Manual CFGtool

Manual CFGtool

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

CFGtool é um sistema de gerência de configuração de dispositivos.

Principais recursos

- 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.
- Banco de dados de alta performance para dados históricos armazenados.
- Alarmes de alteração de configuração de um dispositivo e de integridade de arquivos.
- Gerenciamento de scripts de provisionamento, exportação de configuração e login.

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.

Dispositivos

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

Procedimento 2.1. Passos da configuração dos dispositivos

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

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

Tabela 2.1. 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 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

Campo	Descrição
	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: • 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**.

Campo	Descrição
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 configuração usando filtro de trap, selecione **Passivo**.
Habilitar Integridade de Segurança.	Selecione **Sim** para habilitar a Integridade de Segurança, ou **Não** para desabilitar.
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

Campo	Descrição
	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.
Perfis de alarme	Associa o dispositivo a um perfil de alarme.

Exportando a configuração do dispositivo

Clicando no botão **Agente de exportação de configuração** você executará os scripts exportadores de configuração.

Cheque o resultado da exportação clicando em **Resumo** na área de seleção.

Configurando a Integridade de Segurança de dispositivos.

Para habilitar o sistema e Integridade de Segurança, marque a opção **Sim** no formulário ao criar ou editar um dispositivo.

A instalação de um agente é requerida, O **Telcomanager Windows Security Agent** (TSA) está localizado em **Ferramentas** → **Software Externo** e após instalado coletará informações sobre os arquivos que estão sendo monitorados pelo CFGtool. O TSA deve ser instalado na máquina que contém os arquivos a serem monitorados.

Habilitando a Integridade de Segurança, serão habilitados 2 alarmes de dispositivo, localizados em **ALARMmanager** → **Alarmes**. Estes alarmes se tornarão ativos quando algum arquivo estiver faltando ou for alterado.

Clicando no botão Verificação de Segurança na lista de Dispositivos, localizada em **Dados Históricos** → **Dispositivos**, é possível obter um relatório sobre os arquivos monitorados, bem como o status de cada um (ausente, alterado ou normal).

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 2.2. Campos do arquivo de dispositivo

Campo	Descrição
Nome	Possíveis caracteres para o campo de nome.
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.

Campo	Descrição
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.

Relatórios

Verificação de Segurança

A Verificação de Segurança é um relatório que mostra informações dos arquivos monitorados pela Integridade de Segurança.

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 2.3. 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.

Histórico de configuração

As alterações de configuração podem ser visualizadas diretamente na tela do dispositivo clicando em **Resumo** na área de seleção de gráfico.

O relatório de histórico de configuração disponibiliza todas as alterações de configuração em um determinado período. O resultado do relatório contém os dispositivos, os tipos do script de exportação de configuração, as versões e as datas de criação.

Tabela 2.4. Formulário do relatório de histórico de configuração

Campo	Descrição
Filtro por nome	Filtre o dispositivo pelo nome.
Instante inicial	Entre com o horário do início do período.
Instante final	Entre com o horário do final do período.
Formato de saída	Selecione um dos formatos para o relatório: HTML ou CSV.

Importante

Você pode comparar versões selecionando dois itens que contenham o mesmo dispositivo e o mesmo tipo de script.

Policy Compliance

O relatório de policy compliance mostra uma relação entre dispositivos e regras e políticas.

Dessa forma, você poderá visualizar quais regras não estão sendo respeitadas pelos dispositivos.

Quando a versão do dispositivo estiver de acordo com uma regra, aparecerá um check em verde. Caso contrário, aparecerá um "X" em vermelho.

Tabela 2.5. Formulário do relatório de Policy Compliance

Campo	Descrição
Gerar relatório | Salvar template	Escolha **Gerar relatório** para apenas uma execução ou **Salvar template** para salvar o relatório como template.
Tipo de configuração	Selecione se você quer analisar apenas versões do tipo **running**, **startup**, **baseline** ou **Todos** os tipos.
Formato de saída	Escolha o formato desejado de saída: HTML, PDF ou CSV. Opção disponível apenas para relatório que não é template.
Policy compliance	Selecione as policies que serão analisadas.
Dispositivo	Associe os dispositivos a terem suas versões de configuração analisadas.

Capítulo 3. Provisionamento

Scripts

Você pode executar facilmente, em um dispositivo, algum script já existente ou pode criar um novo e executá-lo sem ser necessário que ele seja salvo.

Essa execução pode ser imediata ou agendada e os logs serão disponibilizados em **Provisionamento** → **Tarefas** por um período de tempo que você pode definir em **Sistema** → **Parâmetros** → **Provisionamento** .

Além disso, é possível acompanhar os detalhes do último provisionamento usando a aba **Última tarefa** disposta no final da página.

Criando scripts

Para criar um novo script, clique no sinal de + e edite a caixa de texto. Após isso, selecione o modo de execução (**Lua**, **Send/Expect** ou **Texto**), clique em **Rodar** e selecione o dispositivo 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.

Executando scripts

Para executar algum script já criado, clique nele no menu à esquerda. Você pode editá-lo usando a caixa de texto. Também é possível selecionar o modo de execução: **Lua**, **Send/Expect** ou **Texto**. Por fim, clique em **Rodar** e selecione o dispositivo em que o script será executado.

Caso você queira agendar a execução, selecione a opção **Agendar template**. Você precisará definir um nome e o tipo de agendamento (**Uma execução**, **Diário**, **Semanal** ou **Mensal**). Você pode acessar e editar seus agendamentos a qualquer momento em **Provisionamento** → **Tarefas**.

Tarefas

Nessa aba, será exibida uma lista de tarefas com informações a respeito dos últimos scripts rodados.

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**.

As tarefas agendadas podem ser interrompidas com o botão **Suspender** e retomadas com o botão **Retomar**.

Capítulo 4. Configuração

Scripts

Você pode criar e executar scripts dos tipos: **Exportador de configuração**, **Login** 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 Exportação de Configuração

Crie um Script de Exportação de Configuração para fazer a gerência da configuração de um dispositivo.

Use o exemplo a seguir para criar seu script de exportação de configuração:

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

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

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

if(c == nil) then
 return nil
end

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

c:send('show config')

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

r=tmlUtils.removeTerminalEscape(r)

return r

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

Script de 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.

Assim como os scripts de provisionamento, os scripts de Login podem ser escritos em três modos: **Texto**, **Lua** e **Send/Expect**.

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 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**.

Você pode agendar a execução deste tipo de script. Para isso, após clicar em **Rodar**, selecione a opção **Agendar template**. Você precisará definir um nome e o tipo de agendamento (**Uma execução**, **Diário**, **Semanal** ou **Mensal**). Esses agendamentos podem ser acessados e editados a qualquer momento em **Provisionamento** → **Tarefas**.

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.
- 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 4.1. 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.

Policy Compliance

Crie políticas de conformidade formadas por regras que garantam que as configurações de seus dispositivos estão de acordo com o esperado.

Você pode gerar relatórios que mostrem de maneira clara como os dispositivos estão se comportando em relação às policies e regras, ou seja, se eles as estão respeitando ou não.

Dessa forma, você terá maior facilidade no controle e administração de possíveis riscos de segurança, além de ter seu tempo otimizado, visto que não precisará analisar manualmente cada configuração.

Regra

Você pode criar regras que busquem, em suas versões de configurações de dispositivos, expressões específicas e verifiquem que as configurações dos seus dispositivos estão corretas.

Para isso, acesse **Configuração** → **Policy Compliance** → **Nova regra** ou **Configuração** → **Policy Compliance** → **Regra** e clique no botão **Novo**.

Tabela 4.2. Formulário de Regra de Policy Compliance

Campo	Descrição
Nome	Defina o nome da regra.
Descrição	Descreva a regra, caso desejar.
Texto de busca	Adicione filtros de strings. Você pode adicionar quantos filtros quiser e escolher as operações entre eles: **E** ou **OU**.

As regras podem ser editadas a qualquer momento através do botão **Editar** e removidas com o botão **Apagar**.

> **Importante**
> Você não poderá remover uma regra que esteja associada à alguma policy.

Policy

A policy trata-se, basicamente, de um conjunto de regras.

Para criar uma nova policy, acesse **Configuração** → **Policy Compliance** → **Nova policy** ou **Configuração** → **Policy Compliance** → **Policy** e clique no botão **Novo**.

Tabela 4.3. Formulário de Policy Compliance

Campo	Descrição
Nome	Defina o nome da Policy.
Regra	Associe uma regra ou mais à policy compliance.

Você pode editar a policy e quais regras a compõem. Para isso, clique no botão **Editar**.

Caso queira remover uma policy, use o botão **Apagar**.

Filtro de Trap

Alguns equipamentos disparam traps sempre que suas configurações são alteradas.

Crie filtros para essas traps e, assim, toda vez que o sistema recebê-las, irá exportar a nova configuração do equipamento.

Importante

É necessário que o dispositivo tenha o modo de exportação de configuração configurado como **Passivo**.

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

Tabela 4.4. Formulário de Filtro de Trap

Campo	Descrição
Nome	Defina um nome para o filtro de trap.
Varbind identificador	Insira as varbinds que devem estar presentes na trap. Separe-as por vírgula.
Varbind de usuário	Insira a varbind que informa o usuário que efetuou a alteração. Este campo é opcional.
Varbind de host	Insira a varbind informando o host que efetuou a alteração. Este campo é opcional.

Use o botão **Editar** para alterar o filtro e o botão **Apagar** para removê-lo.

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 4.5. 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**.

Campo	Descrição
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.

Capítulo 5. Ferramentas

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.

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 6. 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 6.1. 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 6.2. 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 6.3. 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 6.4. 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 6.5. 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 pelo Java ALARMmanager Console se esta função também estiver habilitada no console. Para habilitá-la, acesse **ALARMmanager** → **Console** → **botão ALARMmanager** → **Ferramentas**

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

Alarmes

O CFGtool dispõe de 2 tipos de alarmes, **Configuration Check** and **Integridade de Segurança**.

O tipo **Configuration Check** possui 2 alarmes (running and startup) que são disparados no caso de uma mudança na configuração de um dispositivo ocorrer.

O tipo **Integridade de Segurança** possui 2 alarmes (file change and file missing) que são disparados no caso de uma alteração ou falta de algum arquivo.

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

Além disso, você pode criar novos alarmes para saber quando as configurações de seus dispositivos não estão respeitando as políticas e regras de Policy Compliance.

Tabela 6.6. Formulário de alarme CFGtool

Campo	Descrição
Nome	Defina um nome para o alarme.
Tipo de alarme	Escolha entre **Configuration check** e **Integridade de Segurança**.
Tipo de configuração	Escolha entre **running** e **startup**.
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 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

Campo	Descrição
	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.
Provisionamento	Selecione **Sim** para habilitar o provisionamento para esse alarme.
Script de provisionamento	Selecione um script de provisionamento para ser executado.
Enviar email após (minutos)	O email será enviado após o número de minutos definido nesse campo, a partir do horário de ativação.
Enviar mensagens de dispositivo móvel após (minutos)	as mensagens dispositivo móvel após 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.
Executar provisionamento após (minutos)	Um script de provisionamento será executado 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.
Desabilitar provisionamento para alarme suprimido	Selecione "Sim" para impedir que o provisionamento aconteça quando um alarme estiver suprimido.
Nível de urgência	Selecione um nível para o alarme.
Policy Compliance	Associe as policies a serem monitoradas.
Perfis de Alarme de dispositivo	Selecione os perfis de alarme aos quais este alarme irá pertencer.

Gerência de supressão de alarme

Para suprimir um alarme, siga o procedimento abaixo:

1. Vá à aba to **ALARMmanager** → **Alarmes** e clique no botão Alarmes suprimidos.
2. Preencha os campos do filtro no formulário para selecionar os alarmes/objetos e clique no botão Filtro.
3. Selecione os alarmes/objetos na lista.
4. Preencha o **Motivo da supressão**, se desejar.
5. Clique no botão Salvar para suprimir os alarmes/objetos selecionados.

Para desuprimir os alarmes, siga o mesmo procedimento, mas deselecione os alarmes/objetos desejados.

Importante

Note que se o alarme já está suprimido, ele não será suprimido novamente e o mesmo acontece para a ação de desuprimir.

Perfis de alarme

Perfis são utilizados para fazer a união entre alarmes e os dispositivos monitorados.

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

Tabela 6.7. Formulário de perfil de alarme

Campo	Descrição
Nome	Defina um nome para o perfil de alarme.
Tipo de associação de objeto	Escolha **Manual** para associar manualmente ou **Automático** para usar uma regra para associar.
Alarme de dispositivo	Selecione os alarmes desejados para pertencer ao perfil.
Dispositivos	Selecione os dispositivos desejados para pertencer a esse perfil, caso o tipo de associação seja **Manual**.
Regra de associação	Selecione as regras usadas para associar os dispositivos, caso o tipo de associação seja **Automático**.

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 6.8. 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.

Capítulo 7. 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 7.1. Formulário de backup remoto

Campo	Descrição
Versão do IP	Escolha se é IPv4 ou IPv6.

Campo	Descrição
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 7.2. 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.
Servidor	Digite o endereço do servidor Active Directory. Exemplo: kerberos.example.com

Campo	Descrição
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

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 7.3. 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

Campo	Descrição
	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.
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 7.4. 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 7.5. 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 7.6. 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 7.7. 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 7.8. 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 7.9. 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.

EPM

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

Tabela 7.10. 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!

Gerência de configuração

Selecione o intervalo para coletar todas as configurações dos dispositivos com um script associado. Este script pode ser criado na seção Scripts.

Tabela 7.11. Intervalo de gerência de configuração

Campo	Descrição
Limite de número de versões	Defina o número máximo de versões a serem mantidas por cada dispositivo. Quando este limite for atingido, as versões mais antigas serão descartadas. O valor máximo é 4320.
Intervalo de gerência	Configure o intervalo em horas para exportar a configuração do dispositivo. O padrão é 8 horas.

Histórico de configuração

Selecione o período de armazenamento para diferentes áreas de configuração.

Tabela 7.12. 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 7.13. Integridade de Segurança

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

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

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.

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 7.14. 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.

Tag	Descrição
%d	Refere-se ao **tipo de dispositivo** (Câmera, Firewall, Roteador, Servidor, Switch ou Sem fio).

Preferências locais

Tabela 7.15. 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.

Provisionamento

Configure os parâmetros para o provisionamento de scripts.

Tabela 7.16. Parâmetros de provisionamento

Campo	Descrição
Período máximo de log a manter (meses)	Defina o tempo em que os logs dos scripts serão mantidos. Escolha um valor menor ou igual a 120. O valor padrão é 1.
Limite de processos de provisionamento simultâneos	Defina o limite de processos de provisionamento a serem rodados simultaneamente. Escolha um valor menor ou igual a 50. O valor padrão é 10.
Limite de tempo para espera de execução (minutos)	Defina o tempo limite de espera caso o limite de processos simultâneos tenha atingido o valor máximo definido. Escolha um valor menor ou igual a 120. O valor padrão é 60.

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 7.17. Configurações de redundância

Campo	Descrição
Habilitar redundância	Escolha Sim.

Campo	Descrição
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 7.18. 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 7.19. 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.

Campo	Descrição
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 7.20. 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 7.21. 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.
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 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 7.22. 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 7.23. 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 7.24. 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 7.25. 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 7.26. Formulário de usuário

Campo	Descrição
Nome de usuário	Login de usuário.
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.

Campo	Descrição
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.
Permissão para definir configuração de baseline	Esta opção é disponível apenas para usuários dos tipo **Administrador** e **Configurador**. Selecione **Sim** para que o usuário possa indicar uma versão de configuração como ideal para um equipamento.
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** .
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 de usuários

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

Procedimento 7.1. Gerenciando grupos de usuários

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

Tabela 7.27. Formulário de usuário

Campo	Descrição
Nome	Nome do grupo de usuários.

Campo	Descrição
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 7.2. Gerenciando perfis de usuários

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

Tabela 7.28. 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 7.29. Colunas ALARMmanager console

Coluna	Descrição
INÍCIO	Tempo da primeira ocorrência.
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.

Coluna	Descrição
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 7.30. 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.
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. 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 8. 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**.