configuração

Perfis de ameaça

Você pode criar perfis de ameaça e associá-los às subredes desejadas. Nesses perfis, você definirá os limites das taxas por segundo dos dados acumulados no período configurado em **Sistema** → **Parâmetros** → **Análise de Ameaças** , assim, caso eles sejam ultrapassados em alguma subrede associada, um alarme será disparado.

Você poderá configurar o perfil para detectar se foram ultrapassados os limites de **tráfego absoluto** e **ataques comuns** como SYN flood, ICMP flood, amplificação de DNS, amplificação de SNMP, amplificação de NTP e **ataques na porta 0**.

Para criar um novo perfil de ameaça, acesse **Configuração** → **Perfis de ameaça** e clique no botão **Novo**.

Visualize o histórico de configuração do perfil através do botão **Histórico**.

Os perfis podem ser editados através do botão **Editar** e removidos pelo botão **Apagar**.

Tabela 3.1. Formulário de Perfil de Ameaça

Campo	Descrição
Nome	Defina um nome para o perfil.
Origem Mb/s	Limite da taxa de megabits por segundo enviados para um host para ativar um alarme.
Destino Mb/s	Limite da taxa de megabits por segundo recebidos por um host para ativar um alarme.
Origem Pacotes/s	Limite da taxa de pacotes por segundo enviados para um host para ativar um alarme.
Destino Pacotes/s	Limite da taxa de pacotes por segundo recebidos por um host para ativar um alarme.
Origem Fluxos/s	Limite da taxa de fluxos por segundo enviados para um host para ativar um alarme.
Destino Fluxos/s	Limite da taxa de fluxos por segundo recebidos por um host para ativar um alarme.
Número de Endereços IP de origem	Limite de conexões feitas para um host no período de 60 segundos.
Número de Endereços IP de destino	Limite de conexões recebidas por um host no período de 60 segundos.
Threshold para syn flood (fluxos/s)	Limite da taxa de fluxos por segundo com a flag SYN para um único destino.
Threshold para ICMP flood (pacotes/s)	Limite da taxa de pacotes por segundo de ICMP echo request para um único destino.
Threshold para amplificação de DNS (Mb/s)	Limite da taxa de megabits por segundo de DNS response para um único destino.
Threshold para amplificação de SNMP (Mb/s)	Limite da taxa de megabits por segundo de SNMP response para um único destino.

Campo	Descrição
Threshold para amplificação de NTP (Mb/s)	Limite da taxa de megabits por segundo de NTP response para um único destino.
Origem Mb/s - Porta 0	Limite da taxa de megabits por segundo enviados para um host na porta 0 (zero).
Destino Mb/s - Porta 0	Limite da taxa de megabits por segundo recebidos por um host na porta 0 (zero).
Origem Pacotes/s - Porta 0	Limite da taxa de pacotes por segundo enviados para um host na porta 0 (zero).
Destino Pacotes/s - Porta 0	Limite da taxa de pacotes por segundo recebidos por um host na porta 0 (zero).
Origem Fluxos/s - Porta 0	Limite da taxa de fluxos por segundo enviados para um host na porta 0 (zero).
Destino Fluxos/s - Porta 0	Limite da taxa de fluxos por segundo recebidos por um host na porta 0 (zero).
Endereços IP excluídos da análise	Preencha com os endereços IP ou subredes a serem excluídos da análise de ameaças. Separe-os por vírgulas.
Subredes	Selecione as subredes que vão fazer parte deste perfil de ameaça.

Dica

Para configurar os limites das taxas, você pode usar as estatísticas de **Média** e **Máximo** exibidas na tela inicial de cada subrede em **Dados Históricos** → **Subredes**

Adicionar metadados de perfis de ameaça

Para acessar a página de configuração de metadado, acesse **Configuração** → **Perfis de ameaça** e clique no botão **Metadado**.

Clique no botão **Novo** para criar um novo metadado. Ele pode ser do tipo **Texto**, **Inteiro** ou **Enum**.

Você pode alterar o metadado quando desejar usando o botão **Editar** e verificar o histórico de alterações através do botão **Histórico**.

Para remover um metadado, clique no botão **Apagar**.

Tabela 3.2. Campos de um metadado

Campo	Descrição
Nome	Nome do metadado.
Descrição	Descrição do metadado.
Tipo de dado	Escolha se o metadado será do tipo **Texto**, **Inteiro** ou **Enum**.
Valores	Este campo só é disponível se o **Tipo de dado** for **Enum**. Entre com uma lista de valores, separando-os por ponto e vírgula (;).

Para associar o metadado criado a um perfil de ameaça, acesse a lista de perfis e clique no botão **Metadado** ao lado do perfil que será configurado.

Após, preencha os metadados de acordo com o tipo. Você pode preencher todos eles ou apenas os que desejar.

Scripts

Você pode criar e executar scripts dos tipos: **Login** e **Blackhole**.

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.processMapper**: Mapeia os processos do dispositivo.
- **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.
- **tmlMsSql.msSqlNew**: Acessa a dbms (Database Management System) Microsoft SQL server.
- **setTimeout**: Altera o timeout da conexão.

- **tmlSocket.http**: Executa requisição HTTP. Para isso, basta informar uma URL e um método. Os métodos válidos são **GET** e **POST** em caixa alta.
- **tmlSequence.getNext**: Gera números sequenciais e sem repetição. Retorna o valor atual somado a 1 e a sequência começa pelo número 1.
- **tmlBGP.addToBlackHole**: Adciona a subrede ao blackhole.
- **tmlBGP.removeFromBlackHole**: Remove a subrede do blackhole.

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['mobj'][<MAPEADOR>][<DESCRIÇÃO>]['ifindex']**: ifIndex do objeto mapeado, onde MAPEADOR é o nome do mapeador e DESCRIÇÃO é o nome do objeto mapeado (sem o nome do dispositivo).
- **params['mobj'][<MAPEADOR>][<DESCRIÇÃO>]['description']**: Descrição do objeto mapeado, onde MAPEADOR é o nome do mapeador e DESCRIÇÃO é o nome do objeto mapeado (sem o nome do dispositivo).
- **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.
- **params['connection']**: Objeto de conexão a um dispositivo.
- **params['metadata'][<NOME_DO_METADADO>]**: Valor do metadado do dispositivo, onde NOME_DO_METADADO é o nome do metadado.

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 Login

Esse tipo de script é usado para fazer a autenticação quando o protocolo de conexão de um dispositivo for do tipo **Telnet**, uma vez que, ao contrário do SSH, ele não possui uma camada própria de autenticação.

Veja a seguir o exemplo do script de autenticação Cisco Telnet escrito no modo Lua.

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

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

Script de Blackhole

Este tipo de script é utilizado para fazer anúncio de endereços IP na lista blackhole, bem como para retirá-los.

Ele pode ser escrito de três modos: **Texto**, **Lua** e **Send/Expect**.

Em **Configuração** → **Blackhole**, você associará um dispositivo a dois scripts deste tipo, um para o anúncio dos IPs em blackhole e outro para remoção.

Em **Sistema → Parâmetros → Análise de Ameaças** você pode configurar o período máximo, em minutos, em que um endereço IP ficará em blackhole antes que este script de remoção seja executado.

O script a seguir já vem configurado no TRAFwatcher e ele é um script genérico para dispositivos Cisco.

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

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

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

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

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

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

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

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

Wildcards

Tabela 3.3. Lista de wildcards

Variáveis	Descrição
%username%	Campo de usuário do formulário de configuração do dispositivo.
%passwd%	Campo de senha de usuário do formulário de configuração do dispositivo.
%enable_passwd%	Habilitar campo de senha do formulário de configuração do dispositivo.
%blackhole_ipaddr%	Endereço IP que será anunciado em Blackhole.
%blackhole_ipaddr_mask_N%	Bloco de rede do endereço IP que será anunciado em Blackhole com a máscara N aplicada a ele.

Blackhole

Associe scripts para anunciar e remover endereços IP do blackhole, ou seja, da lista de IPs suspeitos.

Tabela 3.4. Formulário de Blackhole

Campo	Descrição
Tipo de execução	Selecione **Manual** para anunciar um determinado endereço IP em Blackhole manualmente através do Relatório de Análise de Ameaças ou **Automático** para que o sistema anuncie automaticamente todos os endereços IP em Blackhole.
Script	Selecione o script que anunciará um endereço IP em blackhole.

Campo	Descrição
Script de remoção	Selecione o script que removerá o endereço IP do blackhole.
Dispositivo	Selecione o dispositivo desejado.

Capítulo 4. 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 4.1. 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 4.2. 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.
Instante final	Período final de análise.

Campo	Descrição
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.

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 4.3. 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 4.4. 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.

Variáveis	Descrição
$object$	Nome do objeto.
$path$	Exibe o caminho para o objeto no SLAview.
$alarm$	Nome do alarme.
$action$	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 4.5. 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 no console do ALARMmanager, uma vez que esta função também esteja habilitada no console. Habilite-a em **ALARMmanager** → **Console** → **Habilitar aviso sonoro** .
Alarmes	Selecione os alarmes que irão receber esta prioridade.

Campo	Descrição
Alarmes de serviço	Selecione os alarmes de serviço que irão receber esta prioridade.

Adicionando metadados de nível de urgência

Para acessar a página de configuração de metadado, acesse **ALARMmanager** → **Níveis de urgência de alarme** e clique no botão **Metadado**.

Clique no botão **Novo** para criar um novo metadado. Ele pode ser do tipo **Texto**, **Inteiro** ou **Enum**.

Você pode alterar o metadado quando desejar usando o botão **Editar** e verificar o histórico de alterações através do botão **Histórico**.

Para remover um metadado, clique no botão **Apagar**.

Tabela 4.6. Campos de um metadado

Campo	Descrição
Nome	Nome do metadado.
Descrição	Descrição do metadado.
Tipo de dado	Escolha se o metadado será do tipo **Texto**, **Inteiro** ou **Enum**.
Valores	Este campo só é disponível se o **Tipo de dado** for **Enum**. Entre com uma lista de valores, separando-os por ponto e vírgula (;).

Para associar o metadado criado a um nível de urgência, acesse a lista de níveis e clique no botão **Metadado** ao lado do nível que será configurado.

Após, preencha os metadados de acordo com o tipo. Você pode preencher todos eles ou apenas os que desejar.

Alarmes

O TRAFwatcher já vem com oito alarmes do tipo **Possível ameaça** pré-configurados: **DNS Amplification threshold reached**, **ICMP Flood threshold reached**, **IP Flood threshold reached**, **NTP Amplification threshold reached**, **Port 0 threshold reached**, **SNMP Amplification threshold reached**, **Syn Flood threshold reached** e **Traffic threshold reached**.

Você não pode remover esses alarmes, mas seus campos podem ser editados.

Tabela 4.7. Formulário de alarme TRAFwatcher

Campo	Descrição
Nome	Nome do alarme.
Tipo de alarme	Classificação do alarme.
Varbind	Campo de texto livre que pode ser usado para reconhecer os alarmes que são encaminhados como traps.
Email	Um email será enviado aos usuários. O servidor SMTP deve ser configurado, bem como o email

Campo	Descrição
	de cada usuário no formulário de configuração do usuário.
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.
Enviar email após (minutos)	O email será enviado após o número de minutos definido nesse campo, a partir do horário de ativação.
Enviar mensagnes de dispositivo móvel após (minutos)	as mensagens de dispositivo móvel serão enviadas após o número de minutos definido nesse campo, a partir do horário de ativação.
Enviar trap após (minutos)	A trap será enviada após o número de minutos definido nesse campo, a partir do horário de ativação.
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 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 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.
Nível de urgência	Selecione um nível de urgência para o alarme.

Campo	Descrição
Perfis de Alarme	Selecione os perfis de alarme aos quais este alarme irá pertencer.

Adicionando metadados de alarme

Para acessar a página de configuração de metadado, acesse **Alarmes** → **Alarmes** e clique no botão **Metadado**.

Clique no botão **Novo** para criar um novo metadado. Ele pode ser do tipo **Texto**, **Inteiro** ou **Enum**.

Você pode alterar o metadado quando desejar usando o botão **Editar** e verificar o histórico de alterações através do botão **Histórico**.

Para remover um metadado, clique no botão **Apagar**.

Tabela 4.8. Campos de um metadado

Campo	Descrição
Nome	Nome do metadado.
Descrição	Descrição do metadado.
Tipo de dado	Escolha se o metadado será do tipo **Texto**, **Inteiro** ou **Enum**.
Valores	Este campo só é disponível se o **Tipo de dado** for **Enum**. Entre com uma lista de valores, separando-os por ponto e vírgula (;).

Para associar o metadado criado a um alarme, acesse a lista de alarmes e clique no botão **Metadado** ao lado do alarme que será configurado.

Após, preencha os metadados de acordo com o tipo. Você pode preencher todos eles ou apenas os que desejar.

Perfis de alarme

Perfis de alarme são usados para juntar os alarmes e os objetos monitorados.

Para configurar um perfil de alarme, vá em **Alarmes** → **Perfil de alarme**, clique no botão **Novo** e preencha o formulário.

Tabela 4.9. Formulário de perfil de alarme

Campo	Descrição
Nome	Texto descritivo para um perfil de alarme.
Alarme	Selecione os alarmes que pertencerão a este perfil.
Subrede	Selecione as subredes que pertencerão a esse perfil.

Adicionando metadados de perfil de alarme

Para acessar a página de configuração de metadado, acesse **Alarmes** → **Alarmes** e clique no botão **Metadado**.

Clique no botão **Novo** para criar um novo metadado. Ele pode ser do tipo **Texto**, **Inteiro** ou **Enum**.

Você pode alterar o metadado quando desejar usando o botão **Editar** e verificar o histórico de alterações através do botão **Histórico**.

Para remover um metadado, clique no botão **Apagar**.

Tabela 4.10. Campos de um metadado

Campo	Descrição
Nome	Nome do metadado.
Descrição	Descrição do metadado.
Tipo de dado	Escolha se o metadado será do tipo **Texto**, **Inteiro** ou **Enum**.
Valores	Este campo só é disponível se o **Tipo de dado** for **Enum**. Entre com uma lista de valores, separando-os por ponto e vírgula (;).

Para associar o metadado criado a um perfil de alarme, acesse a lista de perfis e clique no botão **Metadado** ao lado do perfil de alarme que será configurado.

Após, preencha os metadados de acordo com o tipo. Você pode preencher todos eles ou apenas os que desejar.

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.
- 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.

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.

O console possui as seguintes colunas:

Tabela 4.11. 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

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.

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.

Dica

Os níveis de urgência são mostrados no final da página. Ao clicar em algum deles, serão filtrados todos os alarmes deste nível. Ao clicar novamente no nível, o filtro é removido.

Capítulo 5. 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. Selecione o tipo de protocolo que deseja utilizar para fazer o backup remoto. As opções disponíveis são os protocolos FTP e S3.

Tabela 5.1. Formulário de backup remoto utilizando um servidor FTP

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.

Tabela 5.2. Formulário de backup remoto utilizando um servidor S3

Campo	Descrição
Versão do IP	Escolha se é IPv4 ou IPv6.
Diretório de backup	Diretório no servidor de backup.
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.
Chave de acesso	Chaves de acesso do usuário.
Chave secreta	Chaves secreta do usuário.
Nome do bucket	Nome do bucket onde será armazenado os backups.
Host base	URL do Servidor S3.
Host bucket	URL de estilo hospedado virtual.

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 5.3. 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.
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.

Agentes de associação

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

Tabela 5.4. Formulário de agente de associação automática

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.

Análise de ameaças

Nesta seção, você configurará os parâmetros de detecção de ameaças.

Tabela 5.5. Formulário de parâmetros da Análise de ameaças

Campo	Descrição
Janela de tempo para descartar fluxos (seg)	É o limite de tempo, em segundos, para acumular tráfego, ou seja, este limite define o período em

Campo	Descrição
	que as análises ocorrem. No caso, somente serão considerados os dados com diferença de tempo entre o primeiro e o último que fiquem dentro deste limite.
Porcentagem mínima para caracterização de tráfego	Quando em arquitetura distribuída, pode-se definir que o tráfego seja caracterizado como suspeito nas coletoras quando apenas uma porcentagem do total dos thresholds for atingida. Defina essa porcentagem mínima usando este campo.
Tolerância de diferença entre horário local e do exportador (seg)	Defina o tempo de tolerância, em segundos, para considerar que um dado fluxo está dentro do período sendo analisado e não ser descartado. O valor mínimo a ser preenchido deve ser **60**.
Período máximo de armazenamento de Tráfegos suspeitos (dias)	Configure o máximo período de tempo, em dias, em que os eventos de tráfego suspeito ficarão armazenados no sistema.
Intervalo para rodar script para desabilitar blackhole (min)	Período, em minutos, em que um endereço IP ficará em blackhole antes de um script de remoção retirá-lo.
Máximo permitido de IPs alarmados	Defina um limite para a quantidade de IPs alarmados. Quando este valor é ultrapassado, significa que o perfil de ameaça está mal configurado para a subrede com muitos IPs alarmados. Então, um Warning é mostrado ao lado do Logo. Este parâmetro preserva a performance do sistema.
Número de ameças a serem exibidas	Defina o número de ameaças que serão exibidas no Painel de Controle.
Período máximo de armazenamento de IPs em blackhole (min)	Configure o máximo período de tempo, em minutos, em que os IPs que sairam do blackhole ficarão armazenados no sistema.

Importante

É necessário habilitar a análise de ameaças no formulário de cada subrede desejada.

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 5.6. 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.
Limpar dados históricos	Habilita a exclusão de dados históricos antigos.
Limpar alarmes	Habilita a exclusão do histórico de alarmes antigos.
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.

Campo	Descrição
Dados de alteração de comportamento do SLAview	Armazenamento dedicado para os dados de alteração de comportamento, como dados de alarmes históricos, por exemplo.
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 5.7. 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.

Campo	Descrição
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 5.8. 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.

BGP

Anuncie ou remova rotas de suas tabelas de roteamento

Tabela 5.9. Formulário BGP

Campo	Descrição
Habilitar BGP	Selecione esta opção se você desejar anunciar ou remover uma rota.
Identificador BGP	Valor inteiro que identifica unicamente o emissor.
Número de AS local	Número do AS do emissor.
Número de AS do peer	Número do AS do receptor.
Ip do peer	IP do roteador do AS receptor.
Comunidade BGP	Conjunto de tags genéricas que podem ser usadas para sinalizar várias políticas administrativas entre roteadores BGP.

Circuito

Defina o Metadado desejado para criar a pasta.

Os circuitos serão agrupados de acordo com o metadado escolhido.

Tabela 5.10. Formulário de circuito

Campo	Descrição
Modo de geração do nome do circuito	Selecione **Automático** para gerar o nome do circuito de forma automática.

Campo	Descrição
Script	Este campo só é disponível se o **Modo de geração do nome do circuito** for **automático**. Selecione o script. Crie um na seção Scripts.
Metadado para agrupamento	Selecione o nome do metadado.

Cisco WAAS

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

Tabela 5.11. Formulário de Cisco WAAS

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

Configuração de HTTPS

Configure o modo HTTPS (HyperText Transfer Protocol Secure).

Tabela 5.12. Formulário de HTTPS

Campo	Descrição
Habilitar https	Escolha **Sim** e o servidor será reiniciado no modo HTTPS.
Certificado	Importe o certificado https. O arquivo deve ter a extensão .pem e precisa ser assinado por uma CA (Certification Authority) para que seja válido.

Configuração do agente de captura

Configure o número permitido de agentes em execução simultânea.

Tabela 5.13. 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 5.14. 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.

Campo	Descrição
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.

EPM

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

Tabela 5.15. 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!

Grafador

Ajuste dos parâmetros do grafador

Tabela 5.16. 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.
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.
Horário comercial	Essa opção possibilita modificações na exibição dos gráficos de acordo com horário comercial definido em Preferências locais. Escolha entre **Sem ações**, **Destacar horário comercial** ou **Exibir somente horário comercial**.

Histórico de configuração

Selecione o período de armazenamento para diferentes áreas de configuração.

Tabela 5.17. 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** .

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://<IP>/cgi-bin/login?dip=<USUÁRIO>**.

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.

Nível de log

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

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

Preferências locais

Tabela 5.18. 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.

Campo	Descrição
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.

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.

Ativação

Tabela 5.19. Configurações de ativação de redundância

Campo	Descrição
Habilitar redundância	Escolha Sim.
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.
Estado preferencial	Selecione **Mestre** ou **Slave**.

Vá à seção redundância para detalhes de habilitação deste recurso.

Comutação

Tabela 5.20. Configurações de comutação de redundância

Campo	Descrição
Interfaces	Adicione a interface que irá compartilhar os endereços de IP entre os dois appliances. Use o botão **Adicionar** para adicionar 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.

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 5.21. 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.

Relatórios agendados

Configure as características que os relatórios agendados possuirão.

Tabela 5.22. 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.

Também é possivel enviar os relatórios agendados para um servidor FTP.

Tabela 5.23. Formulário de configuração do servidor FTP

Campo	Descrição
Servidor	Endereço de IP do servidor FTP.
Diretório	Diretório no servidor FTP.
Usuário	Usuário para ser autenticado no servidor FTP.
Senha	Senha usada para conectar ao servidor FTP.
Porta	Número da porta.
Limite de armazenamento (MB)	Defina o tamanho máximo que pode ser ocupado pelos relatórios.

Para enviar um relatório para o servidor FTP, vá em **Relatórios** e crie ou edite um template selecionando a opção **Agendar template** e em seguida marque **sim** no **campo Enviar relatório para servidor FTP**.

Servidor SMS

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

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

Tabela 5.24. 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 5.25. 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.
Senha SMTP	Entre com a senha. Se o servidor SMTP não solicitar autenticação este campo pode ser deixado em branco.

Campo	Descrição
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

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 de pacotes	Número máximo de pacotes por segundo que um coletor SNMP irá enviar para cada dispositivo.
Taxa máxima global de envio de pacotes	Limite global para o número de pacotes enviados por segundo. Considera todos os dispositivos cadastrados. Preencha 0 se quiser que não tenha limites.
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 5.26. 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.

Telcomanager Host Agent

Preencha este formulário com o endereço IP e a porta do servidor onde está instalado o Telcomanager Host Agent. Esse endereço será usado para coletar todos os dispositivos configurados para utilizar a coleta THA no modo Gateway. Por padrão, o THA usa a porta 8888.

Importante

Para que o THA consiga coletar informações remotamente em um Active Directory (AD), é necessário que os seguintes serviços estejam habilitados nas maquinas remotas:

- Chamada de procedimento remoto (RPC)
- Registro remoto

Telcomanager JMX Agent

Preencha este formulário com o endereço IP e porta do servidor onde está instalado o Telcomanager JMX Agent. Esse endereço será usado para coletar todos os dispositivos configurados para utilizar a coleta JMX.

Tema

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

Tabela 5.27. Configuração do tema

Campo	Descrição
Tema padrão	Escolha o tema padrão para o sistema: **Dark**, **Green & Yellow**, **Red & white** or **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 5.28. 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.
Nome de usuário utilizado pela API de configurações	Digite o usuário.

Dados brutos do TRAFip

Configure o acesso aos dados brutos do TRAFip.

Tabela 5.29. TRAFip's raw data form

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

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 5.30. Formulário de usuário

Campo	Descrição
Nome de usuário	Login de usuário.

Campo	Descrição
Nome	Nome de usuário.
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 usando o protocolo SMPP ou celular@teste.com para enviar pequenos emails com alarmes. O sistema também pode enviar SMSs através da integração com um portal web.
Usar gráfico compacto	Compacte os gráficos para que caibam na mesma página ou visualize-os no tamanho normal.
Usar sumarização de grupo	Habilita a visualização da Sumarização de grupo para o usuário.
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** .
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.
Subredes	Selecione as subredes que o usuário será capaz de acessar.

Desativando usuários

É possível desativar um usuário, tornando-o inativo. Um usuário inativo não pode logar nem receber notificações do sistema. Para desativar um usuario, use o botão **Desativar** ao lado do usuário desejado.

Grupos de usuários

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

Procedimento 5.1. Gerenciando grupos de usuários

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

Tabela 5.31. 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 5.2. Gerenciando perfis de usuários

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

Tabela 5.32. 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 5.33. 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.
CAMINHO	Mostra o primeiro caminho de grupo do SLAview para o objeto.

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 5.34. 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.

Coluna	Descrição
Quantidade máxima de pacotes	Preencha o número máximo de pacotes a serem analisados. Preencha 0 se quiser que não tenha limites.
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.

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.
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** .

Fuso horário

Este menu é usado para configurar o fuso horário correto para o servidor. Você pode selecionar um dos fusos pré-definidos no sistema ou fazer o upload de um novo.

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

Suporte

Abertura de chamado

Clique no botão **Abrir chamado** e você será redirecionado para o formulário de suporte técnico da Telcomanager através de uma nova aba no seu navegador.

Importante

Você precisará ter acesso à internet.

Verificar se há atualizações do sistema

Clique no botão **Verificar atualizações** para descobrir se há patches disponíveis para a sua versão ou se é possível atualizar o sistema para novas versões.

Importante

Você precisará ter acesso à internet.

Configuração de túnel para suporte remoto

Esta opção pode ser usada para estabelecer uma conexão segura para os servidores de suporte 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 valor diferente.

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 6. 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**.

Capítulo 7. Glossário

Siglas

Essa seção mostra as siglas e abreviações presentes neste manual.

Tabela 7.1. Lista de siglas e abreviações

Sigla	Descrição
AD	Active Directory.
API	Interface de programação de aplicações. Do inglês, Application Programming Interface.
AS	Sistema autônomo. Do inglês, Autonomous system.
ASN	Número de sistema autônomo. Do inglês, Autonomous system number.
Avg	Média. Do inglês, average.
CDP	Protocolo Cisco Discovery. Do inglês, Cisco Discovery Protocol.
CLI	Interface de linha de comando. Do inglês, Command line interface.
CNT	É um tipo de análise de perfil de tráfego: Conteúdo.
CPU	Unidade central de processamento. Do inglês, Central processing unit.
DNS	Sistema de Nomes de Domínios. Do inglês, Domain Name System.
DoS	Negação de serviço. Do inglês, Denial of service.
DST	É um tipo de análise de perfil de tráfego: Distribuição.
Enum	Enumerate.
EPM	É um módulo extendido do SLAview. Do inglês, Expanded Processing Modules.
FTP	Protocolo de Transferência de Arquivos. Do inglês, File Transfer Protocol.
GB	Gigabyte.
GIS	Sistema de Informação Geográfica. Do inglês, Geographic Information System.
HTTP	Protocolo de Transferência de Hipertexto. Do inglês, Hypertext Transfer Protocol.
HTTPS	Protocolo de Transferência de Hipertexto Seguro. Do inglês, Hyper Text Transfer Protocol Secure.
ICMP	Protocolo de Mensagens de Controle de Internet. Do inglês, Internet Control Message Protocol.
IETF	Internet Engineering Task Force.
IP	Protocolo de internet. Do inglês, Internet Protocol.

Sigla	Descrição
IPFIX	IP Flow Information Export.
IPv4	Protocolo de internet na versão 4. Nela, os endereços IP são compostos por 32 bits.
IPv6	Protocolo de internet na versão 6. Nela, os endereços IP são compostos por 128 bits.
ISP	Provedor de Serviço de Internet. Do inglês, Internet Service Provider.
Kb	Kilobit.
KPI	Indicador-Chave de Desempenho. Do inglês, Key Performance Indicator.
LAN	Rede de área local. Do inglês, Local Area Network.
LLDP	Link Layer Discovery Protocol.
Max	Máximo.
Mb	Megabit.
MIB	Base de informações de gerenciamento. Do inglês, Management information base.
Min	Mínimo.
MPLS	Multi-Protocol Label Switching.
MTX	É um tipo de análise de perfil de tráfego: Matriz.
NaN	Quando o valor não é um número. Do inglês, Not a number.
NTP	Network Time Protocol.
OID	Identificador de objeto. Do inglês, Object Identifier.
QoS	Qualidade de Serviço. Do inglês, Quality of Service.
RFC	Request for Comments.
RFI	Repeated Flow Interface.
SMS	Serviço de mensagens curtas. Do inglês, Short Message Service.
SMPP	Protocolo de mensagem curta peer-to-peer. Do inglês, Short Message Peer-to-Peer.
SMTP	Protocolo de transferência de correio simples. Do inglês, Simple Mail Transfer Protocol.
SNMP	Protocolo Simples de Gerência de Rede. Do inglês, Simple Network Management Protocol.
SSH	Secure Shell.
TACACS	Terminal Access Controller Access-Control System.
TCP	Protocolo de controle de transmissão. Do inglês, Transmission Control Protocol.
TCS	Telcomanager Custom Script.
THA	Telcomanager Host Agent.

Sigla	Descrição
ToS	Tipos de Serviços. Do inglês, Type of Services.
TSA	Telcomanager Windows Security Agent.
UDP	User Datagram Protocol.
URL	Localizador Uniforme de Recursos. Do inglês, Uniform Resource Locator.
WAAS	Wide Area Augmentation System.
WAN	Rede de longa distância. Do inglês, Wide Area Network.