Unidade IV

7 FERRAMENTAS DE MONITORAMENTO DISTRIBUÍDAS POR GPL

Existem diversas ferramentas de monitoramento baseadas em licenças públicas GPL. Muitas delas formam importantes comunidades, que auxiliam no desenvolvimento de *plugins* para as ferramentas.

A Licença Pública Geral (General Public Licence – GPL) garante liberdades como a execução do programa para qualquer propósito, o estudo do funcionamento do programa e a adaptação às suas necessidades, a redistribuição de cópias para auxiliar os próximos usuários e a possibilidade de aperfeiçoar o programa e liberar suas modificações, a fim de permitir que toda a comunidade se beneficie com as alterações.

Nas seções a seguir serão detalhadas algumas das mais importantes dessas ferramentas.

Lembrete

GPL é um dos tipos de licença pública mais comuns para programas de código aberto e requer que evoluções baseadas no programa original sejam disponibilizadas com a mesma licença.

7.1 Squid

Em 1994, foi iniciado o projeto Harvest, financiado pelo Internet Research Task Force Group on Resource Discovery, e cujo objetivo era a construção de um conjunto de ferramentas integradas para atuar na coleta, extração, categorização e busca, além de fazer cache e multiplicar as informações na internet. Uma parte do desenvolvimento do projeto teve uma nova direção em relação aos objetivos iniciais. Essa frente recebeu o codinome Squid.

O *software* Squid para servidor *proxy*, projetado com base em sistemas Unix, foi implementado para desempenhar tanto a função como HTTP quanto como *proxy* e cache. As primeiras versões desse *software* surgiram em 1996.

Desde então, novas versões foram lançadas e o Squid evoluiu em funcionalidades e tamanho. São exemplos das funções mais elaboradas: opções de armazenamento com técnicas avançadas, suporte de funções, como o redirecionamento de URL, interceptação HTTP, *traffic shaping* e diversos módulos para a autenticação.

O Squid é um *software* compatível com os sistemas operacionais Windows, Linux, FreeBSD, OpenBSD e NetBSD. Uma das vantagens da utilização do Squid é a redução do tráfego no servidor *web*. Isto ocorre porque o servidor *proxy* é um elemento intermediário entre o usuário que está buscando informação e o servidor *web*. O servidor *proxy* executará uma série de etapas e processos, como a aceitação da requisição desse cliente, a realização do processamento e o futuro encaminhamento para o servidor *web*. Com isso, a solicitação do usuário poderá ser registrada, rejeitada ou até modificada antes do encaminhamento final, sem que o servidor *web* tenha feito qualquer operação.

Em relação ao cache, o Squid funciona como uma espécie de caixa postal que guarda todos os conteúdos que foram recebidos. No caso, o cache irá utilizar os conteúdos analisados na *web* para aplicá-los futuramente. Em alguns casos, o usuário requisita o mesmo conteúdo repetidas vezes. Esse conteúdo fica armazenado no cache e pode ser acessado por meio dele, dispensando a comunicação com o servidor *web*.

Para a utilização do Squid, deve-se configurá-lo através da edição do arquivo squid.conf, que é o responsável por todas as configurações – por exemplo, as Listas de Acesso (Access Lists – ACLs), a inserção e a modificação de parâmetros importantes no sistema.

Assim, deve-se ter um vasto conhecimento do funcionamento de rede e da programação de *scripts* para utilizar somente esta ferramenta, pois ela é gratuita e não existe muito detalhamento no *site* dedicado ao *software*, bem como não há uma equipe de suporte para atender seus usuários.

Figura 39 – *Site* oficial da ferramenta Squid

Saiba mais

Mais especificações sobre o Squid podem ser encontradas no *site* dedicado ao *software*:

<http://www.squid-cache.org/>.

7.1.1 Squid Guard

Uma extensão aplicada ao Squid é o Squid Guard, que possibilita o bloqueio de um conjunto de listas específicas, categorizadas, que são denominadas Blacklists. Algumas dessas listas estão disponíveis gratuitamente na internet e são constantemente atualizadas. Elas podem ser divididas quanto ao uso em: não comercial e comercial.

7.1.2 Squid Guard Manager

A ferramenta *web* Squid Guard Manager foi desenvolvida por Gilles Darold e é disponibilizada sob os termos GNU GPL. Com esse *software*, incrementam-se as funções do Squid Guard, pois é possível configurar e gerenciar esse *software* através da leitura de seu arquivo de configuração, o squidGuard.conf.

Nesse *software*, algumas das funcionalidades adicionais são o redirecionamento de URLs desejadas, a criação e o emprego de filtros de controle mediante o uso de listas cadastradas, o bloqueio de listas com datas e horários definidos previamente e a administração das listas por meio de cadastro ou exclusão de domínios.

Um ponto a observar é que, após qualquer alteração de configuração no Squid Guard Manager, para que a mudança seja aplicada, é preciso reiniciar o Squid. Para facilitar essa ação, existe no menu uma opção chamada Restart Squid. A figura a seguir ilustra a interface desse *software*.

Figura 40 – Interface da ferramenta Squid Guard Manager

Um dos pontos a desenvolver nesta ferramenta é a funcionalidade dela, pois pode parecer complexa para pessoas com pouco conhecimento técnico – ela não possui uma interface intuitiva e de fácil utilização.

Além disso, não é possível configurar as Blacklists de forma automática: isso deve ser feito manualmente.

7.2 Nagios

Nagios é um programa GPL de monitoramento de redes que verifica constantemente a disponibilidade do serviço, seja local, seja remota, e avisa por *e-mail* ou SMS sobre o problema ocorrido. É possível obter relatórios de disponibilidade e configurar ações corretivas para os problemas ocorridos na rede.

Figura 41 – Logotipo do *software* Nagios

Em princípio, o Nagios foi desenvolvido para o sistema operacional Linux, mas também pode rodar em outros sistemas Unix. Foi desenvolvido em C e Perl.

O Nagios pode ser expandido através de *plugins*. Existem vários *sites* com estas extensões para o *software*. Alguns desses *plugins* são:

- nrpe: execução remota de *plugins*;
- nsca: *checks* passivos (automáticos).

Saiba mais

Para mais informações, visite os *sites* dedicados a este programa:

<http://www.nagios.org/>.

< http://nagiosplug.sourceforge.net/>.

<http://nagios-br.com/>.

Já o Nagios Core é o sistema de monitoramento *open source* que permite às organizações identificar e resolver problemas de infraestrutura de TI antes que eles afetem os processos críticos de negócios.

O Nagios Core possibilita o monitoramento de toda a infraestrutura de TI para garantir que os sistemas, aplicativos, serviços e processos de negócios estejam funcionando corretamente. No caso de uma falha, ele pode alertar os responsáveis técnicos do problema, permitindo-lhes começar a correção antes que as interrupções afetem os processos de negócios, usuários finais ou clientes.

A figura a seguir ilustra a interface *web* para a visualização de: atual *status* da rede, notificações, histórico de problemas e arquivos de *log* presentes no *software* Nagios.

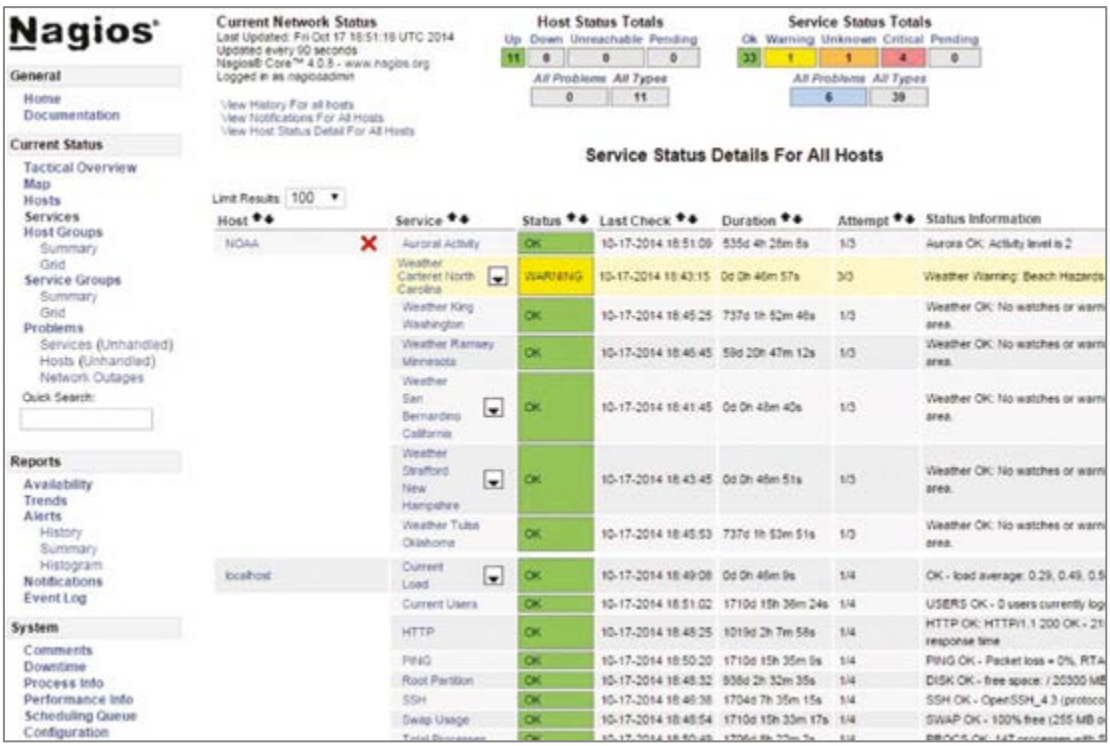

Figura 42 – Gerenciamento de alertas do Nagios

Uma característica do *software* Nagios Core é o monitoramento compreensível para o usuário de diversos serviços da rede, como SMTP, POP3, HTTP, NNTP, ICMP e SNMP. Também é possível monitorar os recursos de computadores ou equipamentos de rede, como carga do processador, uso de disco e *logs* do sistema.

Toda o monitoramento remoto é suportado através de túneis encriptados SSH ou SSL, e existe o desenvolvimento de diversos *plugins*, simplificando a customização. Como a checagem é paralelizada, uma eventual demora em uma atividade não tem impacto nas demais.

Adicionalmente existe a capacidade de definição da rede de forma hierárquica, distinguindo equipamentos que não estão mais disponíveis dos que não são mais alcançáveis.

Por ser uma ferramenta de gerenciamento de alarme, é possível notificar quando um serviço ou equipamento tem um problema ou quando este já foi resolvido. Esse aviso pode ser enviado por *e-mail*, SMS ou outras formas definidas pelo usuário através dos *plugins*.

Uma dificuldade da ferramenta é que a configuração é realizada por meio de arquivos-texto, o que torna complexo o processo para usuários menos experientes. O arquivo de configuração principal contém diversas diretivas que alteram o funcionamento do Nagios.

Além dos arquivos de configuração, existem os arquivos de recurso que armazenam as macros criadas pelos usuários, bem como as configurações de conexão a banco de dados. Os arquivos de configuração de objetos são utilizados para a definição de serviços, clientes, grupos de clientes, contatos, grupos de contatos, entre outros. Já o arquivo de configuração de CGI contém diretivas que afetam a operação dos CGIs.

Muitas vezes, uma única ferramenta de rede não é suficiente para cumprir todos os objetivos de monitoramento. Pode-se combinar a ferramenta Nagios com a ferramenta de desempenho Catci, pois, enquanto o Cacti faz uso de mais elementos gráficos, o Nagios Core se preocupa em mostrar o estado da rede sem o uso de gráficos. Desse modo, os dois podem ser utilizados em conjunto, um complementando o outro.

7.3 Zabbix

O Zabbix é uma solução desenvolvida e distribuída através da licença pública GPLv2. Assim, trata-se de uma ferramenta *open source*. O Zabbix é uma ferramenta de código aberto de nível *enterprise*, com suporte à monitoração distribuída.

Quanto às funções, o Zabbix é um *software* que monitora vários parâmetros da rede, dos servidores e da saúde dos serviços. Ele apresenta um mecanismo flexível de notificação que permite configurar alertas por *e-mail* para praticamente qualquer evento. As notificações possibilitam que se reaja rapidamente a problemas no ambiente. O Zabbix oferece excelentes recursos de relatórios e visualização de dados armazenados. Este *software* é capaz de monitorar a disponibilidade e a *performance* de toda a sua infraestrutura de rede, além de aplicações.

A ferramenta possui agentes compatíveis com várias plataformas: Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, NetBSD, Mac OS e Windows.

São características desse *software*: o suporte nativo ao protocolo SNMP; a existência de uma interface de gerenciamento *web*, de fácil utilização; a possibilidade de integração com bancos de dados como MySQL, Oracle, PostgreSQL ou SQLite. A geração dos gráficos e mapas ocorre em tempo real e o *software* permite customizações.

Adicionalmente, o *software* possui suporte a *triggers* e envio de notificações, em caso de eventos, por SMS, *e-mail* e *scripts* personalizados. Também permite a realização de inventário da rede, autenticação de usuário e *log* de auditoria.

O Zabbix agrupa diversas funções e configurações. É possível organizá-las em quatro grupos fundamentais, definidos por: coleta de dados, armazenamento de dados, alertas e notificações e visualização dos dados coletados.

A arquitetura do Zabbix é composta de servidor, banco de armazenamento, interface *web*, agente e *proxy*, que é opcional. O servidor Zabbix pode ser considerado como o componente central da solução em ambientes centralizados – os agentes enviam os dados coletados (sobre integridade, disponibilidade e estatística) para o servidor. Este último deve ser uma máquina Linux, que monitora sistemas (clientes) em diferentes plataformas e elementos de rede.

O *software* utiliza um banco de armazenamento para guardar as informações de configuração e os dados recebidos em um Sistema Gerenciador de Banco de Dados (SGBD).

A interface *web* (GUI) auxilia no acesso rápido, e a partir de qualquer dispositivo.

O agente Zabbix é instalado nos servidores. Ele realiza o monitoramento e pode acompanhar ativamente os recursos e as aplicações locais.

Um recurso útil do Zabbix é a criação de *templates* de máquinas. Ao utilizá-los é possível herdar características comuns, bem como personalizar dispositivos.

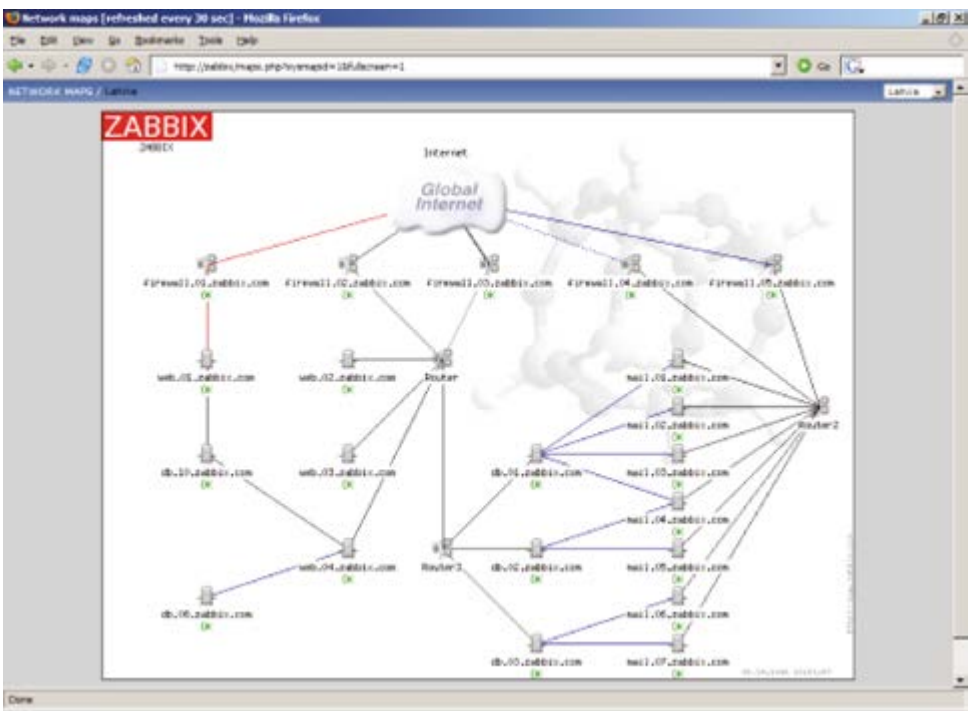

Figura 43 – Mapa de rede desenhado pelo Zabbix

Saiba mais

O *site* oficial do Zabbix possui *wiki*, documentação e fóruns com diversos artigos, perguntas e resposta de usuários:

<http://www.zabbix.org/>.

Observação

Ao comparar o Zabbix com outras ferramentas, nota-se que ele consegue agregar valores de duas ferramentas, como o Nagios Core e o Cacti.

8 FERRAMENTAS DE GERENCIAMENTO COMERCIAL

Quase a totalidade das ferramentas de gerenciamento disponibilizadas gratuitamente não oferecia interfaces muito amigáveis para o usuário. Adicionalmente, a configuração dessas ferramentas, para que o monitoramento fosse inicializado, não era nada simples, sendo necessário um amplo conhecimento técnico para conseguir operar esses *softwares*. Muitas vezes, quando o usuário encontrava um problema no *software*, não havia nenhuma documentação ou suporte ao usuário.

Com isso, as ferramentas gratuitas atendiam às necessidades de um público ávido por tecnologia, mas não satisfaziam todas as necessidades do público empresarial. Assim, diversas empresas de *software*, como HP, IBM e Computer Associates (CA), criaram soluções de gerenciamento de redes cuja licença de uso é cobrada, provendo uma maior quantidade de serviços aos usuários, interfaces mais amigáveis e intuitivas e suporte aos usuários.

Alguns produtores de *software* gratuito também desenvolveram versões pagas de suas ferramentas.

8.1 Nagios XI

O Nagios XI possui componentes *open source* da classe empresarial comprovada, os quais oferecem a melhor solução de monitoramento para os exigentes requisitos organizacionais atuais.

Projetado com escalabilidade e flexibilidade, o Nagios XI foi desenvolvido para tornar as tarefas de monitoramento mais simples, mantendo os atributos de um poderoso sistema voltado para a classe empresarial. A figura a seguir mostra a tela de monitoramento desta ferramenta.

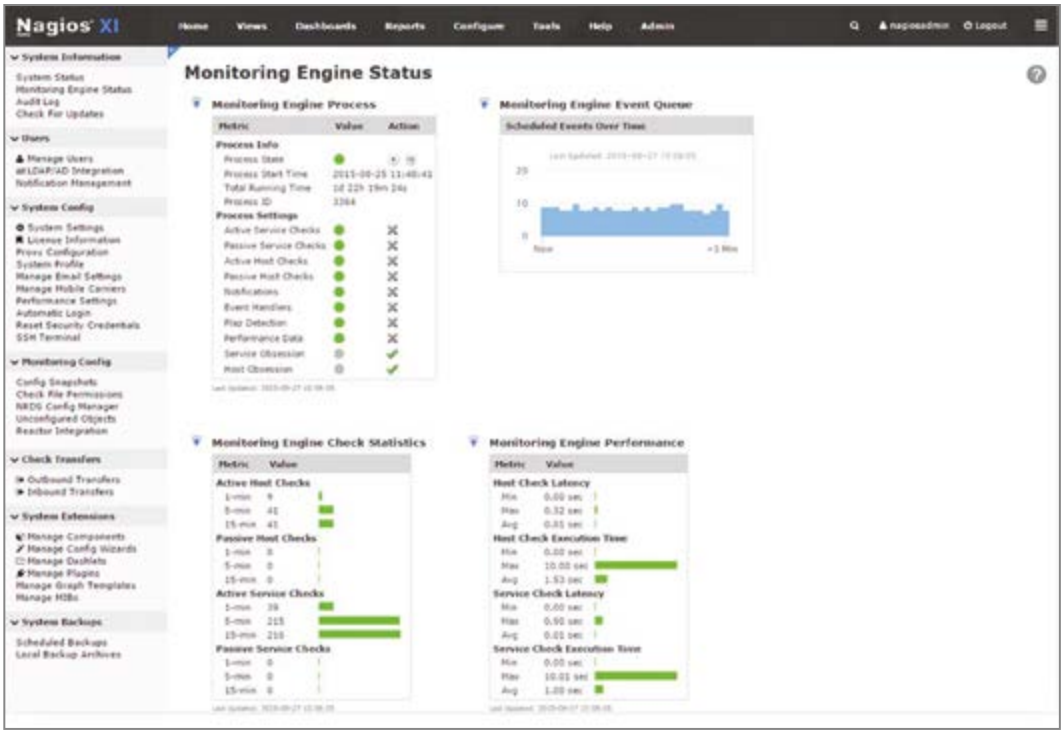

Figura 44 – Tela de monitoramento do Nagios XI

Foi desenvolvida uma interface *web* gráfica com *dashboard* que proporciona informação detalhada dos dispositivos monitorados pelo Nagios XI, como é possível observar a seguir.

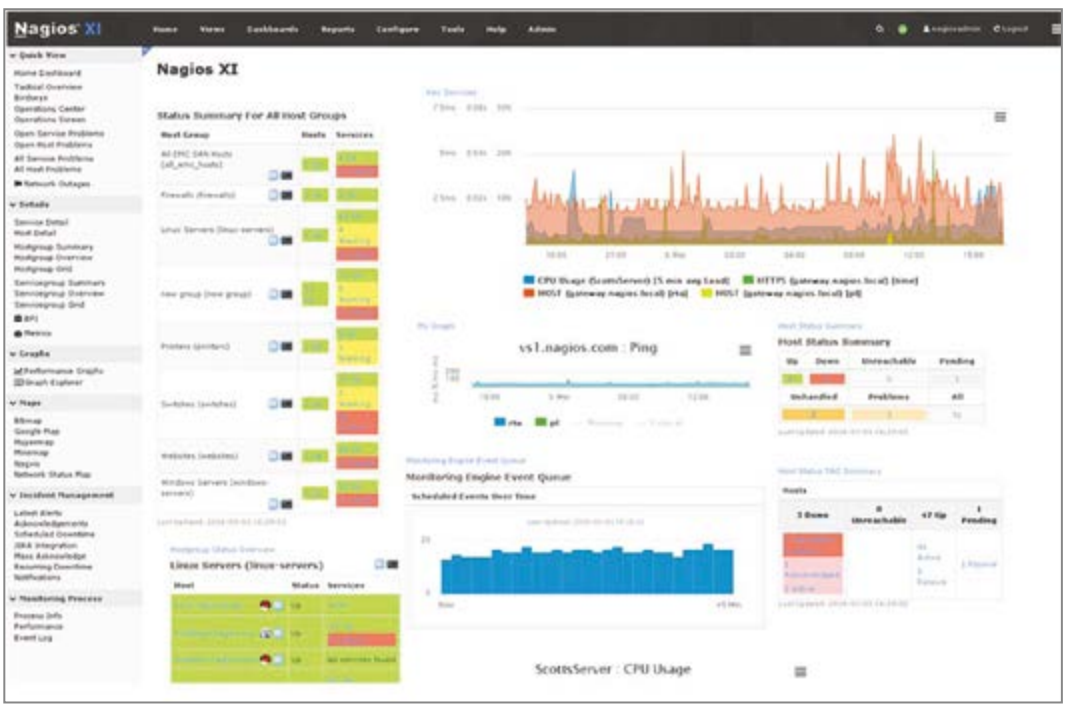

Figura 45 – *Dashboard* na interface do Nagios XI

Com o gerenciamento da capacidade no Nagios XI, é possível que as empresas programem seus *upgrades* a partir das tendências históricas da rede. Tal previsão é muito importante para as empresas que funcionam com base em orçamentos para os períodos seguintes. A figura a seguir retrata essa funcionalidade.

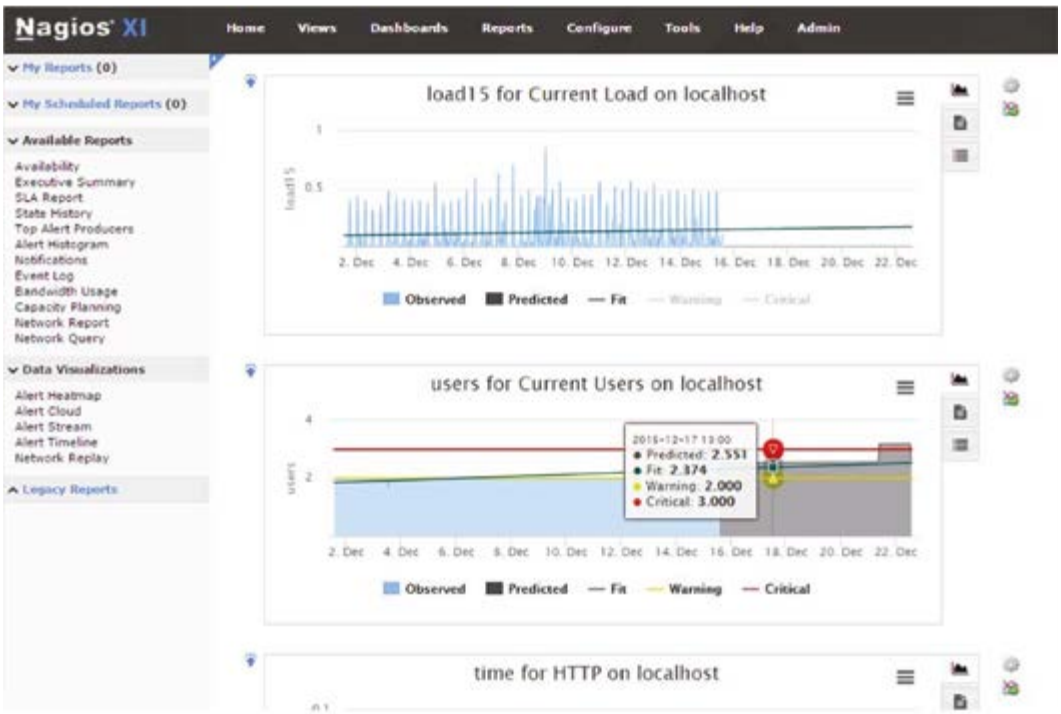

Figura 46 – Gerenciamento da capacidade do Nagios XI

Comparando-se as versões do Nagios Core com o Nagios XI, verifica-se que o Nagios Core possui basicamente as funções de monitoramento da infraestrutura e de alerta.

Já a ferramenta Nagios XI, além de todos os alertas de monitoramento da infraestrutura, do serviço de alertas por *e-mail*, telefone celular e métodos customizados, inseriu dois novos tipos de alerta: *feeds* RSS e notificações *per-user*. Além disso, o Nagios XI implementa relatórios, inclusive avançados, sobre o desempenho da rede, os níveis de serviço e o planejamento da capacidade, e também customiza a criação dos relatórios.

Em relação à interface com o usuário, o Nagios XI apresenta *dashboards*, customizações de usuários e sessões de autenticação. Ambas as versões suportam o monitoramento distribuído, mas somente a versão Nagios XI é capaz de enviar *traps*.

Por fim, somente a versão Nagios XI possui características de configuração através de interfaces, ferramentas de manutenção e mapas da rede.

Feature	Nagios XI	Nagios Core
Infrastructure Monitoring		
Servers	✓	✓
Network Elements	✓	✓
Applications	✓	✓
System Metrics	✓	✓
Custom Services	✓	✓
Alerting		
Email	✓	✓
Mobile Phone	✓	✓
Custom Method	✓	✓
RSS Feed	✓	
Per-User Notifications	✓	
Reporting		
Basic Reports	✓	✓
Advanced Reports	✓	
CSV and PDF Export	✓	
Performance Graphs	✓	
SLA Reports	✓	
Scheduled Reporting	✓	
Capacity Planning	✓	
Custom Report Creation	✓	
User Interface		
User-Specific Customization	✓	
Advanced Dashboards	✓	
Session Authentication	✓	
Instant Remote Host Access	✓	
Custom Actions	✓	
Sharable/Deployable Dashboards	✓	
Custom Branded Interface Capabilities	✓	
Distributed Monitoring		
Basic Capabilities	✓	✓
Advanced Capabilities	✓	
Supported Plugins	3000+	3000+
Send & Receive SNMP Traps	✓	
Third-Party Ticketing/Solution Integration	✓	
Configuration		
Web Configuration Interface	✓	
Bulk Host Cloning & Modification Tool	✓	
Configuration Snap-Shot Archive	✓	
Configuration Wizards	✓	
Auto-Discovery & Auto-Decommissioning	✓	
Mass Acknowledgment Tool	✓	
Recurring Downtime	✓	
Maintenance Tools		
Automated Back-Up Sidedoor	✓	
Upgrade Via Web Interface	✓	
Help System Functionality	✓	
Network Maps		
Basic Map	✓	✓
Google Maps Integration	✓	
Custom Maps with Nagvis	✓	
Network Replay	✓	
Database Backend	✓	
Multi Tenant Capabilities	✓	✓
Customizable	✓	✓
Distributed Monitoring Capabilities	✓	✓
Extendable Architecture	✓	✓
Proven OSS Core	✓	✓
Professional Support Options	✓	✓
Easy Integration With Other Nagios Solutions	✓	

Figura 47 – Comparação entre Nagios XI e Nagios Core

8.2 WhatsUp Gold

O WhatsUp Gold é um *software* que permite um monitoramento da rede inteira de forma bastante fácil em relação a outros *softwares* comerciais.

Com ele, é possível obter rapidamente o valor dos abrangentes recursos de detecção e monitoramento. A poderosa descoberta de camada 2/3 do WhatsUp Gold resulta em um detalhado mapa interativo dos principais dispositivos de rede, servidores, recursos virtuais e sem fio. Com uma única licença, é possível monitorar quaisquer combinações de redes, servidores, máquinas virtuais, aplicativos, fluxos de tráfego e configurações em ambientes Windows, Lamp e Java.

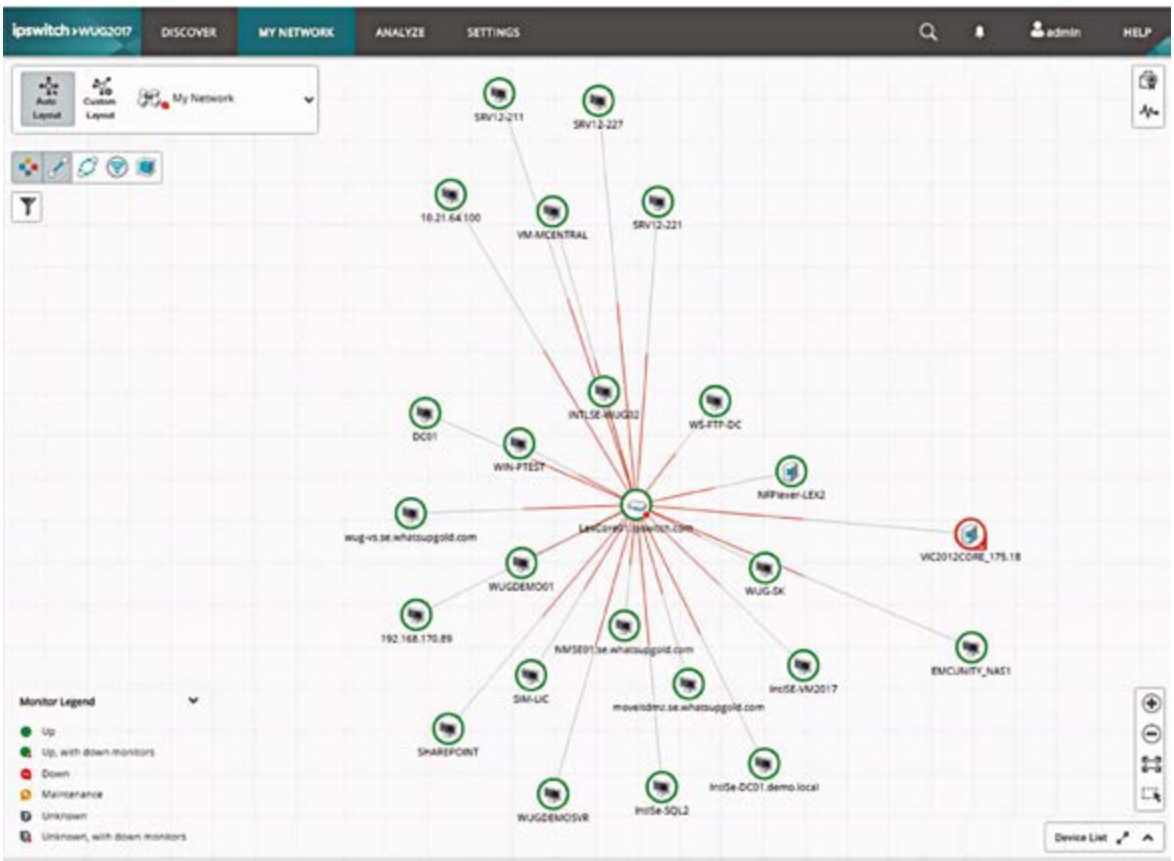

Figura 48 – Mapa da rede obtido pela ferramenta WhatsUp

Uma das vantagens dessa ferramenta é a criação de alertas proativos e visibilidade instantânea. Adicionalmente, pode garantir o mais alto nível de desempenho e disponibilidade para atender ou superar níveis de serviço. Esta ferramenta permite gerenciar redes, tráfegos, servidores físicos, máquinas virtuais (VMs) e aplicativos com mapas, *dashboards* e alertas personalizáveis fáceis de usar. Igualmente, ao clicar em qualquer dispositivo, obtém-se acesso imediato a uma grande variedade de relatórios e configurações de monitoramento.

8.3 HPE Network Node Manager i

O primeiro *software* para gerenciamento de redes lançado pela HP foi o HP OpenView. Em 2007, houve uma mudança, não sendo mais utilizada a marca HP Open View. Desse modo, passou-se a utilizar a marca HPE para a divisão de *software*.

O *software* HPE Network Node Manager i (NNMi) permite a utilização de ferramentas para gerenciar física e virtualmente redes de grande escala. Os módulos de *plugins* expandem o conhecimento do NNMi sobre o ambiente específico da rede, possibilitando que sejam passadas as informações necessárias para identificar e corrigir problemas mais rapidamente.

Como a complexidade da rede é crescente, o *software* de gerenciamento precisa possuir formas para a navegação sobre a rede, mostrando os elementos e as métricas de interesse.

Com essa finalidade, o NNMi implementou *workspaces* e *dashboards*. Os *workspaces* mostram grupos de elementos gerenciados e têm um propósito bem definido. Já os *dashboards* fornecem um fluxo de informação guiado através de um problema e pelos elementos gerenciados. A figura a seguir mostra um exemplo de *dashboard* do NNMi.

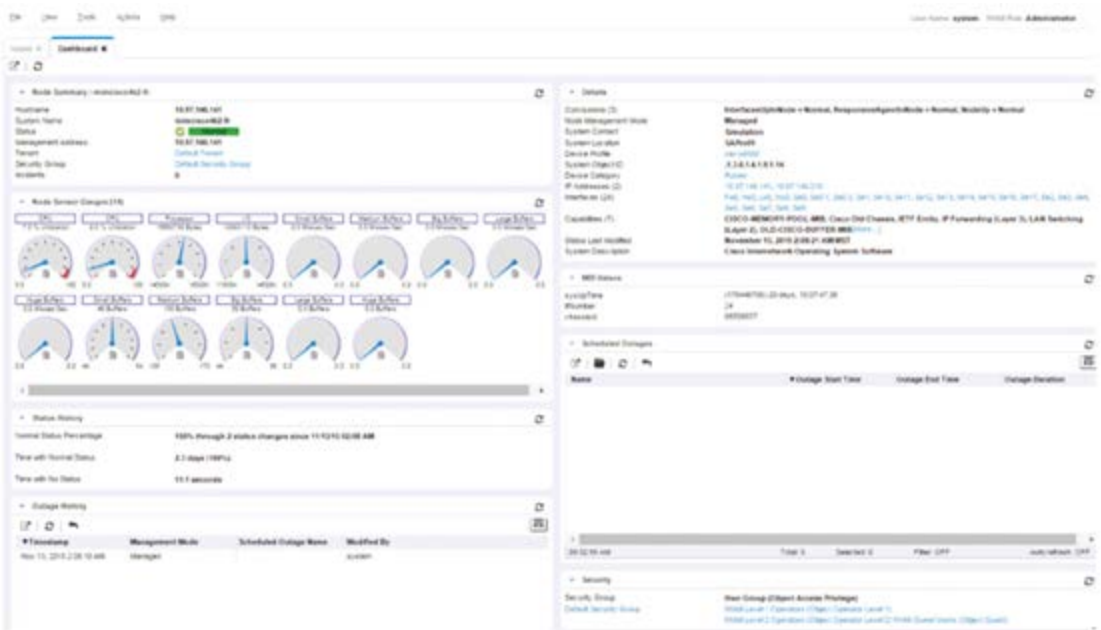

Figura 49 – *Dashboard* do *software* HPE NNMi

Observação

Em 2017, a Micro Focus se fundiu com a HPE, divisão de *software* da HP, criando uma das maiores empresas de *software* do mundo.

8.4 CA NetMaster Network Management for TCP/IP

A empresa Computer Associates desenvolveu a ferramenta NetMaster Network Management for TCP/IP, capaz de gerenciar proativamente as aplicações de *mainframes*. Essa solução automatiza o gerenciamento e o monitoramento da infraestrutura da rede, de equipamentos, eventos e conexões, para proporcionar alta disponibilidade e *performance* para aplicações *mainframe* baseadas na arquitetura TCP/IP.

Uma das características desse *software* é a chamada SmartTrace Network Tracing, uma função em tempo real de traçado para verificar o *status* temporal das conexões da rede. O NetMaster coleta estatísticas detalhadas para todos os recursos monitorados. Além disso, com o histórico de dados armazenado, é possível identificar rapidamente as causas de eventos passados ou consertar erros e anomalias da *performance* da rede.

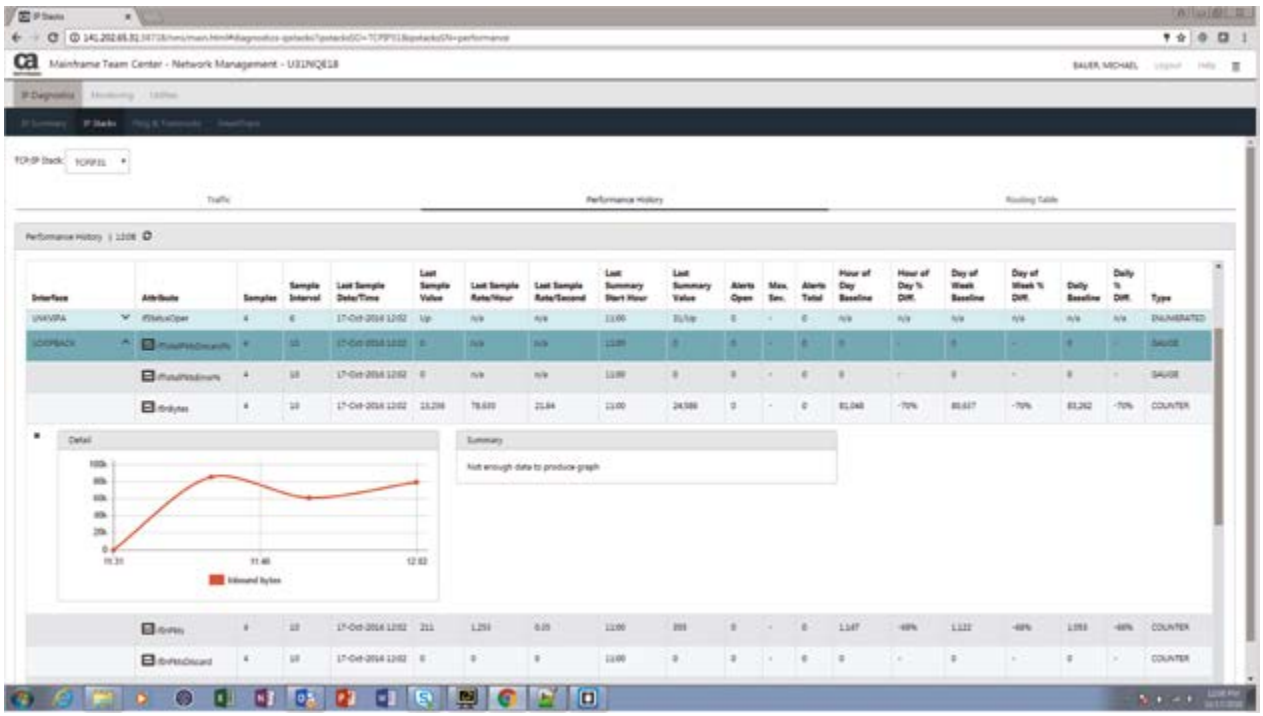

Figura 50 – Estatísticas e gráficos da ferramenta CA NetMaster

8.5 Pandora FMS

O Pandora FMS (Flexible Monitoring System) é um *software* de monitoramento de rede que é mantido pela empresa espanhola Ártica Soluciones Tecnológicas.

O projeto desse *software* foi iniciado em 2003, inicialmente como um *open source* na sua totalidade. Entretanto, com o passar do tempo, empresas privadas passaram a se interessar pelo projeto. Com base nesse fato, foi incluída uma visão mais corporativa na ferramenta para atender requisitos que não eram observados no projeto inicial.

Assim, desde 2005, a Ártica disponibiliza duas versões do Pandora FMS: *open source* e *enterprise*.

Saiba mais

O Pandora FMS disponibiliza uma apostila comparando as versões *open source* e *enterprise*:

<https://pandorafms.com/downloads/funcionalidades-EN.pdf>.

O Pandora FMS é uma ferramenta desenvolvida para atender ambientes de todos os portes, inclusive ambientes com grande quantidade de dispositivos a gerenciar. A arquitetura é formada basicamente por quatro componentes principais: servidores Pandora FMS, console *web*, banco de dados e agente de *software*.

Os servidores são os componentes que farão testes, validações e notificações e determinarão as ações a serem executadas. As ações que ocorrem nos servidores são, por exemplo, geração de alarmes e notificações pelos meios determinados, coletas e interações com os dispositivos gerenciados. Existem servidores de dados, de redes, SNMP, WMI, de reconhecimento, de complemento ou *plugins*, de predição, de testes *web* (goliat), de exportação, de inventário, de dependência e servidores *enterprise* da rede SNMP e ICMP.

O console *web* refere-se à interface com os usuários, na qual é realizada toda a administração de usuários, privilégios de acesso e dispositivos, além de outras atividades administrativas. No banco de dados da plataforma FMS, são mantidos os dados recebidos pelos servidores, sendo utilizado o MySQL como sistema de gerenciamento de banco de dados.

Já o agente Pandora FMS é opcional e é suportado por alguns sistemas operacionais. Este agente possui o propósito de atuar sobre o dispositivo gerenciado, e é responsável pelo envio de informações no padrão XML (eXtensible Markup Language) para o servidor FMS.

Lembrete

Algumas ferramentas que iniciaram como *open source* tiveram impactos tão positivos que posteriormente surgiram versões comerciais delas, as quais tinham muito mais recursos gráficos e funcionalidades, além de documentação mais ampla. São exemplos as ferramentas Nagios XI e Pandora FMS.

8.6 IBM Netcool Network Management

O IBM Netcool Network Management coopera com o time do *datacenter* e de rede para descobrir, visualizar, detectar, configurar, ativar, integrar e remediar a rede. A solução única combina o IBM Tivoli Netcool/OMNIbus, o IBM Tivoli Network Manager e o IBM Tivoli Netcool Configuration Manager.

Com essa ferramenta, esperam-se a redução das indisponibilidades, a automatização, a visibilidade e o controle sobre a rede

Alguns dos recursos do Netcool Network Management são um conjunto integrado de ferramentas que fornece descoberta, monitoramento, gerenciamento de eventos e configuração de rede. Além disso, a descoberta e o monitoramento de rede podem melhorar a disponibilidade e a eficiência desta. Os relatórios estão centralizados e abrangem todos os ambientes complexos e dispersos da rede. Com o gerenciamento de evento e falha é possível analisar problemas da rede e, muitas vezes, resolvê-los rapidamente. Por fim, com os recursos de configuração, é possível suportar a implementação e o gerenciamento de mudanças.

Ao analisar um conjunto integrado de gerenciamento de rede, é necessário que a ferramenta forneça o monitoramento centralizado, quase em tempo real, de redes complexas e domínios de tecnologia com escalabilidade que pode exceder milhões de eventos por dia. Também deve ser responsável pela coleta de dados de rede a partir de aplicativos de negócios, protocolos da internet, dispositivos de rede, dispositivos de segurança e outros geradores de dados para o gerenciamento centralizado.

Em relação à visibilidade e aos relatórios centralizados, o Netcool apresenta um portal *web* no qual agrega diversas informações de gerenciamento e monitoramento. Os relatórios de gerenciamento possuem informações de eventos entre domínios, dispositivos de rede e fornecedores.

O Netcool ainda permite a descoberta e o monitoramento de rede: entrega informações de conectividade, desempenho, disponibilidade e inventário da rede e também gera mapas dela, atualizando-os automaticamente caso ocorra alguma mudança. Adicionalmente, identifica gargalos da rede e outros problemas a fim de evitar indisponibilidades.

Em gerenciamento de falha e evento, o Netcool realiza diagnósticos automáticos e analisa as causas na busca de melhorias de disponibilidade e desempenho, além de permitir a correlação, o isolamento e a resolução automatizada de eventos, identificando e resolvendo problemas sem intervenção manual.

Em relação a recursos de configuração de redes, a ferramenta automatiza a configuração e o gerenciamento de dispositivos de rede para serviços baseados em nuvem. Também possibilita que os administradores visualizem dados de mudança na configuração, para que estes estejam informados sobre alterações na rede. A ferramenta ainda auxilia no gerenciamento de um amplo rol de protocolos, sistemas, aplicativos de negócios, dispositivos de rede e de segurança.

Resumo

Nesta unidade vimos que existem diversas ferramentas de monitoramento baseadas em licenças públicas (GPL), as quais são distribuídas de forma gratuita.

Uma das formas de expansão dessas ferramentas foi por meio de comunidades, que muitas vezes permitem criar *plugins* com novas funcionalidades para as ferramentas.

São exemplos desses tipos de ferramenta: Squid, Squid Guard, Squid Guard Manager, Zabbix, Nagios Core e Pandora FMS, as quais foram aqui apresentadas.

Vimos, entretanto, que essas ferramentas não possuem as interfaces mais amigáveis para o usuário e que a configuração delas não é nada trivial, sendo necessário um amplo conhecimento técnico para conseguir operá-las.

Como as ferramentas gratuitas não atendiam todas as necessidades do público empresarial, diversas empresas de *software*, como HP, IBM e Computer Associates (CA), criaram soluções de gerenciamento de redes para as quais é cobrada uma licença de uso. A partir disso, foram oferecidos serviços e suporte aos usuários, bem como interfaces mais amigáveis e intuitivas.

Neste material foram analisadas algumas ferramentas de gerenciamento comerciais: Nagios XI; WhatsUp Gold; HPE Network Node Monitor i; CA NetMaster Network Management for TCP/IP; Pandora FMS; IBM Netcool Network Management.

A fim de descobrir qual ferramenta é a mais adequada para uma determinada rede, deve-se avaliar cada situação específica, analisando-se os sistemas operacionais envolvidos, os objetivos do monitoramento, as funções de monitoramento que devem ser suportadas, as ações que o monitoramento deve tomar, os equipamentos de rede envolvidos e o custo dessa operação.

Nesse sentido, vimos que não é possível determinar qual a melhor ferramenta de gerenciamento de rede, pois isso depende de muitos fatores, como a própria rede que será gerenciada, os usuários do sistema e os objetivos do gerenciamento. Além disso, as ferramentas de gerenciamento de redes estão em constante evolução, aspecto fundamental a que o usuário deve se atentar.

Exercícios

Questão 1. (HUGG/UNIRIO 2016) Assinale a alternativa correta.

Popular aplicação de monitoramento de rede de código aberto distribuída sob a licença GPL. Ele pode monitorar tanto *hosts* quanto serviços, alertando quando ocorrerem problemas e também quando os problemas são resolvidos:

A) Audacity.

B) Azureus.

C) Eclipse.

D) Nagios.

E) LaTeX.

Resposta correta: alternativa D.

Análise das alternativas

A) Alternativa incorreta.

Justificativa: audacity é um programa de gravação e edição de áudio.

B) Alternativa incorreta.

Justificativa: a grafia correta é Azure. É a plataforma de computação em nuvem da Microsoft.

C) Alternativa incorreta.

Justificativa: eclipse é uma IDE (ambiente de desenvolvimento integrado). Tem sido muito utilizada para desenvolver *softwares* JAVA.

D) Alternativa correta.

Justificativa: é uma ferramenta de monitoramento de rede de código aberto. Nagios é uma popular aplicação de monitoramento de rede de código aberto distribuída sob a licença GPL. Ele pode monitorar tanto *hosts* quanto serviços, alertando quando ocorrerem problemas e também quando os problemas são resolvidos.

O Nagios foi originalmente criado sob o nome de Netsaint, foi escrito e é atualmente mantido por Ethan Galstad, junto com uma equipe de desenvolvedores que ativamente mantém *plugins* oficiais e não oficiais.

Nagios primeiramente foi escrito para o sistema operacional Linux, mas pode rodar em outros Unix-like também.

E) Alternativa incorreta.

Justificativa: LaTeX é um conjunto de macros para o programa de diagramação de textos TeX, muito usado na produção de textos matemáticos.

Questão 2. (TRT/24ª REGIÃO 2017) Um Analista, ao consultar a documentação do Zabbix Appliance (3.0.0) para o sistema operacional Linux (Ubuntu 14.04.3), obteve as informações a seguir.

O Zabbix Appliance utiliza-se do IPTables com as seguintes regras configuradas:

- Portas abertas
- SSH (22 TCP)
- Zabbixagent (10050 TCP) e Zabbixtrapper (10051 TCP)
- HTTP (80 TCP) e HTTPS (443 TCP)
- SNMP trap (162 UDP)
- Consultas NTP liberadas (53 UDP)
- Pacotes ICMP limitados a 5 por segundo
- Qualquer situação diferente sendo bloqueada

Considerando os fundamentos de redes de computadores e as informações acima é correto afirmar:

A) O Zabbix é uma ferramenta de monitoramento de redes, servidores e serviços que não permite monitoramento *agentless* (sem agentes).

B) Como o servidor Zabbix é obrigatoriamente instalado em sistemas Unix ou Linux, não há agentes Zabbix disponíveis para ambientes Windows e OS.

C) O ICMP, assim como o TCP e o UDP, é um protocolo de controle também usado para a transmissão de dados, que desempenha diversas funções exclusivas para Linux como o *ping*, para verificar se uma determinada máquina está *on-line*.

D) No SNMP o item a ser monitorado ou gerenciado é um agente. Quem consulta (GET) ou solicita modificações (SET) é um gerente. O agente também tem a função de gerar alertas (TRAP).

E) Dentre as regras do IPTables para configurar o firewall pode-se utilizar o parâmetro "-s ALL", que se aplica simultaneamente aos três protocolos (SSH, HTTP e HTTPS), sem que seja necessário incluir uma regra separada para cada um.

Resolução desta questão na plataforma.

FIGURAS E ILUSTRAÇÕES

Figura 1

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013. p. 576. Adaptada.

Figura 2

FERRETO, T. *Gerência de redes*. [s. d.]. p. 36. Disponível em: <http://www.inf.pucrs.br/~benso/gerencia_redes/2007/mat_tiago/introgerredes.pdf>. Acesso em: 1 nov. 2017.

Figura 3

FERRETO, T. *Gerência de redes*. [s. d.]. p. 39. Disponível em: <http://www.inf.pucrs.br/~benso/gerencia_redes/2007/mat_tiago/introgerredes.pdf>. Acesso em: 1 nov. 2017.

Figura 4

FERRETO, T. *Gerência de redes*. [s. d.]. p. 41. Disponível em: <http://www.inf.pucrs.br/~benso/gerencia_redes/2007/mat_tiago/introgerredes.pdf>. Acesso em: 1 nov. 2017.

Figura 5

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013. p. 573.

Figura 7

OLIVEIRA, F. S. G. *Gerenciamento de redes de computadores com o uso do raciocínio baseado em casos e ferramentas auxiliares*. 2007. Tese (Doutorado em Ciências em Engenharia Civil). Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2007. p. 5. Disponível em: <http://www.coc.ufrj.br/index.php?option=com_docman&task=doc_details&gid=886>. Acesso em: 9 nov. 2017.

Figura 13

SPECIALSKI, E. S. S. *Gerência de redes de computadores e telecomunicações*. [s. d.]. p. 44. Disponível em: <http://cassio.orgfree.com/disciplinas/gredes/ApostilaGerenciamento.pdf>. Acesso: 9 nov. 2017.

Figura 14

SPECIALSKI, E. S. S. *Gerência de redes de computadores e telecomunicações*. [s. d.]. p. 45. Disponível em: <http://cassio.orgfree.com/disciplinas/gredes/ApostilaGerenciamento.pdf>. Acesso: 9 nov. 2017.

Figura 15

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013. p. 698.

Figura 17

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013. p. 699.

Figura 18

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013. p. 703.

Figura 19

LOPES, R. *Melhores práticas para gerência de redes de computadores*. São Paulo: Editora Campus, 2003. p. 18.

Figura 20

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013. p. 702.

Figura 22

SPECIALSKI, E. S. S. *Gerência de redes de computadores e telecomunicações*. [s. d.]. p. 31. Disponível em: <http://cassio.orgfree.com/disciplinas/gredes/ApostilaGerenciamento.pdf>. Acesso: 9 nov. 2017.

Figura 23

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013. p. 710.

Figura 24

SOUZA, J. S. de. *Software livre no gerenciamento de redes*: solução eficiente e de baixo custo numa empresa alfa do polo industrial. 2015. Dissertação (Mestrado em Engenharia de Processos). Universidade Federal do Pará, Belém, 2015. p. 22. Disponível em: <http://ppgep.propesp.ufpa.br/ARQUIVOS/dissertacoes/Dissertacao2015-PPGEP-MP-JanainaSilvadeSouza.pdf>. Acesso em: 9 nov. 2017.

Figura 25

AMARAL, F. K. do; WESZ, R.; JUCHEM, M. *WMI*: instrumentação e gerenciamento em ambientes distribuídos. Porto Alegre: Pontifícia Universidade Católica do Rio Grande do Sul, 2007. p. 3. Disponível em: <http://www.inf.pucrs.br/~gustavo/disciplinas/sd/material/Artigo_WMI.pdf>. Acesso em: 9 nov. 2017.

Figura 26

CISCO. *Introduction to Cisco IOS NetFlow*. [s. d.]. p. 3. Disponível em: <https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.pdf>. Acesso em: 9 nov. 2017.

Figura 27

OVERVIEW.GIF. Disponível em: <http://nfdump.sourceforge.net/overview.gif>. Acesso em: 9 nov. 2017.

Figura 31

PS_NETWORK_TRAFFIC.PNG. Disponível em: <https://oss.oetiker.ch/rrdtool/gallery/PS_Network_traffic.png>. Acesso em: 9 nov. 2017.

Figura 33

PUB/GRAPHS/CMS-WEB-MINI-GRAPH.CGI?TYPE=PNG;TARGET=%2FOVERVIEW%2FGEANT-TOT;INST=0;DSLIST=IFINOCTETS%2CIFOUTOCTETS;RANGE=151200;RAND=595. Disponível em: <https://traffic.lan.switch.ch/pub/graphs/cms-web-mini-graph.cgi?type=png;target=%2FOverview%2Fgeant-tot;inst=0;dslist=ifInOctets%2CifOutOctets;range=151200;rand=595>. Acesso em: 9 nov. 2017.

Figura 34

GRAPHS/CMS-WEB-MINI-GRAPH.CGI?TYPE=PNG;TARGET=%2FOVERVIEW%2FGEANT-TOT;INST=0;DSLIST=IFINOCTETS%2CIFOUTOCTETS;RANGE=864000;RAND=771. Disponível em: <https://traffic.lan.switch.ch/pub/graphs/cms-web-mini-graph.cgi?type=png;target=%2FOverview%2Fgeant-tot;inst=0;dslist=ifInOctets%2CifOutOctets;range=864000;rand=771>. Acesso em: 9 nov. 2017.

Figura 35

GRAPHS/CMS-WEB-MINI-GRAPH.CGI?TYPE=PNG;TARGET=%2FOVERVIEW%2FGEANT-TOT;INST=0;DSLIST=IFINOCTETS%2CIFOUTOCTETS;RANGE=3628800;RAND=609. Disponível em: <https://traffic.lan.switch.ch/pub/graphs/cms-web-mini-graph.cgi?type=png;target=%2FOverview%2Fgeant-tot;inst=0;dslist=ifInOctets%2CifOutOctets;range=3628800;rand=609>. Acesso em: 9 nov. 2017.

Figura 36

CMS-WEB-MINI-GRAPH.CGI?TYPE=PNG;TARGET=%2FOVERVIEW%2FGEANT-TOT;INST=0;DSLIST=IFIN OCTETS%2CIFOUTOCTETS;RANGE=41472000;RAND=909. Disponível em: <https://traffic.lan.switch.ch/pub/graphs/cms-web-mini-graph.cgi?type=png;target=%2FOverview%2Fgeant-tot;inst=0;dslist=ifInOctets%2CifOutOctets;range=41472000;rand=909>. Acesso em: 9 nov. 2017.

Figura 47

NAGIOS-XI-VS-NAGIOS-CORE-FEATURE-COMPARISON.PDF. Disponível em: <https://assets.nagios.com/handouts/nagiosxi/Nagios-XI-vs-Nagios-Core-Feature-Comparison.pdf>. Acesso em: 9 nov. 2017.

REFERÊNCIAS

Textuais

AMARAL, F. K. do; WESZ, R.; JUCHEM, M. *WMI*: instrumentação e gerenciamento em ambientes distribuídos. Porto Alegre: Pontifícia Universidade Católica do Rio Grande do Sul, 2007. Disponível em: <http://www.inf.pucrs.br/~gustavo/disciplinas/sd/material/Artigo_WMI.pdf>. Acesso em: 9 nov. 2017.

BURGESS, M. *Princípios de administração de redes e sistema*. 2. ed. Rio de Janeiro: LTC, 2006.

CARVALHO, T. C. M. de B. (Org.). *Gerenciamento de redes*: uma abordagem de sistemas abertos. São Paulo: Makron Books, 1993.

FLORIANO, W. D. *Gerenciamento do proxy squid através de uma ferramenta web com base na criação de perfis de controle*. 2016. Trabalho de Conclusão de Curso (Tecnólogo em Redes de Computadores). Universidade Federal de Santa Maria, Santa Maria, 2016. Disponível em: <http://www.redes.ufsm.br/docs/tccs/Willian-Floriano.pdf>. Acesso em: 9 nov. 2017.

FOROUZAN, B. A.; MOSHARRAF, F. *Redes de computadores*: uma abordagem *top-down*. Porto Alegre: AMGH, 2013.

HARNEDY, S. *Total SNMP*: exploring the Simple Network Management Protocol. New Jersey: Prentice Hall, 1997.

ISO. *ISO/IEC DIS 10040*: information technology/open systems interconnection/systems management overview. 1998. Disponível em: <https://www.iso.org/standard/24406.html>. Acesso em: 9 nov. 2017.

KLEINSCHMIDT, J. H. *Gerenciamento e interoperabilidade de redes*: ferramentas de gerenciamento de redes. 2017. Disponível em: <http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/ger2017/ferramentas.pdf>. Acesso em: 9 nov. 2017.

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013.

LOPES, R. *Melhores práticas para gerência de redes de computadores*. São Paulo: Editora Campus, 2003.

MAURO, D.; SCHMIDT, K. *Essential SNMP*: help for system and network administrators. 2. ed. Sebastopol: O´Reilly, 2005.

NAKAMURA, T. J.; SANTOS, R. R. dos. *Minicurso de gerenciamento de redes*. São Paulo: Ceptro.br, 2015. Disponível em: <forumdainternet.cgi.br/files/MiniCursoGerenciamentoRedes.pdf>. Acesso em: 9 nov. 2017.

OLIVEIRA, F. S. G. *Gerenciamento de redes de computadores com o uso do raciocínio baseado em casos e ferramentas auxiliares*. 2007. Tese (Doutorado em Ciências em Engenharia Civil). Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2007. Disponível em: <http://www.coc.ufrj.br/index.php?option=com_docman&task=doc_details&gid=886>. Acesso em: 9 nov. 2017.

SOUSA, L. B. de. *Administração de redes locais*. São Paulo: Editora Érica, 2014.

SOUZA, J. S. de. *Software livre no gerenciamento de redes*: solução eficiente e de baixo custo numa empresa alfa do polo industrial. 2015. Dissertação (Mestrado em Engenharia de Processos). Universidade Federal do Pará, Belém, 2015. Disponível em: <http://ppgep.propesp.ufpa.br/ARQUIVOS/dissertacoes/Dissertacao2015-PPGEP-MP-JanainaSilvadeSouza.pdf>. Acesso em: 9 nov. 2017.

VEEAM. *Veeam Availability Report 2017*. Disponível em: <https://www.veeam.com/br/2017_availability_report_wpp.pdf >. Acesso em: 9 nov. 2017.

Sites

<https://www.cacti.net/>.

<hpe.com/software/nnmi>.

<http://iptrack.sourceforge.net/>.

<https://www.ibm.com/br-pt/?lnk=m>.

<https://oss.oetiker.ch/mrtg/>.

<https://oss.oetiker.ch/rrdtool/index.en.html>.

<http://www.squid-cache.org/>.

<http://www.nagios.org/>.

<http://www.zabbix.org/>.

<http://www.wireshark.org>.

Exercícios

Unidade I – Questão 1: CONSELHO FEDERAL DE PSICOLOGIA (CFP). *Concurso Público nº 01/2015 Analista Técnico*: Conhecimentos Específicos. Questão 34.

Unidade I – Questão 2: DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO. *Concurso Público 2013 Oficial de Defensoria Pública*: Noções de Informática. Questão 34.

Unidade II – Questão 1: CENTRO DE SELEÇÃO E PROMOÇÃO DE EVENTOS (CESPE). Tribunal Regional Eleitoral do Rio Grande do Sul (TRE-RS). *Concurso Público 2015 Analista Judiciário*: Conhecimentos Específicos. Questão 41.

Unidade II – Questão 2: DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO. *Concurso Público 2015 Agente de Defensoria Pública*: Conhecimentos Específicos. Questão 56.

Unidade III – Questão 1: TRIBUNAL REGIONAL ELEITORAL DE RORAIMA (TRE-RR). *Concurso Público 2015 Analista Judiciário*: Conhecimentos Específicos. Questão 47.

Unidade III – Questão 2: UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ). *Concurso Público 2012 Engenheiro de Telecomunicações*: Questões Específicas. Questão 50.

Unidade IV – Questão 1: HOSPITAL UNIVERSITÁRIO GAFFRÉE GUINLE DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (HUGG/UNIRIO). *Concurso Público Analista de Tecnologia da Informação 2016*: Conhecimentos Específicos. Questão 37.

Unidade IV – Questão 2: TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO (TRT/24ª REGIÃO). *Concurso Público Analista Judiciário 2017*: Conhecimentos Específicos. Questão 49.

Interativa

Informações:
www.sepi.unip.br ou 0800 010 9000