
RELEASE NOTES

BACKUP NA NUVEM

ARMAZENE SEUS DADOS USANDO S3

Para você que pensa em usar os serviços de armazenamento S3 ou já os utiliza, você pode utilizá-los para fazer backup de dados do sistema.

Basta preencher as configurações do seu servidor e deixar a ferramenta fazer o resto!

Data

IP version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Backup directory	<input type="text" value="bkpdir"/>
Backup protocol	<input type="text" value="S3"/>
Server size (GB)	<input type="text" value="5"/>
Activate backup	<input type="radio"/> Yes <input checked="" type="radio"/> No
Backup start time	<input type="text" value="11 : 00"/>
Access key	<input type="text"/>
Secret key	<input type="text"/>
Bucket name	<input type="text"/>
Host base	<input type="text" value="s3.amazonaws.com"/>
Host bucket	<input type="text" value="%(bucket)s.s3.amazonaws.com"/>

Figura 1: Configuração de backup S3

RELATÓRIO POR FTP

UMA NOVA FORMA DE RECEBER SEUS RELATÓRIOS

Os relatórios têm uma nova opção para serem enviados por FTP. Mais uma facilidade para armazenar remotamente seus relatórios.

CONFIGURAÇÃO DE ENDEREÇOS IPS EXCLUÍDOS

IGNORAR BLOCOS DE ENDEREÇO

Em perfis de ameaça agora é possível definir blocos de IPs que serão filtrados para facilitar sua configuração.

Common attacks

Syn flood threshold (flows/s)	<input type="text" value="0"/>
ICMP flood threshold (packets/s)	<input type="text" value="0"/>
DNS amplification threshold (Mb/s)	<input type="text" value="0"/>
SNMP amplification threshold (Mb/s)	<input type="text" value="0"/>
NTP amplification threshold (Mb/s)	<input type="text" value="0"/>

Port 0 attack

Source Mb/s	<input type="text" value="0"/>
Destination Mb/s	<input type="text" value="0"/>
Source Packets/s	<input type="text" value="0"/>
Destination Packets/s	<input type="text" value="0"/>
Source Flows/s	<input type="text" value="0"/>
Destination Flows/s	<input type="text" value="0"/>

Filter

Subnets

Filter ?

Available

>>>
<<<<

Selected

IP address list excluded from the analysis

Figura 2: Blocos de endereço excluídos

HIERARQUIA DE ATAQUES

PRIORIZE ATAQUES MAIS ESPECÍFICOS

Ataques comuns do TRAFWatcher geralmente representam um subconjunto dos ataques absolutos.

Com isso criamos uma opção para suprimir os ataques absolutos caso ataques comuns específicos sejam ativados.

New threat profile

Save Cancel

Name *

Prioritize attacks Yes No

Absolute traffic

Source Mb/s	<input type="text" value="0"/>
Destination Mb/s	<input type="text" value="0"/>
Source Packets/s	<input type="text" value="0"/>
Destination Packets/s	<input type="text" value="0"/>
Source Flows/s	<input type="text" value="0"/>
Destination Flows/s	<input type="text" value="0"/>
Source IP address number	<input type="text" value="0"/>
Destination IP address number	<input type="text" value="0"/>

Common attacks

Syn flood threshold (flows/s)	<input type="text" value="0"/>
ICMP flood threshold (packets/s)	<input type="text" value="0"/>
DNS amplification threshold (Mb/s)	<input type="text" value="0"/>
SNMP amplification threshold (Mb/s)	<input type="text" value="0"/>
NTP amplification threshold (Mb/s)	<input type="text" value="0"/>

Figura 3: Priorizar ataques mais específicos

TRAFWatcher - v8.2.9

PROTOCOLO BGP

FECHE SESSÃO COM SEU ROTEADOR

Em época de ataques cada vez mais comuns na Internet, técnicas de blackhole são bastante usadas ao detectar um endereço IP sendo atacado.

Para enriquecer as opções de blackhole, a ferramenta tem uma nova opção de configuração de BGP.

Nesta configuração você pode adicionar um vizinho para fechar a sessão BGP e definir a community que será usada para o anúncio do filtro de endereço IP.

BGP

Enable BGP Yes No

BGP identifier

Local AS number

Peer AS number

Peer IP address

BGP community

Save

Figura 4: Configuração de BGP

NOVAS OPÇÕES PARA O DISCOVERY

MELHORA O SCAN NA REDE

O discovery ganhou uma nova opção para concentrar endereços IPs de um mesmo host numa mesma linha do relatório.

Além disso foi criado o agendamento de discovery. Basta definir um horário para seu scan na rede ser executado.

NAVEGAÇÃO NO MAPA

Volte para o último nível visitado

O mapa agora te dá opção de subir para o nível anterior. Esta funcionalidade facilita muito a navegação do mesmo, não perdendo o caminho até o nível corrente.

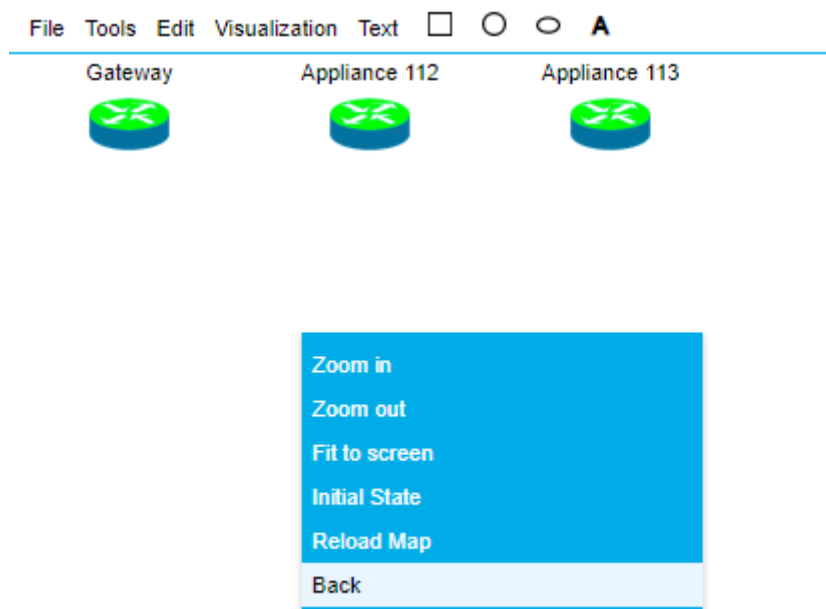


Figura 5: Navegação no mapa

NOVAS OPÇÕES NO RELATÓRIO DE VARIÁVEIS

ESCOLHA A FORMA DE AGREGAÇÃO DA VELOCIDADE

No relatório de análise de variáveis, ao escolher agregação por grupo, uma nova opção aparece para escolher como agregar a velocidade das interfaces: não exibir, soma, média, máximo e mínimo.

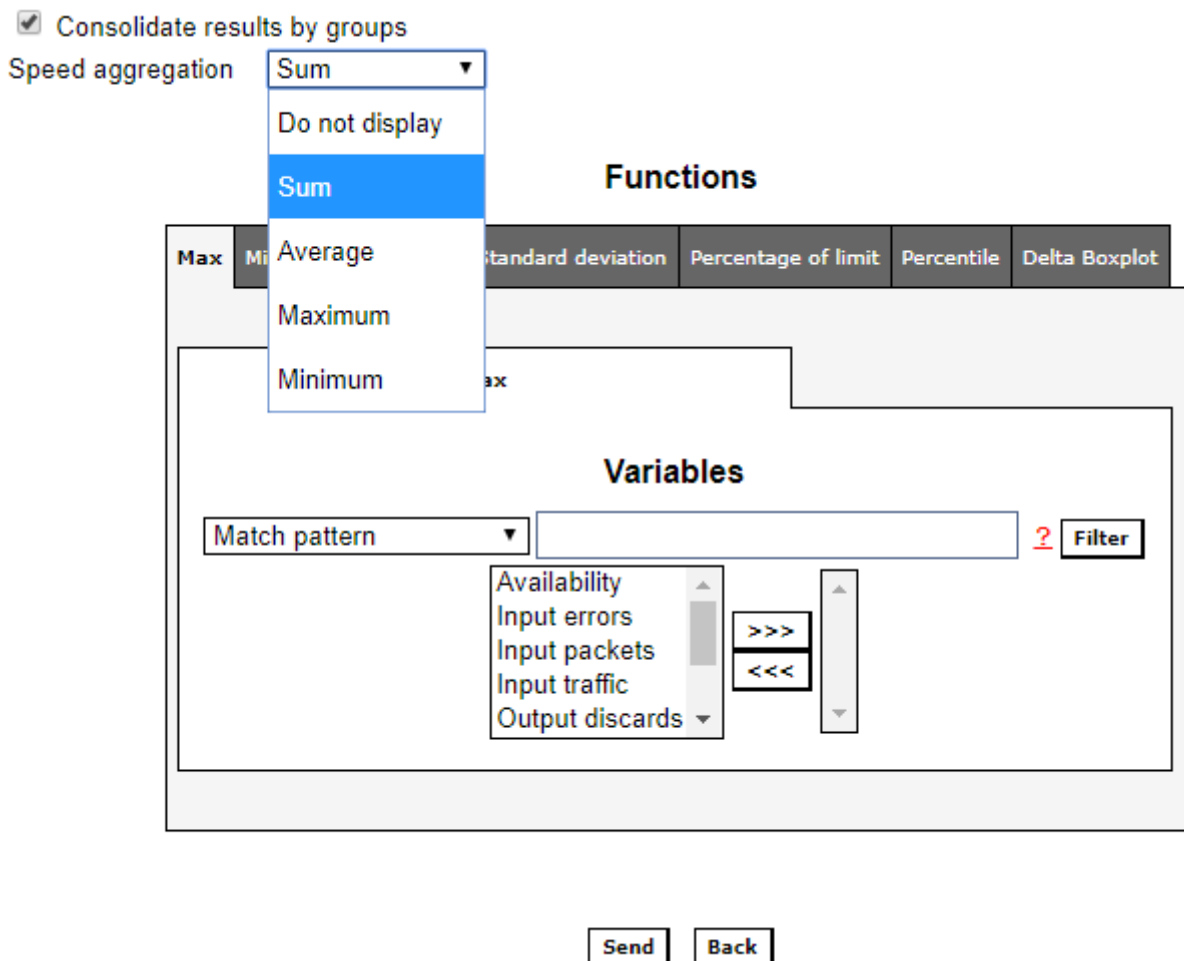


Figura 6: Funções de agregação

ANÁLISE DE TENDÊNCIA

EXECUÇÃO SOB DEMANDA

Análise de tendência é uma ferramenta muito importante para estar preparado para as mudanças na sua infraestrutura.

Para facilitar a visualização das curvas de tendência do seu sistema o quanto antes, criamos uma opção para você chamar o processo de cálculo das curvas de tendência sob demanda para um objeto específico.

DASHBOARD

FILTRO DE ALARMES

A partir do dashboard do SLAview você pode aplicar um filtro do alarme do widget selecionado no console de alarmes.

RELATÓRIO DE PERFIL DE TRÁFEGO

NOVAS OPÇÕES DE AGREGAÇÃO

O relatório de perfil de tráfego ganhou novas opções de agregação dos dados para exibição: média, mínimo, máximo e percentil.

Traffic profile report

Generate report Save template

Domain

Profile association type

Profile object type

Object type filter Case sensitive

Object type

Object filter Case sensitive

Unit

Way

Start time

End time

Exclude weekends Yes No

Interval - All day

Percentage of limit Yes No

Output format

Use SI prefix Yes No

Functions

Average	<input type="button" value="Delete"/>
Maximum	<input type="button" value="Delete"/>
Sum	<input type="button" value="Delete"/>

Figura 7: Opções de agregação

GRÁFICOS A PARTIR DO TOP N

UM ATALHO PARA SEUS DADOS

O relatório top N do TRAFip ganhou um atalho direto para o gráfico do objeto selecionado.

NOVO CAMPO LABEL PARA OBJETOS MAPEADOS

NOMEIE OS OBJETOS COMO PREFERIR

Os objetos mapeados ganharam uma opção de preenchimento de label. O label poder usado para ser exibido em vez da descrição do objeto, que muitas vezes não são muito amigáveis.

Editing mapped object

Name	<input type="text" value="Gateway-ether3"/> *
Description	<input type="text"/>
Label	<input type="text" value="Interface/Saída"/> *
ifDescr	<input type="text" value="ether3"/>
Index	<input type="text" value="4"/>
ifAlias	<input type="text"/>
ifSpeed	<input type="text" value="100000000"/>
ifType	<input type="text" value="6"/>
Device	<input type="text" value="Gateway"/>
Mapper	<input type="text" value="Interface"/>
Enable trend analysis	<input type="radio"/> Yes <input checked="" type="radio"/> No

Metadata association

Figura 10: Preenchimento de label

Interface customization

Device formula name

List interfaces by ▼

- Description
- Description
- Label

Figura 11: Opção de exibição

METADADOS

NOVAS OPÇÕES DE USO

Metadados são muito úteis para enriquecer o sistema com informações do ambiente corporativo local.

Após configurados eles podem ser exibidos na lista de objetos.

Outra funcionalidade muito interessante é usar um metadado como máscara em uma OID. Isto pode ser útil em muitas MIBs onde não basta o índice SNMP do objeto.

Em conjunto com a máscara de metadado aparece a máscara para descartar números do índice SNMP do objeto. Essas duas funcionalidades juntas podem ser muito poderosas!

New metadata

Name *

Description

Datatype *

Required field Yes No

Show in object list Yes No

Figura 12: Opções de metadado

Metadata configuration

Name ? Case sensitive

↑ ↓

Priority	Name	Datatype	Values	Operation
<input type="checkbox"/> 0	UF	text		<input type="button" value="History"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/> 1	Contato	text		<input type="button" value="History"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/> 2	Localidade	text		<input type="button" value="History"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Showing 1 to 3 of 3 entries

Figura 13: Ordenação de metadados

New profile: Mapped object

Name *

Export Yes No

Automatic association Yes No

Collect variables

SNMP	bgpPeerAdminStatus	1.3.6.1.2.1.15.3.1.3.%INDEX_POP_1%.%METADATA_IP Peer BGP%	✕
SNMP	bgpPeerState	1.3.6.1.2.1.15.3.1.2.%INDEX_POP_1%.%METADATA_IP Peer BGP%	✕

Summarization variables

Per second

Graphs

Figura 14: Máscara de metadados na OID

SLAview - v8.2.9

AGENTE DE ASSOCIAÇÃO DE PERFIS DO SLAVIEW

OPÇÃO DE DESASSOCIAÇÃO AUTOMÁTICA

Os perfis do SLAview agora tem a opção para desassociar objetos caso eles não atendam às regras de associação automática.

SLAview - v8.2.9

CIRCUITOS

CRIAÇÃO MANUAL DE LINKS

Links podem agora serem criados manualmente fora dos mapas. Essa opção é muito interessante para representar conexões lógicas entre 2 sites ou até mesmo já preparar um link que virá a existir no futuro.

Os circuitos também exibem gráficos que representam as os dados coletados das 2 interfaces que fazem parte do mesmo.

New circuit

Name *

Device A ▼

Mapper A ▼

Interface A

Device B ▼

Mapper B ▼

Interface B

Metadata association

Figura 15: Criação manual de circuito

DEPENDÊNCIA DE REGRAS

VEJA RAPIDAMENTE ONDE SUAS REGRAS SÃO USADAS

Para facilitar a configuração de regras de associação para os agentes do sistema, foi criado um botão para exibir a quais perfis uma regra específica está associada.

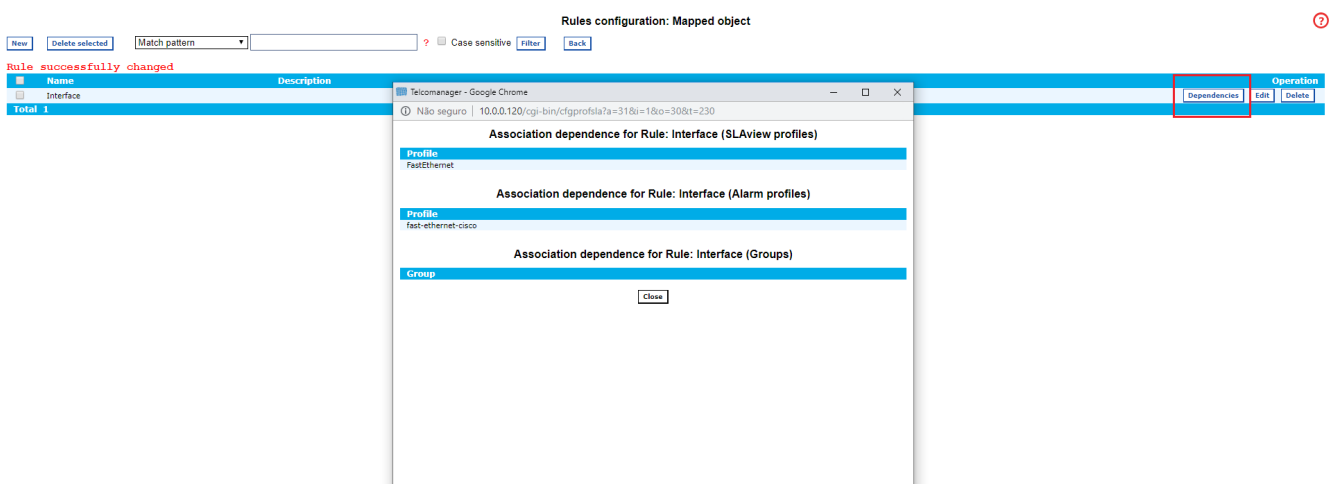


Figura 16: Dependência de regras

GRAPHSET E NOC NO SEU TELÃO

NOVAS OPÇÕES

O graphset e o NOC display agora podem ser destacado da tela principal.

Ótima opção para visualizar seus gráficos no seu telão.

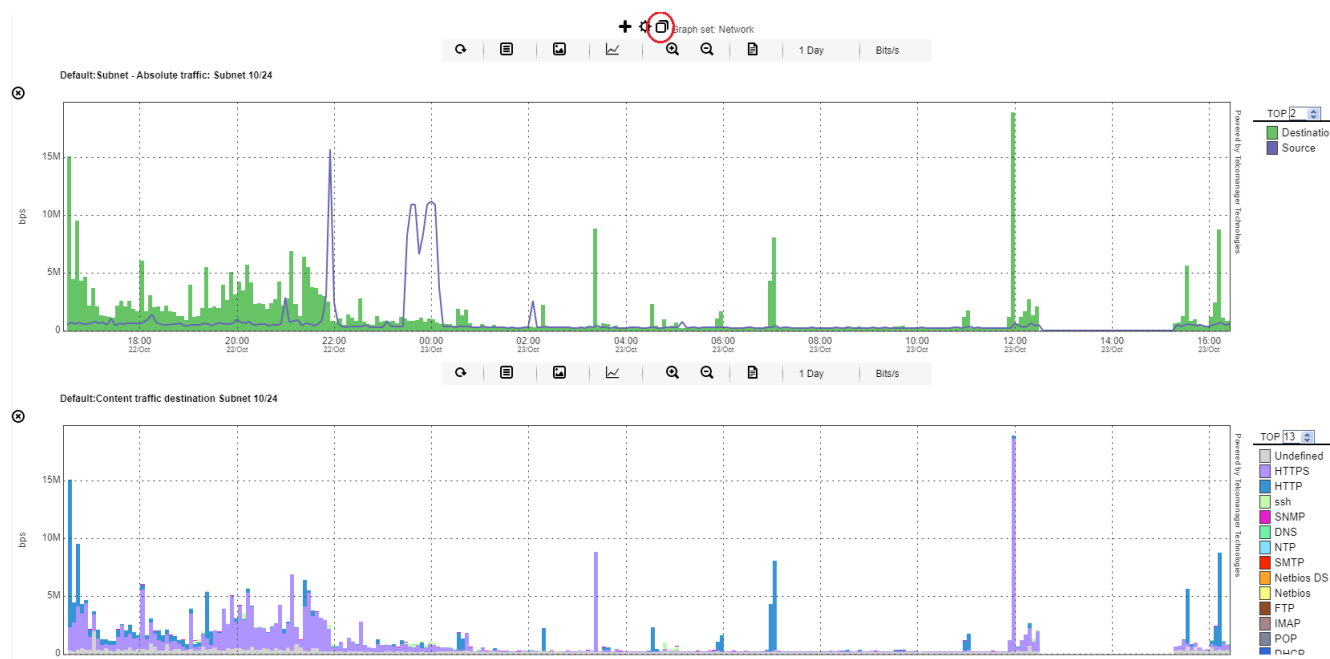


Figura 17: Destacar graphset

RELATÓRIO DE POLICY COMPLIANCE

CONTEÚDO DA REGRA NO RELATÓRIO

O relatório de policy compliance é muito útil para testes de configuração em massa.

A partir do mesmo é possível verificar quais dispositivos não estão atendendo às políticas escolhidas.

Para enriquecer este relatório você pode agora conferir o conteúdo de cada regra escolhida.

SEGURANÇA PARA USUÁRIOS

EXPIRAÇÃO DE SENHA

Para melhorar a segurança dos usuários do sistema, uma nova opção foi criada para expiração de senha.

Após o período definido o usuário será forçado a definir uma nova senha.

TIMEOUT DE SESSÃO

TIMEOUT AGORA É CONFIGURÁVEL

Cada ambiente de trabalho possui políticas específicas para o uso de ferramentas.

Para flexibilizar o sistema a se adequar mais com seus usuários o timeout das sessões pode agora ser parametrizado.