Análise Comparativa entre Ferramentas de Monitoramento de Redes de Computadores

Carlos Eduardo Peglow Holz [1]

[1]Curso Superior de Tecnologia em Redes de Computadores
Faculdade de Tecnologia SENAC Pelotas (FATEC)
Rua Gonçalves Chaves 602 – 96015560 – Pelotas – RS – Brazil

cepholz@gmail.com

Abstract. *This article demonstrates a comparative analysis between two monitoring tools being an open source and a commercial one where the tests consist of monitoring multiple hosts in virtualized environments using the CORE emulator and the results will be evidenced by the comparative analysis of the response time.*
Keywords: comparative, tools, monitor.

Resumo. *Este artigo demonstra uma análise comparativa entre duas ferramentas de monitoramento sendo uma de código-fonte aberto e outra comercial onde os testes consistem em monitorar múltiplos hosts em ambientes virtualizados utilizando o emulador CORE e os resultados serão evidenciados pela análise comparativa do tempo de respostas.*
Palavras-Chave: comparativa, ferramentas, monitorar.

1. Introdução

O monitoramento de redes é importante para gerenciar e analisar todos os dados trafegados na rede com isso podendo economizar tempo, aumentar a eficiência e minimizar a interrupção dos serviços evitando problemas como indisponibilidade de serviços.

A disponibilidade dos serviços é um fator importante sendo assim pode-se dizer que surgiu a importância do monitoramento de redes, uma das formas mais abrangentes do gerenciamento de redes.

Manter o ambiente de rede em constante monitoramento é fundamental para o crescimento de qualquer entidade mesmo que não seja da área de TI.

Praticamente tudo está relacionado com a informatização dos serviços, então é de suma importância que falhas sejam detectadas antes que o usuário possa perceber e sejam sanadas sem a percepção do mesmo para isto é necessário a utilização de ferramentas de monitoramento de redes.

2. Monitoramento de Redes

As redes de computadores se tornam cada vez maiories e mais complexas com diferentes dispositivos interligados e conforme as tecnologias vem surgindo começam a substituir as mais antigas para o aumento proporcional das redes.

É fundamental que se tenha o monitoramento das redes de computadores não somente dos equipamentos que fazem parte da rede mas também dos dados que por ela trafegam, pois monitorar falhas na rede ajudam evitar incidentes como perdas de dados.

Ferramentas de monitoramento de redes utilizam diversos conceitos tecnológicos, os protocolos de gerenciamento de redes são definidos pela RFC *"Requests for Comments"* são documentos que contém notas técnicas e organizacionais sobre a Internet.

3. Protocolos de monitoramento de redes

O Protocolo SNMP (*Simple Network Management Protocol*) é usado para comunicar o gerenciamento de informações entre as estações de gerenciamento de rede e os agentes em elementos de rede. O SNMP minimiza explicitamente o número e a complexidade do gerenciamento. Cada instância de qualquer tipo de objeto definido na MIB *Management Information Base* é identificada em operações SNMP por um nome exclusivo chamado "nome da variável" [IETF 1990].

É um importante protocolo de gerencia definido a nível de aplicação, é utilizado para obter informações de servidores SNMP agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP, onde os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP *User Datagram Protocol* para enviar e receber suas mensagens através da rede [Dias and Alves Jr 2002, Dias and Alves Jr 2013].

O Protocolo ICMP *Internet Control Message Protocol* é um protocolo de mensagens de controle de internet faz parte integrante do IP, e deve ser implementado por cada módulo IP, as mensagens ICMP são encaminhadas em várias situações uma delas por exemplo é quando o datagrama não pode alcançar seu destino. Como o protocolo Internet não foi projetado para ser extremamente confiável o objetivo destas mensagens de controle é fornecer um retorno sobre os problemas no ambiente de comunicação, salientando que não é para tornar o IP confiável, ainda que não há garantias de que um datagrama seja entregue ou até mesmo a mensagem de controle será retornada [IETF 1981].

Segundo Tanenbaum [Tanenbaum 2003] existe por volta de uma dezena de tipos de mensagens ICMP já definidos, cada tipo de mensagem ICMP é encapsulado em um pacote IP, as mensagens ICMP mais importantes estão listados na Tabela 1 .

Tabela 1. Os principais tipos de mensagens ICMP

Tipo de mensagem	Descrição
Destination unreachable	Quando não consegue localizar o destino
Time exceeded	Enviado quando um pacote é descartado
Parameter problem	Campo de cabeçalho foi detectado um valor inválido
Source quench	Ajustava o host que enviava pacotes demais
Echo	Utilizado para verificar se um destino está acessível e ativo
Echo reply	Resposta se o destino está acessível e ativo
Timestamp request	Os dados enviados são recebidos com adicional de hora
Timestamp reply	Os dados recebidos são devolvidos com adicional de hora
REDIRECT	Quando roteamento pode ter sido feito incorretamente

4. Ferramentas de monitoramento de redes de computadores

Foram selecionadas duas ferramentas de monitoramento de redes sem requisitos específicos levando em consideração o custo para o comparativo sendo elas o Zabbix [Zabbix 2016] e o PRTG [Paessler], utilizando os mesmos propósitos e protocolos.

4.1. Zabbix

O Zabbix é o produto principal da empresa Zabbix LLC tem sede nos Estados Unidos, Europa e Japão, com o Zabbix é possível coletar tipos de dados praticamente ilimitados da rede o monitoramento em tempo real de alto desempenho significa que dezenas de milhares de servidores, máquinas virtuais e dispositivos de rede podem ser monitorados simultaneamente. Os dados podem ser armazenados além dos recursos de visualização como mapas, gráficos e visão geral do sistema.

Segundo a empresa Zabbix [Zabbix 2016] a ferramenta oferece um excelente desempenho para a coleta de dados podendo ser dimensionado em ambientes muito amplos, vem com uma interface web onde os usuários se autenticam onde o acesso pode ser restringido por meio de permissões conforme necessidade.

A ferramenta pode realizar descobertas automaticamente para coletar os dados ou também por agentes instalados nos equipamentos a serem monitorados, tendo a possibilidade de criar gatilhos específicos para determinados eventos, é uma ferramenta open source e é disponibilizada em vários idiomas [Zabbix 2016, Neto and Uchôa 2006, Junior].

4.2. PRTG

O PRTG *Network Monitor* é um produto da empresa Paessler AG. Fundada em 1997 na região metropolitana de Nuremberg. A ferramenta PRTG *Network Monitor* é executada plataforma Windows, possui o código fonte proprietário, se encontra disponível na versão trial disponível por 30 dias sem limitações, após este período fica restrita a 100 sensores.

O PRTG monitora todos os sistemas, dispositivos e aplicativos de sua estrutura de TI usando tecnologias: SNMP, WMI,SSH, Fluxos e Sniffing de pacotes, Ping, solicitações HTTP e dados push, SQL e dentre outras, está disponivel em vários idiomas e com uma gama de relatórios bem ampla.

O sistema conta com diversas características: alerta flexível, várias interfaces de usuário, *failover*, *cluster*, mapas, painéis, monitoramento distribuído, geração de relatórios[Paessler , Paessler 2008, Silva and Lima].

O PRTG *Network Monitor* pode ser adquirido além da versão gratuita também em outras versões conforme Tabela2.

Tabela 2. Versões e valores

Licença	Quantidade de Sensores	Valor
Free	100	100
Trial 30 dias	Sem restrições	Gratuita 30 dias
PRTG 500	500	$1,600.00
PRTG 1000	1000	$2,850.00
PRTG 2500	2500	$6,150.00
PRTG 5000	5000	$10,500.00
PRTG XL1/Unlimited	Ilimitados (1 Servidor)	$16,900.00
PRTG XL5/Unlimited	Ilimitados (5 Servidores)	$60,000.00

5. Ambiente de testes

No ambiente de testes foram utilizados dois Hardwares conforme Tabela 3.

Tabela 3. Configurações de Hardware

Especificações	Hardware 1	Hardware 2
Memória	8 GB	8 GB
HD	1 TB	1 TB
Processador	I5	I7
Sistema Operacional	Windows 7	Windows 7

No Hardware 1 foi instalado a VM da ferramenta Zabbix e do PRTG e no Hardware 2 foi instalado o Emulador CORE, configurações das VMs conforme Tabela 4.

Tabela 4. Configurações das máquinas virtuais

VM	Memória	HD	Sistema Operacional
Zabbix	3 GB	60 GB	Ubuntu Server
PRTG	3GB	60 GB	Windows 7
CORE	2 GB	75 GB	Lubuntu

As ferramentas de monitoramento serão testadas em sistemas virtalizados e terão seus resultados documentados para análise dos dados coletados, serão executados testes com quantidades de hosts variados no Emulador CORE para testar o desempenho das ferramentas, o cenário será formado conforme Figura 1.

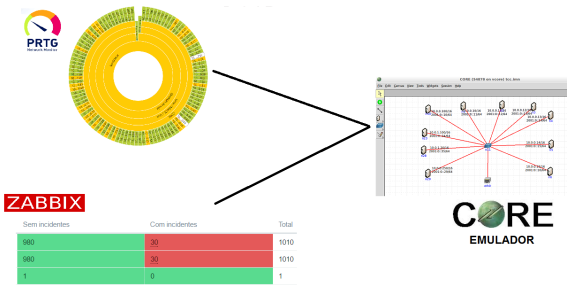


Figura 1. Cenário de teste

5.1. Emulador CORE

O CORE *(Common Open Research Emulator)* é uma ferramenta para emular redes em uma ou várias máquinas desenvolvido por um grupo de pesquisas de Tecnologias de Redes sendo apoiado pelo Laboratório de Pesquisa Naval dos Estados Unidos é um projeto de código aberto.

O CORE consiste em uma GUI para desenhar topologias de máquinas virtuais leves e conta com módulos *Python* para *scripting* de emulação de redes. Suas principais caracteristicas são: escalonabidade, interface de fácil interação, configuração e controle centralizado, executa aplicativos e protocolos sem modificá-los, pode ser distribuído em vários COREs e é altamente personalizável [RESEARCH].

5.2. Metodologia dos testes

Consistem na comparação de tempos em relação ao Ping e ao Serviço Apache, nos testes serão colocados diferentes quantidades de hosts emulados no Emulador CORE e serão analisados os resultados. No teste com o Ping será inicializada a VM do Emulador CORE verificando quando as ferramentas identificam o Ping, após todos os hosts serem identificados será pausada a VM do Emulador CORE e analisado quando as ferramentas identificaram a ausência do Ping. No teste do Serviço Apache será inicializado o Emulador CORE após as ferramentas identificarem que todos os hosts conseguiram identificar o Serviço Apache será desconectado da rede o Emulador CORE ocasionando indisponibilidade e após todos os hosts identificarem será recolocado novamente na rede e analisado quando as ferramentas identificaram o Serviço Apache em todos os hosts.

5.3. Teste comparativo em relação ao tempo de resposta com Ping

No teste realizado utilizou-se 100, 200, 300 e 1000 hosts emulados no Emulador CORE tendo como referência o tempo de resposta do Ping. Foi analisado desde quando o Ping parou e voltou a responder, foram coletados os dados de hosts realizando a comparação entre os tempos.

Os dados coletados foram apresentados na Figura 2 e demostram que a quantidade de hosts não é significativa para as ferramentas que estão sendo comparadas, levando em consideração que os hosts são emulados e não possuem perdas na rede, ambas as ferramentas conseguiram identificar a ausência de sinal praticamente em mesmos tempos, pela quantidade de hosts a diferença entre as coletas foram de 1 segundo os que apresentaram diferenças e em alguns testes não apresentaram nenhuma diferença, no Anexo estão apresentados os gráficos das capturas dos testes realizados.

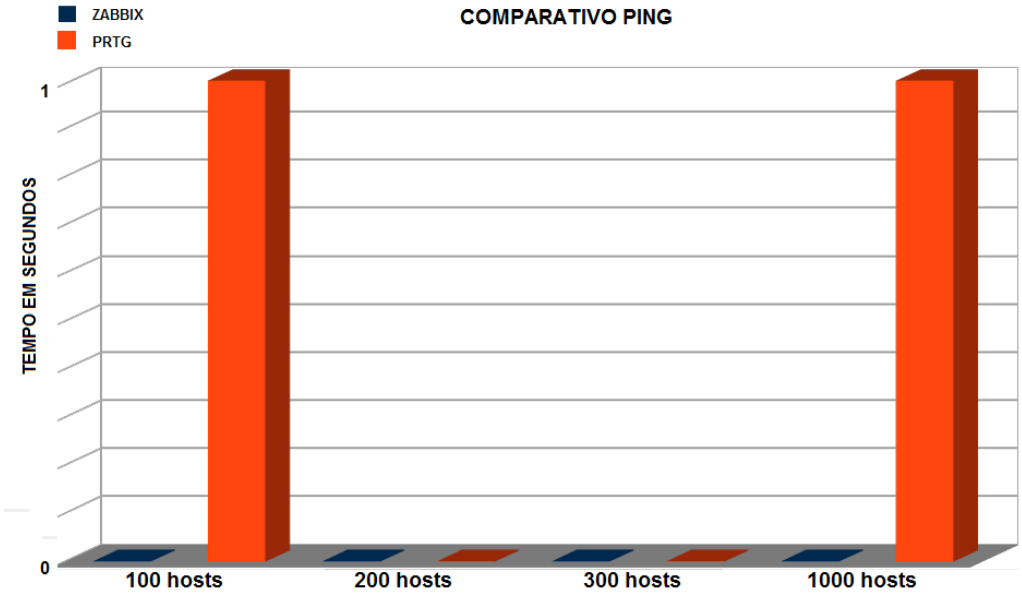


Figura 2. Tempo de resposta para o ping

5.4. Teste comparativo em relação a inatividade do serviço

Neste teste utilizou-se 10, 50, 100, 200 hosts tendo como referência o tempo de resposta do Servidor Apache simulando o tempo que a ferramenta levou para detectar a inatividade do Serviço Apache em todos hosts relacionados.

Os dados coletados foram apresentados na Figura 3 e demostram que o tempo de identificação da inatividade do Serviço Apache aumenta proporcionalmente em ambas as ferramentas conforme o números de hosts, este aumento de tempo se dá devido ao hardware do hospedeiro onde está a ferramenta de monitoramento, pela quantidade de hosts a diferença entre as ferramentas é pequena e em um dos testes se comportaram da mesma forma.

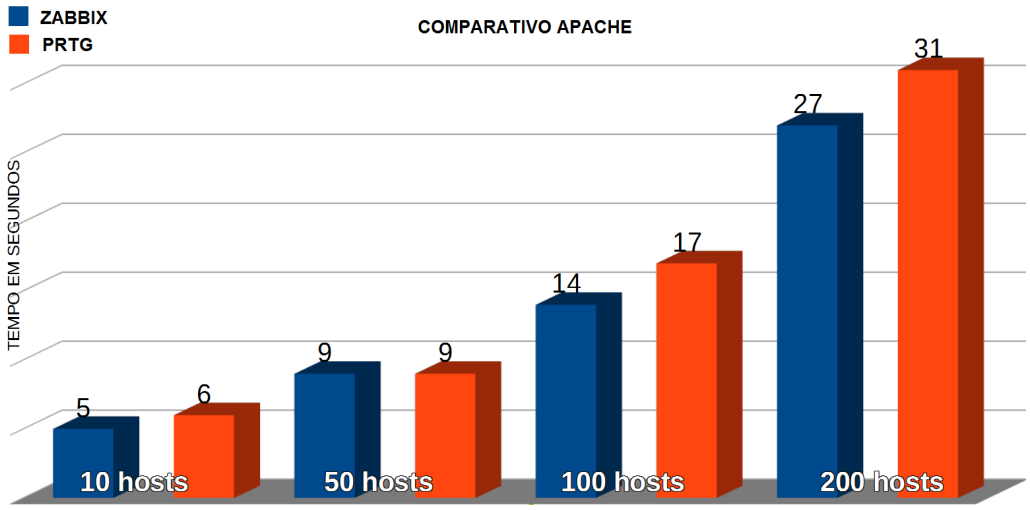


Figura 3. Tempo de resposta para inatividade do serviço Apache

6. Conclusões

Pode-se concluir neste estudo comparativo entre duas ferramentas de monitoramento, sendo uma open source e outra comercial que as duas obtiveram resultados satisfatórios já que conseguiram executar os testes propostos em laboratório, tendo algumas variações de tempos que no ambiente de testes não possuem valores significativos.

A grande dificuldade do sistema open source é que necessita de um profissional capacitado para a configuração e criação do sistema pois alguns templates e gatilhos para que o sistema funcione não vem predefinidos e isto requer um pouco mais de conhecimento na configuração do mesmo. Já no sistema comercial desde a instalação é mais simples não requer conhecimentos muito aprofundados já que o próprio sistema vem com uma ferramenta de varredura que faz a coleta dos dados no sistema.

É de suma importância o hardware onde o hospedeiro da ferramenta está instalado pois o consumo com a alta carga do sistema é notável, podendo levar a atrasos em informações bem como a inatividade do mesmo.

Nota-se no manuseio das ferramentas que a ferramenta open source se mostrou mais rápida em alguns momentos já que estava instalada em um sistema operacional Linux e a ferramenta comercial se mostrou um pouco mais lenta em determinados casos pois trabalha instalado em um sistema operacional Windows, levando em consideração que foram virtualizadas com mesmas configurações.

O investimento de uma ferramenta de monitoramento comercial é levado em consideração no quesito de opção e de manuseio pois fica provado neste comparativo entre as mesmas que se demostraram eficazes para os testes propostos.

Baseado nos testes a ferramenta comercial é de mais fácil aplicação e se mostrou mais dinâmica em relação a descoberta de serviços e hosts a serem monitorados pois a ferramenta possui o sistema de descoberta automática sem precisar instalar ou configurar módulos ou agentes.

6.1. Dificuldades encontradas

O hardware onde estava o Emulador CORE teve de ser substituído pois como havia instalado todas as VMs em um único harware o mesmo não suportou devido o Emulador CORE ter de emular uma carga muito alta de hosts, foi preciso colocar o Emulador CORE em uma VM com 4 núcleos para que os testes fossem concluídos, com a troca do hardware do Emulador CORE foi preciso refazer os testes que já haviam sido executados anteriormente para que não apresentasse alguma divergência de resultados.

6.2. Trabalhos futuros

Com o conhecimento adquirido na realização deste artigo pretende-se implementar as ferramentas em um cenário real para fazer o monitoramento de toda estrutura de rede de um provedor de internet.

Referências

Dias, B. Z. and Alves Jr, N. (2002). Protocolo de gerenciamento snmp. *artigo extraído da Internet*.

Dias, B. Z. and Alves Jr, N. (2013). Protocolo de gerenciamento snmp. *artigo extraído da Internet*.

IETF (1981). RFC 792 - INTERNET CONTROL MESSAGE PROTOCOL. Disponível em: <https://tools.ietf.org/html/rfc792>. Acesso em: junho de 2017.

IETF (1990). RFC 1157 - A Simple Network Management Protocol (SNMP). Disponível em: <https://tools.ietf.org/html/rfc1157>. Acesso em: junho de 2017.

Junior, E. R. F. Monitoramento de ambiente de redes utilizando zabbix.

Neto, A. F. and Uchôa, J. Q. (2006). Ferramentas livres para monitoraç ao de servidores.

Paessler, D. (2008). Server virtualization and network management. *Database and network journal*, 38(5):13.

Paessler, P. Network monitor. Disponível em: <https://www.br.paessler.com/prtg>. Acesso em: maio de 2017.

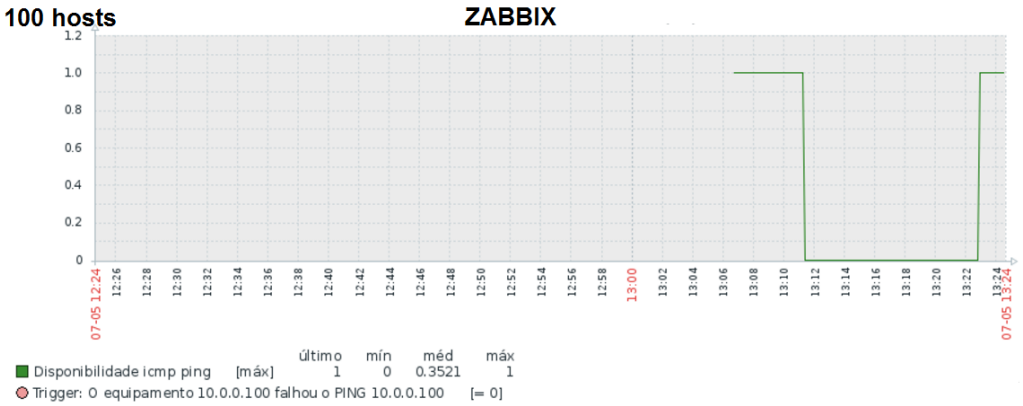
RESEARCH, U. Core. Disponível em: <https://www.nrl.navy.mil/itd/ncs/products/core>. Acesso em: maio de 2017.

Silva, É. C. and Lima, J. F. Ferramenta para monitoramento da latência de equipamentos de telecomunicação ip via web browser.

Tanenbaum, A. S. (2003). Redes de Computadores, 4ª Edição. Elsevier Editora Ltda.

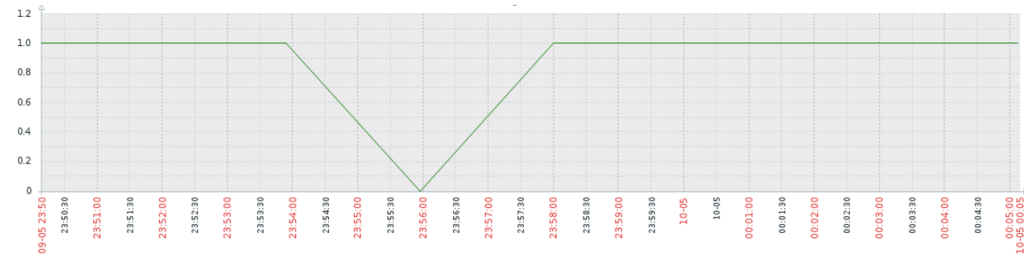
Zabbix, S. (2016). Homepage of zabbix:: An enterprise-class open source distributed monitoring solution. *Online, http://www. zabbix. com*, pages 02–16.

7. Anexos

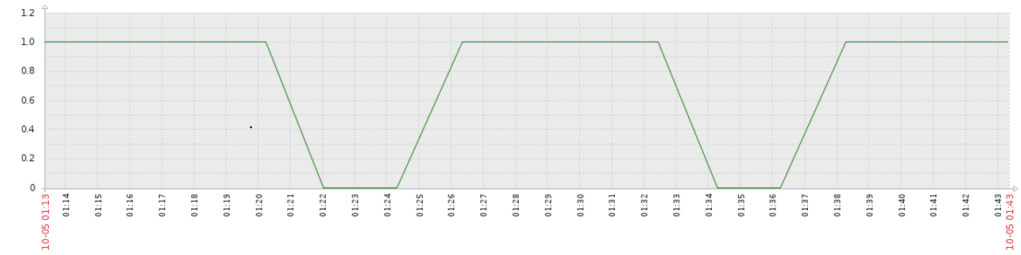


200 hosts

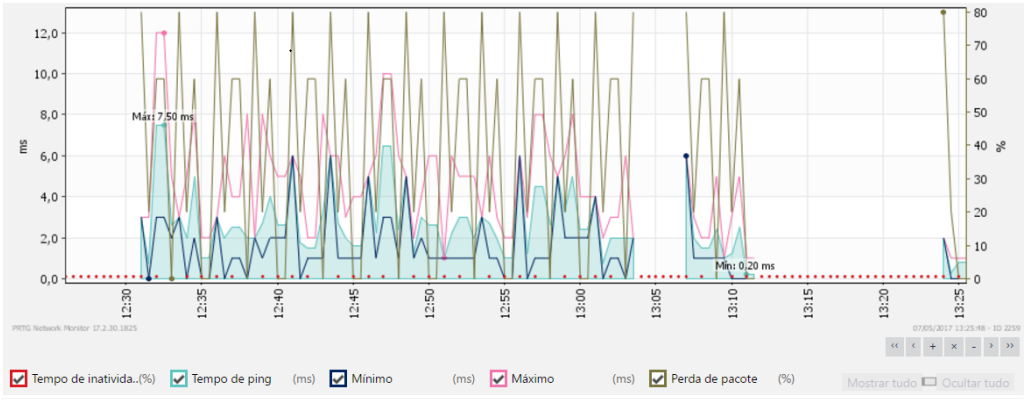
300 hosts

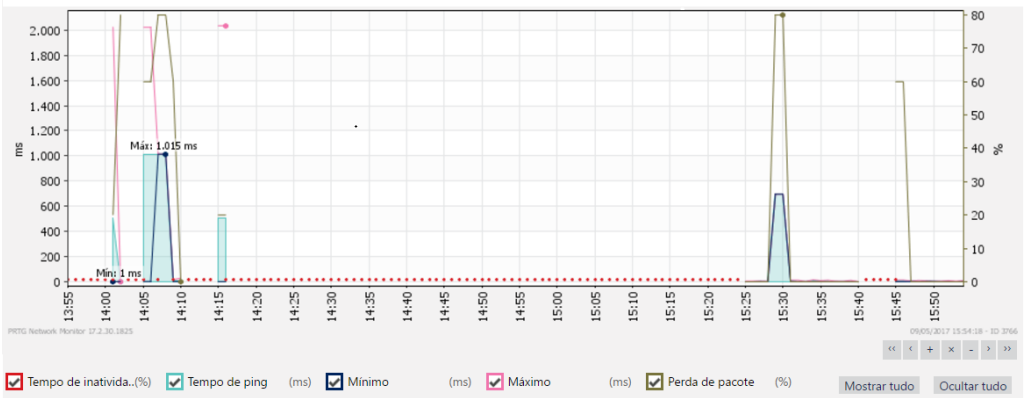


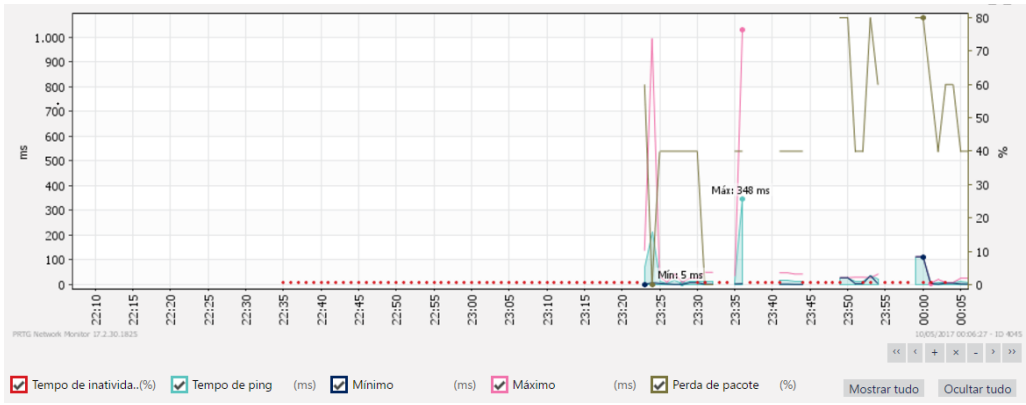
1000 hosts

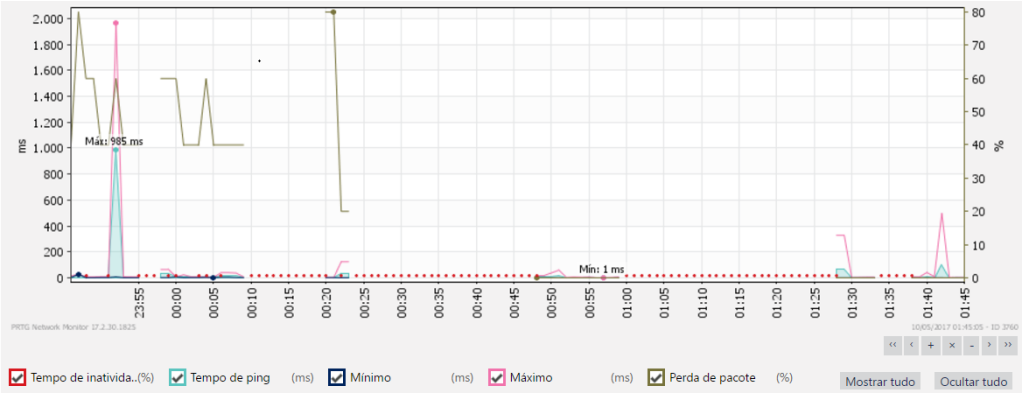


PRTG






ms
%
Máx: 348 ms
Mín: 5 ms
Tempo de inatividade..(%)
Tempo de ping (ms)
Mínimo (ms)
Máximo (ms)
Perda de pacote (%)
Mostrar tudo
Ocultar tudo


ms
%
Máx: 985 ms
Mín: 1 ms
Tempo de inatividade..(%)
Tempo de ping (ms)
Mínimo (ms)
Máximo (ms)
Perda de pacote (%)
Mostrar tudo
Ocultar tudo