Mini curso de Monitoramento

Instrutor: Bruno Ramos e Silva
Monitor: Fábio Machado Costa

Agenda

- Conceitos de monitoramento
- O que monitorar na rede
- Ferramentas e Protocolos
  - SNMP
  - ICMP
  - Cacti
  - Zabbix
  - NFSen e NFDump
- Prática de monitoramento
  - Cacti
  - Zabbix
  - PHPIPAM (extra)

Motivação

- Você será **avisado** de
  - **Problemas** quando eles ocorrerem
  - Comportamentos **anormais**
- Você terá um
  - Históricos de **eventos**
  - Histórico de **saúde** e **funcionamento**
- Você terá condições de **reagir** a problemas rapidamente
- Você conseguirá identificar e **resolver** problemas **antes** do cliente ligar

Como identificar a causa e localização de eventuais problemas na rede?

Motivação (cont.)

- Você terá dados para
  - Planejar **capacidade** de ambientes
  - Planejar **aquisição** de hardware
  - Avaliar a **qualidade** do serviço (SLA/ANS)
- Indisponibilidade de aplicações custa caro para o
  - Cliente (prejuízo)
  - Prestador (multa)

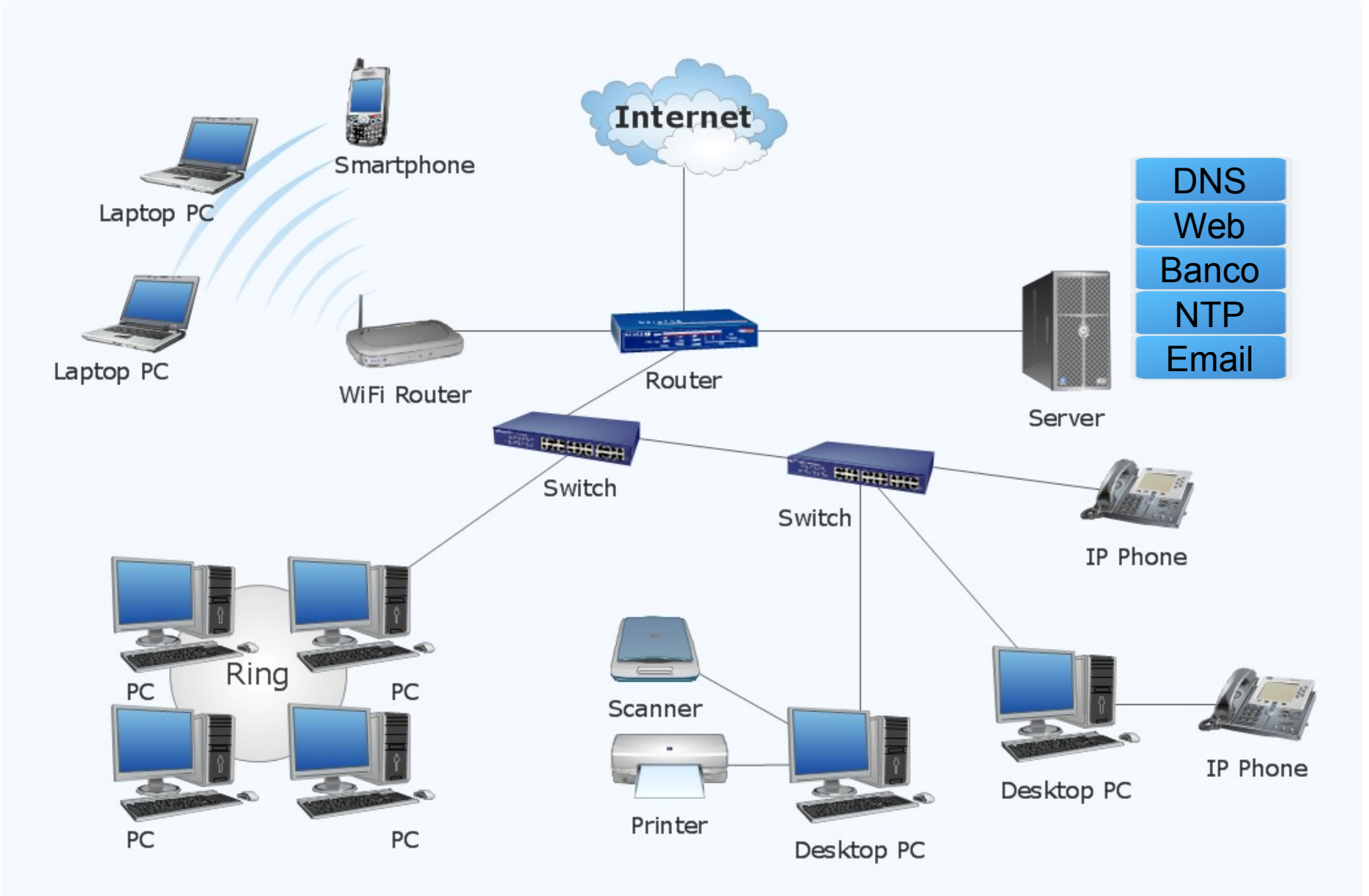
Um ambiente monitorado passa confiança ao cliente e facilita a vida da equipe de TI

Estratégia

A estratégia para detecção de problemas ou funcionamento anormal da rede tem dois passos:

- Uso de *Ferramentas de Diagnóstico* para localizar os problemas
  - Chamado *monitoramento em tempo real*
  - Ferramentas de monitoramento ativo (ex. Latência, largura de banda disponível)
  - Ferramentas de monitoramento passivo (ex. Contadores de erros)
- *Monitoramento Regular* para identificar o funcionamento normal (baseline) e gerar alertas quando cairem as expectativas
  - Chamado *monitoramento histórico*
  - Visualização de dados e alarmes
  - Uso de ferramentas de diagnóstico de uma forma estruturada

O que monitorar?



Métricas de Interesse

- Atraso de ida e volta (RTT – Round Trip Time)
- Pacotes com erros
- Utilização de banda
- Variação do atraso (jitter)
- Largura de banda alcançável (TCP, UDP)
- MOS (Mean Opinion Score)
- Fluxos de rede (volume de pacotes, bytes, tipo de protocolo, origens/destinos e portas)
- Status dos protocolos de roteamento
- Status e desempenho de serviços e aplicações
- Status e desempenho de máquinas físicas e virtuais

Nossa regras

Colete todas as métricas possíveis/razoáveis que possam ajudar no tratamento de problemas;

Gere alertas daquelas que requerem nossa atenção;

Foque em prever e evitar que as falhas ocorram ao invés de apenas apagar incêndios.

Tipos de Monitoramento

- Métricas de desempenho de Rede
  - Bytes e pacotes enviados e recebidos em interfaces de rede
  - Perda/erros em pacotes
  - Pacotes de broadcast
  - Atraso e *jitter*
  - Verificar SLA

```
PING ifba-pafonso.intranet.pop-ba.rnp.br (200.128.12.67) 56(84) bytes of data.
64 bytes from 200.128.12.67: icmp_seq=1 ttl=62 time=16.0 ms
64 bytes from 200.128.12.67: icmp_seq=2 ttl=62 time=15.4 ms
```

- Fluxos de Rede
  - ex. Métricas:
    - Volume de pacotes e bytes, tipo de protocolo, origens/destinos e portas
  - Visão dos padrões e tipos de tráfego da rede
  - Traçado de estatísticas sobre os cabeçalhos e até conteúdo dos pacotes

Tipos de Monitoramento

- Análise de roteamento
  - Monitora os protocolos de roteamento OSPF, IS-IS, EIGRP ou BGP
  - Identifica as atualizações que ocorrerem nos protocolos dos roteadores
    - Ex. “Roteador da GVT não está divulgando rotas”
  - Armazena histórico completo dos eventos de roteamento, facilitando debugging

Tipos de Monitoramento

- Monitoramento de servidor físico e serviços
  - Serviço
    - Banco de dados
    - Serviço web
    - Email
    - DNS, etc
  - Servidor físico ou virtual
    - Disponibilidade
    - Desempenho
    - Conectividade

Ex:

- Tempo de acesso
- Largura de banda no acesso
- Código de resposta da porta de rede e da aplicação
- Execução dos daemons

- Recursos de hardware
  - Uso/carga de CPU, uso de disco e RAM, partições HD físicas/lógicas, processos em execução, uso de banda, temperatura, fans, etc

- Responsável pelos protocolos de Internet:
  - HTTP, HTTPS, FTP, SNMP, SMTP, SSH, TELNET, POP3, IMAP, DNS, SSL, TCP, UDP.

Tipos de Monitoramento

- Banco de Dados
  - Métricas de sistema
    - Tempo médio, quantidade e banda transferida de escritas/leituras, tempo médio de espera I/O
  - Disponibilidade, erros, conexões, buffers e consultas
    - Uptime, clientes conectados, máximo de conexões e as abortadas
    - Processo do banco em execução, logs de erro, uso de buffers e cache, presença dos bancos e tabelas
  - Desempenho
    - Operações por segundo, acertos no cache, operações lentas, deadlocks

Mais informações: https://blog.serverdensity.com/how-to-monitor-mysql/

Monitoramento fim-a-fim de serviços

- Monitoramento atuando como um usuário do serviço
  - ex. Enviar e-mail p/ mail server; requisitar páginas web que gere consultas no BD e checar conteúdo de resposta
  - Simular atuação do usuário por menus e até mesmo cliques e preenchimento de formulários
  - Medição de tempo e conteúdo das respostas
  - Usualmente feito via scripts customizados e associado a ferramentas de monitoramento

Monitoramento do servidor de monitoramento

- Como detectar que houve problema no sistema de monitoramento?
  - Monitoramento externo
    - Sites externos: http://uptimerobot.com/
  - Servidores distribuídos
    - Um monitora o outro

Desempenho de código

- Tempo de resposta de funções, acesso ao banco de dados e chamadas de sistema nos códigos de aplicações
  - Inovador
  - Não será tratado no curso
  - Grandes players utilizam (Facebook, Google, etc)
    - Sistema BrowserLab do Facebook automaticamente analiza a performance de toda modificação no código

Monitoramento do servidor de monitoramento

- Como detectar que houve problema no sistema de monitoramento?
  - Monitoramento externo
    - Sites externos: http://uptimerobot.com/
  - Servidores distribuídos
    - Um monitorar o outro

Protocolo SNMP

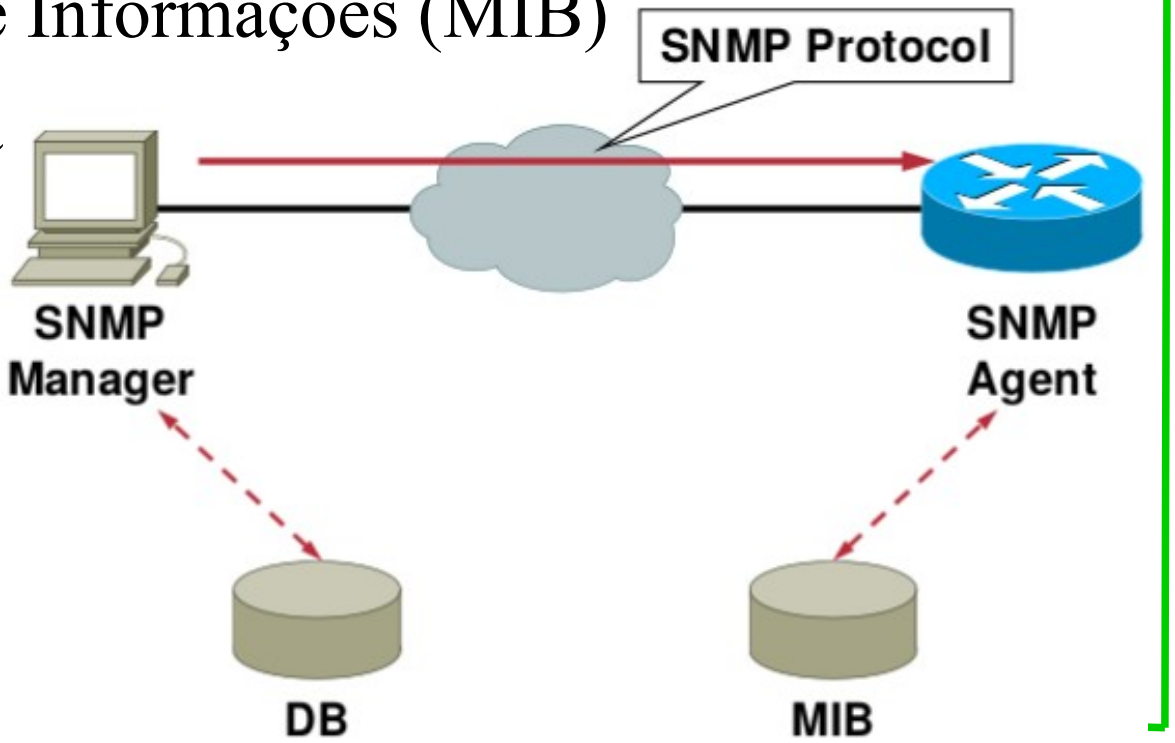
SNMP – Simple Network Management Protocol

- Padrão **de facto** de monitoramento de redes
- Pode-se monitorar CPUs, uso de memória, uso de disco, etc
- Arquitetura cliente-servidor
- Possível criar novos itens de monitoramento via SNMP (UserParameters, AgentX, etc)
- Presente em qualquer equipamento de rede decente (APs, Routers, Switches, Servidores, etc)
- Protocolo UDP, porta 161

Arquitetura de monitoramento SNMP

Modelo básico:

- Estação de Gerenciamento (Manager)
- Estação Agente
- Base de Gerência de Informações (MIB)
- Protocolo para troca de informações



Cliente ↔ Servidor

Servidor ↔ Cliente

Funções

O *gerente* (manager) é um agente que uma aplicação de gerência.

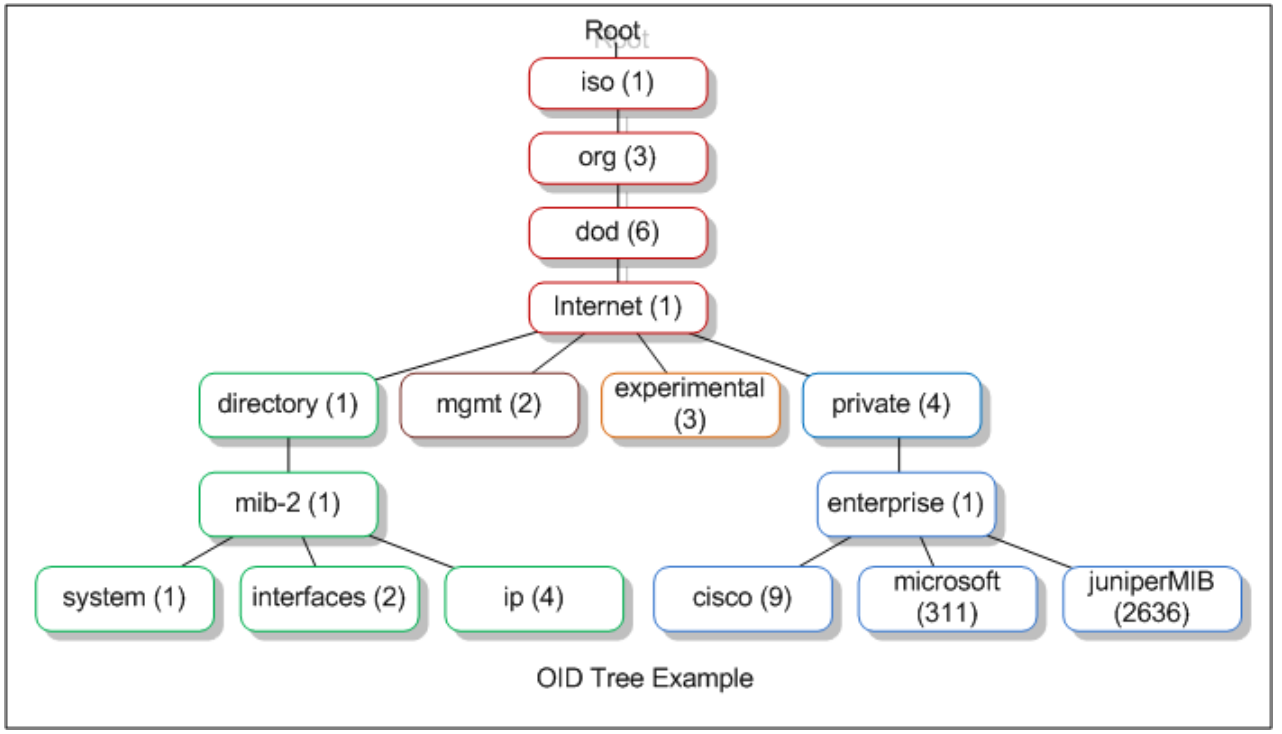
- Aplicação que inclui uma interface de operador, permitindo a uma ferramenta ou usuário autorizado a gerenciar a rede

O software *agente* é executado dentro do dispositivo

- Responde a requisições de informações e ações
- Pode enviar notificações de falha ao gerenciador, i.e. uma mensagem *trap*
- Troca informações pelo protocolo de rede SNMP

MIB

- Para gerenciar recursos na rede, cada recurso é representado como um objeto (OID – object ID)
  - A coleção de objetos é conhecida como MIB - Management Information Base (conjunto padrão de objetos - RFC 1213)



OID Tree Example

- MIB de fabricantes: *http://www.oidview.com/mibs/detail.html*

Protocolo SNMP

Três funcionalidades chaves:

- GET: Permite ao gerente (estação) recuperar valores de objetos dos agentes
- SET: permite ao gerente configurar valores de objetos nos agentes
- NOTIFY: Permite que agentes notifiquem o gerente a ocorrência de eventos significativos

Versões do SNMP

- SNMPv1
  - Centralizado (pouca escalabilidade)
  - Não permite transferência de porções maiores de dados
- SNMPv2 *
  - Permite monitoramento descentralizado
  - Permite transferência de maiores porções de dados
  - Maior deficiência é a falta de segurança efetiva
- SNMPv3
  - Autenticação
  - Autorização de usuários para monitorar e ler informações da rede
  - Privacidade

SNMP

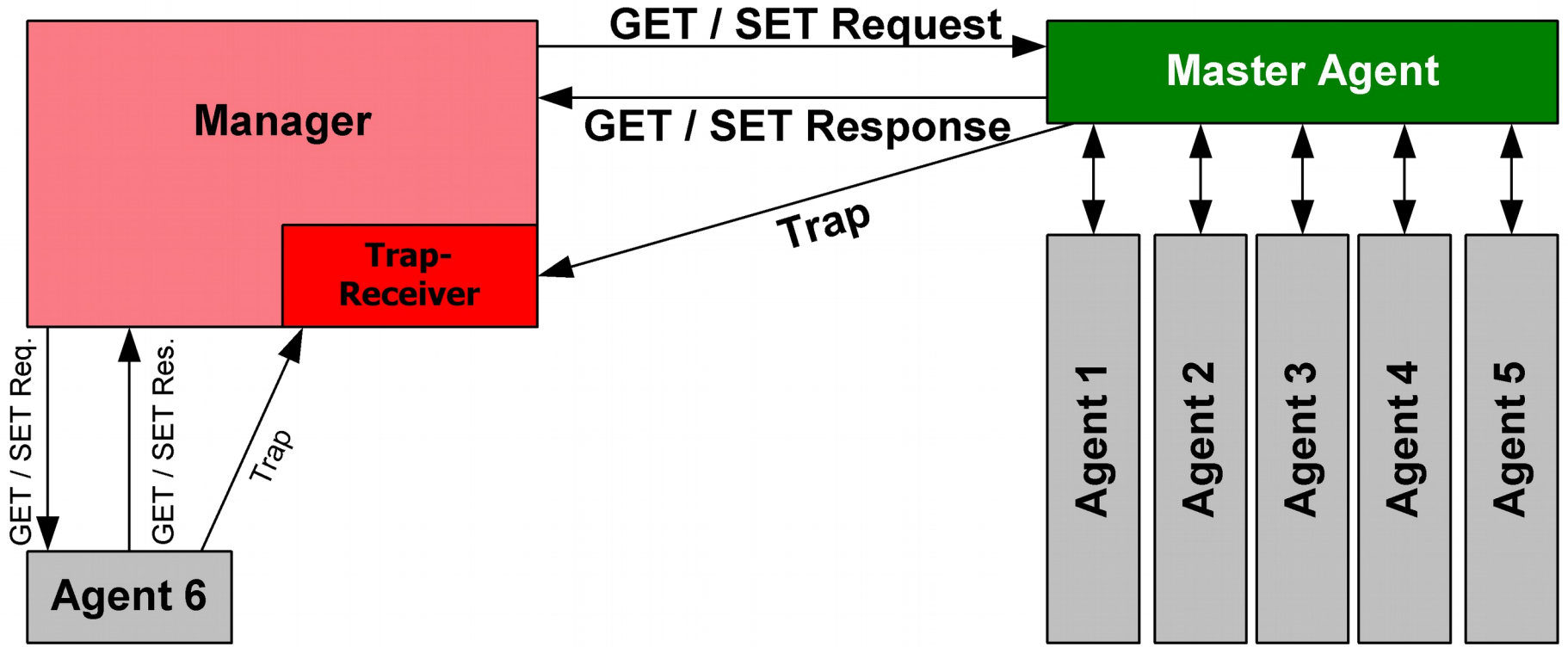
Como efetuar consultas manualmente:

- **snmpwalk** -v 2c -c public 10.0.0.1 1.3.6.1.2.1.3.1.1.2

```
prompt$ snmpwalk -v 2c -c community 192.168.0.1 1.3.6.1.2.1.3.1.1.2
RFC1213MIB::atPhysAddress.2.1.10.X.X.X = HexSTRING: 00 1B 21 19 52 38
RFC1213MIB::atPhysAddress.2.1.10.X.X.X = HexSTRING: 00 04 AC C5 44 6C
RFC1213MIB::atPhysAddress.2.1.10.X.X.X = HexSTRING: 00 16 3E DF 10 23
RFC1213MIB::atPhysAddress.2.1.10.X.X.X = HexSTRING: 00 22 64 F5 1D 28
RFC1213MIB::atPhysAddress.2.1.10.X.X.X = HexSTRING: 1C AF F7 E9 5B BF
RFC1213MIB::atPhysAddress.2.1.10.X.X.X = HexSTRING: 00 1E C9 FF 1F 1B
RFC1213MIB::atPhysAddress.2.1.10.X.X.X = HexSTRING: 00 04 96 1E 56 04
RFC1213MIB::atPhysAddress.1000036.200.128.X.X = HexSTRING: 00 1D 70 E3 FF B9
RFC1213MIB::atPhysAddress.1000036.200.128.X.X = HexSTRING: 00 1D 70 E3 FF B9
RFC1213MIB::atPhysAddress.1000036.200.128.X.X = HexSTRING: 00 1D 70 E3 FF B9
RFC1213MIB::atPhysAddress.1000036.200.128.X.X = HexSTRING: 00 1D 70 E3 FF B9
RFC1213MIB::atPhysAddress.1000036.200.128.X.X = HexSTRING: 00 1D 70 E3 FF B9
...
```

SNMP

MIBs + OIDs + Agentes + SNMP + Gerente(s)



Protocolo ICMP

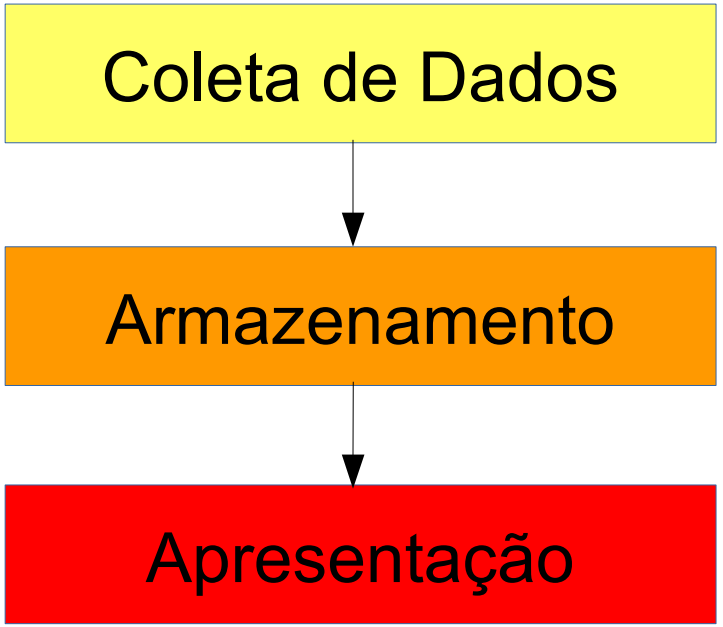
Internet Control Message Protocol – ICMP

- Mecanismo de *report* de erros e informações à origem do datagrama IP
- Executado nativamente em qualquer dispositivo IP
- Firewalls podem bloquear alguns tipos de ICMP
- Não detecta todos os erros
  - ex. destino final não ter rota conhecida para a origem do pacote IP
- Usos comuns:
  - Teste de conectividade IP, Ping
  - Descoberta de nós intermediários e seus atrasos, traceroute

Cacti

- Cacti é a evolução do MRTG
  - Interface de administração e infraestrutura para o RRDTool
  - Pode obter informações via scripts ou automaticamente via SNMP
  - Criado por Ian Berry, desenvolvido em PHP e MySQL, distribuído sob GPL.
- Mais informações:
  - http://www.cacti.net

Arquitetura Cacti

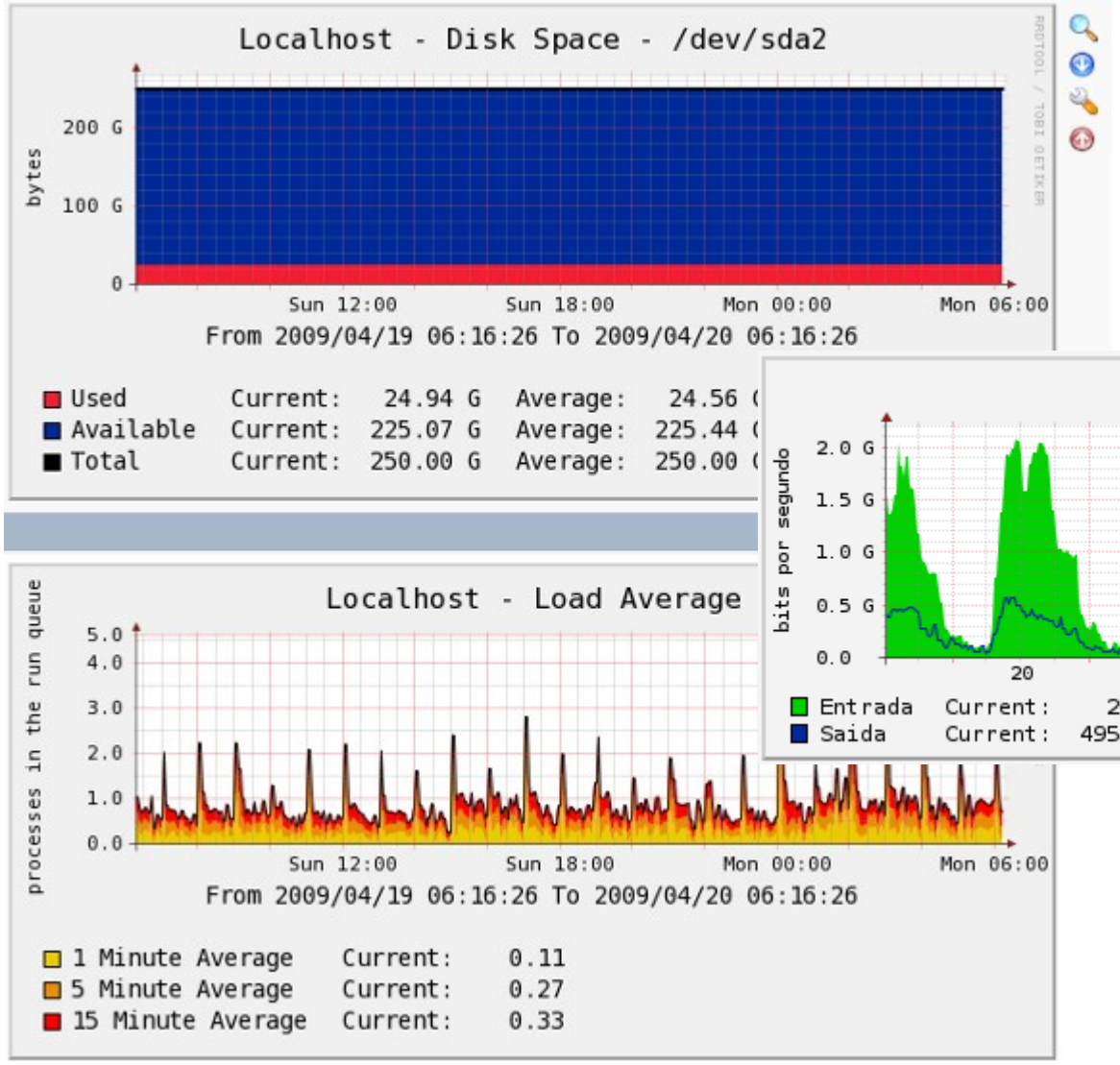


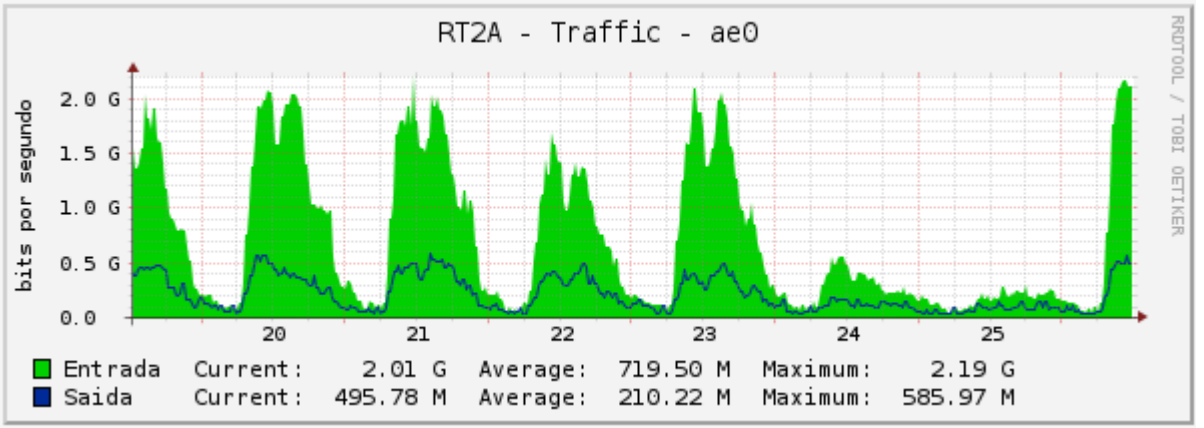
Coleta de Dados: poller + (SNMP || scripts)
Armazenamento de dados: RRDTool
Apresentação: RRDTool + web server

Cacti – RRD e RRDTool

- Round Robin Database para armazenar séries dedados temporais, principalmente sobre redes de computadores
  - Armazenamento com tamanho fixo
  - Útil para provimento de tendências históricas, com interface simples
- RRDTool manipula os RRDs
  - Apresenta, cria, deleta, insere e remove dados
    - *rrdtool create|update|graph|fetch|dump [options]*

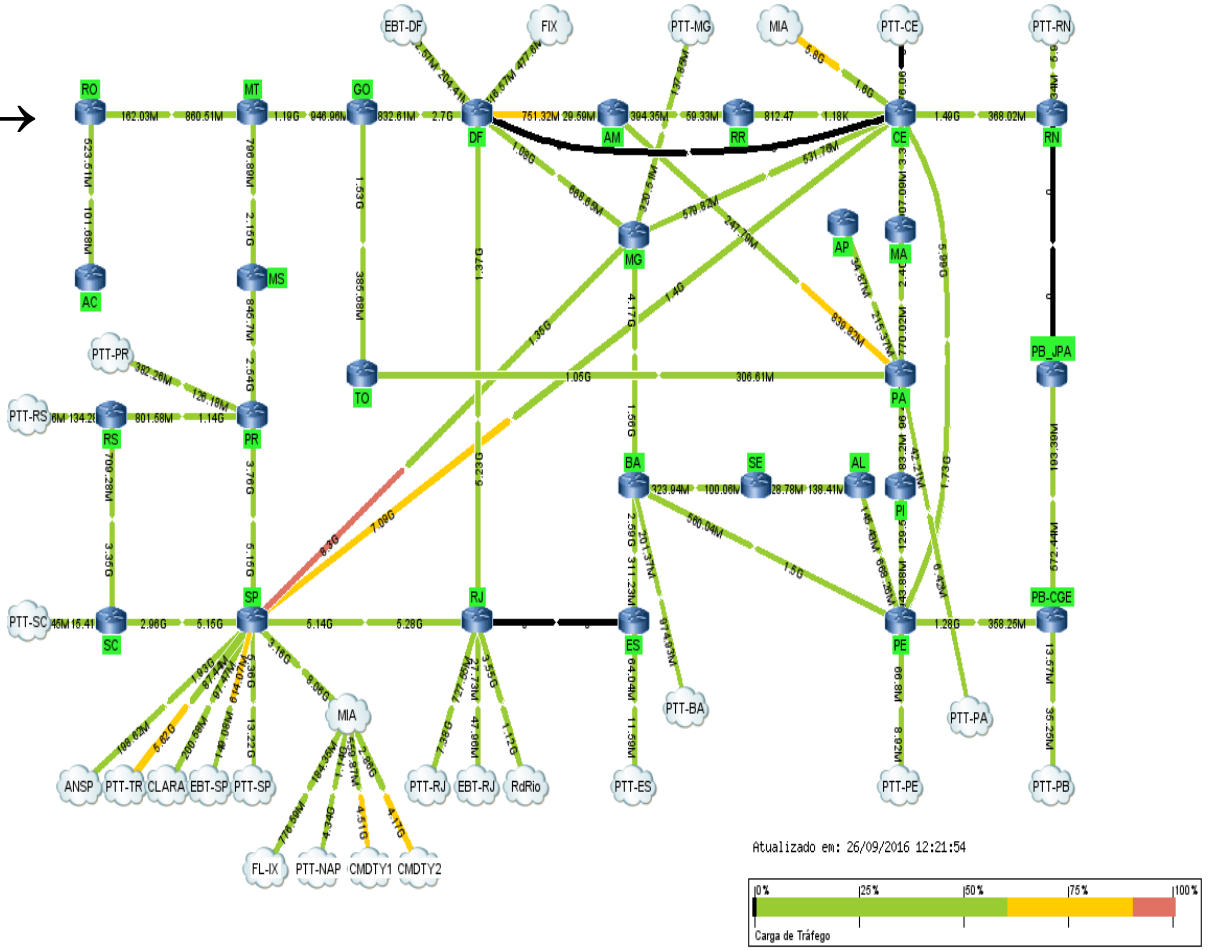
Cacti - Gráficos





Cacti - Plugins

- É possível estender as funcionalidades básicas com plugins:
  - Weathermap →
  - Syslog
  - Thold
  - Discovery
  - Etc



- Mais: http://cactiusers.org/downloads/

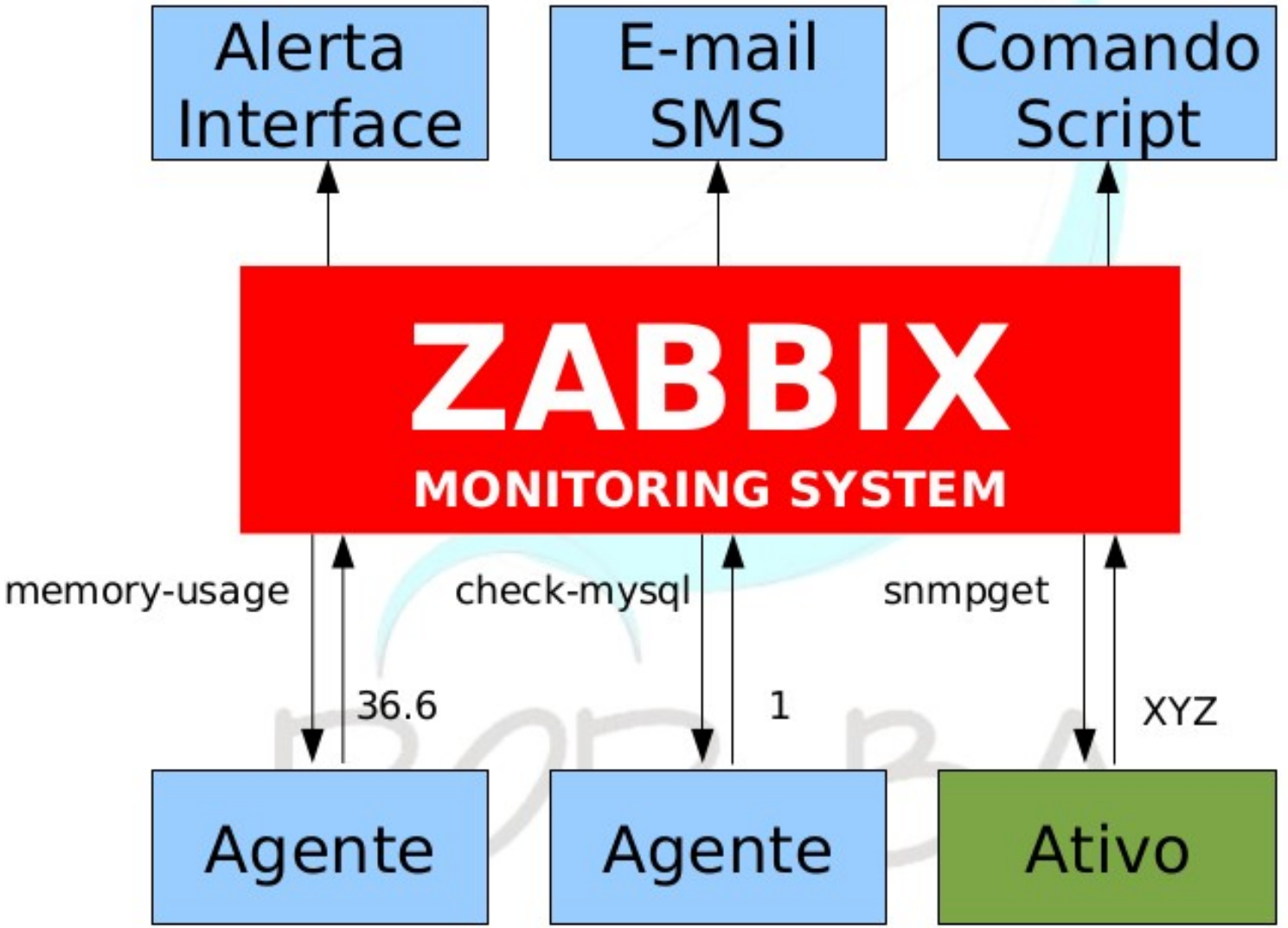
O que é o Zabbix

- Ferramenta código aberto para monitoramento completa de sistemas
- Suporta diversos bancos (PostgreSQL, MySQL, SQLite, etc)
- Agentes FreeBSD, GNU/Linux, Windows, etc
- Suporta IPv4 e IPv6
- Pode monitorar hosts diretamente (agentless)
- Oferece notificações em diferentes níveis
- Visualização via gráficos, mapas, telas e slideshow

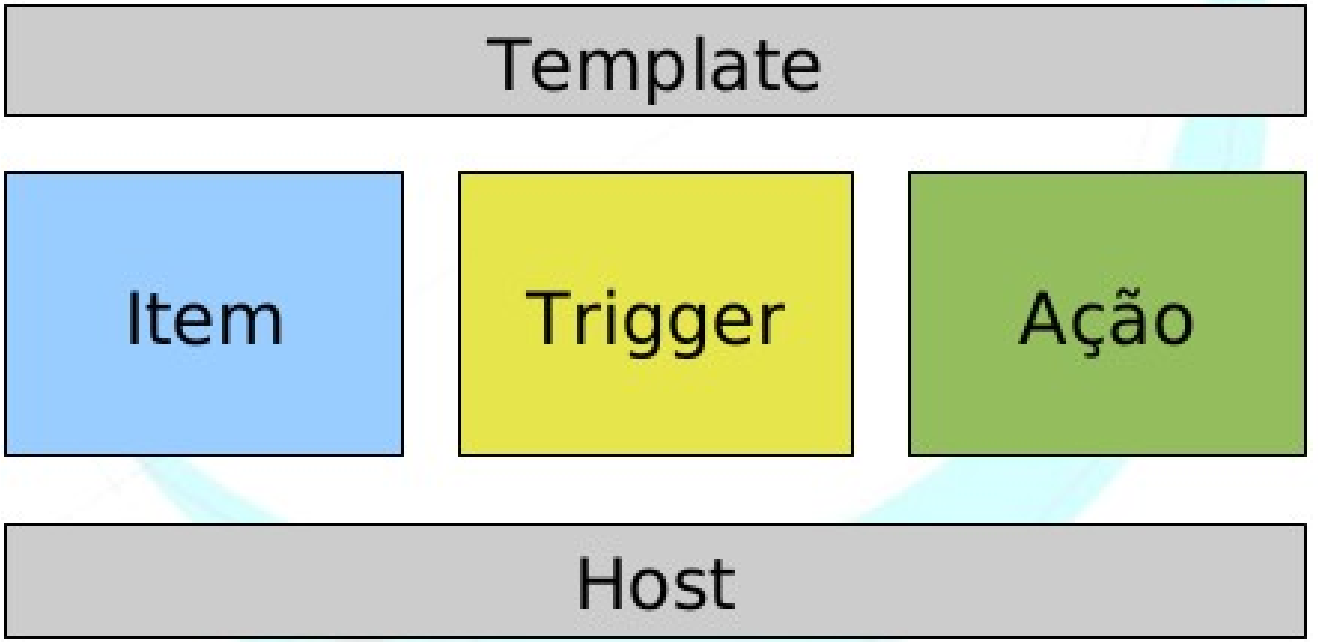
O que é o Zabbix (cont.)

- Frontend web para visualização, relatórios e configuração
- Monitoração distribuída (proxys e nodes)
- Automatização:
  - Templates
  - Descoberta automática (LLD) de hosts e atribuição de itens, alertas e gráficos (com base em critérios)
- Monitoração funcional de sites
- Monitoração pró-ativa com ações remotas nos hosts
- Monitoração ICMP, SNMP, Java Gateway, scritps de usuário, API própria, etc

Como Funciona

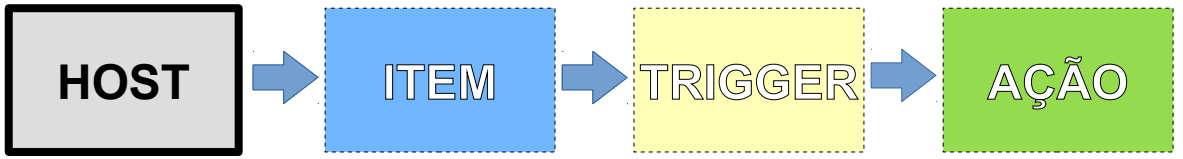


Servidor Zabbix



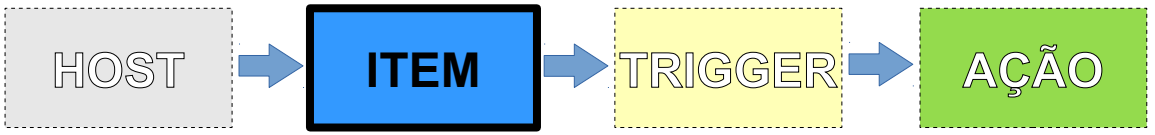
Conceitos:
Host - Ativos configurados no sistema
Itens - Objetos de monitoramento do sistema
Triggers - Alarmes do sistema
Action - Ações do sistema
Discovery - Serviço de descoberta da rede

Zabbix



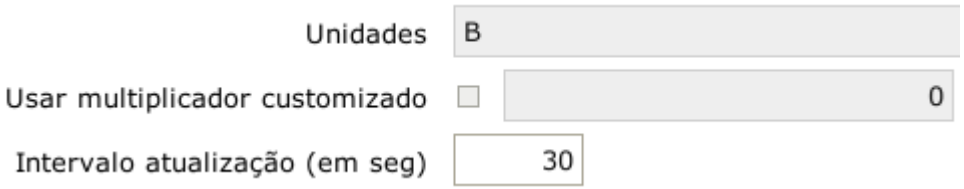
- Configuração do ativo a ser monitorado
  - Tudo começa configurando um host e sua interface seja Zabbix Agent, SNMP, IPMI ou JMX
  - Contém os seguintes parâmetros
    - Nome do host
    - Endereço IP (ou nome DNS)
    - Grupo de hosts associado
    - Templates de monitoramento associado
    - Contém um ou mais **ITEM** e **TRIGGER**
    - Outros...

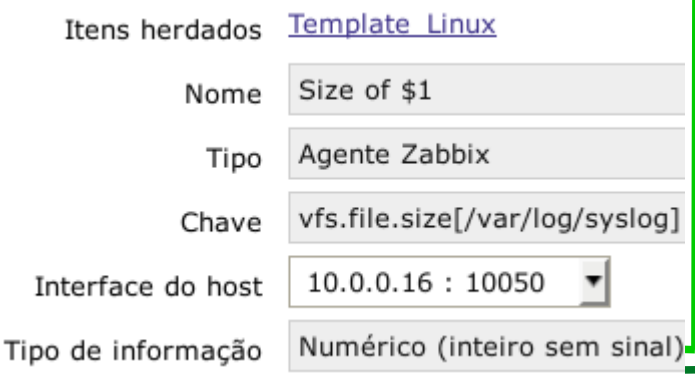
Zabbix



ITEM é o objeto monitorado dentro de um **HOST**

- Ex: monitorar o tráfego na **interface se0/1** do **router1**
- Contém os seguintes parâmetros:
  - Tipo (Ping, Agente Zabbix, SNMP, Script Externo, Trap, etc.)
- Chave de monitoramento
  - Formato: **<nome da chave>** [<*parâmetros*>]
  - **cbgpPeerState.sh**[*192.168.8.254*] → Script Externo
  - **IfOutDiscards.3** → SNMP
  - **vfs.fs.size**[*/var,pfree*] → Agente Zabbix
- Tipo de variável (texto, inteiro ou fracional)
- Outros…

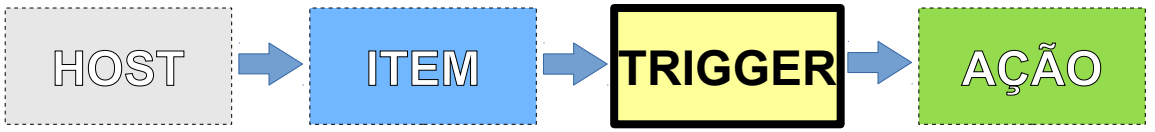




Zabbix

TEMPLATE

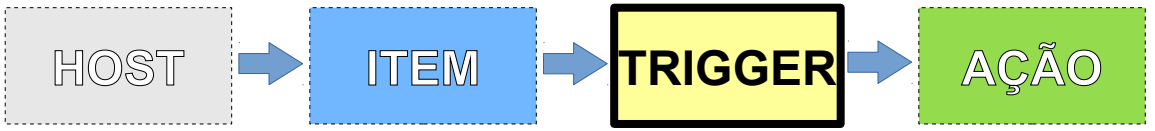
- Round Robin Database para armazenar séries dedados temporais, principalmente sobre redes de computadores
- Configuração padrão de itens, triggers, ações, gráficos, etc.
- Configuração automática ao associar o host a um template
  - Agilidade na adição de hosts
  - Facilidade de alteração/correção
  - Prático e organizado
  - Templates feitos pela comunidade



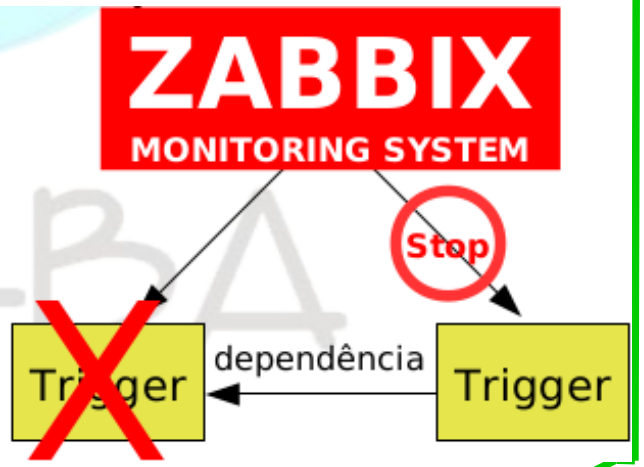
TRIGGER são regras associadas aos itens dentro de um host ou template

- Condições lógicas que disparam alertas no dashboard do Zabbix, caso o resultado de um **ITEM** case com a condição
- Expressões lógicas:
  - valor_retorno.**último** = *0*
  - valor_retorno.**média(120s)** > *5*
- Representam o estado atual do sistema
- Disparo de gatilhos para **Ações** adicionais
- Status das triggers: OK, PROBLEM ou UNKNOWN
- Criticidade das triggers:
  - Não classificada
  - Atenção
  - Média
  - Alta
  - Desastre

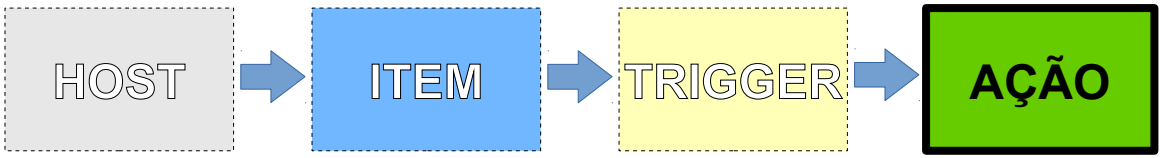
Zabbix



- Modelo de expressão
  - {<host>:<chave>(<parâmetro>)}<função_trigger><constante>
  - {vmserver1:vfs.fs.size[/var,pfree].last(0)}<10
- Alguns exemplos de funções_trigger:
  - média(#tempo)
  - último(#número de coletas)
  - soma(#tempo)
  - máximo(#número de coletas)
- Dependência de triggers
  - Caso a trigger que possui dependentes disparar, sua dependente não será monitorada até retorno da primeira



Zabbix



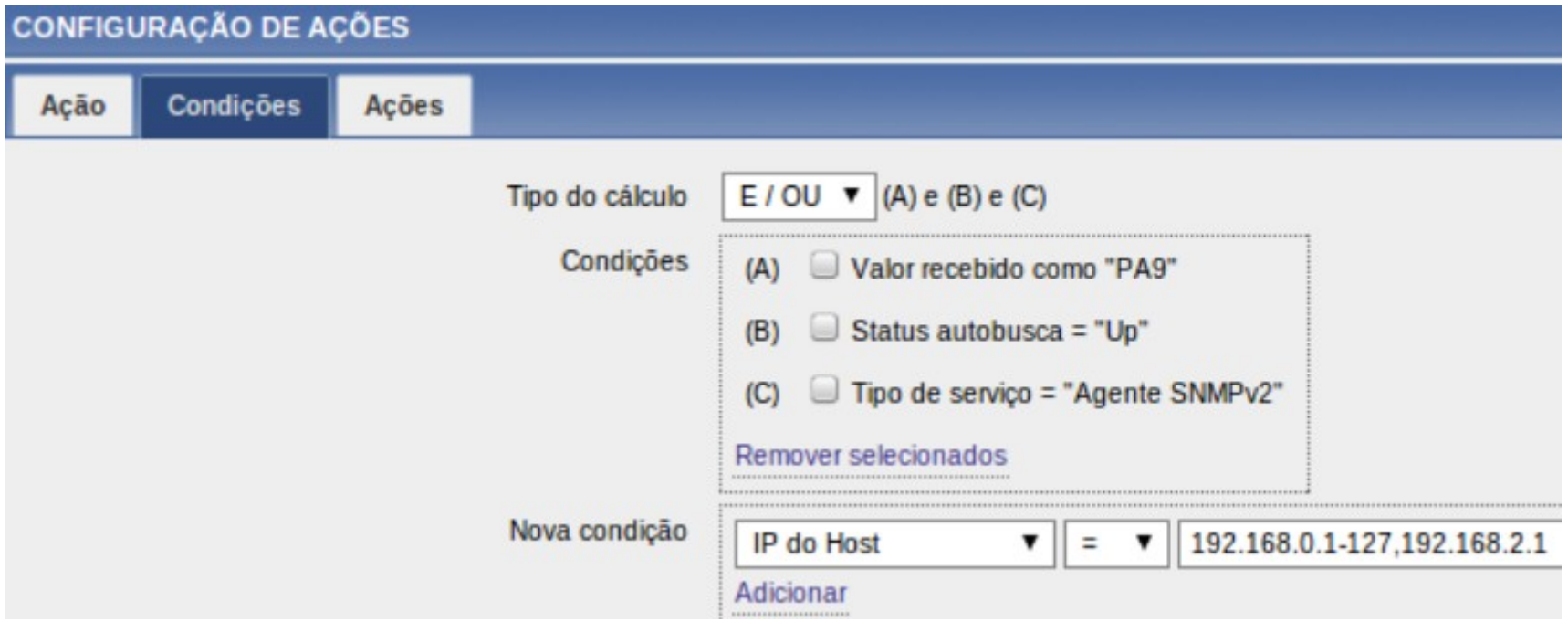
- Ações (ou eventos) são gerados por 3 origens:
  - Triggers: caso a trigger mude seu status
  - Descoberta: na detecção de hosts ou serviços
  - Eventos gerados pelos agente
- **Ação** pode ser customizada
  - Envio de e-mail para grupo responsável
  - Execução de scripts de usuário
    - Envio SMS, WhatsApp, etc
    - Intervenção no ativo (ex: acesso SSH e restart no processo X)
  - Baseadas no horário e dia da semana

Zabbix

- Regras de auto-descoberta
  - Chamada de LLD (Low Level Discovery)
  - Criação automática de hosts e associação de itens, triggers e gráficos a eles com base em diferentes critérios
  - Regras de autobusca estão em Templates e em Ações
    - Ações: adicionam novo host e associam-no a grupo ou template
    - Templates: adicionam itens, triggers e gráficos aos hosts do template
      - Configurações genéricas, preenchidas pelo resultado do SNMP, por exemplo

Regra de autobusca – Ação

- Exemplo:
  - Configurar uma **Ação** de discovery do zabbix para encontrar os hosts via SNMP
    - O OID da busca deve ser algo que vai ser usado para diferenciar os hosts encontrados



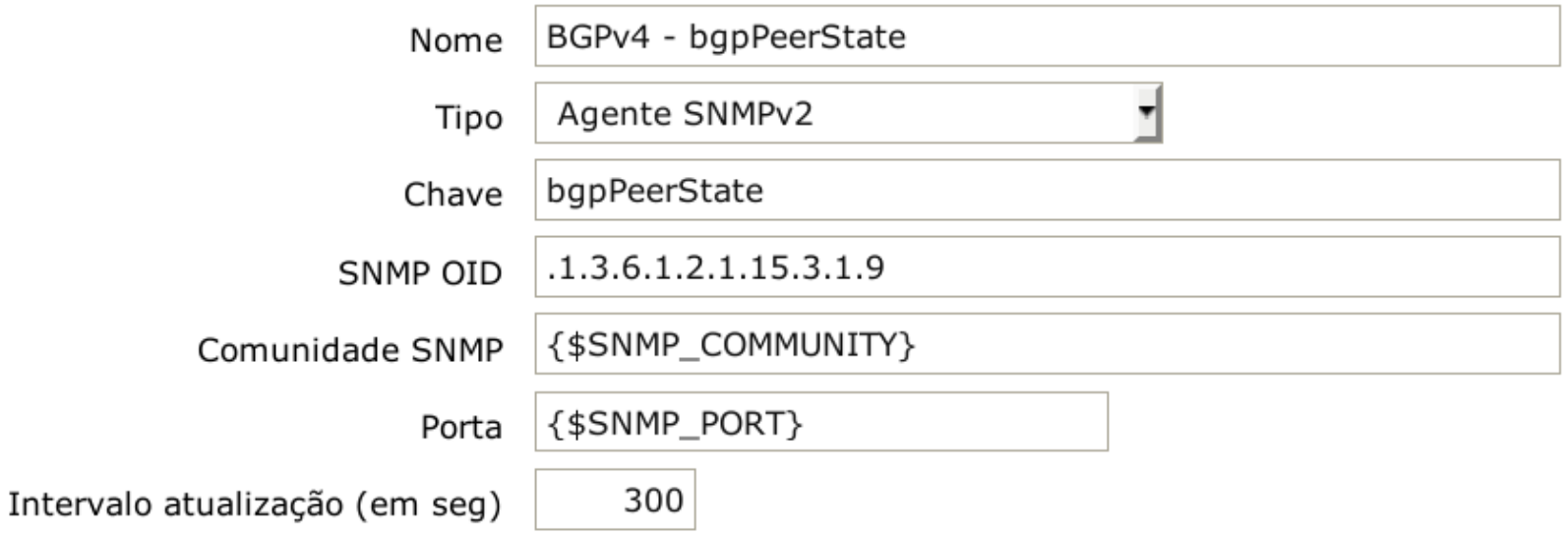
Regra de autobusca – Ação (cont.)

Regra de autobusca - Template

« Lista de templates **Template:** Template_Brocade_BGPv4 Aplicações (2) Itens (0) Triggers (0) Gráficos (0) Telas (0) Regras de descoberta (2) Cenários web (0)

Nome	Itens	Triggers	Gráficos	Hosts	Chave	Intervalo	Tipo
BGPv4 - bgpPeerState	Protótipos de itens (2)	Protótipos de trigger (1)	Protótipo de gráficos (0)	Protótipos de host (0)	bgpPeerState	300	Agente SNMPv2
BGPv4 - bgpPeerSummary	Protótipos de itens (1)	Protótipos de trigger (1)	Protótipo de gráficos (1)	Protótipos de host (0)	bgpPeerSummary	300	Agente SNMPv2

Regra de descoberta no template



Regra de descoberta

Definição de variáveis (Macros)

Regra de autobusca

Nome	bgpPeerAs - {#SNMPINDEX}
Tipo	Agente SNMPv2
Chave	bgpPeerAs.[{#SNMPINDEX}]
SNMP OID	.1.3.6.1.2.1.15.3.1.9.{#SNMPINDEX}
Comunidade SNMP	{$SNMP_COMMUNITY}
Porta	{$SNMP_PORT}
Tipo de informação	Numérico (inteiro sem sinal)
Tipo de dados	Decimal

Definição de item

Nome	|AME} BGP Peer State - {#SNMPINDEX} (AS{#SNMPVALUE})
Expressão	{Template_Brocade_BGPv4:bgpPeerState.[{#SNMPINDEX}].last(0)}#6

Definição de trigger

02 Ago 2016 01:22:49	RT1A BGP Peer State - 200.143.254.153 (AS1916)	OK	Alta	1m 24d 11h
02 Ago 2016 01:18:07	RT1A BGP Peer State - 200.143.254.153 (AS1916)	INCIDENTE	Alta	4m 42s

Desvantagem do LLD

- Cada novo host encontrado pode aumentar bastante a quantidade de itens do servidor
  - A grande quantidade de itens podeprejudicar o desempenho do zabbix
  - Será necessário um bom planejamento do sistema antes de sair colocando vários hosts.

Status do Zabbix		
Parâmetro	**Valor**	**Detalhes**
Zabbix está rodando	Sim	localhost:10051
Número de hosts (monitorados/não monitorados/templates/removidos)	153	130 / 2 / 21
Número de itens (monitorados/desativados/não suportados)	4321	3806 / 12 / 503
Número de triggers (ativas/desativadas)[verdadeiro/desconhecido/falso]	609	600 / 9 [10 / 0 / 590]
Número de usuários (online)	10	2
Desempenho requerido do servidor, novos valores por segundo	44.96	-

Cuidados no Monitoramento

- Monitoramento usa banda da rede
  - Uma regra comum é não exceder 1% da banda disponível
  - Diminuir comunicação entre servidor e agente
  - Utilizar um sistema de Traps (agente enviar informações ao servidor, ao invés de consultas periódicas do servidor
- Monitoramento usa CPU e memória
  - Exceto no *manager*, mal se percebe este uso
- Monitoramento pode ocupar muito espaço em disco
  - Condensar ou expirar os dados dos itens

Período de armazenamento do histórico (em dias)	90
Período de retenção dos dados sobre médias (em dias)	365

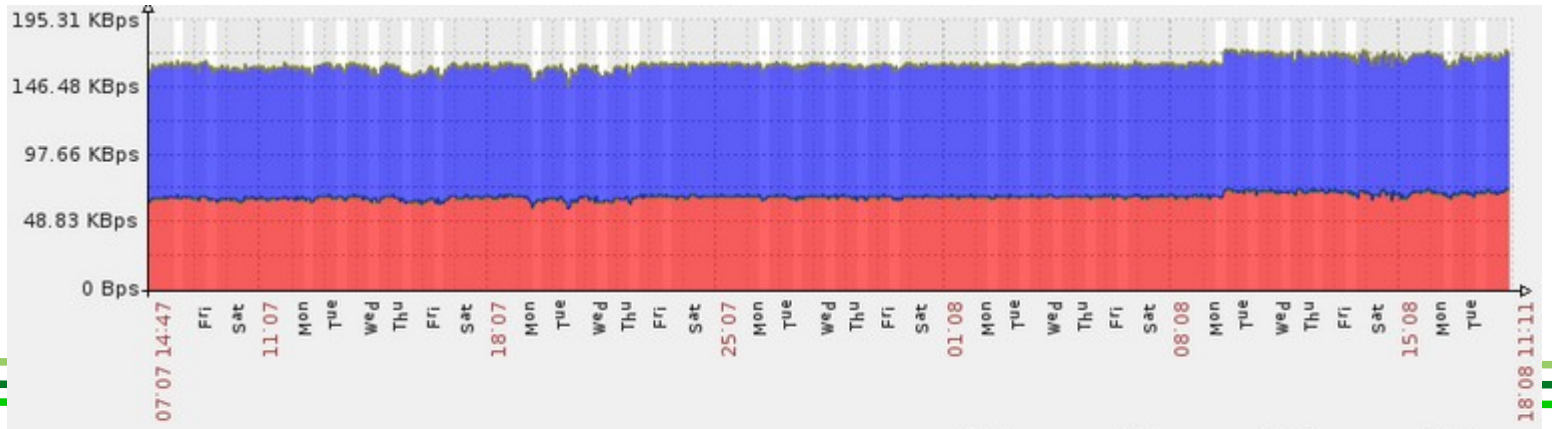
  - Cuidado com o volume alto de leitura e escrita em HD

Zabbix

- Monitoramento de sites
  - Diferentes passos de acesso a um site
    - Em cada um monitora-se, velocidade de download, conteúdo, tempo e código de resposta

DETAILS OF SCENARIO **Zabbix frontend** [18 Aug 2010 11:10:35]

Step	Speed	Response time	Response code	Status
First page	65.32 KBps	0s 100ms	200	OK
Log in	1.15 KBps	0s 83ms	200	OK
Check login	97.7 KBps	0s 93ms	200	OK
Logout	1.14 KBps	0s 83ms	200	OK
TOTAL		0s 359ms		OK



Diversidade no monitoramento

- Qualquer objeto cujo valor possa ser obtido por console/scripts ou afins é possível monitorar
  - No *Zabbix Agent* é possível definir parâmetros de usuário para chaves customizadas que rodam comandos

Arquivo de configuração: ***/usr/local/etc/zabbix_agentd.conf***

```
### Set of parameters for monitoring MySQL server (v3.23.42 and later)
### Change -u and add -p if required
#UserParameter=mysql.ping,mysqladmin -uroot  ping|grep alive|wc -l
#UserParameter=mysql.uptime,mysqladmin -uroot status|cut -f2 -d":"|cut -f2 -d" "
#UserParameter=mysql.threads,mysqladmin -uroot status|cut -f3 -d":"|cut -f2 -d" "
#UserParameter=mysql.questions,mysqladmin -uroot status|cut -f4 -d":"|cut -f2 -d" "
#UserParameter=mysql.slowqueries,mysqladmin -uroot status|cut -f5 -d":"|cut -f2 -d" "
#UserParameter=mysql.qps,mysqladmin -uroot status|cut -f9 -d":"|cut -f2 -d" "
#UserParameter=mysql.version,mysql -V
```

E se minha rede não tiver IP?

- Até então tudo que falamos é sobre a camada IP…
- Ethernet é um procoloco camada 2 amplamente utilizado
  - Ethernet OAM é uma série de ferramentas para Operação, Administração e Gerência de redes Ethernet
    - Padrões IEEE 802.1ag ou ITU-T Y.1731
    - Monitorar disponibilidade e/ou performance
    - Necessário configurá-lo nos dispositivos de rede
    - Em geral mais utilizado por provedores
    - Possível associar Ethernet OAM ao Icinga ou Cacti
      - *http://services.geant.net/edupert/Resources/Documents/EDUpert20140625_slides_Eth-oam.pdf*

Host	Service	Status	Status Information
nge-1.lighthouse.sara.nl	check_ethping	OK	PING 00:00:00:00:03:00 OK - Packet loss = 0%, RTA = 7.8806 ms
	check_ethtrace	WARNING	ETHTRACE b0a8.6e0d.1f03 WARNING - hops = 2 -- Wrong path detected (configured: 00:00:00:00:08:00,00:00:00:00:05:00,00:00;00:00:03:00 detected: 00:00:00:00:08:00,00:00:00:00:04:00,00:00:00:00:03:00)

NfSen / NfDump

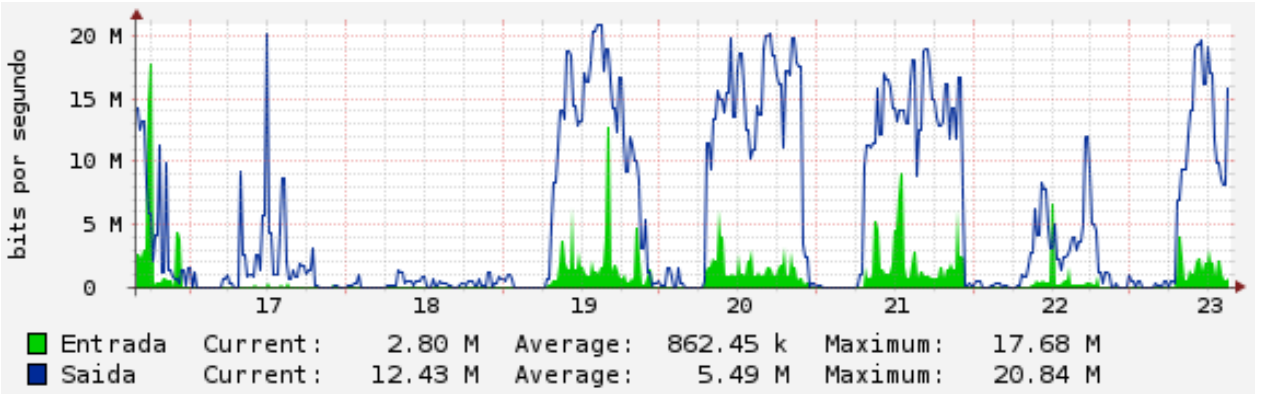
Fonte: Tracking Incidents with NfSen, Peter Haag (SWITCH-CERT)

NfSen / NfDump

- Algumas questões relacionadas ao tratamento de anormalidades em uma rede:
  - O que causou este pico em seu gráfico de rede?
  - Quais hosts/subnets consumem a maioria de nossa largura de banda?
  - Quais são os top talkers em sua rede?
  - Sobre aquele (D)DoS ocorrido, você poderia nos passar maiores informações?
  - Quais são os principais destinos que acessamos?

NfSen / NfDump

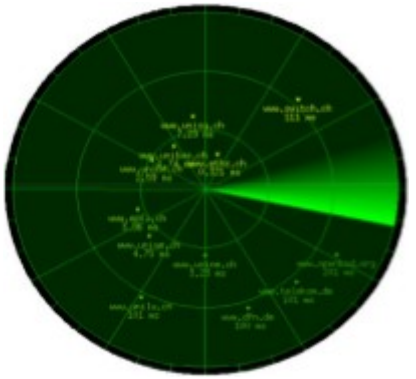
- Necessidade de análise de características de tráfego mais detalhadas
  - Gráficos tradicionais mostram apenas quantidade de tráfego



O monitoramento tradicional não é mais satisfatório!

NfSen / NfDump

- Precisamos de mais informações em nível de conexão:
  - Endereços IP
  - Portas (TCP/UDP)
  - Flags TCP
  - Contadores de Byte/Pacote
  - Número de interfaces
  - E qualquer outro filtro do cabeçalho dos pacotes



Qualquer filtro vai necessitar uma adaptação ao perfil da sua rede

Protocolo NetFlow

- Tecnologia de monitoramento de tráfego desenvolvida pela Cisco Networks. Fluxos são unidirecionais e contém dados relacionados à conexão, ex:
  - Endereços Ethernet de origem e destino
  - Endereços IP de origem e destino
  - Portas de origem e destino
  - Protocolo (TCP, UDP, ICMP, etc.), flags TCP
  - Contadores de pacote e bytes
  - Etc
- Funciona por amostragem
  - Exemplo:

Outra tecnologia usada é o sFlow, especificado pelo consorcio sflow.org

O protocolo IPFIX foi criado pelo IETF para substituir o NetFlow proprietário da Cisco.

```
2016-03-30  00:47:33.728  54.971  TCP  172.16.71.66:13599 → 192.168.10.34:80  .A..SF  215  9890
```

Registros Netflow nunca contém qualquer dado do usuário

Exemplo

- Consulta com top 15 IPs consumindo maior banda

```
forth% nfdump -r /data/rz/nfcapd.200603300150 -K 123… -n 20 -s ip/bps
Top 15     IP Addr ordered by bps:
Date first seen          Duration Proto          IP Addr    Flows  Packets     Bytes      pps       bps   bpp
2006-03-30 00:47:39.999     0.001 TCP      64.132.143.51        2       19     18004    18999  137.4 M   947
2006-03-30 00:45:00.737     0.001 TCP     194.64.105.184        2       20     13600    20000  103.8 M   680
2006-03-30 00:49:16.016     0.001 TCP      163.3.33.241         2        9     12046     9000   91.9 M  1338
2006-03-30 00:49:52.902     0.001 TCP      92.37.170.104        2       10      9208    10000   70.3 M   920
2006-03-30 00:45:06.853     0.001 TCP     214.214.200.81        2        6      6931     6000   52.9 M  1155
2006-03-30 00:46:32.363     0.001 TCP      68.142.57.84         2       10      6720    10000   51.3 M   672
2006-03-30 00:46:30.764     0.001 TCP     151.80.146.115        2        7      6680     7000   51.0 M   954
2006-03-30 00:48:36.966     0.001 TCP      129.4.38.113         2        8      6184     8000   47.2 M   773
2006-03-30 00:49:31.903     0.001 TCP     33.135.213.117        2        6      6104     6000   46.6 M  1017
2006-03-30 01:42:48.834     0.001 TCP      90.38.160.152        2        8      5941     8000   45.3 M   742
2006-03-30 00:48:02.473     0.001 TCP     131.144.55.170        2        6      5608     6000   42.8 M   934
2006-03-30 00:49:29.424     0.001 TCP      24.11.195.220        2        4      4880     4000   37.2 M  1220
2006-03-30 00:48:53.293     0.001 TCP      88.53.69.175         2        6      4721     6000   36.0 M   786
2006-03-30 00:45:41.780     0.001 TCP        49.30.8.60         2        6      3822     6000   29.2 M   637
2006-03-30 01:42:51.618     0.002 TCP      220.24.222.74        2       10      7605     5000   29.0 M   760

IP addresses anonymized
Time window: 2006-03-30 00:40:02 - 2006-03-30 01:49:58
Total flows: 19224 matched: 19224, skipped: 0, Bytes read: 1009920
Sys: 0.046s flows/second: 410112.0   Wall: 0.009s flows/second: 2022089.0
```

Exemplo

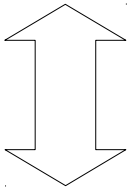
- Consulta das redes /24 com maior troca de tráfego

```
forth% nfdump -r /data/rz/nfcapd.200603300150 -K 123… -n 15 -A srcip4/24,dstip4/24 -s record/bytes
Aggregated flows 7525
Top 15 flows ordered by bytes:
Date flow start          Duration Proto     Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2006-03-30 00:41:06.140  4102.844 TCP      130.20.234.0:0     ->  130.254.221.0:0        79455   95.1 M    14
2006-03-30 00:42:50.622  4022.361 TCP      130.20.234.0:0     ->   194.90.158.0:0        42179   58.2 M    13
2006-03-30 00:40:51.729  4054.221 TCP      130.20.234.0:0     ->    220.63.34.0:0        39593   56.0 M     6
2006-03-30 01:41:42.025   443.957 TCP      130.20.224.0:0     ->     163.3.42.0:0        30543   43.3 M     7
2006-03-30 00:41:06.140  4102.844 TCP     130.254.221.0:0     ->   130.20.234.0:0        60178   29.1 M    14
2006-03-30 01:39:56.087   600.881 TCP      130.20.234.0:0     ->     194.84.7.0:0        17836   24.9 M     9
2006-03-30 00:44:39.128  3900.855 TCP      130.20.234.0:0     ->   214.124.39.0:0        15912   22.6 M     9
2006-03-30 01:41:01.414   529.568 UDP      130.20.223.0:0     ->   130.20.220.0:0        15549   21.4 M     8
2006-03-30 01:41:03.371   329.612 TCP     194.114.160.0:0     ->   130.20.234.0:0        14126   20.1 M     4
2006-03-30 01:40:12.986   300.997 TCP      130.20.234.0:0     ->  194.168.190.0:0        13101   18.7 M     2
2006-03-30 01:41:24.088   506.896 TCP      130.20.234.0:0     ->    24.50.25.0:0         12433   17.8 M     2
2006-03-30 01:43:04.047   300.870 TCP      165.242.80.0:0     ->   130.20.234.0:0         9966   14.3 M     1
2006-03-30 00:43:47.441  3935.542 TCP      130.20.234.0:0     ->   205.175.61.0:0        10445   13.4 M    15
2006-03-30 00:44:01.619   332.758 TCP      130.20.234.0:0     ->   194.61.253.0:0         8973   12.7 M   101
2006-03-30 01:42:43.123   300.860 TCP      130.20.234.0:0     ->    69.155.45.0:0         7872   11.3 M     1

IP addresses anonymized
Time window: 2006-03-30 00:40:02 - 2006-03-30 01:49:58
Total flows: 19224 matched: 18797, skipped: 0, Bytes read: 1009920
Sys: 0.062s flows/second: 307588.9   Wall: 0.010s flows/second: 1839969.4
```

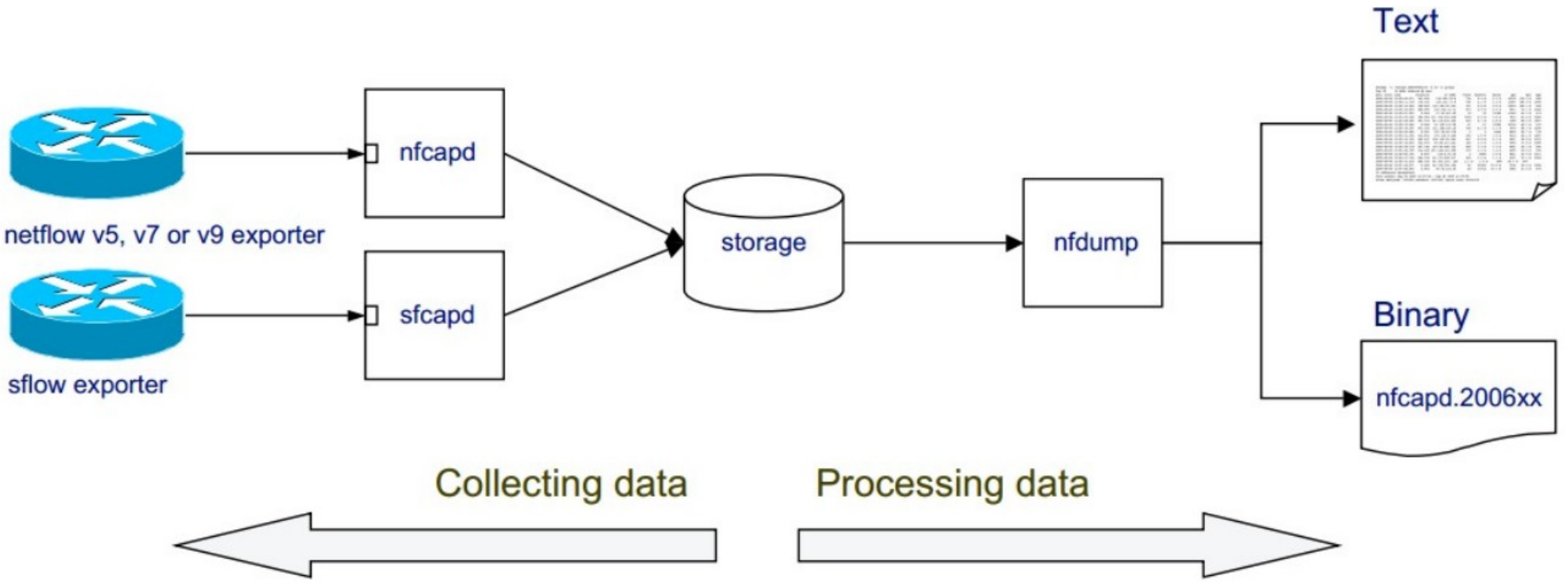
NetFlow / sFlow

NfSen
- Frontend web
- Exibe os fluxos
- Framework para automatizar tarefas



NfDump
- Coleta e armazena os fluxos
- Processa os fluxos na linha de comando

Arquitetura do NFDump



NFDump traz resultados bons, mas gostamos de imagens, correto?

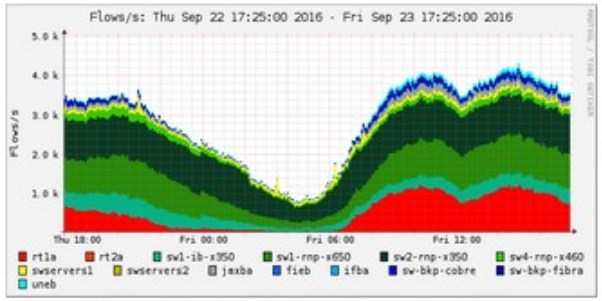
NFSen

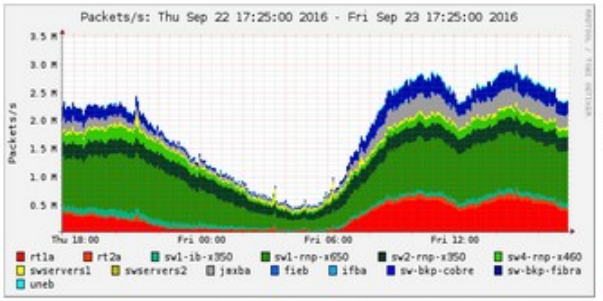
- Funcionalidades do NfSen para análise de incidentes de rede:
  - Uso do nfdump como ferramenta de backend
  - Imagens
  - Partimos da visão geral, para detalhes de um fluxo
  - Gráfico da situação atual da rede
  - Gráficos de perfis específicos da rede
  - Analisar uma janela de tempo específica

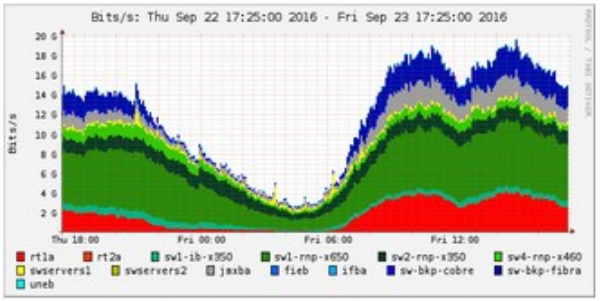
NFSEN

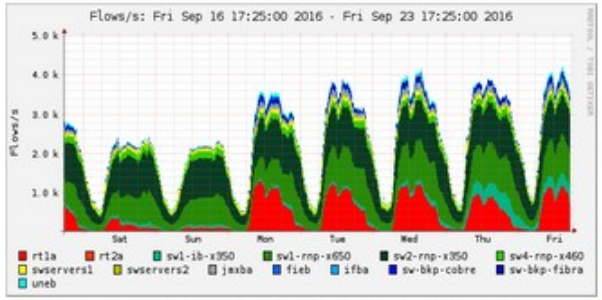
Home | Graphs | Details | Alerts | Stats | Plugins | live | Bookmark URL | Profile: | live ▼

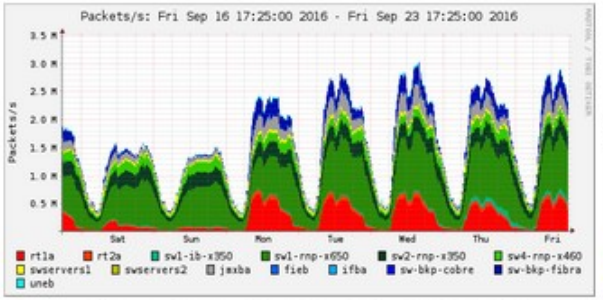
Overview Profile: live, Group: (nogroup)

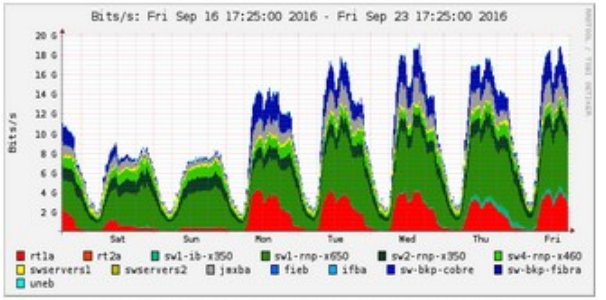


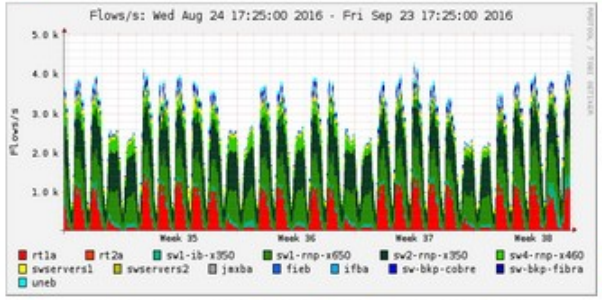


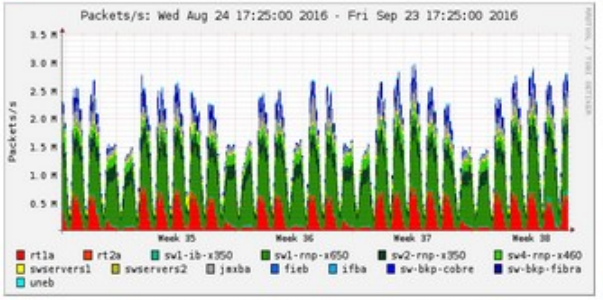


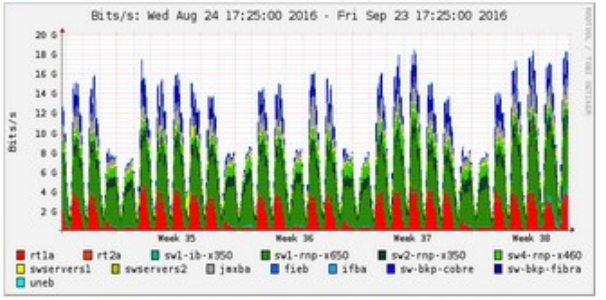


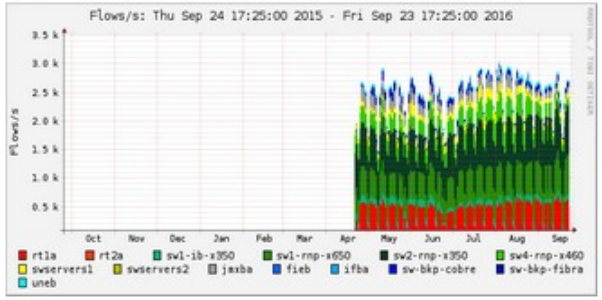


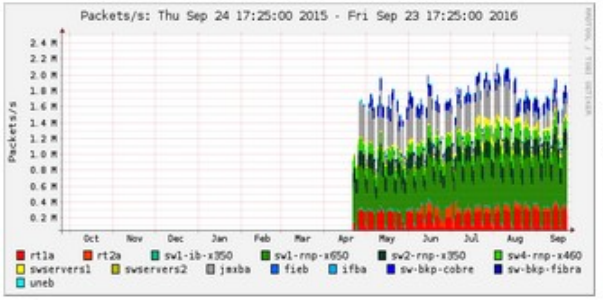


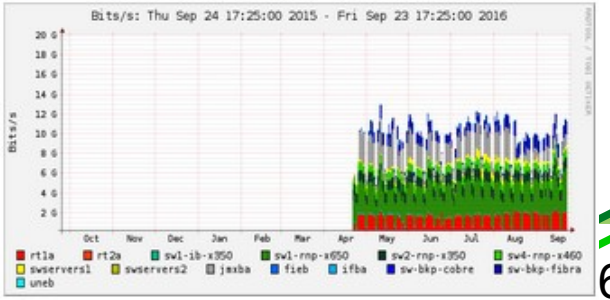




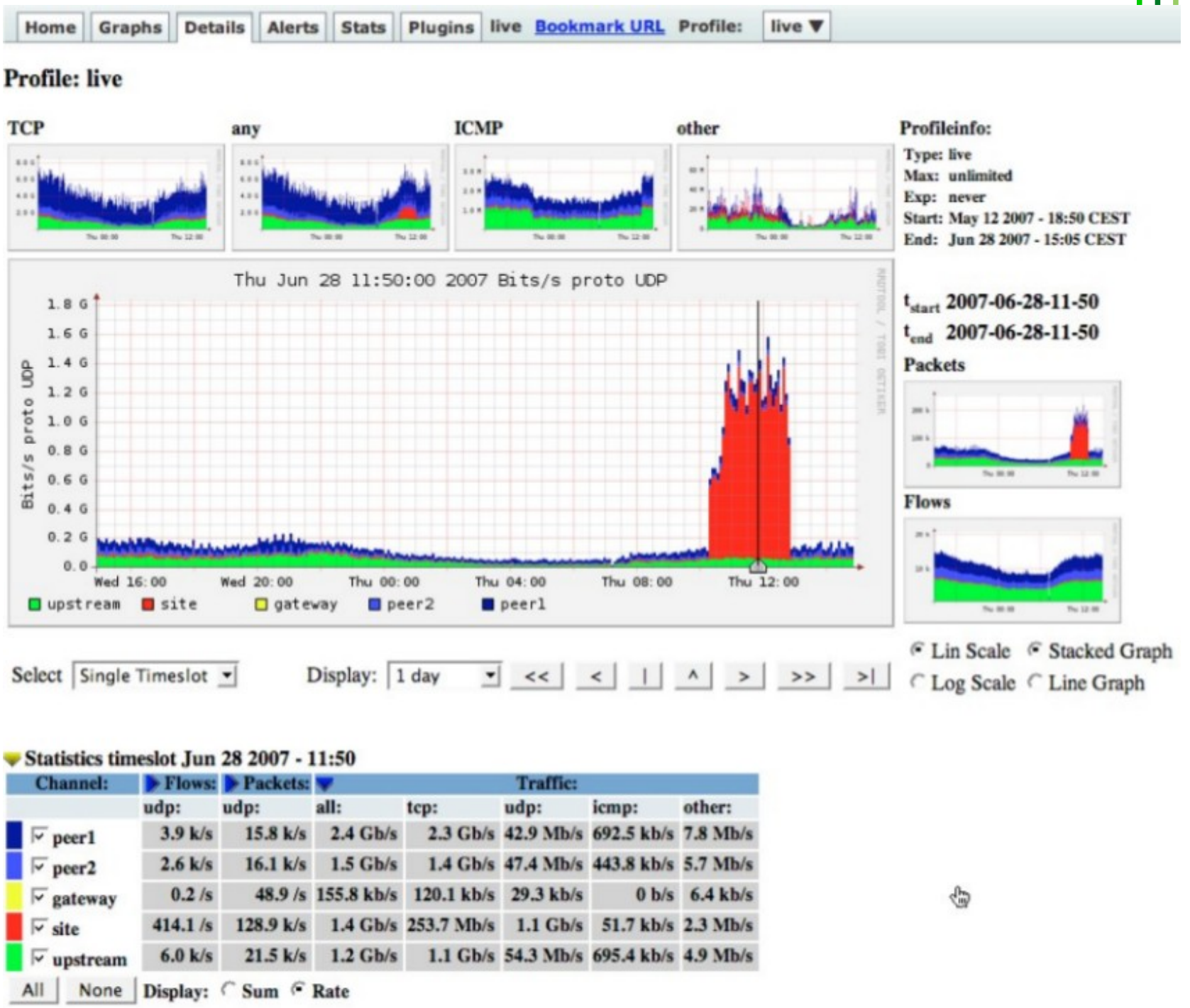






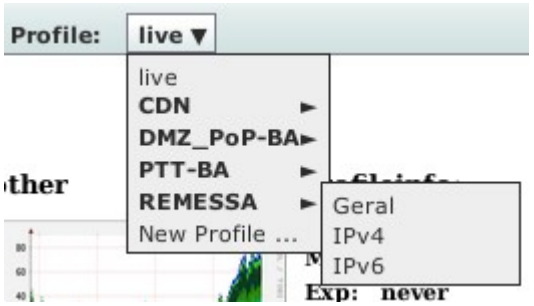


- Alguns eventos não são tão fáceis de visualizar



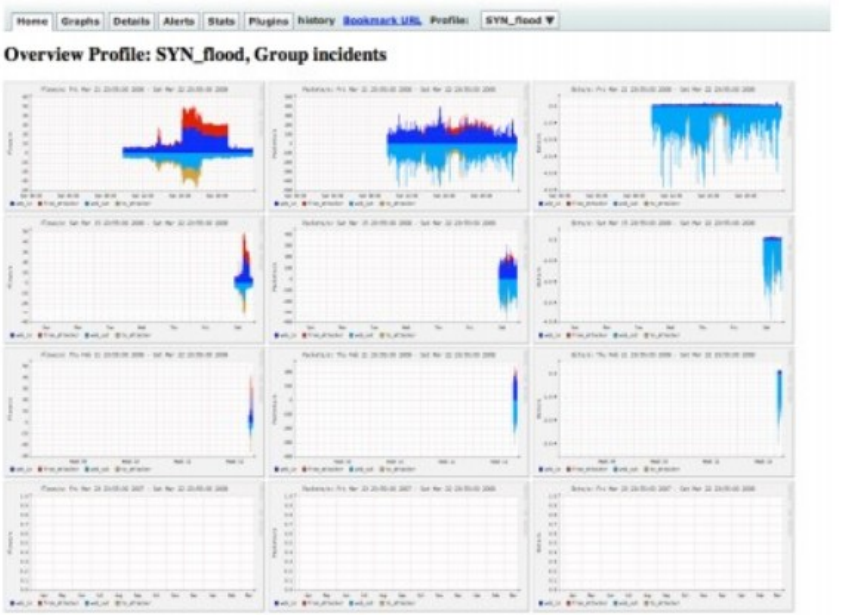
Perfis da Rede

- É uma visão específica dos dados dos fluxos, com filtros aplicados
- Aplicados aos gráficos assim como para a visão detalhada
- Pode ser criado a partir de dados antigos
- Pode ser criado para dados de entrada
- Pode contar um ou mais canais



Perfis de Rede

ip 47.121.141.83 or ip 125.195.247.233



Evento óbvio

NFSen / NFDump

- Detectando outros tráfegos suspeitos:
  - Alertas
  - Extensões
- Alertas
  - Monitoram os fluxos periodicamente
  - Muitas condições
  - Automaticamente dispara uma alarme, quando uma condição é satisfeita
  - Envia uma notificação, ou executa uma ação
- Mais informações: http://nfsen.sourceforge.net/

Referências

- http://www.cisco.com/networkers/nw04/presos/docs/NMS-1N02.pdf
- http://pt.slideshare.net/asimnawaz54/internet-control-message-protocol
- http://www.di.ufpe.br/~flash/ais98/gerrede/gerrede.html
- https://blog.serverdensity.com/how-to-monitor-mysql/

Sessão Prática

- Prática 1
  - Zabbix
- Prática 2
  - Cacti
- Prática 3 (extra)
  - PHPIPAM

PERGUNTAS?


WTR
VII WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA
26 E 27 DE SETEMBRO DE 2016