SENAI

SÉRIE TECNOLOGIA DA INFORMAÇÃO - *HARDWARE*

GERENCIAMENTO E MONITORAMENTO DE REDE

SENAI

Iniciativa da CNI - Confederação Nacional da Indústria

SÉRIE TECNOLOGIA DA INFORMAÇÃO - *HARDWARE*

GERENCIAMENTO E MONITORAMENTO DE REDE

SENAI

Iniciativa da CNI - Confederação Nacional da Indústria

SÉRIE TECNOLOGIA DA INFORMAÇÃO - *HARDWARE*

GERENCIAMENTO E MONITORAMENTO DE REDE

Esta publicação foi elaborada pela equipe do Núcleo de Educação a Distância do SENAI de Santa Catarina, com a coordenação do SENAI Departamento Nacional, para ser utilizada por todos os Departamentos Regionais do SENAI nos cursos presenciais e a distância.

SENAI Departamento Nacional
Unidade de Educação Profissional e Tecnológica – UNIEP

SENAI Departamento Regional de Santa Catarina
Núcleo de Educação – NED

FICHA CATALOGRÁFICA

S491g

Serviço Nacional de Aprendizagem Industrial. Departamento Nacional.
Gerenciamento e monitoramento de rede / Serviço Nacional de Aprendizagem Industrial. Departamento Nacional, Serviço Nacional de Aprendizagem Industrial. Departamento Regional de Santa Catarina. Brasília : SENAI/DN, 2012.
97 p. il. (Série Tecnologia da informação - Hardware).

ISBN

1. Rede de computadores. 2. Protocolo simples de gerenciamento de redes (Protocolo de rede de computação). I. Serviço Nacional de Aprendizagem Industrial. Departamento Regional de Santa Catarina. II. Título. III. Série.

SENAI **Sede**

Serviço Nacional de Aprendizagem Industrial
Departamento Nacional

Setor Bancário Norte • Quadra 1 • Bloco C • Edifício Roberto Simonsen • 70040-903 • Brasília – DF • Tel.: (0xx61) 3317-9001 Fax: (0xx61) 3317-9190 • http://www.senai.br

Lista de Ilustrações

Sumário

Introdução

1

Prezado aluno, seja bem vindo à unidade curricular Gerenciamento e Monitoramento de Rede. Você, que está se preparando para administrar ou operar redes de computadores, grandes ou pequenas, complexas ou simples, muito provavelmente, terá como uma de suas responsabilidades o seu gerenciamento. Essa atividade consiste em buscar o controle dos componentes da rede e tornar a rede confiável, com os melhores índices de disponibilidade, desempenho e segurança possíveis. E para conseguir isso, é preciso utilizar a tecnologia a nosso favor.

Temos à disposição diferentes protocolos, criados especificamente para o gerenciamento de redes, e com o uso de ferramentas de gerenciamento e monitoramento podemos ter informações precisas, praticamente em tempo real, sobre tudo que está acontecendo nela. Essas informações são extremamente úteis para se evitar que um problema aconteça ou, caso não seja possível evitá-lo, que se reduza o seu impacto sobre o negócio. É bom lembrar que, os registros de problemas antigos e outras informações coletadas, podem orientar o administrador nos momentos de tomada de decisão, seja para a aquisição de novos equipamentos ou para a adesão a novas tecnologias.

Nesta unidade curricular vamos estudar o principal protocolo de gerenciamento de redes e conhecer as principais ferramentas disponíveis. Confira na matriz curricular os módulos e unidades curriculares previstos com as respectivas cargas horárias.

Técnico em Redes de Computadores

MÓDULOS	DENOMINAÇÃO	UNIDADES CURRICULARES	CARGA HORÁRIA	CARGA HORÁRIA DO MÓDULO
Básico	Básico	• Eletroeletrônica Aplicada	60h	340h
		• Montagem e Manutenção de Computadores	160h	
		• Ferramentas para Documentação Técnica	120h	
Específico I	Ativos de Rede	• Cabeamento Estruturado	108h	464h
		• Arquitetura de Redes	80h	
		• Comutação de Rede Local	120h	
		• Interconexão de Redes PR	96h	
		• Gerenciamento e Monitoramento de Rede	60h	
Específico II	Servidores de Rede	• Servidores de Rede	120h	396h
		• Serviços de Rede	120h	
		• Serviços de Convergência	60h	
		• Segurança de Redes	96h	

Quadro 1 - Matriz curricular
Fonte: SENAI DN

É hora de entrar no mundo dos serviços de redes e começar a trilhar os caminhos do conhecimento. Procure levar teoria e prática alinhados, contruindo o seu conhecimento e desenvolvimento profissional. Bons estudos!

Anotações:

O Surgimento das Redes e os Principais Modelos de Gerenciamento

2

As redes de computadores existem há muito tempo. No início, poucos tinham o privilégio de utilizá-las mas, nos dias de hoje, estamos constantemente conectados a elas. Nas organizações ela é praticamente indispensável. A maior das redes, a Internet, é utilizada por mais de dois bilhões de usuários no mundo, segundo a ITU[1],

Uma boa administração dos componentes que integram a rede é fundamental para que ela opere de forma adequada, independentemente do seu tamanho ou quantidade de usuários. O objetivo é alcançar os melhores índices de disponibilidade e desempenho possíveis.

Ao final deste capítulo você terá subsídios para:

a) conhecer um pouco sobre o surgimento das redes de computadores, os fatores que motivaram os esforços para torná-las realidade, os primeiros protocolos e modelos de gerenciamento.

2.1 A HISTÓRIA DAS REDES DE COMPUTADORES

A evolução tecnológica é impulsionada em grande parte por questões militares. Um dos primeiros computadores eletrônicos digitais criados foi o ENIAC[2], utilizado para realizar cálculos para a artilharia dos Estados Unidos.

Os meios de comunicação também têm a sua origem ligada a aspectos militares. A criação da ARPANET[3] pelo Departamento de Defesa dos Estados Unidos, na década de 1960, é um marco na história das redes de computadores. Considerada a mãe da Internet, inicialmente interligava apenas quatro computadores, utilizando enlaces de 56 Kbps (kilobits por segundo). Em pouco tempo interligava dezenas de universidades e órgãos do governo americano.

Na década de 1970, com o crescimento da ARPANET e com o surgimento de outras redes, o próximo passo foi possibilitar a conectividade entre estas, dando origem ao termo **Internet**. O NCP[4], utilizado na comutação dos pacotes até então, tornou-se inadequado. Os esforços para a criação de um protocolo mais robusto deram origem aos protocolos TCP[5], IP[6] e UDP[7]. Tais protocolos são utilizados nas redes internas e na Internet até os dias atuais.

Com o crescimento, vieram os problemas, principalmente relacionados à disponibilidade e ao desempenho. Era preciso desenvolver formas de monitorar as redes.

VOCÊ SABIA?

O Brasil está entre os cinco países com o maior número de usuários que acessam à Internet. São aproximadamente 76 milhões de usuários.

SAIBA MAIS

Para saber mais informações sobre a Internet no mundo, principalmente dados estatísticos, consulte os sites do ITU <http://www.itu.int> e do Index Mundi <http://www.indexmundi.com>, ambos em inglês.

Nessa etapa você conheceu um pouco da história do surgimento da maior rede do mundo. Na próxima etapa você conhecerá o modelo FCAPS. Curioso para saber o que é? Então, acompanhe!

[1] ITU

International Telecommunication Union – uma das agências especializadas da ONU (Organização das Nações Unidas). É destinada a padronizar e regular as ondas de rádio e telecomunicações internacionais.

[2] ENIAC

Electrical Numerical Integrator and Computer – primeiro computador digital eletrônico de grande escala, criado em 1946 por John Eckert e John Mauchly, da Eletronic Control Company.

[3] ARPANET

Advanced Research Projects Agency Network – primeira rede de computadores à base de comutação de pacotes.

[4] NCP

Network Control Protocol – primeiro protocolo de comunicação usado na ARPANET, criado em 1971 pela *Network Working Group*.

2.2 O MODELO FCAPS

A *International Organization for Standardization* (ISO), organização fundada em 1947, responsável pela normalização de normas técnicas, classificações e normas de procedimentos, foi uma das primeiras entidades a definir padrões para a conectividade entre computadores. A arquitetura proposta recebeu o nome de modelo OSI[8].

Dentre várias especificações, este modelo divide a gerência de redes em cinco áreas funcionais. Baseado nesses conceitos foi criado o modelo FCAPS. A sigla é formada pelas iniciais (em inglês) de cada uma das áreas funcionais, que são:

a) gerência de falhas (**F**ault);

b) gerência de configuração (**C**onfiguration);

c) gerência de contabilização (**A**ccounting);

d) gerência de desempenho (**P**erformance);

e) gerência de segurança (**S**ecurity).

Na área gerência de falhas, são tratados aspectos referentes à detecção de falhas, assim como o seu isolamento, a notificação, envio de alertas e a sua correção. Também trata da geração de relatórios, além da criação de processos de recuperação dos problemas.

A gerência de configuração é responsável pela documentação dos parâmetros de configuração da rede, seja de hardware ou software. Envolve tanto a análise das configurações como as modificações realizadas. Define também como estas informações serão armazenadas.

O gerenciamento de contabilização trata da administração dos recursos da rede, assim como a sua utilização por parte dos seus usuários. Engloba, também, o levantamento do custo envolvido, a geração de relatórios do uso, os mecanismos de tarifação do consumo e aplicação de cotas, a fim de prevenir a escassez dos recursos.

A gerência de desempenho é a área onde os itens de uma rede são monitorados, dentre eles: enlaces, equipamentos, protocolos e aplicações. Os relatórios gerados nesta área normalmente trazem medições com o histórico do comportamento de cada item da rede. Esses dados são utilizados, por exemplo, para verificar se o desempenho está em conformidade com o que foi acordado com os usuários. É muito útil na identificação de situações onde investimentos são necessários, normalmente ocasionados pelo aumento no uso dos recursos, seja pela implantação de novos sistemas ou pelo crescimento no número de usuários, entre outros.

Por fim, é na gerência de segurança que questões relacionadas às permissões de acesso e à proteção das informações são administradas. Essa área descreve o monitoramento e o armazenamento dos registros (*logs*) relacionados à segurança. Trata também das senhas e das chaves criptográficas. Uma das principais responsabilidades diz respeito à criação e manutenção da política de segurança da informação, e o cumprimento desta por parte dos usuários da rede.

Com base nestas áreas, é possível identificar os requisitos necessários para a avaliação ou desenvolvimento de ferramentas de gerenciamento de redes. Tais ferramentas precisam estar aptas a monitorar os mais diferentes tipos de redes. Para que isso seja possível, é preciso que estes sistemas e os recursos a serem gerenciados operem sobre um mesmo padrão de comunicação.

FIQUE ALERTA

Ao desenvolver ou implantar um sistema de gerenciamento, é desejável que este cubra as cinco áreas funcionais, ou a maioria delas.

Segundo Specialski, "gerenciamento de redes é como seguro contra incêndio: ninguém acha que precisa, senão, depois que já é tarde demais..." (1994, p.467)

Diversos outros modelos para o gerenciamento de redes foram criados, cada qual com a sua finalidade. Entre eles o *Telecommunications Management Network* (TMN), que é utilizado, principalmente, por operadoras de serviços de telecomunicação. Em redes de dados baseadas no protocolo TCP/IP, o modelo SNMP* é amplamente utilizado. Nos próximos capítulos, você acompanhará os detalhes por trás deste simples, mas eficiente protocolo de gerenciamento de redes. Verá também as principais ferramentas de gerenciamento que, dentre outras formas, utilizam o SNMP[9] para realizar o diagnóstico da rede.

Confira, a seguir, o relato de um exemplo, de como as redes contribuem para o aumento da produtividade.

[5] TCP

Transmission Control Protocol – protocolo da camada de transporte utilizado inicialmente na Internet e, atualmente, em praticamente todas as redes de computadores. É orientado à conexão, o que permite a realização de conexões confiáveis.

[6] IP

User Datagram Protocol - protocolo da camada de transporte utilizado na Internet para aplicações que exigem tempos de atraso mínimos. Não é orientado à conexão, o que não traz garantias sobre uma conexão.

[7] UDP

Disposição natural ou adquirida para qualquer coisa. Capacidade.

[8] OSI

Open Systems Interconnection – modelo criado pela ISO para a padronização da forma de conectar computadores em rede.

[9] SNMP

Simple Network Management Protocol - protocolo da pilha TCP/IP utilizado para o gerenciamento dos recursos nas redes de computadores.

CASOS E RELATOS

As contribuições da rede para o aumento da produtividade

Artiva era uma aluna dedicada, muito estudiosa, sempre gostou de ler, mas infelizmente morava longe da biblioteca municipal da sua cidade, então ela aproveitava para usar a biblioteca da sua escola. Infelizmente, não havia uma grande variedade de livros, jornais e revistas, oferecendo poucas opções de pesquisa para os alunos realizarem seus trabalhos escolares. Havia alguns computadores que os alunos utilizavam para digitar seus trabalhos, mas, como os computadores não estavam ligados em rede, os alunos precisavam salvar uma cópia do trabalho em um *pendrive* para poder imprimi-lo no único computador que possuía uma impressora conectada.

Sabendo da dificuldade que os alunos passavam, o diretor da escola tomou uma decisão, e chamou os alunos para comunicar que os computadores seriam ligados em rede e passariam a ter acesso à Internet. Todos adoraram a ideia, e passaram a utilizar a Internet como principal fonte de pesquisa, pois, agora, podiam consultar diferentes fontes, tendo acesso a informações do mundo todo e ainda se divertindo nas horas de folga. Outro benefício foi que os alunos não precisavam mais salvar seus trabalhos para imprimir em outro computador. Agora eles utilizavam a rede para isso. Mesmo não entendendo como funciona a rede, todos perceberam o quanto ela é importante e ajuda na produtividade.

RECAPITULANDO

Neste capítulo você pôde perceber que a evolução tecnológica normalmente é impulsionada por necessidades militares. Em tempos de guerra a tecnologia é uma aliada e, quanto mais avançada, mais decisiva se torna, porém, não é utilizada somente nessas situações. Hoje em dia, países como Estados Unidos e Japão são vistos como os grandes pólos tecnológicos, o que fortalece a indústria e o comércio. O fator militar foi o grande responsável pelo surgimento das redes e da Internet.

Você constatou também que, com o rápido surgimento e crescimento das redes, foi preciso criar técnicas para administrá-las. Para isso, diferentes órgãos passaram a desenvolver e avaliar propostas para a padronização nas comunicações. Graças a estes, é possível a compatibilidade entre equipamentos de diferentes fabricantes e diferentes tecnologias.

Conheça, no próximo capítulo, os protocolos responsáveis por monitorar e gerenciar redes.

Anotações:

Protocolo de Gerenciamento de Redes

3

Você já sabe como surgiram as redes. Sabe também que elas foram e são fundamentais para que, mesmo com o crescimento e a complexidade das redes, o administrador consiga gerenciar toda a estrutura de forma centralizada (ou não, se assim preferir). Os responsáveis pela coleta e envio dessas informações ao centro de monitoramento são os protocolos de gerenciamento.

Ao final deste capítulo você terá subsídios para:

a) conhecer as versões e o funcionamento do SNMP, um dos protocolos de gerenciamento de redes mais utilizados além do padrão RMON, utilizado no monitoramento remoto.

3.1 O PROTOCOLO SNMP E A MIB

Na década de 1980, devido à rápida expansão da Internet e migração para o TCP/IP, a IETF[1] deu início ao desenvolvimento do SNMP. A base para o seu desenvolvimento foi o modelo FCAPS. Para a sua padronização como protocolo, ele precisou ser descrito em uma RFC[2]. A primeira versão do SNMP foi descrita na RFC 1157, que contém toda a especificação do protocolo.

O SNMP segue o modelo cliente-servidor, onde os clientes são os equipamentos a serem gerenciados e o servidor é quem recebe as informações coletadas dos clientes. Tais informações estão estruturadas no que se convencionou chamar de árvore MIB (*Management Information Base*), ou seja, uma base de informações de gerenciamento. As especificações da MIB estão descritas na RFC 1066. As regras para a construção das estruturas da MIB, por sua vez, são descritas pela *Structure of Management Information* (SMI), que define os nomes associados aos objetos gerenciados e os respectivos tipos de dados mantidos por estes objetos. A SMI, por sua vez, segue as notações da ASN.1[3]. Posteriormente, foram propostas algumas melhorias na especificação da MIB. Tais melhorias estão descritas na RFC 1213, o que deu origem ao que conhecemos como MIB II.

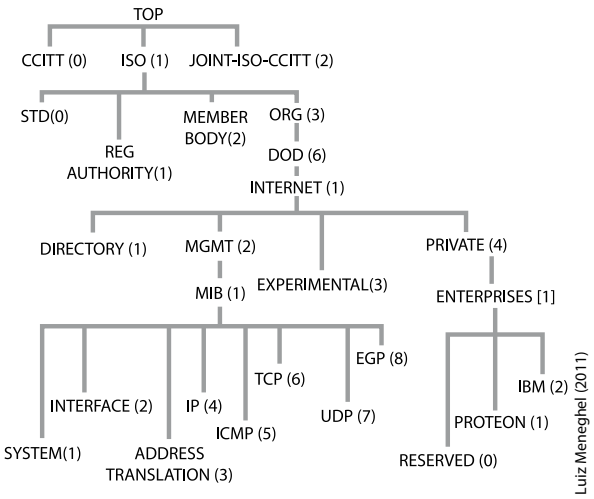


Figura 1 - Os objetos mais altos na hierarquia da MIB II
Fonte: Oracle (2011)

Conforme você pode ver na figura, cada objeto da MIB é identificado por um número, o seu *Object Identifier* (OID). Como estes estão dispostos de forma hierárquica, para termos acesso às informações de um objeto, devemos informar a sequência de números completa, ou seja, o caminho (numérico) completo sobre o seu posicionamento na hierarquia da MIB. Existem basicamente três tipos de MIB:

[1] IETF

Internet Engineering Task Force – comunidade internacional para o desenvolvimento da Internet. Preocupa-se em propor soluções e também com a padronização das tecnologias.

[2] RFC

Request for Comments - documento que descreve os padrões para os protocolos da Internet que são analisados e publicados pela IETF.

[3] ASN.1

Abstract Sintax Notation One – notação para a definição de tipos de dados complexos, assim como os seus possíveis valores.

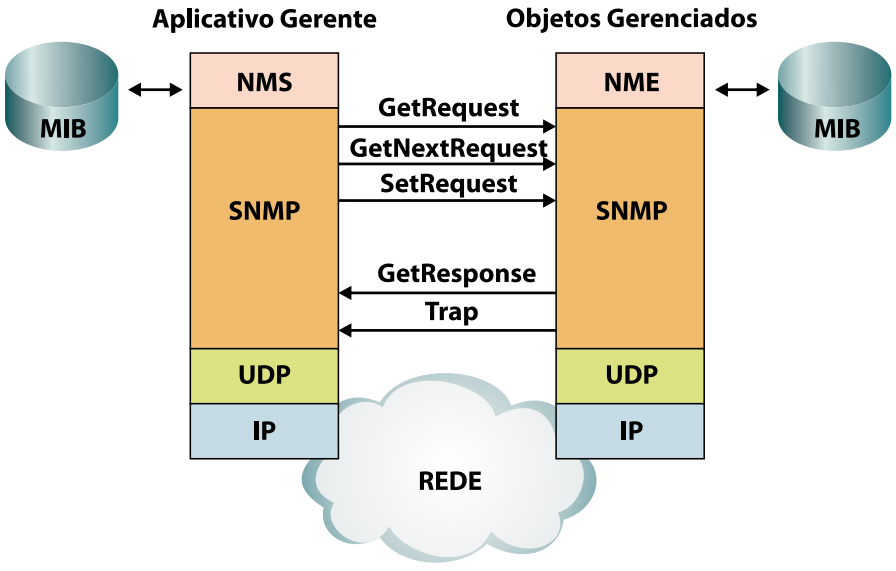
a) **MIB II** – contém as informações básicas sobre um equipamento, como o tempo que o equipamento está ligado, a quantidade de tráfego em suas interfaces de rede, o seu nome, etc.;

b) **MIB experimental** – uma subárvore utilizada para a realização de testes em objetos que estão sendo desenvolvidos;

c) **MIB privada** – uma subárvore que contém objetos específicos para um equipamento, ou seja, uma estrutura utilizada por fabricantes de equipamentos que desejam criar suas próprias hierarquias com diferentes informações.

Por exemplo, a fabricante de equipamentos de rede Cisco Systems possui uma MIB privada, sendo que o seu OID é o número nove. Para termos acesso às informações da sua MIB, o caminho até a sua MIB será o código .1.3.6.1.4.1.9, o que representa o caminho iso (1), org (3), dod (6), internet (1), private (4), enterprise (1) e cisco (9).

Como você pode observar, uma estrutura de gerenciamento TCP/IP é composta por quatro elementos básicos: o(s) servidor(s), ou *Network Management Stations* (NMS); os clientes, ou *Network Management Elements* (NMEs); a base de informações de gerenciamento, ou *Management Information Base* (MIB) e um protocolo de gerenciamento, o SNMP, responsável pela comunicação entre o servidor e os clientes. Para que as informações da MIB presentes nos clientes sejam enviadas ao servidor, os equipamentos precisam enviar mensagens uns aos outros. A figura a seguir mostra alguns tipos de mensagens trocadas entre os clientes e o servidor.



Luiz Meneghel (2011)

Figura 2 - Troca de mensagens entre agentes e gerente

[4] SSH

Secure Shell – protocolo para o acesso remoto a equipamentos de forma segura por meio do uso de criptografia. É o sucesso do telnet.

As setas entre o NMS e o NME indicam de onde a mensagem é enviada. Em uma mensagem GetRequest, o NMS está solicitando informações da MIB do NME. Para solicitar um valor de um objeto no próximo ramo da MIB, uma mensagem GetNextRequest é enviada. Para realizar uma alteração no valor de um objeto, o NMS envia uma mensagem SetRequest. Em ambos os casos, o NME responde com uma mensagem GetResponse. A mensagem trap é enviada pelo NME quando o agente detecta um problema e deseja informá-lo ao NMS, ou seja, ela não é solicitada por este. Na imagem podemos observar que o protocolo de transporte utilizado pelo SNMP é o User Datagram Protocol (UDP). A porta UDP utilizada pelo SNMP é a 161. Mensagens do tipo trap utilizam a porta 162.

Outro conceito existente no modelo de gerenciamento com SNMP é o de comunidade, onde o objetivo é definir perfis de acesso às informações da MIB. É comum que em um equipamento com SNMP existam duas comunidades básicas. Uma é a "public" que, por padrão, permite apenas que as informações da MIB sejam lidas (*read-only*) por meio de mensagens do tipo Get. A outra é a comunidade *private* que, por padrão, além de permitir a leitura, permite também que as informações da MIB sejam alteradas (*read-write*) por meio de mensagens do tipo Set. Ao criar outras comunidades, o administrador define quais ramos da MIB estarão visíveis e as permissões de acesso (somente leitura ou leitura e escrita).

VOCÊ SABIA?

Devido aos problemas de segurança existentes no SNMPv1, referente à sigla SNMP, criou-se a sátira *"Security is not my problem"* (Segurança não é problema meu).

Por questões de segurança, muitos administradores desabilitam as comunidades public e private, pois quem conhece o SNMP sabe da existência destas, sendo assim, para o gerenciamento da rede, o administrador cria uma comunidade com um nome que somente ele saiba, garantindo que ninguém mais terá acesso às informações da MIB. Esta não é a melhor forma de prover segurança ao SNMP, pois, como as informações trocadas entre os agentes e o gerente ocorrem sem criptografia (texto plano), um agressor poderia facilmente obter os nomes de comunidades utilizadas. Uma alternativa seria utilizar túneis criptografados para a troca de mensagens, o que pode ser feito com o SSH[4].

Outra forma seria o uso de autenticação para acesso às informações da MIB, recurso disponível no SNMP versão 3, que será visto mais adiante. A seguir, confira a versão 2 do SNMP.

3.1.1 O SNMP VERSÃO 2

Entendendo que o protocolo SNMPv1 precisava de novas funcionalidades, além de melhores recursos de segurança, a IETF criou grupos de trabalho para o desenvolvimento do que chamou de SNMPv2. As propostas para o aperfeiçoamento nas questões de segurança geraram controvérsias, o que contribuiu para o aparecimento de diferentes modelos. Veja:

a) **SNMPsec**: a primeira tentativa de prover segurança ao SNMPv1. RFCs 1351 a 1353;

b) **SNMPv2c**: baseado no conceito de comunidade, parecido com o SNMPv1. RFCs 1901, 1905 e 1906;

c) **NMPv2u**: baseado no conceito de nomes de usuário. RFCs 1905, 1906, 1909 e 1910;

d) **SNMPv2p**: baseado nos conceitos de perfis e contextos. RFCs 1441, 1445, 1446, 1448 e 1449;

e) **SNMPv2***: tentativa de agregar características do SNMPv2P e do SNMPv2u.

O protocolo SNMPv2 conta com recursos interessantes, como o suporte à transferência de grandes blocos de dados (mensagens GetBulkRequest) e a possibilidade de troca de informações entre gerentes (mensagens InformRequest), além de novos grupos na MIB. Apesar do fato de que as questões referentes à segurança não terem sido resolvidas, os esforços despendidos com o SNMPv2, anos depois, resultaram no surgimento do SNMPv3, que você verá na etapa a seguir.

3.1.2 O SNMP VERSÃO 3

O SNMPv3 é considerado como o sucessor do SNMPv1, ou seja, o SNMPv2 não é reconhecido como uma versão estável e completa para utilização. O SNMPv3 incorpora os melhores recursos das versões intermediárias SNMPv2u e SNMPv2*. Por utilizar uma arquitetura modular, novas funcionalidades e modelos de segurança podem ser agregados ao SNMPv3 sem que, para isso, precise ser desenvolvida uma nova versão.

Com o SNMPv3 os recursos de segurança incluem o uso de criptografia, possibilidade de definir perfis de acesso, definindo quais informações da MIB os usuários terão acesso, além do recurso de autenticação, onde o acesso às informações só é liberado informando um nome de usuário e a respectiva senha. As RFCs que descrevem o SNMPv3 são:

a) **RFC 2271**: descreve a nova arquitetura (framework) do SNMPv3;

b) **RFC 2272**: descreve o processamento das mensagens no SNMPv3;

[5] DOS

DoS: Denial of Service – ataque do tipo negação de serviço, utilizado na tentativa de tornar um serviço de rede indisponível por falta de recursos.

c) **RFC 2273**: descreve as aplicações do SNMPv3;

d) **RFC2274**: *User-Based Security* (USM), o modelo de segurança do SNMPv3;

e) **RFC2275**: *View-Based Access Control Model* (VACM), o modelo de controle de acesso do SNMPv3.

Uma preocupação no desenvolvimento do SNMPv3 foi com a compatibilidade com as versões anteriores. A preocupação era de que fabricantes e usuários não migrassem para o SNMPv3 por não ser compatível com o sistema legado. Um problema nesta versão é o consumo maior de recursos do equipamento, situação explorada por agressores para realizar ataques do tipo DoS[5]. Mesmo assim, é altamente recomendável que novas implantações sejam feitas utilizando a versão 3, devido aos diversos benefícios, conforme você já viu.

SAIBA MAIS

No site do IETF, comunidade internacional para o desenvolvimento da Internet, você encontra informações sobre as RFC's, e diversos documentos técnicos. O IETF preocupa-se em propor soluções e com a padronização das tecnologias. Vale a pena dar uma olhada. Disponível em: http://ietf.org.

Vale a pena, também, conferir o portal para edição e publicação das RFC's. Disponível em <http://www.rfc-editor.org>. Lá você tem acesso ao conteúdo das RFC's já publicadas.

3.1.3 NMP NA PRÁTICA

Agora que você já entendeu os detalhes por trás do funcionamento do SNMP, partiremos para a sua configuração nos equipamentos da rede, entre servidores, roteadores, switches, etc. Uma vez que os equipamentos estão configurados, podemos utilizar uma ferramenta de gerenciamento de redes para realizar a coleta das informações nestes equipamentos e realizar o monitoramento de todos os equipamentos, a partir de um ponto central. As principais ferramentas serão estudadas no próximo capítulo.

CONFIGURANDO O SNMP NO MICROSOFT WINDOWS

As próximas oito figuras mostram os passos para configurarmos o agente SNMP em um servidor com sistema operacional Microsoft Windows. Confira:

a) O acesso é pelo "Painel de Controle", opção "Adicionar ou Remover Programas".

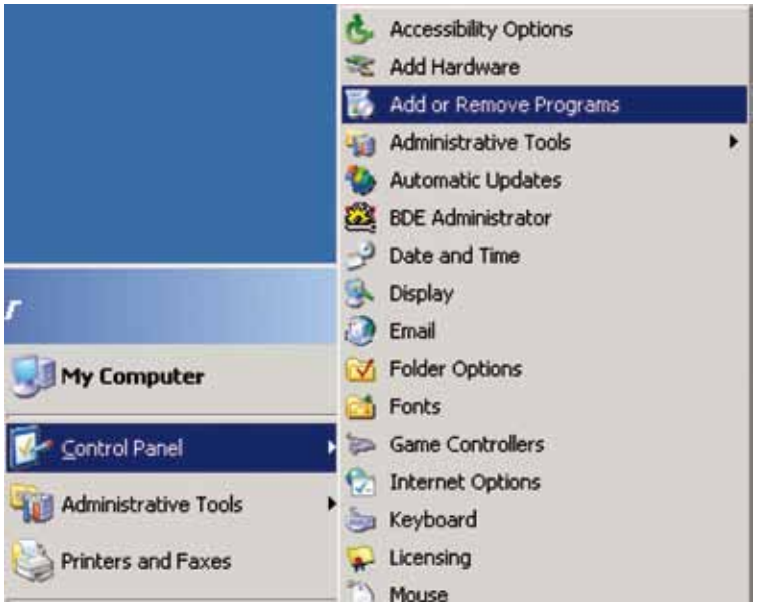


Figura 3 - SNMP no Microsoft Windows - Passo 1

b) Na opção "Adicionar/Remover Componentes do Windows", selecionamos "Ferramentas de Gerenciamento e Monitoração" e pressionamos o botão "Detalhes...".

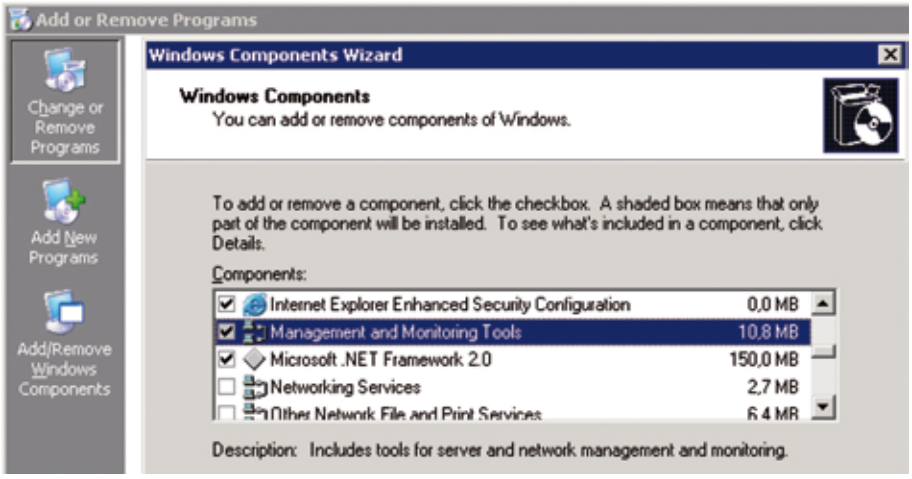


Figura 4 - SNMP no Microsoft Windows - Passo 2

c) Dentre as ferramentas disponíveis, selecionamos o “Protocolo Simples de Gerenciamento de Rede”. Ao pressionar OK, o CD de instalação do Microsoft Windows pode ser solicitado.

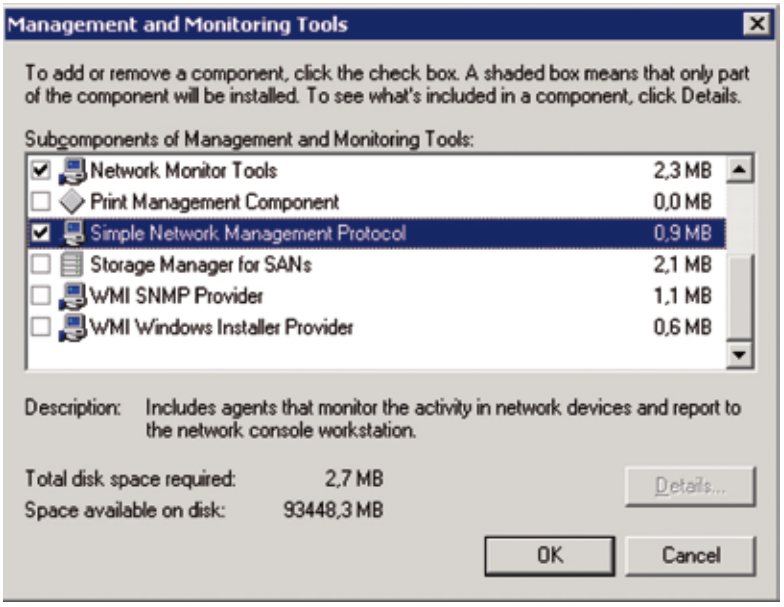


Figura 5 - SNMP no Microsoft Windows - Passo 3

d) Ao término da instalação, acessamos “Painel de Controle/Ferramentas Administrativas” e selecionamos o item “Serviços” para realizarmos a configuração.

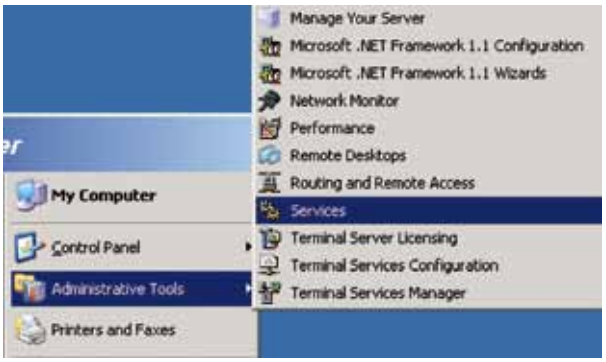


Figura 6 - SNMP no Microsoft Windows - Passo 4

e) Na relação de serviços, clique duplo sobre “Serviço SNMP”.

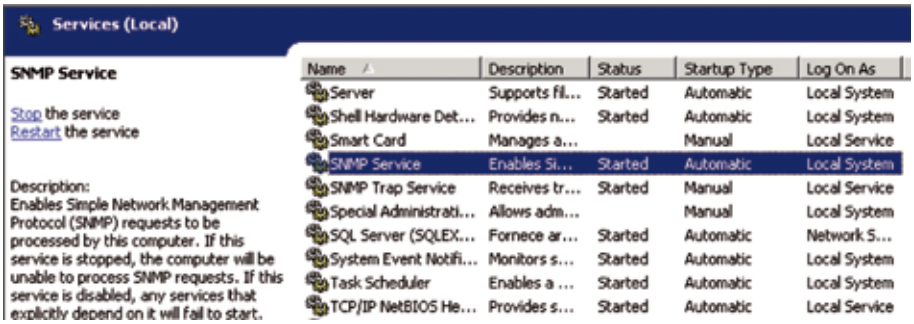


Figura 7 - SNMP no Microsoft Windows - Passo 5

f) Na aba "Segurança", definiremos a comunidade e a máquina autorizada a acessar as informações nos objetos da MIB do NME.

Figura 8 - SNMP no Microsoft Windows - Passo 6

g) Criaremos a comunidade *public* com permissão de somente leitura (*read only*).

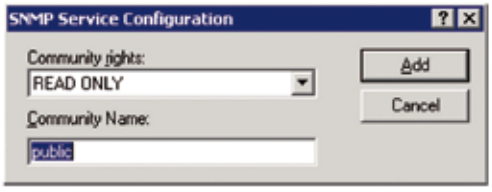


Figura 9 - SNMP no Microsoft Windows - Passo 7

h) Definimos qual equipamento tem permissão de acesso à MIB do equipamento: o NMS.

Figura 10 - SNMP no Microsoft Windows - Passo 8

i) No equipamento que será o NMS, optamos por utilizar o sistema Red Hat Enterprise Linux. Instalaremos alguns utilitários de linha de comando para testes de coleta de informações no equipamento que configuramos o agente SNMP. O nome do pacote que precisamos instalar é o "net-snmp-utils". Para instalá-lo, utilizamos o gerenciador de pacotes YUM[6], com o comando "yum install net-snmp-utils".

j) Em Linux, consultamos o valor de um objeto da MIB com o comando "snmpget". Precisamos informar para o comando o nome da comunidade, a versão do protocolo, o endereço IP do equipamento que queremos coletar as informações e o nome do objeto da MIB.

```
[root@localhost ~]# snmpget -v 2c -c public 10.1.3.115 sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 6 Model 44 Stepping 2 AT/
AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
[root@localhost ~]#
```

Figura 11 - Consultando a MIB com snmpget

k) Para visualizarmos todos os objetos da MIB e os respectivos valores, utilizamos o comando "snmpwalk". Neste caso, não deve ser informado o nome do objeto.

```
[root@localhost ~]# snmpwalk -v 2c -c public 10.1.3.115 | more
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 6 Model 44 Stepping 2 AT/A
T COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.2
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (115740364) 13 days, 9:30:03.64
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: GOETHE
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 76
IF-MIB::ifNumber.0 = INTEGER: 2
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.65539 = INTEGER: 65539
IF-MIB::ifDescr.1 = STRING: MS TCP Loopback interface
IF-MIB::ifDescr.65539 = STRING: vmxnet3 Ethernet Adapter
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.65539 = INTEGER: ethernetCsmacd(6)
```

Figura 12 - Consultando a MIB com snmpwalk

[6] YUM

Yellowdog Updater, Modified - ferramenta utilizada no gerenciamento de pacotes em sistemas Linux que utilizam pacotes RPM. Utilizado por distribuições como Red Hat, Fedora, CentOS. É similar ao APT.

[7] CLI

Command Line Interface – interface para interação com computadores e outros equipamentos, como switches e roteadores, através de comandos.

CONFIGURANDO O SNMP EM UM EQUIPAMENTO CISCO

A figura a seguir mostra os comandos para configurarmos o agente SNMP nos equipamentos da Cisco, como roteadores e switches. Acessamos a CLI[7] do equipamento, e entramos no modo privilegiado (*enable*). Digitamos a senha e entramos no modo de configuração (*configure terminal*). Habilitamos o agente SNMP informando o nome da comunidade (*public*) e o tipo de acesso somente leitura (ro). Por fim, salvamos as configurações (copy running-config startup-config).

```
switch>
switch>enable
Password:
switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#snmp-server community public ro
switch(config)#exit
switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
switch#
```

Figura 13 - Configuração do agente SNMP em um equipamento Cisco

SAIBA MAIS

Navegue pelo site da Cisco Systems, líder de mercado em equipamentos para redes, principalmente roteadores e switches e, recentemente, servidores, e dê uma olhada nas várias informações que você encontra por lá.

Acesse: <http://www.cisco.com>

Para visualizarmos todos os objetos da MIB, utilizamos o comando snmpwalk. Com isso, teremos acesso a diversas informações, como o tráfego nas interfaces do equipamento.

```
[root@localhost ~]# snmpwalk -v 2c -c public 10.1.1.215 | more
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, C2960 Software (C2960-LANLITEK9
-M), Version 12.2(50)SE3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 22-Jul-09 07:03 by prod_rel_team
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.1147
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1891231300) 218 days, 21:25:13.00
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: switch.sc.senai.br
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 2
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 28
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.10001 = INTEGER: 10001
```

D'imitre Camargo Martins (2012)

Figura 14 - Visualizando os objetos da MIB do equipamento Cisco

[8] GNU

Acrônimo recursivo para "GNU *is Not Unix*". Projeto criado por Richard Stallman em 1984, com o objetivo de criar um sistema operacional e aplicações completamente abertas e compatíveis com o sistema Unix.

[9] APT

Advanced Packaging Tool – ferramenta utilizada no gerenciamento de pacotes DEB no sistema operacional Debian GNU/Linux e derivados deste, como o Ubuntu, Kurumin e Mint.

3.1.4 CONFIGURANDO O SNMP NO DEBIAN GNU/LINUX

Para configurarmos o agente SNMP no Debian GNU[8]/Linux, é necessário que o equipamento tenha o pacote "UCD-SNMP" ou seu sucessor "Net-SNMP". Começamos instalando o pacote que contém este programa, o "snmpd", por meio do gerenciador de pacotes APT[9].

Para isso, utilizamos o comando "apt-get install snmpd". Após instalarmos, o agente do SNMP já estará em execução. Por padrão, as comunidades "public" e "private" já estão criadas. Consultaremos os objetos da MIB a partir do próprio servidor, informando o destino da consulta para "localhost" (figura a seguir).

D'imitre Camargo Martins (2012)

Figura 15 - Acessando os objetos da MIB do próprio servidor GNU/Linux

FIQUE ALERTA

Sempre que configurar o SNMP em um equipamento, utilize nomes de comunidades complexas, pois elas fazem o papel de senha de acesso a MIB, além de desativar as comunidades public e private, quando existirem.

Definições sobre as comunidades e permissões de acesso são feitas no arquivo "/etc/snmp/snmpd.conf". Para criar novas comunidades e liberar diferentes tipos de acesso, pode-se utilizar o comando "snmpconf", que irá gravar as informações no mesmo arquivo. Para mais informações sobre a configuração do SNMP no Linux, a documentação está disponível no site do projeto Net-SNMP.

SAIBA MAIS

Você encontra mais informações no material Net-SNMP – Projeto open source para a implementação do SNMP em sistemas operacionais do padrão Unix e Microsoft Windows. Disponível em <http://www.net-snmp.org>.

3.1.5 RMON

O RMON é a sigla para *Remote Network Monitoring* (Monitoramento de Rede Remoto). Segundo Stallings (1999), a especificação do RMON1 foi a maior contribuição ao conjunto de padrões do SNMP. É outro padrão do IETF (RFC 1757), como o SNMP. Apesar de podermos utilizar o SNMP para monitorar equipamentos remotos, a sua utilização em uma WAN (redes de longa distância) pode revelar algumas deficiências. Em uma ocasião onde a capacidade do enlace de dados é pequena, as informações de gerenciamento podem acabar por deixá-lo sobrecarregado. Com o SNMP, conseguimos coletar informações de um equipamento, mas não de um segmento de rede inteiro, onde poderíamos analisar as informações sobre os pacotes trafegados. Com SNMP, não conseguimos criar servidores intermediários, que se reportariam a um servidor central, sendo assim, teremos um único NMS. Se este servidor ficar sobrecarregado, ou indisponível, todo o gerenciamento da rede fica comprometido.

O objetivo do RMON é o de resolver essas (e outras) deficiências do SNMP, uma vez que permite o gerenciamento distribuído. Com ele, conseguimos monitorar segmentos de rede inteiros, e tudo o que acontece neste segmento, será percebido pela sonda RMON, chamada de probe. É ela quem coleta e armazena as informações. Esta pode estar ativa em qualquer equipamento do segmento de rede, em um computador, switch ou roteador, por exemplo. Por fim, teremos a estação de gerenciamento, o NMS, que coletará as informações coletadas pela probe. Uma vez que a probe faz a organização dos dados coletados, o NMS terá acesso a informações específicas, como somente equipamentos com problema num dado segmento de rede. É possível a utilização de mais de um NMS.

Confira, no Casos e relatos a seguir, um exemplo de monitoramento por meio de enlaces lentos.

[10] CRC

Cyclical Redundancy Check – número gerado através de cálculos matemáticos para a identificação de erros na transmissão de dados.

CASOS E RELATOS

Monitoramento remoto através de enlaces lentos

Paulo, gerente de TI de uma grande organização, estava recebendo diversas reclamações dos usuários da rede de uma filial remota, relatando lentidão nos acessos às aplicações corporativas, alocadas na matriz. Ele não entendia o porquê disto, uma vez que os enlaces da empresa são robustos. Paulo trabalha na matriz da empresa e como esta possui muitas filiais, sempre que ocorria algum problema em uma delas, ele precisava se deslocar até o local para realizar a análise e os reparos.

Como, por causa dos deslocamentos, estava ficando sem tempo para realizar as suas atividades, Paulo conversou com um amigo de profissão que o sugeriu o uso de um protocolo de gerenciamento, para que, assim que algo de errado estivesse acontecendo com a rede da matriz ou das filiais, ele pudesse identificar e realizar a correção, em algumas ocasiões, antes que o problema pudesse interferir nos processos de produção.

Inicialmente, Paulo utilizou o protocolo SNMP para coletar as informações dos equipamentos, mas, como os enlaces constantemente estavam lentos, passou a utilizar o RMON para gerenciar as filiais. Logo após a configuração dos equipamentos, por meio das informações coletadas pela probe RMON, Paulo identificou erros de CRC10 na interface serial do roteador, que era conectada ao modem. Esses erros faziam com que o roteador tivesse que retransmitir diversos pacotes. Paulo solicitou o suporte da operadora responsável pelo enlace, que, rapidamente, identificou um problema com o cabo serial que faz a conexão entre os equipamentos. O cabo foi substituído e os erros de CRC pararam imediatamente.

Devido ao gerenciamento pró-ativo que Paulo estava realizando, a quantidade de reclamações sobre problemas na rede diminuiu quase que totalmente. Paulo não precisou mais se ausentar da matriz com tanta frequência e estava tendo mais tempo para realizar as suas atividades.

O RMON atua somente até a camada de enlace (MAC), sendo assim, não tem informações sobre problemas nas camadas superiores, como as camadas IP e TCP. Esta capacidade foi introduzida no RMON II (RFC 2021). Ele não é um protocolo de gerenciamento, mas somente uma extensão da MIB, onde foram criados vinte novos grupos. Os dez primeiros grupos referem-se ao RMON I e os outros dez ao RMON II (veja figura a seguir).

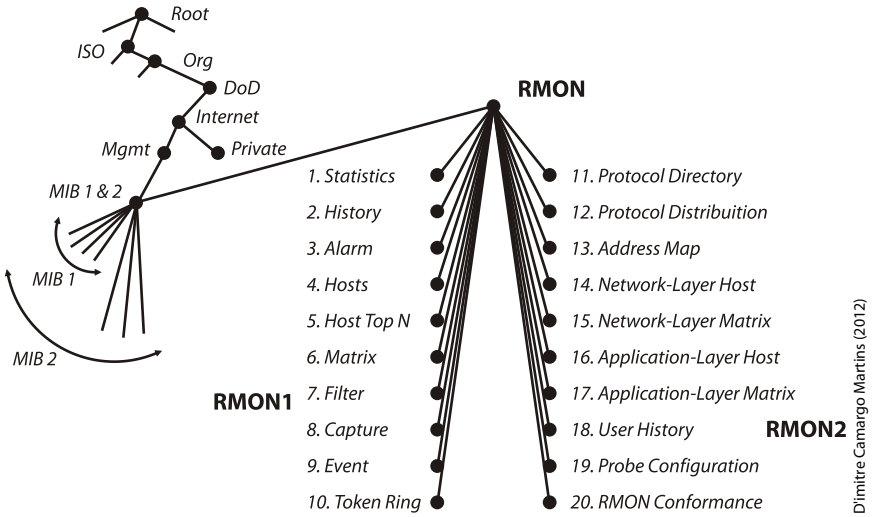


Figura 16 - MIB RMON
Fonte: UFCG CEEI [20--]

As tarefas para o gerenciamento da rede são distribuídas entre os grupos do RMON. Por exemplo, a análise e a geração das estatísticas são tarefas dos grupos History, Host, Host Top N e Matrix. Os eventos são tratados pelos grupos Alarm e Event. A captura de pacotes é responsabilidade dos grupos Filter e Capture. Como já foi mencionado, o RMON não é um protocolo, sendo assim, a responsabilidade para a comunicação entre agentes e gerentes continua sendo do SNMP.

RECAPITULANDO

Neste capítulo, você entendeu o funcionamento do SNMP, principal protocolo para o gerenciamento de redes. Viu que o SNMPv1 foi criado de forma emergencial dada a sua necessidade. Devido aos seus problemas de segurança, levou ao surgimento de diferentes propostas para o seu sucessor, o SNMPv2. As melhores práticas existentes nesses modelos, levou à criação do SNMPv3, considerado o mais seguro, mas ainda pouco utilizado.

Você constatou, também, que as informações de gerenciamento são armazenadas na MIB e que esta é dividida em grupos, cada qual com os seus respectivos objetos. Aprendeu a configurar o SNMP em diferentes equipamentos, assim como os comandos para obter os valores contidos nos objetos da MIB destes equipamentos.

Por fim, percebeu a necessidade para a criação do RMON, uma ótima alternativa para o monitoramento de redes remoto, e que, dentre os principais benefícios deste, está o de gerar pouca carga sobre os enlaces de dados. No próximo capítulo você conhecerá as principais ferramentas de gerenciamento de redes. Acompanhe!

Anotações:

Sistemas de Gerenciamento e Monitoramento de Redes

4

Uma das responsabilidades de um administrador de TI é a de fazer o gerenciamento da rede. Obviamente, quanto maior e heterogênea ela for, maior será a dificuldade em gerenciá-la. Para facilitar essa tarefa, praticamente todo administrador faz o uso de aplicativos desenvolvidos especialmente para estes fins e que ajudam na produtividade desses profissionais.

Neste capítulo, você conhecerá as principais ferramentas de gerenciamento de redes, que têm como objetivo, fazer com que o administrador de TI opte por uma ou mais, dependendo da situação. São comuns os casos em que mais de uma ferramenta são usadas, simultaneamente.

Ao final deste capítulo você terá subsídios para:

a) conhecer as principais ferramentas de gerenciamento de redes, a instalação, configuração e utilização das mesmas.

[1] LINGUAGEM PERL

Linguagem de programação criada por Larry Wall em 1987.

4.1 O MRTG

O MRTG é uma ferramenta de monitoração bastante conhecida por administradores de redes. Ele começou a ser desenvolvido em 1994 por Tobias Oetiker. Inicialmente, o seu código era escrito completamente na linguagem Perl[1].

Em 1996, devido a problemas de desempenho, Dave Rand alterou partes do código para a linguagem C. Com a ferramenta estável, seu código começou a ser disponibilizado para quem quisesse utilizá-lo. Isso fez com que os criadores passassem a receber relatórios de problemas e principalmente sugestões de melhorias. Apesar de antigo, o MRTG ainda é muito utilizado, uma vez que, além de ser extremamente útil, é simples de instalar e configurar, além do fato de ser gratuito. Essa ferramenta é distribuída sob os termos da GPL (*General Public License)* que é um tipo de licença para software livre, idealizada por Richard Stallman em 1989, como parte do projeto GNU. Uma das obrigações desta é que o código fonte acompanhe o programa.

VOCÊ SABIA?

A licença GPL (*General Public License*) é um tipo de licença para software livre idealizada em 1989 por Richard Matthew Stallman, fundador do projeto GNU e da FSF (*Free Software Foundation*), organização sem fins lucrativos criada por Richard Stallman em 1985, dedicada ao movimento do Software Livre.

O MRTG é bastante utilizado para a monitoração dos enlaces, principalmente o tráfego de dados, porém, também é possível monitorar os equipamentos da rede, como roteadores, switches e servidores. A forma mais comum para a coleta das informações é por meio do protocolo SNMP, mas também podem ser coletados através de scripts. Tais informações são coletas em intervalos de, no mínimo, cinco minutos, sendo permitido configurar intervalos maiores.

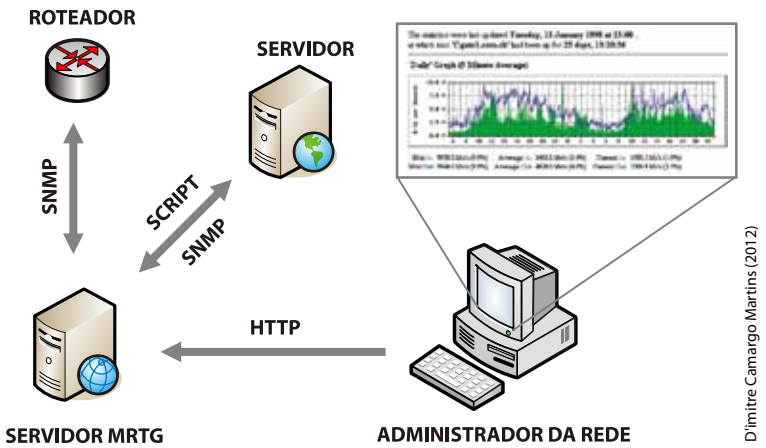


Figura 17 - Estrutura básica do funcionamento do MRTG

4.1.1 INSTALAÇÃO

O MRTG está disponível para ser instalado em sistemas Unix, Linux, Microsoft Windows e Novel Netware. Para uma instalação em sistemas Linux, você pode optar pela compilação do código fonte (disponível no site), ou pelo uso de gerenciadores de pacotes, disponíveis na maioria das distribuições. Veja, por exemplo, os passos de uma instalação, em um servidor com o sistema operacional Debian GNU/Linux. Os passos seriam:

a) Instalar o servidor web Apache (se já não estiver) com o comando"apt-get install apache2";

b) Instalar o MRTG com o comando "apt-get install mrtg";

c) Instalar os pacotes relacionados ao protocolo SNMP com o comando

"apt-get install snmp snmpd".

FIQUE ALERTA

A instalação dos pacotes também pode ser realizada em um único comando. Basta informar o nome de cada pacote que se deseja instalar, separados por espaço. No caso do MRTG faríamos "apt-get install apache2 mrtg snmp snmpd".

CONFIGURAÇÃO

Concluída a instalação, é preciso configurar o MRTG. Este recurso não está disponível na interface web, sendo assim, para cada item que se deseja monitorar, deve ser gerado um arquivo de configuração. Estes podem ser escritos manualmente, gerados por meio de utilitários desenvolvidos por terceiros ou pelo comando cfgmaker. As informações que devem ser repassadas ao utilitário são o nome e o local onde o arquivo de configuração será salvo, o nome da comunidade do SNMP (configurada previamente no equipamento que será monitorado) e o endereço IP do equipamento. Por exemplo:

cfgmaker --output /etc/mrtg/roteador.cfg public@10.1.14.254.

Feito isso, o MRTG tentará coletar informações (via SNMP) do equipamento. Caso tenha sucesso, informações adicionais podem ser inseridas automaticamente no arquivo de configuração criado.

[2] HTML

HyperText Markup Language – linguagem para o desenvolvimento de páginas para a Web;

FIQUE ALERTA

Lembre-se: quando precisar realizar configurações em equipamentos ou servidores, na maioria dos casos, é preciso que se esteja operando no modo administrativo, ou seja, que o acesso ao equipamento seja realizado utilizando credenciais com permissões de administração.

O arquivo de configuração foi criado com as definições mínimas necessárias, porém, outras podem ser adicionadas, de acordo com a necessidade. Por exemplo, podemos alterar o intervalo de coleta das informações e de atualização da página. Alguns dos principais parâmetros de configuração são:

a) **WorkDir**: define em qual diretório serão armazenadas as imagens, os arquivos de log e os arquivos HTML[2];

b) **Options**: utilizado para definir a orientação, assim como as unidades de medida utilizadas nos gráficos;

c) **Refresh**: define o intervalo, em segundos, em que o navegador utilizará a exibição da página (o padrão é 300);

d) **Interval**: define o intervalo, em minutos, em que as informações serão coletadas;

e) **RunAsDaemon**: define que o MRTG seja executado como um serviço, o que faz com que fique em constante execução, caso contrário, será preciso executá-lo manualmente, ou agendar a sua execução;

f) **Language**: define o idioma em que as informações dos relatórios serão geradas;

g) **Unscaled**: define que os gráficos não serão redimensionados conforme os valores coletados, ou seja, a medida máxima do gráfico é um valor fixo.

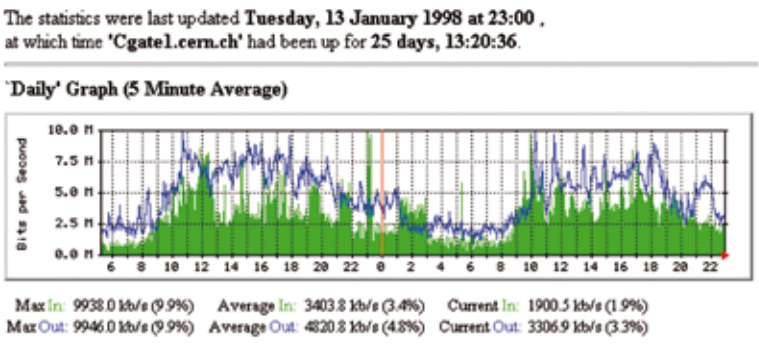
```
WorkDir: /var/www/mrtg
Language: brazilian
Options[_]: bits,growright
RunAsDaemon: yes

Target[EXEMPLO]: 1:public@10.1.14.254:
MaxBytes[EXEMPLO]: 32000
AbsMax[EXEMPLO]: 32000
Unscaled[EXEMPLO]: dwmy
Title[EXEMPLO]: Análise de Tráfego - link de 256kbps
PageTop[EXEMPLO]: <h1>Análise de Tráfego - link de 256kbps</h1>
```

Quadro 2 - Exemplo de arquivo de configuração do MRTG

Com o arquivo de configuração criado, faremos com que o MRTG comece a coletar as informações que serão utilizadas para gerar os relatórios. Uma das maneiras de fazer isso é com o comando "mrtg /etc/mrtg/roteador.cfg".

Além do arquivo de configuração do equipamento a ser monitorado, é preciso gerar os arquivos HTML de índice, por meio dos quais os gráficos serão acessados. Para esta etapa usaremos o comando indexmaker, informando o nome e local do arquivo HTML que será gerado e o arquivo de configuração, por exemplo: indexmaker --output=/var/www/mrtg/index.html /etc/mrtg/roteador.cfg. Após o processamento, as páginas HTML geradas estarão acessíveis para visualização por meio de um navegador (browser), sendo que as informações do monitoramento são apresentadas nestas sob a forma de gráficos estatísticos. Por padrão são gerados quatro gráficos, onde cada um diz respeito ao período a que as informações se referem (diário, semanal, mensal e anual).



D'imitre Camargo Martins (2012)

Figura 18 - Gráfico diário gerado pelo MRTG
Fonte: Laboratory of Information Tecnologies [20--]

Conforme pode ser observado na figura do gráfico diário, por padrão, o MRTG pode representar somente dois valores de coletas de um mesmo equipamento. Em algumas situações pode ser interessante gerar gráficos com múltiplos valores. A solução para isso é a utilização do RRDtool (*Round-Robin Database Too*l), que possui diversos outros recursos interessantes, como a possibilidade de realizar as coletas em intervalos menores que a mínima possível no MRTG (cinco minutos). O RRDtool foi desenvolvido pelo mesmo criador do MRTG (Tobias Oetiker). Ele está disponível para sistemas Unix, Linux e Microsoft Windows.

É importante ressaltar que o RRDtool não é uma ferramenta completa para monitoramento de redes, mas sim, um programa que coleta as informações e gera gráficos estatísticos. Sendo assim, ele foi feito para ser utilizado por ferramentas de gerenciamento, que neste caso, atuariam como *front-end* para o RRDtool, o que pode ser feito com o MRTG. O Cacti é um exemplo. Ele utiliza o RRDtool na coleta e geração dos gráficos. Estudaremos o Cacti ainda neste capítulo.

[3] HTTPS

HyperText Transfer Protocol Secure - protocolo do serviço de redes TCP/IP para a transferência de hipertexto de forma segura, através do uso de criptografia.

[4] *GATEWAY*

Equipamento responsável pelo encaminhamento do tráfego, de e para, redes distintas.

SAIBA MAIS

Você pode fazer o download e encontrar a documentação oficial do MRTG no site Multi Router Traffic Grapher. Disponível em: <http://oss.oetiker.ch/mrtg>.

No site do Round_Robin Database Tool (RRDTool) você encontra o código fonte para download e as versões pré-compiladas para diferentes sistemas operacionais. Está disponível, também, a documentação oficial. Disponível em: <http://oss.oetiker.ch/rrdtool>.

E, no site do Debian GNU/Linux, uma das distribuições Linux mais utilizadas em servidores, você encontra todas as informações sobre a distribuição, notícias, eventos, documentação e áreas para download do sistema operacional. Acesse o site: <http://www.debian.org>.

No item a seguir, você conhecerá a ferramenta NTOP. Confira!

4.2 O NTOP

O Network Top (NTOP) é uma solução de monitoramento de rede desenvolvida por Luca Deri, em 1998. Seu código é escrito na linguagem C e é distribuído sob os termos da licença GPL. Possui versões para instalação em sistemas da família Unix (Linux, BSD e MacOSX) e sistemas Microsoft Windows de 32 bits.

D'imitre Camargo Martins (2012)

Figura 19 - Barra de navegação simples do NTOP

O NTOP é uma solução bastante simples, mas pode gerar informações sobre praticamente tudo que é acessado pelos usuários da rede. Dentre alguns dos seus recursos podemos citar:

a) analisa e classifica conexões IP de acordo com a origem e destino do tráfego;

b) pode identificar o sistema operacional das máquinas da rede;

c) é útil para identificar o uso de programas não permitidos na rede (P2P, torrent, etc.);

d) armazena as informações estatísticas da rede no formato RRD;

e) pode classificar o tráfego com base em diferentes critérios como: protocolos (IPv4, IPv6, TCP, UDP, ICMP, etc.), endereço de origem, endereço de destino, etc.;

f) permite acompanhar todas as conexões ativas de um determinado computador, ou seja, acesso a sites e outros programas que fazem uso da Internet;

g) possui um servidor web integrado, inclusive HTTPS[3];

h) pode gerar estatísticas com base no protocolo de gerenciamento RMON;

i) é de fácil utilização, visto que praticamente não precisamos configurá-lo;

j) pode coletar os fluxos gerados por roteadores e switches, chamados NetFlows/sFlows.

Quanto aos pacotes NetFlow/sFlow, normalmente, apenas os equipamentos mais robustos do mercado geram esse tipo de informação, como equipamentos da Cisco, Juniper, Foundry e Extreme, entre outros. Nestes equipamentos devemos informar para qual servidor os fluxos serão enviados. O destino deve ser um computador contendo um software que coleta, analisa e gera relatórios do uso da rede baseados nos fluxos recebidos. Além do NTOP, outros programas podem ser utilizados para esta finalidade, como o Scrutinizer e o NetFlow Analyzer.

VOCÊ SABIA?

A tecnologia NetFlow é proprietária e foi desenvolvida Cisco Systems. A Cisco é uma multinacional líder de mercado com sede em San Jose (Califórnia) e foi fundada em 1984.

Para que o NTOP consiga coletar tantas informações, ele precisa ser instalado no *gateway*[4] da rede, por exemplo, um computador com sistema Linux responsável pelo roteamento (IProute2), filtragem de pacotes (Iptables), tradução de nomes (DNS), navegação na Internet (Squid), etc. Com isso, temos a garantia de que todo o tráfego entre as redes, obrigatoriamente, passará por este equipamento, onde o NTOP poderá analisar e gerar os relatórios. A figura a seguir ilustra o posicionamento do NTOP na rede.

[5] SSL

Secure Sockets Layer – protocolo de criptografia utilizado para a realização de comunicações seguras na Internet.

[6] URL

Uniform Resource Locator – localização de um recurso na rede onde deve ser informado o protocolo, o endereço e o caminho para este recurso.

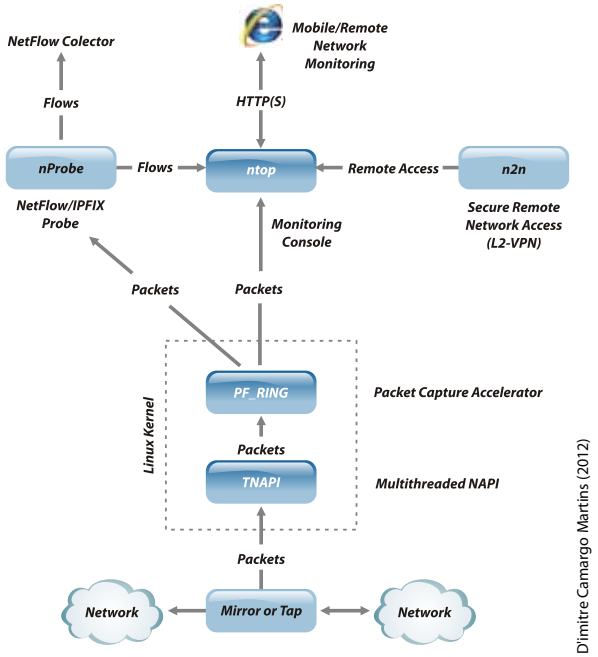


Figura 20 - Estrutura de funcionamento do NTOP
Fonte: NTOP [20--]

Observe, no centro da imagem, a existência de um equipamento com kernel Linux. Todo o tráfego gerado pela rede passa por este equipamento, sendo assim, ele é o *gateway* da rede. Os pacotes são analisados pelo NTOP, tanto os gerados pelo *gateway* como os recebidos via exportação dos fluxos NetFlow/sFlow. O NTOP gera as informações em sua interface web que é acessada por meio de um navegador, com ou sem criptografia *SSL*[5].

4.2.1 INSTALAÇÃO

A instalação do NTOP em um sistema Debian GNU/Linux é bastante simples. Utilizaremos o comando "apt-get install ntop". Ao término da instalação utilizamos o comando "ntop" para definirmos a senha do usuário administrador (admin). Este passo é obrigatório após a instalação. Se não realizado, o serviço não entrará em operação.

Uma vez que o NTOP possui um servidor web integrado (para garantir que não ocorra um conflito com um possível serviço web em execução na máquina), por padrão o serviço entra em execução na porta 3000 (TCP). Com isso, para acessá-lo, informar o endereço do servidor e a porta, por exemplo: <http://www.meuservidor.com.br:3000>. Se optar por acessá-lo com criptografia, na URL[6], informa-se o protocolo HTTPS e a porta 3001.

CONFIGURANDO E UTILIZANDO O NTOP

Apesar de podermos realizar algumas configurações por meio da interface web, os principais parâmetros de configuração são definidos por parâmetros passados para o comando "ntop". Dentre os principais parâmetros estão:

PARÂMETRO	EFEITO
-A	Para definir ou alterar a senha do usuário administrador (admin).
-a <arquivo>	Definir em qual arquivo os registros de acesso ao NTOP serão gravados.
-d	O NTOP será executado como um daemon (como um serviço em segundo plano).
-i	Define a(s) interface(s) (placas de rede) que o NTOP irá monitorar o tráfego.
-M	Separa as informações nos relatórios por interface de rede.
-n	Os endereços serão exibidos no formato numérico, ao invés de nomes.
-u <usuário>	Conta de usuário que será utilizada para executar o serviço do NTOP.
-w <porta>	Define em qual porta (HTTP) o serviço será executado. O padrão é 3000.
-W <porta>	Define em qual porta (HTTPS) o serviço será executado. O padrão é 3001.
-h	Para visualizar todos os parâmetros aceitos pelo comando NTOP (um manual).

Quadro 3 - Principais parâmetros para o comando ntop

Assim que o serviço do NTOP estiver em execução, após poucos minutos já poderemos visualizar as informações geradas por ele. Como algumas dessas informações podem ser confidenciais, podemos restringir o acesso a algumas telas do NTOP. Fazemos isso por meio da sua interface, em "Admin/Configure/Protect URLs". Também podemos configurar parâmetros da inicialização do NTOP, construir expressões para a filtragem de tráfegos específicos, limpar as informações estatísticas, criar contas de acesso e interromper a execução do NTOP. Em "Plugins", pode-se ativar e desativar plugins, além de configurá-los.

[7] PHP

Acrônimo recursivo para "PHP: *Hypertext Preprocessor*" – linguagem interpretada para o desenvolvimento de aplicações dinâmicas para a Web.

[8] *PLUGIN*

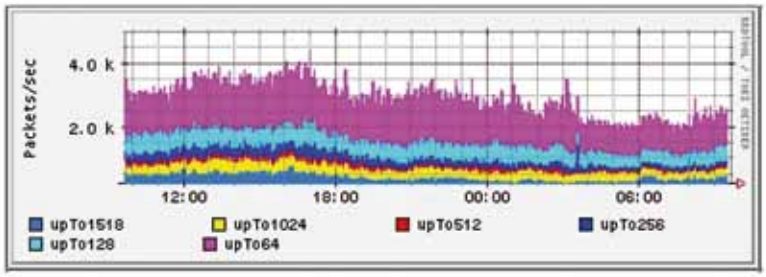
Componentes utilizados para agregar funcionalidades às aplicações. Normalmente não operam independentemente, somente associados a algum software hospedeiro.

Host	Domain	Data		TCP	UDP
89.122.183.124		52.7 MB	26.3 %	52.7 MB	0
fisica.ufpr.br		50.0 MB	25.0 %	50.0 MB	0
h89220202011.dsl.mijnabel.nl		23.1 MB	11.5 %	23.1 MB	0
d154-20-0-157.bchsia.telus.net		11.0 MB	5.5 %	11.0 MB	0
c-98-226-61-7.hsd1.il.comcast.net		10.5 MB	5.2 %	10.5 MB	0
125-15-60-235.rev.home.ne.jp		10.0 MB	5.0 %	10.0 MB	0
adsl-69-154-189-85.dsl.hstntx.swbell.net		7.9 MB	4.0 %	7.9 MB	0
ip98-165-143-78.ph.ph.cox.net		5.2 MB	2.6 %	5.2 MB	0
207-172-248-190.c3-0.eas-ubr5.atw-eas.pa.cable.rcn.com		4.5 MB	2.3 %	4.5 MB	0
190-50-214-32.speedy.com.ar		3.6 MB	1.8 %	3.6 MB	0
201-2-218-189.bnut3702.dsl.brasiltelecom.net.br		2.1 MB	1.0 %	2.1 MB	0
bb-87-82-7-167.ukonline.co.uk		2.0 MB	1.0 %	2.0 MB	0
s0106001346bbebc9.cg.shawcable.net		1.6 MB	0.8 %	1.6 MB	0
ool-182f90d4.dyn.optonline.net		1.6 MB	0.8 %	1.6 MB	0
d66-183-63-128.bchsia.telus.net		1.5 MB	0.7 %	1.5 MB	0

D'imitre Camargo Martins (2012)

Figura 21 - Relatórios detalhados gerados pelo NTOP
Fonte: Hardware [20--]

Já os gráficos e relatórios, podem ser visualizados por meio das seções "Summary", "All Protocols" e "IP". Observe na figura anterior que o NTOP identifica o aplicativo referente a certos tipos de tráfego, o país ao qual pertence um domínio e, em algumas ocasiões, o sistema operacional dos equipamentos envolvidos. Também informa a quantidade de dados tráfegos por conexão. As informações também podem ser apresentadas na forma de gráficos, conforme figura a seguir.



D'imitre Camargo Martins (2012)

Figura 22 - Gráfico gerado pelo NTOP
Fonte: Linuxaria (2010)

Chegamos ao fim do estudo da ferramenta NTOP. Como esta tem o pré-requisito de ser instalada no *gateway* da rede, alguns administradores de TI podem concluir que não é possível utilizá-la, pois em muitas situações, o *gateway* da rede é um roteador. A alternativa para esta situação é instalar o NTOP em um servidor qualquer e, na porta do switch onde este servidor estiver conectado, configurar o espelhamento do tráfego da porta onde está a interface LAN do roteador. Com isso, o servidor onde o NTOP estiver instalado, receberá uma cópia de todo o tráfego do roteador.

SAIBA MAIS

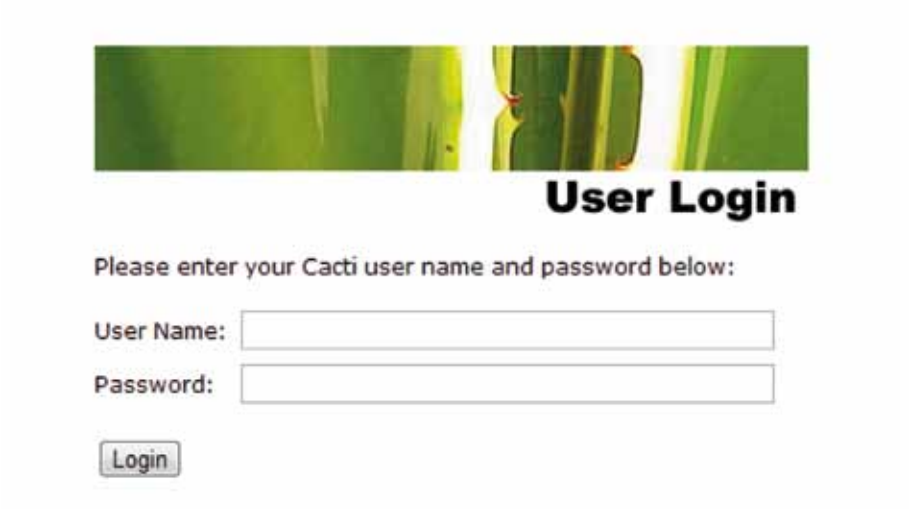
Para saber mais sobre NTOP, acesse o site indicado. Nele você encontrará a documentação oficial da ferramenta e informações sobre suporte. Disponível em: <http://www.ntop.org>.

Você conheceu a ferramenta NTOP. Outra ferramenta utilizada para o gerenciamento de rede é o CACTI. Continue sua leitura e confira as informações!

4.3 O CACTI

O Cacti é uma boa opção para o gerenciamento de redes. Considerado o sucessor do MRTG, surgiu como uma alternativa de front-end para o RRDtool. Foi desenvolvido por Ian Berry e também é distribuído sob a licença GPL. Ele é completamente escrito na linguagem PHP[7] e armazena as informações em um banco de dados MySQL. Pode ser instalado em sistemas Linux e Microsoft Windows. Os dados são coletados por meio do SNMP (o Cacti tem suporte para as três versões do SNMP) ou com o uso de *scripts*.

Além de suas funcionalidades nativas, sua arquitetura permite que *plugins*[8] sejam agregados, o que amplia os seus recursos. Para cada conta de usuário com acesso à sua interface, diferentes níveis de permissões podem ser definidos.



D'imitre Camargo Martins (2012)

Figura 23 - Tela de login do Cacti

4.3.1 INSTALAÇÃO

Assim como qualquer outra ferramenta, o Cacti possui os seus pré-requisitos para instalação. Dependendo do sistema onde será instalado, essas dependências podem ser tratadas automaticamente na sua instalação. Os requisitos para o Cacti são:

a) Servidor Web – por exemplo, o Apache ou IIS (Microsoft Windows);

b) PHP – preferencialmente versão 5 ou superior;

c) Banco de dados MySQL – versão 4.1 ou superior;

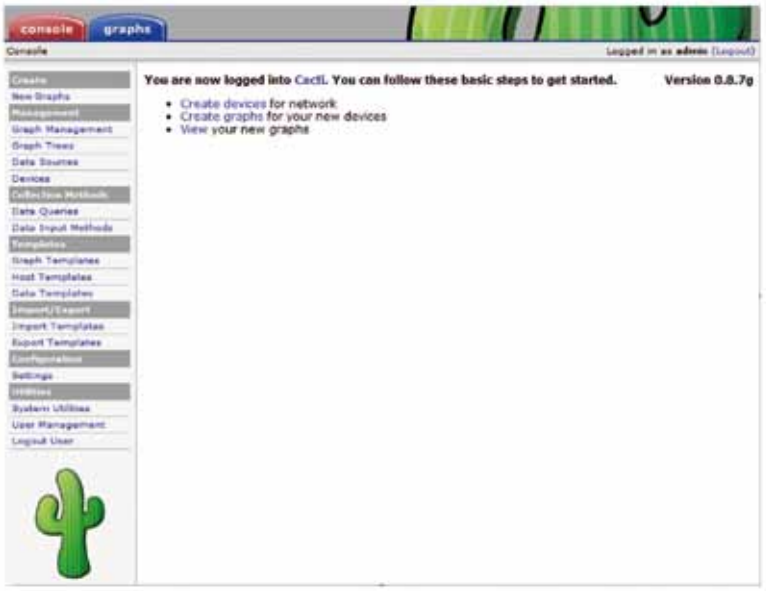
d) SNMP – se pretendido coletar dados por meio deste protocolo;

e) RRDtool.

Em um sistema Debian GNU/Linux, realizaremos a instalação com o comando "apt-get install cacti", sendo que as dependências serão instaladas automaticamente. Durante a instalação será solicitado o nome da base de dados que será criada além das credenciais de acesso do administrador do MySQL. Por fim, é solicitado para que seja informado o tipo de servidor web utilizado pelo Cacti, que no nosso caso, será o Apache versão 2.

Ao término da instalação dos pacotes e configuração da base dados, algumas etapas da configuração inicial são realizadas a partir da interface web. Para isso, iremos acessá-la a partir de um navegar informando o endereço do servidor, por exemplo, <http://www.servidor.com.br/cacti>. A página que será exibida inicialmente contém informações sobre a licença de distribuição do Cacti (GPL) e traz orientações gerais sobre o processo de instalação e configuração. Devemos acessar o botão "Next" no fim da página para avançar. Na página seguinte informamos se estamos realizando uma nova instalação ou uma atualização de uma versão antiga do Cacti. Selecionamos nova instalação e avançamos. Para finalizar, o Cacti verifica se todos os componentes foram encontrados. Se nenhum alerta (em vermelho) for emitido, o botão "Finish" encerra a instalação.

Nesse momento, as configurações serão aplicadas e gravadas no banco de dados. Posteriormente, a tela que se abre é a de *login* para acesso à ferramenta que está pronta para uso. No primeiro acesso devem ser utilizadas as credenciais usuário "admin" e senha "admin". Automaticamente, somos encaminhados para o procedimento de troca da senha, onde iremos informar a nova senha e confirmá-la.



D'imitre Camargo Martins (2012)

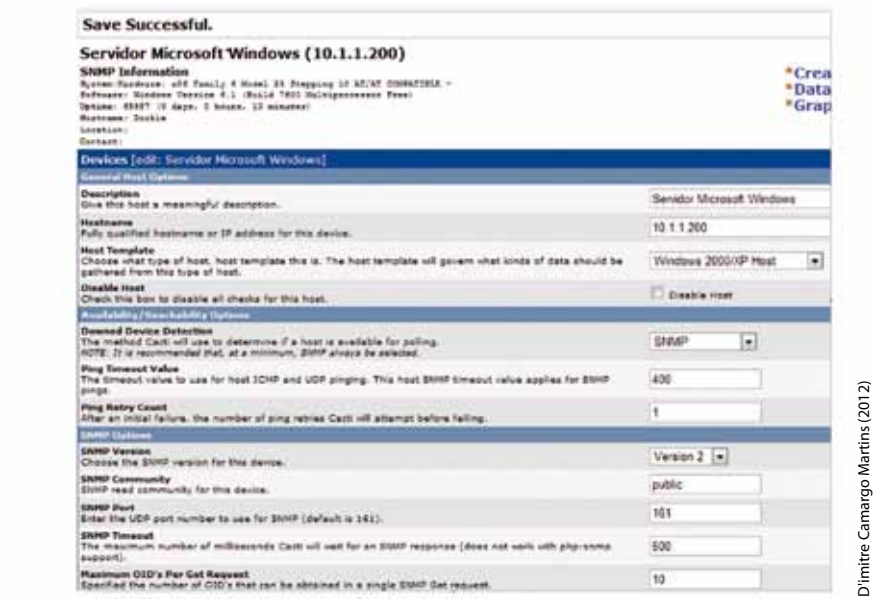
Figura 24 - Interface de administração do Cacti

UTILIZANDO O CACTI

A interface do Cacti é dividida em duas abas. A aba "Console", onde realizamos todas as configurações e a aba "Graphs", onde estão todos os gráficos gerados pelas informações coletadas. Logo após a instalação, o próprio servidor do Cacti já está sendo monitorado. Conforme a mensagem na página inicial sugere, para começar a utilizá-lo precisaremos basicamente cadastrar os demais equipamentos que desejamos monitorar, criar e configurar os gráficos para visualizá-los posteriormente, já com os dados coletados. Faremos isso por meio do menu "Management/Devices/Add". Informaremos uma descrição, o hostname ou endereço IP. Podemos optar por associar a um *template* (modelos de gráficos e itens de monitoramento), também selecionamos como o Cacti irá verificar se o equipamento está ativo (ping, SNMP) e as informações para coletas por meio de SNMP (versão, comunidade e porta). Ao salvar as definições, o Cacti verifica se houve conectividade com o equipamento cadastrado e exibe o resultado.

[9] LDAP

Lightweight Directory Access Protocol – protocolo da pilha TCP/IP utilizado na organização das informações da rede em forma de árvore de diretórios. Armazena informações como nomes dos usuários, senhas e permissões de acesso, computadores, etc.

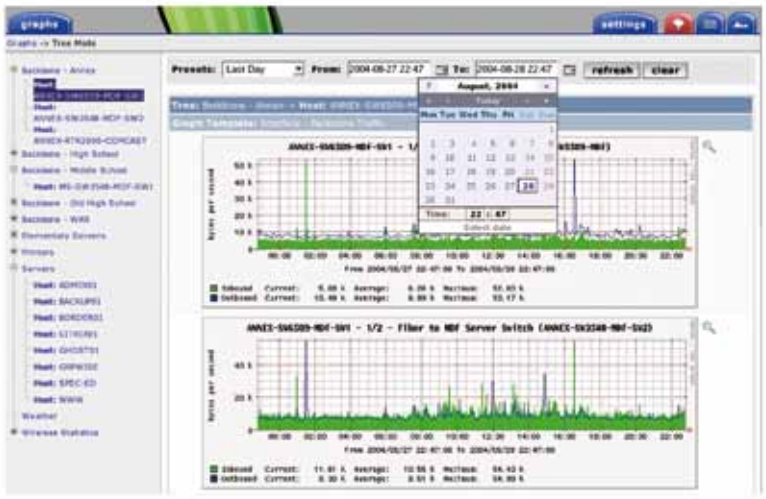


D'imitre Camargo Martins (2012)

Figura 25 - Tela para cadastro de equipamentos

Se não houve problema, será exibida uma mensagem indicando sucesso onde também já teremos um link para a configuração dos gráficos para o equipamento cadastrado. Ao optar por criar os gráficos, serão exibidos os diversos itens que foram identificados por meio do SNMP, como informações sobre os processadores, a memória, discos e partições, interfaces de redes, além de informações sobre usuários conectados na máquina e processos existentes. Selecionamos para quais desses itens queremos gerar gráficos e salvamos. Por fim, adicionamos o equipamento cadastro para ser exibido na árvore padrão de gráficos. Podemos criar uma árvore independente, dividindo por tipos de equipamentos, o que é uma boa prática quando existirem muitos equipamentos.

Visualizamos as árvores existentes por meio da aba "Graphs", na barra superior. É nesta aba que estarão todos os gráficos gerados. Podemos definir os intervalos de tempo aos quais as informações dos gráficos se referem. Podemos também optar por exibi-los em miniaturas, além da quantidade de gráficos que serão exibidos por página. No canto superior à direita, temos alguns botões pelos quais podemos definir como as informações serão exibidas, que podem ser no formato de árvore (padrão), em lista ou no modo *preview*. Para alterar permanentemente a forma como as informações serão apresentadas, utilizamos o botão "Settings".



D'imitre Camargo Martins (2012)

Figura 26 - Visualização dos gráficos no Cacti
Fonte: Cacti (2011)

O Cacti possui o recurso de importação e exportação de templates, com isso, templates criados em um servidor Cacti podem ser exportados para arquivos XML e depois importados em outro servidor Cacti, evitando o retrabalho de realizar todas as configurações novamente. Além da autenticação convencional, o Cacti disponibiliza outras duas formas de validação dos usuários. Uma é a autenticação baseada no servidor web, a outra, é baseada no LDAP[9] .

Para que essa última possa ser utilizada, o módulo LDAP para o PHP deve ser instalado com o comando "apt-get install php5-ldap". Ao término da instalação, o serviço web precisa ser reinicializado, para que as alterações entrem em vigor. Isso pode ser feito com o comando "/etc/init.d/apache2 reload". Posteriormente, alteramos o método de autenticação na aba "Console", através da opção "Configuration/Settings/Authentication".

4.3.2 *PLUGINS*

Como você já estudou, existe a possibilidade de adicionar *plugins* ao Cacti. O passo inicial para isso é instalar e configurar o "Plugin Architecture", que é pré-requisito para a utilização de outros *plugins*. Precisamos baixá-lo do site de *plugins* do Cacti. É importante fazer o download da versão correspondente à versão do servidor Cacti. Para instalar, descompactamos o arquivo em um diretório temporário com o comando "tar xvzf cacti-plugin-0.8.7g-PA-v2.8.tar.gz", depois copiamos o conteúdo do diretório correspondente à versão para o diretório onde o site do Cacti está armazenado, por exemplo "cp –R cacti-plugin-arch/files-0.8.7g/* /

usr/share/cacti/site/" e reinicializamos o servidor web. Por fim, instalamos os *plugins* de nosso interesse.

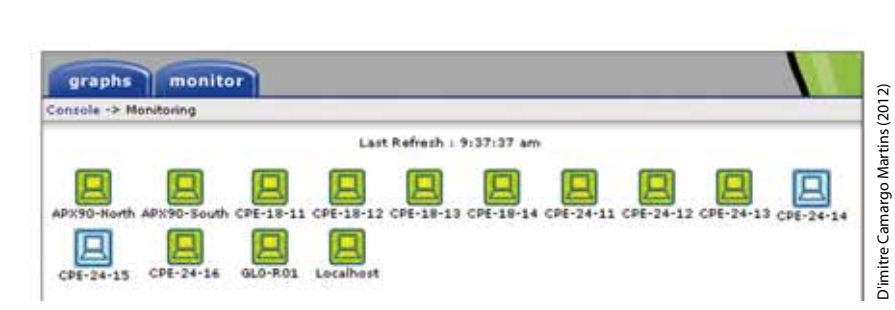
Vamos utilizar o *plugin* "Monitor" como exemplo. Baixamos no site de *plugins* e o descompactamos no diretório "plugins" do servidor Cacti. Para ativá-lo, editamos o arquivo "include/config.php" no servidor onde teremos:

```
$plugins = array();          – esta linha já existe e não precisa ser adicionada/alterada;

$plugins[ ] = 'monitor';     – esta linha foi adicionada para ativar o plugin Monitor.
```

Quadro 4 - Configurações no arquivo config.php do Cacti

Para cada *plugin* que instalamos, será criada uma nova aba na barra superior. Para que ela apareça, precisamos acessar configurações de cada usuário que terá acesso ao *plugin*, e liberar a visualização desta. Fazemos isso em "Utilities/User Management", então selecionamos a conta do usuário e, em "Realm Permissions" liberamos marcando a caixa "View Monitoring". Outra permissão que pode ser liberada é a de acesso gerenciamento de *plugins*, marcando a caixa "*Plugin* Management". Este item será disponibilizado juntamente com os demais itens do menu lateral, em "Configuration/Plugin Management".

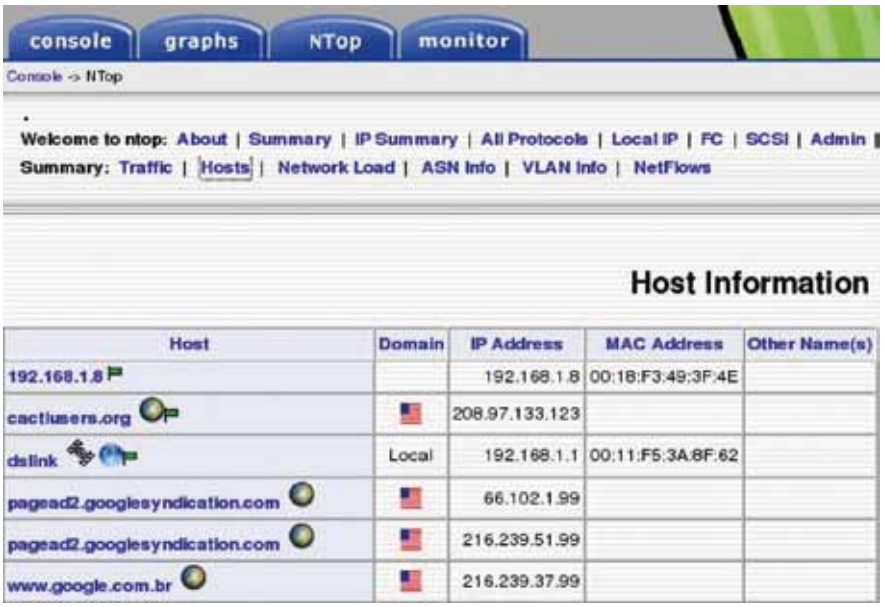


D'imitre Camargo Martins (2012)

Figura 27 - *Plugin* Monitor
Fonte: Networking with OpenBSD (2010)

Com este *plugin* podemos visualizar o *status* de todos os equipamentos que foram cadastrados no Cacti e identificar (pela cor) os que não estão operacionais (figura *Plugin* Monitor). Este é um *plugin* interessante quando a principal preocupação é com a disponibilidade dos equipamentos. Uma boa dica é conectar um televisor ou monitor grande e fixá-lo na parede da sala de TI para que todos os administradores da rede possam identificar rapidamente qualquer problema em um equipamento. Outro *plugin* interessante é o "Ntop", onde o objetivo é visua-

lizar a página de gerenciamento da ferramenta NTOP no *frame* principal do Cacti (figura a seguir). Isso é possível mesmo se o Cacti e o NTOP estiverem instalados em equipamentos distintos.



Júlia Pelachini Farias (2011)

Figura 28 - Acesso ao NTOP através da interface do Cacti

Com o *plugin* thold é possível criar alertas com base nas informações dos gráficos, além de possibilitar o envio de alertas sobre problemas de disponibilidade ou carga nos recursos. Para ativá-los, precisamos adicioná-los ao arquivo de configuração "include/config.php", conforme fizemos na instalação do *plugin* Monitor.

$plugins[ ] = 'ntop';	– esta linha foi adicionada para ativar o *plugin* Ntop;
$plugins[ ] = 'thold';	– esta linha foi adicionada para ativar o *plugin* Thold.

Quadro 5 - Linhas no arquivo config.php para ativação de *plugins*

[10] DHCP

Dynamic Host Configuration Protocol – protocolo do serviço de redes TCP/IP para a configuração automática dos parâmetros de rede dos hosts.

Júlia Pelachini Farias (2011)

Figura 29 - *Plugin* Thold para o Cacti
Fonte: Habrahabr [20--]

[11] SMTP

Simple Mail Transfer Protocol - protocolo da pilha TCP/IP utilizado para o envio de e-mails por meio das redes de computadores.

Terminamos aqui o estudo da ferramenta Cacti. Apesar de simples, ela possui bons recursos. A possibilidade de criar *plugins* faz com que ela seja capaz de realizar diferentes tipos de monitoramento. Basta que alguém crie um *plugin* para o que desejamos fazer. Vale a pena experimentar os diversos outros *plugins* existentes no site de *plugins* do Cacti, ou ainda, desenvolver os seus próprios.

[12] POP3

Post Office Protocol – terceira versão do protocolo da pilha TCP/IP utilizado para o gerenciamento de mensagens de correio eletrônico.

SAIBA MAIS

O site oficial do CACTI, para acessar a documentação, download da ferramenta, atualizações para desenvolvedores e informações sobre suporte é <http://www.cacti.net>

Para fazer o download dos plugins para o CACTI, além das instruções de configuração para uso destes, acesse <http://cactiusers.org>.

[13] IMAP

Internet Message Access Protocol – protocolo para o gerenciamento de mensagens de correio eletrônico. O acesso às mensagens é feito diretamente, sem a necessidade de baixá-las do servidor.

Viu só como essa ferramenta é interessante? A próxima que você conhecerá é a ferramenta NAGIOS. Continue atento!

4.4 O NAGIOS

[14] FTP

File Transfer Protocol - protocolo do serviço de redes TCP/IP para a transferência de arquivos.

O Nagios é outra ferramenta bastante popular de monitoramento de redes. Foi desenvolvido por Ethan Galstad e disponibilizado à comunidade em 1999, onde ainda tinha o nome de "NetSaint". Na ocasião, Nagios era o nome do projeto paralelo ao NetSaint que tratava exclusivamente do desenvolvimento de plugins. Devido a problemas com o registro da marca NetSaint, Ethan optou por utilizar o nome Nagios. O Nagios pode ser instalado em sistema Linux e outras variantes

do Unix. No site oficial pode ser encontrado um pacote do Nagios específico para sistema Windows, mas que é considerado um projeto paralelo, chamado de Nagwin.

VOCÊ SABIA?

Você sabia que o criador do Nagios já veio ao Brasil? Ele veio exclusivamente para o evento "Nagios World Conference Latin America" realizado em São Paulo, em abril de 2011. Este evento é realizado em diversos outros países do mundo.

O Nagios é escrito na linguagem C e é distribuído sob os termos da licença GPL versão 2, apesar de ter uma versão comercial, que conta com recursos adicionais, além do suporte (Nagios XI). Seu principal foco é no monitoramento de equipamentos e seus recursos, como CPU, memória, discos rígidos, etc., e também dos serviços de rede mantidos por estes, como DHCP[10], SMTP[11], POP312.

Para o acesso às mensagens, existe a necessidade de baixá-las do servidor para o equipamento local,IMAP[13], FTP[14], web, DNS[15], banco de dados, etc.

Conta ainda com o recurso de envio de alertas, o que pode ser feito por e-mail, SMS[16] ou pager. Praticamente todo o potencial do Nagios é baseado nos seus *plugins*, ou seja, utilizamos os *plugins* específicos para cada tipo de monitoramento que desejamos realizar.

Os próprios usuários podem desenvolver *plugins* para o Nagios, usando, para isso, linguagens como Bash[17], C[18], C#[19], Perl, Python[20], PHP, etc. As informações do gerenciamento pode ser armazenadas em um banco de dados (MySQL ou PostgreSQL), caso contrário, serão armazenadas em arquivos.

O desenvolvimento de aplicativos para integração com o Nagios foi tão grande que, atualmente, o nome do projeto foi alterado para "Nagios Core", o que faz referência ao sistema principal. No seu site podemos encontrar diversos programas adicionais para o Nagios Core, como interfaces web diferenciadas, utilitários de configuração, *plugins*, temas e aplicativos para dispositivos móveis. A figura a seguir refere-se à interface padrão do Nagios.

[15] DNS

Domain Name System – protocolo do serviço de redes TCP/IP para a tradução automática dos nomes de hosts em seus respectivos endereços IP.

[16] SMS

Short Message Service – serviço para a troca de mensagens de texto através de telefone, web ou sistemas móveis.

[17] BASH

Bourne Again Shell - interpretador de comandos para sistemas operacionais da família Unix.

[18] C

Linguagem de programação compilada criada por Dennis Ritchie em 1972, no AT&T Bell Labs.

[19] C#

Linguagem de programação orientada a objetos criada pela Microsoft em 2001.

[20] PYTHON

Linguagem de programação multiparadigma (interpretada, imperativa e orientada a objetos) criada por Guido van Rossum em 1991.

Júlia Pelachini Farias (2011)

Figura 30 - Interface do Nagios em sua página inicial

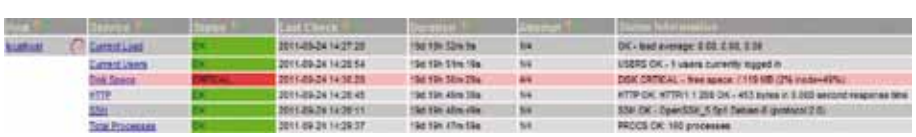
Agora, acompanhe como é feita a instalação e a configuração dessa ferramenta.

4.4.1 INSTALAÇÃO

Faremos a instalação do Nagios Core em um sistema Debian GNU/Linux. Para instalar o Nagios Core em um sistema Debian GNU/Linux, podemos utilizar o comando "apt-get install nagios3" (onde 3 refere-se à versão atual do Nagios).

Outra forma de realizarmos a instalação seria baixarmos os arquivos na página oficial e compilarmos o código fonte. Durante a instalação precisaremos informar a senha para o usuário administrador do Nagios (o usuário "nagiosadmin"), além do nome do grupo de trabalho do qual o servidor faz parte.

Ao término da instalação, já podemos acessar a sua interface gráfica, informando a URL <http://www.meuservidor.com.br/nagios3>, além de informar as credenciais de acesso (usuário "nagiosadmin" e senha conforme definida na instalação). Imediatamente após a instalação, o servidor Nagios entrará em funcionamento e já estará monitorando alguns itens do próprio servidor. Nas opções da interface, acessamos o item "Services" e teremos as informações referentes à carga do processador, número de usuários conectados, utilização das partições dos discos rígidos, status dos serviços em execução e o número total de processo em execução no servidor (figura a seguir).



Júlia Pelachini Farias (2011)

Figura 31 - Monitorando os serviços e os recursos de um servidor

CONFIGURAÇÃO

Um dos pontos fracos do Nagios refere-se à ausência de uma interface de configuração nativa. Tudo é feito editando diretamente os seus vários arquivos de configuração, o que, para usuários iniciantes, pode ser bastante complexo. Mesmo usuários experientes levam certo tempo até que se ambientem com a sintaxe dos arquivos. Na instalação que realizamos os arquivos de configuração principais estão no diretório "/etc/nagios3" e no subdiretório "/etc/nagios3/conf.d". Os arquivos de configuração são:

NOME DO ARQUIVO	DESCRIÇÃO/FUNÇÃO
cgi.cfg	Arquivo de configuração para o recurso de execução de comandos por meio da interface web do Nagios.
commands.cfg	Criação ou configuração dos comandos que podem ser utilizados, por exemplo, para o envio de alertas.
htpasswd.users	Arquivo com as contas e senhas (cifradas) dos usuários que terão acesso ao Nagios. Não editamos este arquivo diretamente. O cadastro de usuários é feito por meio do comando "htpasswd /etc/nagios3/htpasswd.users <usuário>".
nagios.cfg	O arquivo de configuração principal do Nagios.
resource.cfg	Configurações extras como o caminho de diretórios com *plugins* para o Nagios, diretivas para fontes de dados externas, etc.
contacts_nagios2.cfg	Arquivo de configuração referente ao envio de alertas (período, níveis de criticidade para envio de alertas, endereço de e-mail, grupo de contatos, etc.).
extinfo_nagios2.cfg	Configuração dos ícones utilizados na interface para cada equipamento que está sendo monitorado.
generic-host_nagios2.cfg	Template de um arquivo de configuração de equipamentos.
generic-service_nagios2.cfg	Template de um arquivo de configuração de serviços.
hostgroups_nagios2.cfg	Configuração de grupos de equipamentos, por exemplo, roteadores, switches, servidores Microsoft Windows, servidores Linux, etc.
localhost_nagios2.cfg	Arquivo de configuração do monitoramento do próprio servidor Nagios. Pode ser usado como modelo para a criação dos arquivos de configuração de outros equipamentos.

services_nagios2.cfg	Arquivo de configuração do monitoramento dos serviços do próprio servidor Nagios. Pode ser usado como modelo para a criação dos arquivos de configuração dos serviços de outros equipamentos.
timeperiods_nagios2.cfg	Definição dos períodos de checagem dos itens de monitoramento (dias da semana e os horários).

Quadro 6 - Principais arquivos de configuração do Nagios

Referente ao arquivo "extinfo_nagios2.cfg", é possível definir o posicionamento para a apresentação dos *hosts* na visualização na forma de mapa (figura a seguir). Com isso é possível ter uma boa visão no que se refere às conexões entre os *hosts*, além do tipo de sistema operacional, distribuição, fabricante, etc.

Dependendo da versão do Nagios podem existir outros arquivos de configuração, além dos mencionados. Cada *plugi*n também possui o seu arquivo de configuração. Na instalação que realizamos, esses arquivos estão presentes no diretório "/etc/nagios-plugins/config/" sendo que os *plugins* propriamente ditos estão no diretório "/usr/lib/nagios/plugins/".

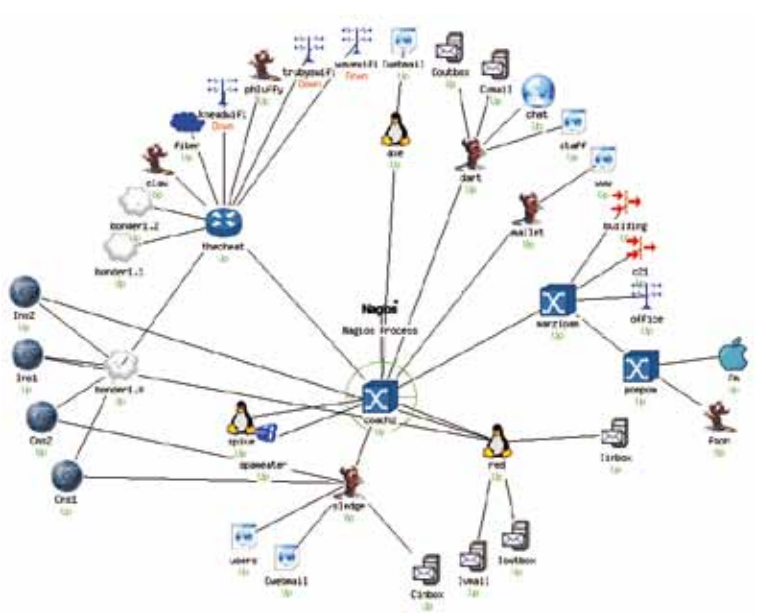


Figura 32 - Visualização dos equipamentos em forma de mapa
Fonte: Dcala´s Blog (2010)

Plugins são pequenos programas, que podem ser executados diretamente no terminal para realizarmos testes e validarmos a forma como o utilizaremos no Nagios. Para sabermos como devem ser executados, basta analisar a sintaxe no seu respectivo arquivo de configuração. Alguns possuem instruções de uso inclusas. Se executarmos o *plugin* sem parâmetros, serão exibidas instruções so-

bre os parâmetros mínimos necessários e a sintaxe. Quando executamos o *plugin* acrescentando o parâmetro "-h" ou "--help" (por exemplo:./check_ldap –h), são exibidas informações sobre os diversos parâmetros que podem ser passados para o *plugin* no momento da sua execução, desde os necessários até os opcionais (exemplo a seguir).

```
root@debian:/usr/lib/nagios/plugins# ./check_users
Usage: check_users -w <users> -c <users>

root@debian:/usr/lib/nagios/plugins# ./check_users -w 1 -c 2
USERS WARNING - 2 users currently logged in |users=2;1;2;0

root@debian:/usr/lib/nagios/plugins# ./check_ssh
Usage: check_ssh [-46] [-t <timeout>] [-r <remote version>] [-p <port>] <host>

root@debian:/usr/lib/nagios/plugins# ./check_ssh -4 -p 22 127.0.0.1
SSH OK - OpenSSH_5.5p1 Debian-6 (protocol 2.0)
```

Quadro 7 - Testando o funcionamento dos *plugins*

Vamos realizar o cadastro de um equipamento para que seja monitorado pelo Nagios. Criaremos um diretório com o nome de "datacenter" para armazenar os arquivos de configuração dos nossos servidores (comando: mkdir /etc/nagios3/conf.d/datacenter).

Neste diretório, criaremos dois arquivos de configuração, um para *hosts* (hosts_linux.cfg) e outro para serviços (services_linux.cfg), com as definições de como as checagens e notificações serão realizadas. A intenção é utilizar estes dois arquivos como modelos para todos os equipamentos e serviços cadastrados, com isso, não precisaremos definir essas informações em cada equipamento e em cada serviço que cadastrarmos. Posteriormente, no cadastro dos *hosts* e serviços, informamos que, além das informações específicas de cada *host* ou serviço, as definições contidas nestes arquivos devem ser utilizadas. Isso facilita o processo de configuração, além de diminuir o tamanho dos arquivos de configuração dos *hosts* e serviços.

Além destes dois arquivos, criaremos o arquivo de configuração do equipamento, além das definições de quais serviços queremos monitorar neste equipamento. Em nosso exemplo, cadastraremos um servidor Linux com o serviço de e-mail Postfix, sendo assim, iremos monitorar o serviço SMTP, utilizando o *plugin* "check_smtp" do Nagios. Para o cadastro do servidor criamos o arquivo "servidor_smtp.cfg".

ARQUIVO HOSTS_LINUX.CFG		ARQUIVO SERVICES_LINUX.CFG	
define host {		define service{	
name	*hosts*-linux	name	services-linux
notifications_enabled	.1	active_checks_enabled	1
event_handler_enabled	1	passive_checks_enabled	1
flap_detection_enabled	1	check_freshness	0
failure_prediction_enabled	1	notifications_enabled	1
process_perf_data	1	event_handler_enabled	1
retain_status_information	1	flap_detection_enabled	1
retain_nonstatus_information	1	failure_prediction_enabled	1
check_command	check-host-alive	process_perf_data	1
max_check_attempts	10	retain_status_information	1
notification_interval	0	retain_nonstatus_information	1
notification_period	24x7	notification_interval	0
notification_options	d,u,r	is_volatile	0
contact_groups	admins	check_period	24x7
register	0	normal_check_interval	5
}		max_check_attempts	4
		notification_period	24x7
		notification_options	w,u,c,r
		contact_groups	admins
		register	0
		}	

Quadro 8 - Exemplo de arquivos de configuração do Nagios

Em cada arquivo de configuração definimos um nome (linha "name") e, principalmente, períodos das checagens e do envio das notificações. Optamos por um monitoramento em tempo integral (24x7 quer dizer: 24 horas por dia, 7 dias por semana). Quando monitoramos um equipamento, o Nagios monitora o seu *status*, que pode ser:

a) **up**: o equipamento está ativo, ou seja, está acessível;

b) **down**: o equipamento não está acessível;

c) **unreachable**: o equipamento está inalcançável. Isso ocorre quando configuramos a hierarquia e, neste caso, deve haver um problema com o(s) equipamento(s) do qual este depende;

d) **pending**: a checagem está pendente, ou seja, o Nagios ainda não verificou o status do servidor. Isso ocorre normalmente após o cadastro de novos equipamentos.

Sendo assim, na linha "notification_options" (*hosts*) defiinimos que queremos ser notificados quando um *host* alterar o seu *status* para down (d), inalcançável (u) e quando retornar ao *status* up (r). No caso dos serviços, definimos valores para que o Nagios os classifique como:

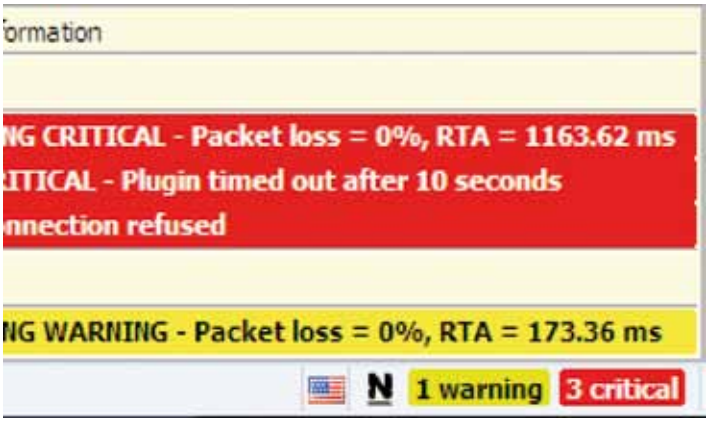
a) **warning**: o serviço está em estado de alerta, ou seja, está acessível, porém, pode haver algum problema, como sobrecarga, perda de pacotes, etc.;

b) **unknow**: o Nagios não consegue verificar o estado do serviço, o que pode ocorrer quando há um problema na configuração do *plugin*, ou o *plugin* não foi encontrado;

c) **critical**: o serviço está em estado crítico, onde geralmente está inacessível ou em uma condição que está praticamente inutilizável;

d) **recovery**: o serviço se recuperou de um problema e está acessível novamente.

O plugin Nagios Checker" para o Firefox, um indicador de estados dos eventos do Nagios exibe informações sobre *hosts* e serviços com problemas na barra inferior do navegador Firefox. Através dele é possível acessar diretamente as páginas do Nagios. Observe a figura a seguir.



Júlia Pelachini Farias (2011)

Figura 33 - *Plugin* "Nagios Checker" para o Firefox
Fonte: ADD-ONS [20--]

Na configuração dos serviços, definimos que queremos ser notificados quando um serviço estiver em estado de alerta (w), desconhecido (u), crítico (c) ou retornou ao funcionamento (r). Agora vamos o arquivo de configuração do equipamento propriamente dito onde, no mesmo arquivo, definimos quais serviços deste equipamento iremos monitorar (pode-se separar em dois arquivos). Criamos o arquivo de configuração do equipamento da seguinte forma:

[21] FIREWALL

Equipamento de rede composto por hardware e software que atua na filtragem do tráfego da rede. Um dos recursos mais utilizados para prover segurança às redes.

ARQUIVO MEUS_SERVIDORES.CFG

```
define host {
use             hosts-linux
host_name       servidor-x
alias           Servidor-X
address         10.1.1.21
parents         switchB1
}

define service {
use                     services-linux
host_name               servidor-x
service_description     SMTP
check_command           check_smtp!25!10!20
}
```

Quadro 9 - Arquivo de configuração dos servidores e serviços

Neste arquivo definimos o nome do servidor (host_name), uma descrição (alias), o seu endereço IP (address) e o nome do equipamento (switchB1) do qual ele depende para estar acessível (parents). Este é o nome do equipamento conforme foi cadastrado no Nagios. No mesmo arquivo configuramos o serviço que iremos monitorar. Definimos qual *host* responde pelo serviço (ele mesmo), a descrição do serviço (service_description) e o comando (plugin check_smtp) utilizado para verificar o estado do serviço. Os valores após o nome do *plugin* são os parâmetros exigidos por ele onde, 25 é o número da porta do SMTP, e os valores para que o tempo de resposta do serviço seja considerado como estado de alerta (10 segundos) ou estado crítico (20 segundos).

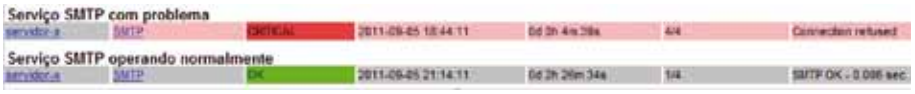
Para que o Nagios saiba utilizar os *plugins*, eles devem estar definidos no arquivo de "commands.cfg". O plugin "check_smtp" está definido da seguinte forma:

ARQUIVO COMMANDS.CFG

```
define command {
    command_name check_smtp
    command_line $USER1$/check_smtp –H $HOSTADDRESS$ -p $ARG1$ -w $ARG2$ -c $ARG3$}
```

Quadro 10 - Configuração do comando referente ao plugin check_smtp

Caso o serviço esteja com problema, o Nagios emitirá um alerta. Se for considerado apenas um alerta, a linha aparece na cor amarela, se for crítico, na cor vermelha e se não for identificado nenhum problema, na cor verde.



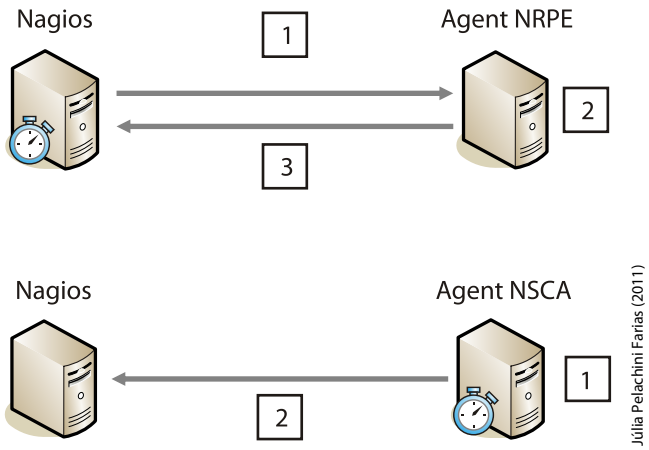
Júlia Pelachini Farias (2011)

Figura 34 - Monitoramento de serviços

OS PLUGINS NRPE E NSCA

O *Nagios Remote Plugin Executor* (NRPE) permite a execução de *plugins* remotos, ou seja, ao invés do Nagios executar os testes a partir do próprio servidor onde está instalado, ele faz isso executando o *plugin* diretamente na máquina que está sendo monitorada. Isso é interessante, pois, se quisermos monitorar serviços remotos a partir do servidor do Nagios, é preciso que as portas (TCP/UDP) desses serviços estejam liberadas no *firewall*[21] para que o Nagios consiga realizar a verificação. Com o NRPE, basta liberar uma porta utilizada pelo *plugin* (5666/tcp). O NRPE é dito como um serviço ativo, visto que o servidor Nagios interage com ele, ou seja, controla quando NRPE deve ser executado.

O *Nagios Service Check Acceptor* (NSCA) tem o mesmo objetivo, executar *plugins* remotamente, porém, o servidor do Nagios não interage com o serviço, por isso é dito como um serviço passivo. Ele é executado periodicamente conforme configurado. Após a execução as informações são enviadas ao servidor Nagios. A vantagem é que não precisam ser liberados acessos de um servidor externo do Nagios, visto que é o NSCA quem envia as informações, sendo assim, apenas o tráfego de saída precisa ser liberado (5667/tcp).



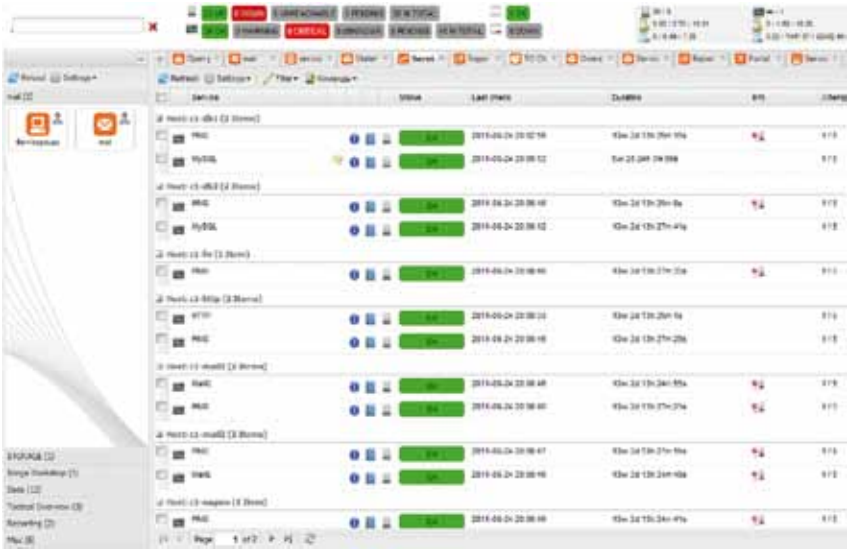
Júlia Pelachini Farias (2011)

Figura 35 - Funcionamento dos serviços NRPE e do NSCA

MAS AFINAL, O QUE É O ICINGA?

Insatisfeitos com a demora no lançamento de atualizações e novidades para o Nagios, parte da comunidade decidiu criar um projeto paralelo, batizado de Icinga. Ele nada mais é do que um *fork* do Nagios, ou seja, o código fonte do Nagios com algumas alterações.

Isso não é considerado ilegal, uma vez que o Nagios é distribuído sob a licença GPLv2, o que permite o acesso ao seu código fonte, modificação e redistribuição. Inclusive, muitos dos arquivos de configuração e *plugins* do Nagios funcionam normalmente no Icinga. Em um primeiro momento, o Icinga pode parecer uma ferramenta completamente diferente do Nagios, principalmente devido a sua interface, bastante diferente (figura a seguir).



Júlia Pelachini Farias (2011)

Figura 36 - Interface do Icinga
Fonte: Icinga [20--]

Aqui concluímos o estudo da ferramenta Nagios. Conforme verificamos, a sua configuração é bastante complexa, situação que pode ser contornada utilizando interfaces de configuração desenvolvidas pela comunidade, que não fazem parte do projeto Nagios. E ainda, a sua interface nativa pode ser melhorada com a instalação de temas.

SAIBA MAIS

Acesse a página oficial do Nagios e confira a vasta documentação, os código fonte e utilitários disponíveis, como frontends e plugins. Você pode, também, fazer o download. A página possui uma área destinada ao suporte comercial. Disponível em: <http://www.nagios.org>.

Na página do Icinga você pode fazer o download do código fonte ou de pacotes pré-compilados, além de acessar informações, conferir as formas de obter suporte e acessar páginas de demonstração. Confira! <http://www.icinga.org>.

Conheça, no item a seguir, outra ferramenta de gerenciamento de redes muito conceituada> o Zabbix.

4.5 O ZABBIX

O Zabbix é uma ferramenta de gerenciamento de redes que possui todas as funcionalidades encontradas no Cacti e no Nagios. É escrito na linguagem C, sendo que a sua interface de administração (web) é escrita na linguagem PHP. Foi desenvolvido por Alexei Vladishev, que o disponibilizou para utilização em 2001. É outra ferramenta gratuita, distribuída sob a licença GPL versão 2.

Dentre as ferramentas que estudamos neste capítulo, o Zabbix é uma das mais utilizadas. No Brasil, algumas instituições que utilizam o Zabbix são: Banco Central, Caixa, IBAMA, INEP, TCU e SERPRO. Alguns fatores que levam os administradores de redes a optar pelo Zabbix:

a) é considerado por muitos como uma das ferramentas mais completas no que diz respeito a funcionalidades;

b) é possível monitorar praticamente tudo que faça parte da rede (servidores, aplicações, switches, roteadores, access points, no breaks, etc.);

c) possui um mecanismo de autodescoberta de servidores e dispositivos de rede;

d) é possível armazenar as informações em diferentes tipos de bancos de dados (Oracle, SQLite, PostgreSQL DB2, e MySQL);

e) além do envio de alertas por e-mail, é possível configurar o envio de mensagens de texto via SMS e Jabber;

f) possui uma versão traduzida para o português (Brasil);

g) tem suporte às três versões do SNMP e ao IPv6;

h) é estável, ou seja, pouca ocorrência de problemas (*bugs*);

i) outro ponto forte é a quantidade e a qualidade da sua documentação, algo que é muito valorizado na área de TI como um todo;

j) possibilidade de criar perfis para acessos com diferentes permissões;

k) o seu desenvolvimento é bastante ativo. Isso é uma preocupação principalmente nos projetos de software livre;

l) possui uma comunidade bastante participativa, que contribui com a correção de erros e sugestões para novas funcionalidades.

Outro recurso interessante é o conceito de dependência onde, em uma situação com diversos servidores conectados a um switch, na ocorrência de um pro-

blema com o switch, os servidores ficarão inacessíveis. Se configurado para analisar as dependências, o Zabbix irá gerar somente um alerta, referente ao switch, e não irá um para cada servidor, visto que há problema com os servidores, mas estes dependem do switch para poderem ser acessados.

O servidor Zabbix pode ser instalado em sistemas Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD e OS X. No site oficial são encontradas versões pré-compiladas, conhecidas como *appliances*, dentre elas para os sistemas de virtualização VMware, Virtualbox e Xen. Estas são construídas utilizando o sistema OpenSuSE Linux e banco de dados MySQL. Já o agente, que é uma das formas para a coleta de informações nos equipamentos que serão monitorados, está disponível para sistemas Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X, Tru64/OSF1, Windows NT4.0, Windows 2000, Windows 2003, Windows XP e Windows Vista. O *download* do programa agente pode ser realizado no site oficial do Zabbix ou, no caso de sistemas Linux, normalmente está disponível nos repositórios de pacotes da própria distribuição.

4.5.1 COMPONENTES

A estrutura do Zabbix é composta por alguns componentes. Os componentes do servidor podem ser instalados em um mesmo computador, mas dependendo da quantidade de equipamentos que serão monitorados, por questões de desempenho, uma recomendação é instalar alguns componentes em máquinas diferentes. A estrutura completa é composta por:

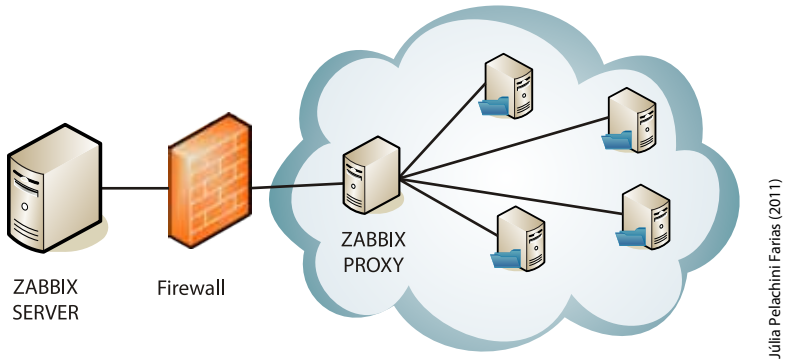
a) **Zabbix Server**: o servidor propriamente dito, sendo o principal componente. É a parte da ferramenta responsável pela coleta e processamento de todas as informações;

b) **Interface WEB**: é o componente por meio do qual, a partir de qualquer lugar, o analista da rede administra a ferramenta (*front-end*). É por meio dela que são realizadas as configurações e onde temos acesso aos dados de monitoramento. Este componente pode ser instalado em outro computador. Conforme consta na documentação do Zabbix, se o banco de dados utilizado for o SQLite, a interface web precisa ser instalada no mesmo computador onde será instalado o banco de dados;

c) **Agentes**: é o *software* que será instalado nos equipamentos que serão monitorados. Se a coleta for por meio do SNMP, o agente não precisa ser instalado, porém, ao instalar o agente em computadores, inúmeros itens do equipamento podem ser monitorados, entre eles, informações detalhadas dos discos rígidos, memórias e processadores. É possível inclusive utilizar tanto o agente como o SNMP para coletar informações de um mesmo equipamento. No caso de ativos de rede, como switches, roteadores, no breaks e

acess points, como não é possível realizar a instalação do agente, a coleta só poderá ser feita pelo SNMP;

d) **Zabbix Proxy**: este é um componente opcional do Zabbix. É utilizado principalmente para monitoramento de grandes redes, inclusive sites remotos. A sugestão é instalar o Zabbix Proxy em cada site remoto que realizará as coletas. Estes, por sua vez, farão o envio das informações ao servidor central (Zabbix Server), distribuindo a carga do processamento das informações. Este recurso é útil ao monitorar sites remotos, pois, além do já exposto, como possivelmente tais sites terão firewall, não será preciso liberar a comunicação de todas as máquinas da rede com o Zabbix Server. Basta liberar a comunicação do Zabbix Proxy (figura a seguir).



Júlia Pelachini Farias (2011)

Figura 37 - Uma das vantagens de se utilizar o Zabbix Proxy
Fonte: Zabbix [20--]

INSTALAÇÃO DO SERVIDOR ZABBIX

A instalação do Zabbix em sistemas Linux pode ser realizada por meio da compilação do seu código fonte (disponível no site oficial) e, no caso das distribuições que possuem repositórios de pacotes, basta utilizar os comandos apropriados. Em um servidor com sistema Ubuntu Server, usaremos o comando "apt-get install zabbix-frontend-php zabbix-server-mysql". Neste caso estaremos utilizando o banco de dados MySQL e não será utilizado o Zabbix Proxy, que como você já estudou, é opcional. Durante a instalação, será solicitado que sejam informados o nome da base dados (onde todas as informações do Zabbix serão armazenadas), além das credenciais de acesso a essa base que será criada (usuário e senha).

CONFIGURAÇÕES INICIAIS

Após a conclusão da instalação dos pacotes, a próxima etapa é a de configuração, e será realizada por meio da sua interface de administração web. Para isso,

informaremos no navegador o endereço do servidor seguido de "/zabbix" (por exemplo, <http://www.meuservidor.com.br/zabbix>). Após carregar a página será preciso informar as credenciais de acesso que são: usuário "Admin" e senha "zabbix". É altamente recomendável alterar a senha, pois, é uma senha padrão para toda instalação do Zabbix. Um usuário na rede, sabendo da existência do servidor e conhecendo a ferramenta, conseguiria acessá-la com permissões totais (administrador). É comum que no primeiro acesso a ferramenta apresente alguns itens em vermelho, com orientações de configurações que devem ser realizadas para o seu correto funcionamento. Tais configurações são feitas no arquivo de configuração do PHP (linguagem na qual o Zabbix é escrito). O local do arquivo depende do sistema utilizado. No nosso exemplo é "/etc/php5/apache2/php.ini". As alterações a serem feitas neste arquivo são:

date.timezone = America/Sao Paulo	– Definições do fuso horário. Depende da região do país.
post_max_size = 16M	– Tamanho máximo permitido de dados enviados.
max_execution_time = 300	– Tempo máximo em que um código será executado até ser finalizado (em segundos).
max_input_time = 300	– Tempo máximo permitido para análise dos dados de entrada, como em upload de arquivos (em segundos).

Quadro 11 - Alterações necessárias no arquivo de configuração do PHP

Com isso, estamos com o Zabbix corretamente instalado. A partir daí, precisamos configurá-lo para as nossas necessidades, ou seja, cadastrar os equipamentos que desejamos monitorar. Lembre-se de instalar o agente (quando necessário), o que veremos como fazer, a seguir. Além disso, é importante realizar diversas outras configurações, conforme veremos em seguida.

Júlia Pelachini Farias (2011)

Figura 38 - Após o login, a tela inicial do Zabbix

INSTALAÇÃO DO AGENTE ZABBIX

A partir do momento que o servidor Zabbix está operacional, começamos a preparação dos equipamentos que serão monitorados. No caso de um equipamento de rede (switch, roteador, etc.), basta configurar o SNMP (conforme estudado no capítulo 2). No caso de um servidor, precisaremos instalar o agente do

Zabbix, e no caso de um servidor Debian GNU/Linux, o comando que realiza a instalação é "apt-get install zabbix-agent".

Concluída a instalação, precisamos configurar o agente. A principal configuração consiste em definir o endereço do servidor Zabbix, ou seja, para qual endereço as informações coletadas pelo agente serão enviadas. No equipamento que instalamos, o arquivo de configuração do agente do Zabbix é "/etc/zabbix/zabbix_agentd.conf". Poucas linhas precisam ser alteradas.

Server=172.20.13.254	– O endereço IP do servidor Zabbix para envio das informações;
ServerPort=10051	– Define a porta na qual o servidor recebe as conexões (padrão);
ListenPort=10050	– Define a porta na qual o agente recebe as conexões (padrão);
ListenIP=127.0.0.1	– O endereço IP no qual o agente recebe conexões do servidor.

Quadro 12 - Alterações necessárias no arquivo de configuração do agente do Zabbix

Podemos instalar o agente no próprio servidor do Zabbix e então monitorar os seus recursos. Podemos monitorar inclusive o banco de dados MySQL que está sendo utilizado pelo servidor para armazenar todas as informações. No mesmo arquivo de configuração constam outras linhas que utilizaremos para isso. Tais linhas possuem o caractere "#" no início. Esse caractere faz com que tais configurações não sejam interpretadas, ou seja, o mesmo que se elas não estivessem no arquivo. Basta remover este caractere e informar a senha do banco de dados, que foi definida durante a instalação (com a opção –p senha). Confira o exemplo no quadro a seguir.

```
UserParameter=mysql.ping,mysqladmin -uroot –p zabbix ping|grep alive|wc -l
UserParameter=mysql.uptime,mysqladmin -uroot –p zabbix status|cut -f2 -d":"|cut -f1 -d"T"
UserParameter=mysql.threads,mysqladmin -uroot –p zabbix status|cut -f3 -d":"|cut -f1 -d"Q"
UserParameter=mysql.questions,mysqladmin -uroot –p zabbix status|cut -f4 -d":"|cut -f1 -d"S"
UserParameter=mysql.slowqueries,mysqladmin -uroot –p zabbix status|cut -f5 -d":"|cut -f1 -d"O"
UserParameter=mysql.qps,mysqladmin -uroot –p zabbix status|cut -f9 -d":"
UserParameter=mysql.version,mysql -V
```

Quadro 13 - Monitorando o banco de dados MySQL

Sempre que realizar alterações em arquivos de configuração, é preciso reinicializar o serviço que foi alterado. Isso é necessário para que as novas configurações entrem em vigor. No nosso servidor faremos "/etc/init.d/zabbix-agent restart". Assim que o agente se conectar ao servidor, já teremos diversas informações sobre o equipamento (veja a figura anterior). Ao concluir a instalação do agente

e a configuração do SNMP nos equipamentos, passamos a administrar o Zabbix por meio da sua interface web.

Júlia Pelachini Farias (2011)

Figura 39 - Informações que foram coletadas sobre o equipamento

Mas, como iremos utilizar o Zabbix? Será que é fácil? Essas perguntas, e muitas outras, serão respondidas a seguir. Acompanhe.

UTILIZANDO O ZABBIX

Até aqui preparamos o nosso sistema de monitoramento com Zabbix, agora precisamos começar a coletar as informações e gerar os relatórios e gráficos. Todas as configurações são feitas por meio da barra de opções no topo da interface web. São cinco grupos de opções onde, para cada grupo, diferentes itens de configuração estão disponíveis. Os cinco grupos (botões) principais são:

a) **Monitoring:** onde estão disponíveis todas as informações coletadas dos equipamentos da rede. Quando tudo estiver configurado, este será o grupo que mais utilizaremos;

b) **Inventory:** onde podemos cadastrar informações dos equipamentos da rede, como número serial, mac address, sistema operacional, localização, patrimônio, etc. Na versão estável atual (1.8) isso é feito manualmente (o que faz ser pouco utilizado) porém, no site oficial consta que na próxima versão (2.0), o Zabbix terá a capacidade de realizar o inventário automatizado;

c) **Reports:** acesso aos relatórios de monitoramento da rede;

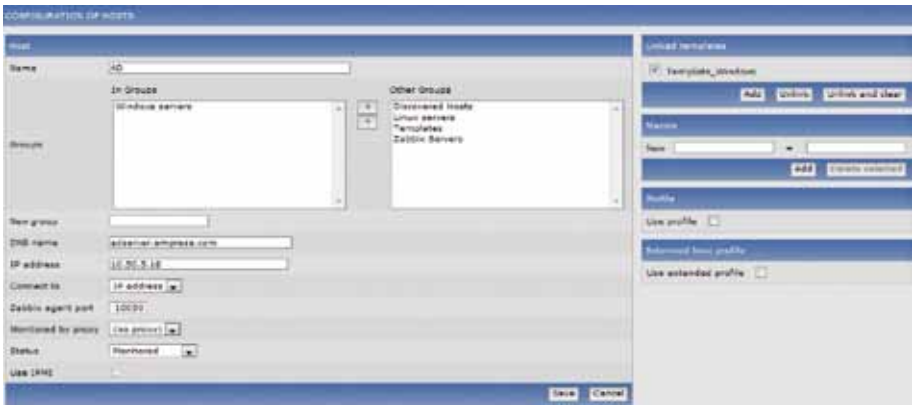
d) **Configuration:** onde são realizadas as configurações, como cadastro dos equipamentos, configuração dos gráficos, templates, mapas, parâmetros para o discovery, importação e exportação de informações, etc;

e) **Administration:** onde gerenciamos as contas de acesso ao Zabbix, assim como as permissões de acesso, o modo de autenticação (dentre elas LDAP), as formas de envio de alertas, etc.;

VOCÊ SABIA?

Além do acesso via navegador, existem aplicativos para *iPhone* e *smartphones* com sistema Android por meio dos quais temos acesso ao servidor Zabbix. Em "Administration/Users" cria-se o usuário no grupo "API Access". No aplicativo utilizado, informamos as credenciais de acesso e o endereço do servidor.

Começamos a configuração cadastrando os equipamentos. Nestes, previamente, instalamos os agentes e/ou configuramos o SNMP. Em "Configuration/ Hosts" realizamos o cadastro de diversos itens como, *hosts*, templates, gráficos, triggers, etc. Neste momento, utilizamos o botão "Create Host" (figura a seguir).



Júlia Pelachini Farias (2011)

Figura 40 - Tela de cadastro de equipamentos

Primeiro precisamos informar um nome para o equipamento. Podemos adicioná-lo a um grupo onde normalmente temos grupos de equipamentos com características semelhantes, por exemplo, servidores Microsoft Windows, servidores Linux, switches, roteadores, etc.

É recomendável utilizar os grupos, principalmente quando são muitos equipamentos, pois posteriormente, você pode aplicar configurações ou visualizar as informações de todos os equipamentos de um mesmo grupo, facilitando a administração. É preciso informar também o seu nome, conforme cadastrado no DNS

[22] IPMI

Intelligent Platform Management Interface – tecnologia que permite a administração e monitoramento dos computadores remotamente.

da rede, o seu endereço IP, o modo de conexão (pelo nome DNS ou endereço IP), a porta do agente Zabbix, conforme configurado na instalação do agente (o padrão é 10050), e se as informações serão enviadas para o Zabbix Proxy (quando existir). Por fim, definimos se queremos começar a monitorar o equipamento imediatamente após o cadastro e se o equipamento tem suporte ao IPMI[22].

Outro recurso interessante é associar o equipamento a um template (modelo), que contém pré-definições de itens a serem monitorados no equipamento, ações a serem tomadas na ocorrência de certos eventos (triggers), além de gráficos. É um recurso excelente, pois reduz drasticamente o trabalho que o administrador do Zabbix teria para configurar todos esses itens manualmente. O Zabbix já traz diversos templates, mas podemos criar outros. Uma vez que o template existe, podemos utilizá-lo com todos os equipamentos que possuem as mesmas características. Ao término da configuração, utilizamos o botão "Save" para que o equipamento seja cadastrado.

Confira, na figura a seguir, o aplicativo Zabbix para *smartphones*.

Júlia Pelachini Farias (2011)

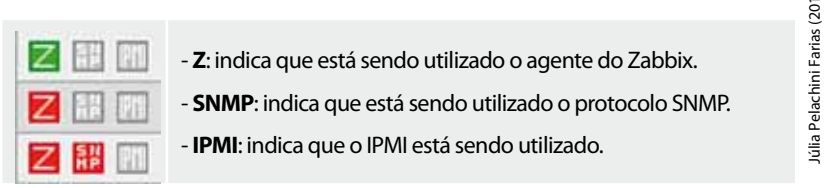
Figura 41 - Aplicativo Zabbix para *smartphones*
Fonte: Mozaby (2011)

VOCÊ SABIA?

Você pode gerenciar um computador, remotamente, por meio do IPMI. Ele monitora diversos itens da máquina como temperatura, ventoinhas, tensão e intrusão ao chassi. Você pode, inclusive, ligar e desligar este computador por meio da rede. Basta que a placa-mãe do equipamento tenha este recurso. O IPMI independe do sistema operacional.

Após o cadastro de todos os equipamentos, além das informações definidas no momento do cadastro, o Zabbix possui uma coluna referente à disponibilidade do equipamento, ou seja, se o equipamento está enviando as informações coletadas ao servidor.

Confira os três ícones e o que eles representam.



Júlia Pelachini Farias (2011)

Figura 42 - Ícones representando o tipo de estado do agente

De acordo com a cor do ícone, podemos identificar se existe um problema de comunicação do equipamento com o servidor. As cores apresentadas são:

a) **verde**: de acordo com o ícone, significa que, por meio daquele método de comunicação que foi configurado, o equipamento tem conectividade com o servidor;

b) **vermelho**: de acordo com o ícone, significa que, por meio daquele método de comunicação que foi configurado, o equipamento não tem conectividade com o servidor;

c) **cinza**: de acordo com o ícone, significa que, aquele método não foi configurado como uma forma de comunicação entre o servidor e o equipamento.

Agora chegou a hora de criar os "Screens", que são um conjunto de informações coletadas. Em "Configuration/Screen" utilizaremos o botão "Create Screen". Definimos um nome e a quantidade de linhas e colunas, dependendo da quantidade de informações que teremos, ou seja, criando um screen com duas linhas e duas colunas, teremos quatro áreas para exibir informações como gráficos, mapas, informações em texto, URL´s, entre outros. Isso é definido após cadastrar o screen e acessar as suas propriedades.

Nas quatro áreas temos a opção "Change". Por meio dessa opção, escolhemos na opção "Graph", o equipamento e o gráfico deste que queremos que faça parte do screen, além do tamanho e alinhamento. Precisaremos definir essas informações nas quatro áreas do screen. Depois de definidos, visualizaremos o screen no caminho "Monitoring/Screens".

Em "Configuration/Hosts/Triggers" definimos os valores aceitáveis para os itens que estamos medindo, por exemplo, o valor máximo aceitável para o uso de memória no equipamento. Baseado nisso, definimos a severidade e as ações a

serem tomadas pelo Zabbix. Caso tais valores sejam atingidos ou ultrapassados, é enviado um e-mail de alerta para o administrador da rede.

Em "Administration/Media Types" configuramos as diferentes formas de envio dos alertas. Posteriormente, em "Administration/Users", para cada usuário, definimos a forma como este será alertado, o período em que os alertas serão enviados e selecionamos quais tipos de severidades devem ser enviadas. No caso de termos mais servidores do Zabbix, podemos exportar ou importar configurações por meio da opção "Configuration/Export/Import", o que possibilita você replicar configurações já realizadas para outros servidores. Isso nos permite reduzir bastante o trabalho de configuração do Zabbix.

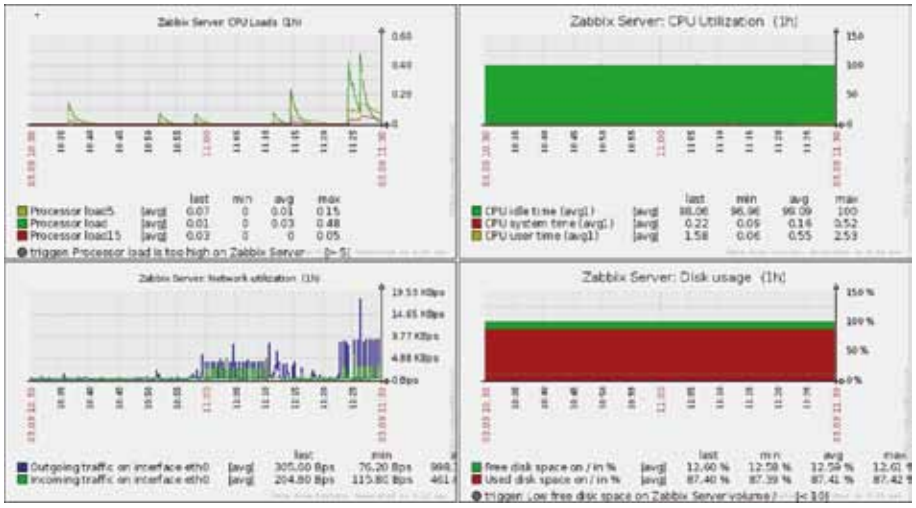


Figura 43 - *Screen* com quatro gráficos

Para entender melhor esse assunto, acompanhe o relato de um caso que você pode encontrar pela frente no dia a dia da sua função.

CASOS E RELATOS

O uso de diferentes ferramentas para a criação de uma central de monitoramento

Cláudio é administrador da rede de uma média empresa e estava parcialmente satisfeito com a sua ferramenta de monitoramento de rede. Ele utilizava o MRTG e conseguia acompanhar, quase que em tempo real, o consumo da banda do enlace para acesso à Internet. Porém, quando os gráficos acusavam um consumo excessivo, Cláudio não conseguia identificar o motivo. Ele pedia aos usuários que não abusassem, mas ninguém respeitava.

Pesquisando por formas de identificar os causadores do problema, Cláudio encontrou relatos de administradores que utilizavam outras ferramentas, e resolveu testá-las. Percebeu que com o NTOP, ele conseguia identificar não só os usuários, mas também os tipos de tráfego que estavam sobrecarregando o enlace. Como o MRTG não enviava alerta nessas ocorrências, ele aproveitou para substituí-lo pelo Zabbix, onde conseguia gerenciar não só os enlaces, como também todos os servidores, os serviços em cada um deles, as impressoras, no breaks e access points.

Cláudio configurou o envio de alertas por SMS e, mesmo quando estava ausente da sua sala, ficava sabendo da ocorrência dos problemas quase que imediatamente. Os usuários da rede passaram a respeitá-lo, pois Cláudio conseguiu controlar o uso dos recursos da rede.

Você conheceu essa incrível ferramenta de gerenciamento de rede que é o Zabbix. Não deixe de explorar os demais recursos que ela oferece. Um administrador de rede estará muito bem preparado para gerenciar a rede se souber aproveitar de suas múltiplas funcionalidades. Confira a mensagem da equipe no site oficial sobre o Zabbix, que é uma ferramenta extremamente profissional e confiável.

> Nossos objetivos são o de desenvolver uma solução de monitoramento excepcional e fornecer suporte ágil e confiável para resolver quaisquer problemas quanto à sua instalação, operação e utilização.
>
> (ZABIXX, 2011)

Para conhecer melhor o Zabbix, acesse os sites indicados a seguir. No Zabbix você encontra uma vasta documentação, além de diversos artigos em diferentes línguas. É onde pode ser obtido o código fonte do Zabbix, ter informações sobre suporte e sobre treinamentos a respeito do Zabbix. Site do Zabbix: <http://zabbix.com>.

Já no site da comunidade brasileira de usuários do Zabbix, é onde temos acesso a diversos documentos em português sobre o Zabbix, além de notícias e casos de sucesso de uso do Zabbix no Brasil. Acesse: <http://zabbixbrasil.org>.

Zabbix para *smartphone*. Sites onde podem ser encontrados aplicativos para dispositivos móveis para acesso ao servidor Zabbix. Disponíveis em: <https://market.android.com/search?q=zabbix&so=1&c=apps>; <http://www.mozaby.com>; <http://www.mozbx.net>.

Fórum oficial do Zabbix, área destinada aos usuários do Zabbix para troca de informações, resolução de problemas e compartilhamento de arquivos. Disponível em: <http://www.zabbix.com/forum>.

4.6 OPENNMS

A próxima ferramenta que você estudará é o OpenNMS. Também é gratuito e distribuído sob a licença GPL. É escrito em Java e começou a ser distribuído no ano 2000. A proposta do projeto é que ele não seja somente mais uma ferramenta de monitoramento, mas uma plataforma de gerenciamento completa, baseada no modelo FCAPS, além de ser estruturada para monitorar grandes quantidades de equipamentos (algo em torno de cem mil máquinas). Todos os dados são armazenados em um banco de dados PostgreSQL.

O OpenNMS conta com recursos interessantes, como a descoberta automática de equipamentos e serviços, monitoração adaptativa, definição de janelas de manutenção, execução automática de comandos baseada em eventos, além do comum nesse tipo de ferramenta, como geração de relatórios, gráficos, criação de perfis com diferentes permissões de acesso, suporte ao SNMP, envio de notificações, etc. No site do projeto está disponível o cliente do OpenNMS para dispositivos móveis (iPhone, iPad e iPod Touch), com isso, o administrador pode visualizar o estado dos equipamentos diretamente de um celular, por exemplo.

4.6.1 INSTALAÇÃO

Antes da instalação, podemos fazer a avaliação por meio de uma versão de demonstração, disponível no site do projeto, onde podem ser obtidos os pacotes para instalação em sistemas GNU/Linux, Solaris, BSD, Microsoft Windows e Mac

OSX. Para uma instalação em sistemas Linux, podemos optar pela compilação do código-fonte ou pela instalação dos pacotes pré-compilados. Entre eles, estão disponíveis pacotes em formato RPM (Red Hat, CentOS, Fedora, etc.) e DEB (Debian, Ubuntu, etc.). Os pré-requisitos para o funcionamento do OpenNMS são:

a) **Java**: máquina virtual Java (JVM) para execução da aplicação;

b**) PostgreSQL**: banco de dados;

c) **RRDtool**: geração dos gráficos.

Acompanhe as informações de como é a instalação no sistema Debian GNU/Linux. Uma vez que os repositórios oficiais do Debian não tenham os pacotes do OpenNMS, precisaremos adicionar o repositório extra, do mantido pelo próprio projeto do OpenNMS, na listas de repositórios do APT. Para isso, adicionamos as seguintes linhas no arquivo "/etc/apt/sources.list".

```
deb http://debian.opennms.org stable main

deb-src http://debian.opennms.org stable main
```

Quadro 14 - Adicionando os repositórios do OpenNMS no APT

Após acrescentarmos essas linhas, é preciso obter a nova lista de pacotes conhecidos, mas, para que isso seja possível, antes precisamos importar as chaves PGP[23] do repositório do OpenNMS, uma vez que o APT utiliza criptografia para garantir a integridade dos pacotes. Para isso utilizamos o comando:

```
wget –O – http://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add –
```

Quadro 15 - Adicionando as chaves PGP do repositório do OpenNMS

Agora já é possível obter a nova lista de pacotes dos repositórios utilizados com o comando "apt-get update". Para a instalação utilizamos o comando "apt-get install opennms" onde todas as dependências foram automaticamente tratadas, inclusive o banco de dados PostgreSQL. Alguns ajustes precisam ser feitos na configuração deste. Primeiro liberamos o acesso sem senha do próprio servidor ao banco de dados, alterando as seguintes linhas do arquivo que contém as definições de permissões de acesso, o arquivo "/etc/postgresql/8.4/main/pg_hba.conf":

[23] PGP

Pretty Good Privacy) – programa criado por Phil Zimmermann para a criptografia de arquivos e e-mails.

ANTES					DEPOIS				
local	all	all		ident	local	all	all		trust
host	all	all	127.0.0.1/32	md5	host	all	all	127.0.0.1/32	trust
host	all	all	::1/128	md5	host	all	all	::1/128	trust

Quadro 16 - Liberando o acesso ao banco de dados

Após salvarmos, reinicializamos o serviço do PostgreSQL para que as alterações entrem em vigor, com o comando "/etc/init.d/postgresql restart". Agora criamos e exportamos as variáveis de ambiente necessárias ao funcionamento do OpenNMS. Faremos isso adicionando as seguintes linhas no final do arquivo /etc/profile:

```
export JAVA_HOME=/usr/lib/jvm/java-6-openjdk/jre

export OPENNMS_HOME=/usr/share/opennms
```

Quadro 17 - Definição das variáveis de ambiente

Na sequência, criamos o banco de dados onde o OpenNMS irá armazenar as informações e executamos o script para a instalação do procedimento de armazenamento IPLIKE, com os respectivos comandos:

```
su - postgres -c "createdb -h localhost -U postgres -E UNICODE opennms"

su - postgres -c "/usr/sbin/install_iplike.sh"
```

Quadro 18 - Criando o banco de dados e execução do script do IPLIKE

Para finalizar a configuração inicial, verificamos o funcionamento do Java e executamos o processo de configuração do OpenNMS onde, entre outras definições, as tabelas no banco de dados serão criadas:

```
/usr/share/opennms/bin/runjava –s

/usr/share/opennms/bin/install -dis
```

Quadro 19 - Comandos para a configuração inicial do OpenNMS

Ao término do processo, se todas as etapas foram executadas corretamente, será exibida uma mensagem informando que a instalação foi realizada com sucesso. Com isso, podemos iniciar o serviço do OpenNMS com o comando "/etc/init.d/opennms start", e então passaremos a utilizá-lo a partir da sua interface web.

No navegador, informamos a URL <http://www.meuservidor.com.br:8980/opennms>. Para o primeiro acesso, informamos o usuário "admin" e senha "admin" (usuário e senha padrão em uma nova instalação) e então estaremos prontos para utilizá-lo.

Figura 44 - OpenNMS após a autenticação

UTILIZANDO O OPENNMS

Primeiro iremos alterar a senha do usuário "admin". Na barra superior à direita, ao lado da opção de log out, com um clique no nome do usuário e na sequência o botão "Change Password", informamos a senha atual (admin) e uma nova senha mais forte. O cadastro de equipamentos pode ser feito de diferentes formas. Um método interessante é o uso do autodescobrimento de *hosts* e serviços. Para isso, selecionamos a opção "Admin" onde, na seção "Operations", temos a opção "Configure Discovery".

Dentre as opções, podemos informar o endereço de um *host* específico ou um range, onde todos os *hosts* existentes neste segmento serão detectados automaticamente, assim como os respectivos serviços em execução nestes. Após informarmos o range (figura a seguir), selecionamos o botão "Save and Restart Discovery" para que o OpenNMS comece a explorar a rede informada.

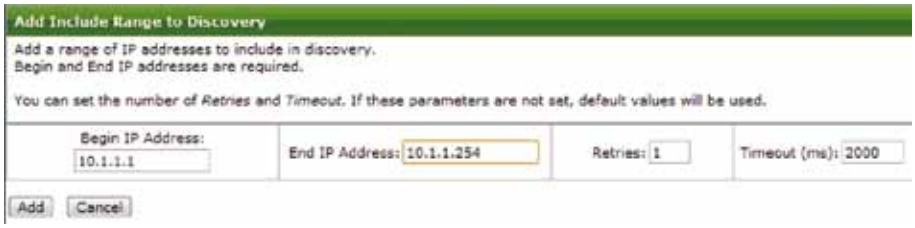


Figura 45 - Cadastro de um range de endereços IP

Com a lista de *hosts* gerada, é possível organizar os equipamentos encontrados em grupos, como por exemplo, roteadores, switches, servidores de produção, servidores de homologação, etc. O OpenNMS passará a monitorar tais equipamentos em intervalos de cinco minutos. O motivo de utilizar este intervalo é o de verificar se o índice de disponibilidade está dentro da taxa de 99,99% (o que caracteriza uma indisponibilidade de 4,32 minutos no mês). Essa taxa de tolerância na disponibilidade pode ser alterada, conforme necessidades da empresa.

Veja um exemplo de relatório de item monitorado.

Availability Over the Past 24 Hours

Categories	Outages	Availability
Network Interfaces	7 of 46	81.935%
Web Servers	9 of 29	68.213%
Email Servers	2 of 28	92.857%
DNS and DHCP Servers	2 of 4	50.000%
Da	2 of 4	44.111%
JM	0 of 0	100.000%
MobileMe Servers	0 of 28	99.979%
Other Servers	4 of 21	77.799%
Total	**Outages**	**Availability**
Overall Service Availability	27 of 139	78.487%

This category includes all managed interfaces which are running either DNS (name resolution) servers or DHCP servers.

Figura 46 - Taxas de disponibilidade de cada item monitorado
Fonte: OpenNms (2011)

O OpenNMS pode monitorar os equipamentos de diferentes formas, como: por meio do SNMP, ICMP[24], testes em serviços, como DNS, HTTP, SSH, etc., testes em URL´s, utilizar *plugins* do Nagios e o serviço WMI (*Windows Management Instrumentation*), utilizado para administração de equipamentos com Microsoft Windows.

Na ocorrência de qualquer problema, o OpenNMS pode notificar o administrador de diferentes formas, como envio de e-mail, SMS, IRC[25], XMPP[26] e até mesmo por telefone. Ele também permite a definição de parentesco entre os *hosts*, para que, na ocorrência de um problema com um equipamento do qual outros equipamentos dependem para funcionar, o OpenNMS envie somente uma notificação, reportando a ocorrência com o host mais alto da hierarquia de parentesco.

Se a empresa possui filiais, o OpenNMS permite a utilização de mapas. Com isso, o administrador pode importar uma imagem do mapa do mundo, ou ainda do país, estado ou cidade, dependendo da localização física das filiais. Com a imagem, o administrador pode posicionar ícones no mapa referente a cada filial, ou referente a cada host ou serviço. É útil quando se tem a disposição monitores grandes, para que toda a equipe tenha a visibilidade do estado da rede.

Veja, a seguir, exemplos de gráficos estatísticos exibidos no OpenNMS.

[24] ICMP

Internet Control Message Protocol – protocolo da pilha TCP/IP utilizado nos testes de comunicação através do envio de mensagens entre os equipamentos.

[25] IRC

Internet Relay Chat – protocolo de comunicação (bate-papo) utilizado na Internet.

[26] XMPP

Extensible Messaging and Presence Protocol – protocolo baseado em XML para sistemas de mensagens instantâneas. Utilizado pelo Google Talk e Facebook.

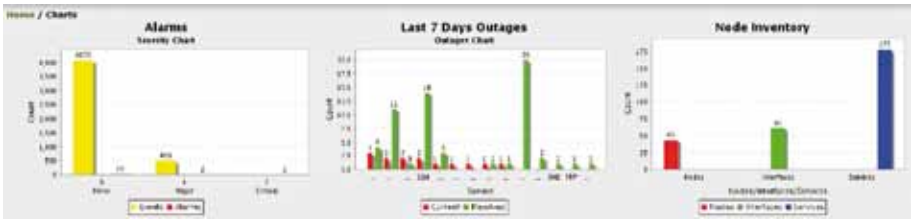


Figura 47 - Gráficos estatísticos OpenNMS
Fonte: Fonte: OpenNms (2011)

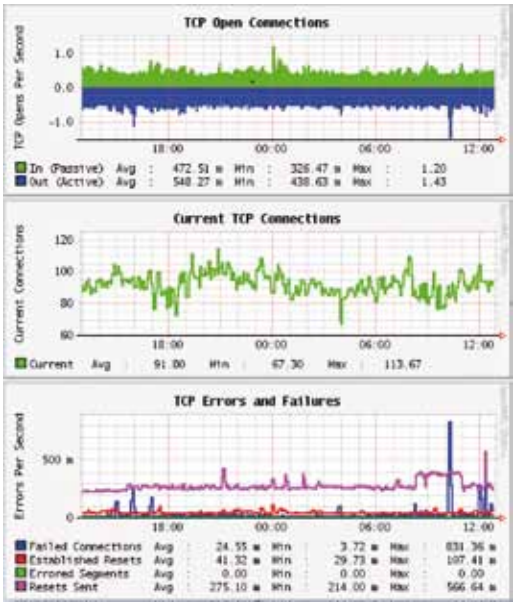


Figura 48 - Gráficos sobre as conexões TCP em um host
Fonte OpenNms (2011)

Por fim, para acompanharmos o estado da rede, podemos gerar diferentes tipos de relatórios, muitos já existentes por padrão, ou podemos criar relatórios customizados. Também é possível agendar a geração automática destes, além do envio por e-mail.

Confira mais informações sobre essa ferramenta nos sites indicados a seguir:

Site do projeto do OpenNMS: <http://www.opennms.org>. Nele encontramos a documentação oficial e podemos realizar o download do código fonte e orientações para a obtenção dos pacotes pré-compilados.

Site do grupo OpenNMS, destinado ao relacionamento comercial, como suporte corporativo, treinamento e desenvolvimento customizado: <http://www.opennms.com>.

Página de demonstração do OpenNMS, onde os interessados em utilizar a ferramenta podem realizar testes e avaliar os seus recursos. Disponível em: <http://demo.opennms.org>.

Site oficial do Java, para o download do *Java Runtime Environment*, necessário para o funcionamento do OpenNMS: <http://java.com>.

Essa é mais uma excelente ferramenta de gerenciamento de redes. O principal diferencial do OpenNMS é a sua arquitetura que, uma vez que é escrita em Java, desde que instalado em um equipamento robusto, permite o gerenciamento de milhares de equipamentos. Vale a pena explorar todos os recursos que esta ferramenta oferece. Para as empresas que julgarem necessário, o grupo responsável pelo OpenNMS disponibiliza suporte comercial (pago). No item a seguir, você conhecerá o NetFlow Analyzer, uma solução de monitoramento dos enlaces da organização.

4.7 NETFLOW ANALYZER

O NetFlow Analyzer é comercializado pela empresa Manage Engine. Apesar de ser pago, é possível utilizá-lo durante 30 dias de forma completa. Após este período, podemos monitorar até duas interfaces de forma gratuita, ou seja, é possível monitorar até dois enlaces sem precisar comprá-lo, o que para muitos casos é o suficiente. As informações são obtidas por meio dos fluxos enviados pelos equipamentos (roteadores, switches, etc.), dos pacotes NetFlow, sFlow, JFlow, entre outros. Essa ferramenta:

a) monitora a largura de banda rede;

b) identifica os protocolos utilizados na rede;

c) mapeia aplicativos e analisa o seu impacto sobre a rede;

d) avalia as políticas de QoS existentes nos equipamentos;

e) identifica o tráfego não autorizado;

f) identifica e corrige problemas de forma rápida;

g) agenda a geração de relatórios;

h) permite definir diferentes permissões para os perfis de acesso;

i) apresenta uma interface de operação simples;

j) monitora diversos tipos de equipamentos e fabricantes.

Dentre os fabricantes suportados pelo NetFlow Analyzer estão: Cisco, 3Com, Juniper, Riverbed, Extreme, Foundry, Nortel, HP, Dell, D-Link, entre outros. Quanto aos fluxos NetFlow, ele tem suporte para as versões 5,7 e 9.

Podemos avaliá-lo sem precisar instalá-lo, uma vez que possui uma versão de demonstração na web. Os relatórios podem ser exportados para os formatos PDF, CSV ou podem ser enviados por e-mail. Na ocorrência de certos eventos, alertas podem ser enviados para os responsáveis.

A ferramenta pode ser instalada em sistemas Microsoft Windows e GNU/Linux, onde temos à disposição três versões: Professional Edition, Professional Plus Edition e Enterprise Edition. A diferença entre elas é a quantidade de recursos, além, obviamente, do preço. A sua interface é escrita em Java. Todas as informações são armazenadas em um banco de dados MySQL. Tanto o Java quanto o MySQL estão embutidos no pacote de instalação.

4.7.1 INSTALAÇÃO

Faremos a instalação do NetFlow Analyzer em um servidor Microsoft Windows. Para isso, precisamos realizar o download da versão correspondente no site oficial. Durante a instalação, devemos informar o diretório onde o programa será instalado, a porta TCP da interface web e, opcionalmente, o nome da comunidade e a porta do SNMP (com, pelo menos, permissão de leitura).

Podemos optar por executarmos o NetFlow Analyzer como um serviço do Windows, o que é recomendável na maioria dos casos. É possível informar os dados para o registro por meio do qual poderá ser solicitado suporte comercial. Por fim, é mostrado o resumo das escolhas realizadas para conferência (figura a seguir).

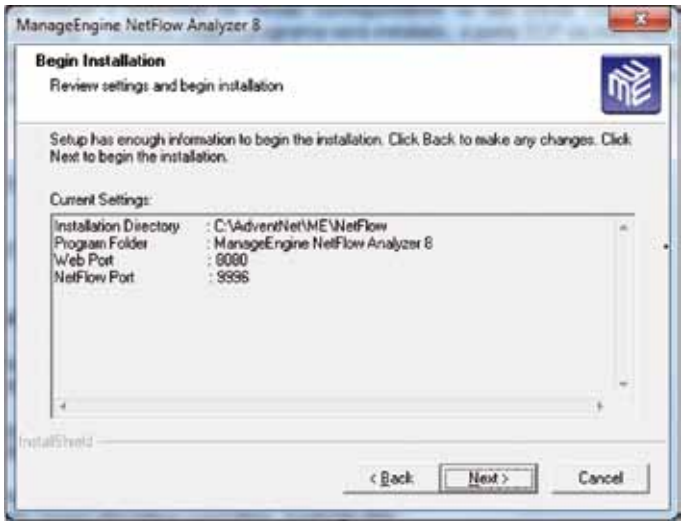


Figura 49 - Parâmetros de instalação do NetFlow Analyzer

Ao término da instalação podemos optar por iniciar o serviço do NetFlow Analyzer. O próximo passo é a sua configuração, que é feita pela interface web. Para acessá-la informamos a URL <http://meuservidor.com:8080>. As credenciais para o primeiro acesso são: usuário "admin" e senha "admin".

CONFIGURANDO UM ROTEADOR CISCO PARA ENVIO DOS FLUXOS

Para que o NetFlow Analyzer possa gerenciar os enlaces, precisamos configurar os roteadores para que enviem os fluxos com as informações ao servidor. Como exemplo, faremos a configuração de um roteador da Cisco Systems. Os comandos necessários estão na figura a seguir.

```
Router>enable
Password:
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip flow-export destination 10.1.1.254 9996
Router# exit
Router#copy running-config startup-config
Router#exit
```

Figura 50 - Configurando o envio de fluxos em um roteador Cisco

Com isso, o roteador Cisco começará a enviar os pacotes NetFlow para o servidor do NetFlow Analyzer, que no nosso exemplo, tem o endereço IP 10.1.1.254. A porta é a 9996/udp, conforme informado na instalação do servidor (esta é a porta padrão). Sendo assim, é preciso configurar o *firewall* da rede para permitir a passagem deste tráfego.

CONFIGURANDO O NETFLOW ANALYZER

Por questões de segurança, a primeira configuração que vamos realizar é a alteração da senha do usuário administrador. Para isso, em "Admin Operations", utilizamos a opção "User Management". Na coluna "Password" do usuário "admin", informamos uma nova senha com um clique sobre "Assign New". Em "License Management" definimos quais equipamentos e quais interfaces queremos monitorar. Os equipamentos aparecerão automaticamente nesta seção, desde que o envio dos fluxos tenha sido configurado (figura a seguir).

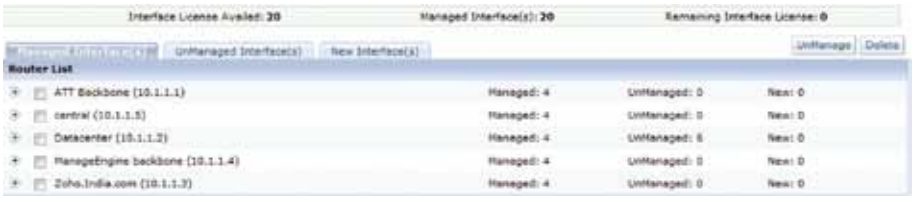


Figura 51 - Seleção dos equipamentos e interfaces para monitoramento
Fonte: ManageEngine - NetFlow Analyzer Professional [20--]

Se você estiver utilizando uma versão *trial*, após 30 dias, poderá gerenciar somente duas interfaces. Podemos definir também grupos de endereços IP, para que assim, consigamos identificar tipos de tráfego específicos. Fazemos isto por meio da opção "IP Groups". Em uma nova instalação, alguns grupos são criados automaticamente. Se não nos interessar, podemos desativá-los, com um clique de mouse sobre o botão "Enabled", que será alterado para "Disabled".

Agora criaremos nossos próprios grupos, por exemplo, um grupo para o segmento de rede dos "programadores" (figura a seguir). Lembre-se que o uso de grupos facilita a administração da rede.

Figura 52 - Cadastrando um IP Group no NetFlow Analyzer
Fonte: ManageEngine - NetFlow Analyzer Professional [20--]

Damos um nome para o grupo, uma descrição e definimos se o critério para identificação do tráfego será baseado no endereço IP, porta e protocolo ou pelo código DSCP (*Differentiated Services Code Point*), que identifica o nível de serviço QoS (*Quality of Service*). Para este último, o roteador deve estar configurado para realizar a priorização de tráfego, que é o princípio para a implementação de QoS.

Como na nossa rede fictícia cada departamento possui a sua VLAN própria, utilizaremos o filtro baseado no endereço IP da VLAN. Por fim, selecionamos a interface do roteador, por meio do qual o tráfego desta VLAN é encaminhado, além de informar a velocidade da interface que selecionamos (em bits por segundo). Isso é importante para que o NetFlow Analyzer possa apresentar os gráficos estatísticos de forma correta.

Uma vez salva a configuração do grupo, em alguns minutos o NetFlow Analyzer já começará a exibir as informações sobre o tráfego nesta rede. As informações serão visualizadas pela seção "IP Group/Programadores". Podemos definir qual o período utilizado para a geração dos gráficos e demais relatórios. Apesar de possuir alguns valores fixos para a definição do período, utilizado para a geração dos gráficos e demais relatórios (por exemplo, últimos 15 minutos, últimas 6 horas, última semana, último mês, etc.), podemos definir intervalos customizados, informando a data e a hora de início e fim (veja o gráfico a seguir). Os tipos de gráficos disponíveis são relacionados ao volume, à velocidade, à utilização e à quantidade de pacotes.

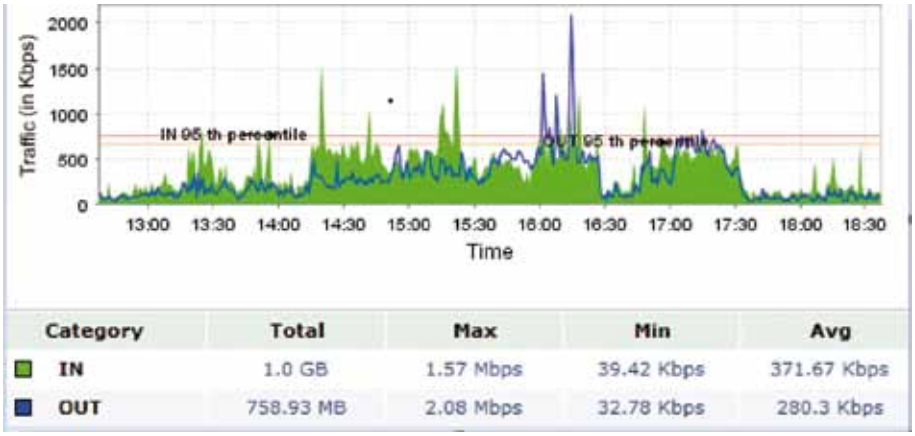


Figura 53 - Gráfico de tráfego de entrada e saída da rede
Fonte: ManageEngine - NetFlow Analyzer Professional [20--]

Além do tráfego total, o NetFlow Analyzer gera informações sobre os tipos de tráfegos identificados. Por meio da aba "Application", podemos visualizar os protocolos e a quantidade de dados trafegados referente a cada um destes (figura a seguir).

Protocol Distribution — Showing 1 to 25 — View per page 100

Application	Traffic(Total: 1.02 GB)	% of total traffic
UDP_App	465.26 MB	45%
https	274.21 MB	27%
netmeeting	78.74 MB	8%
TCP_App	53.82 MB	5%
http	53.32 MB	5%
imaps	43.8 MB	4%
domain	24.57 MB	2%
icmp	6.69 MB	1%
ldap	4.84 MB	<1%
snmp	3.12 MB	<1%

Figura 54 - Quantidade de tráfego por protocolo
Fonte: ManageEngine - NetFlow Analyzer Professional [20--]

Na aba "Source" podemos visualizar todo o tráfego gerado por cada equipamento da rede (tráfego de origem) e, na aba "Destination", podemos identificar os endereços acessados pelos equipamentos da rede, além da respectiva quantidade de tráfego (tráfego de destino).

Na aba "QoS" visualizamos a quantidade de tráfego por tipo de serviço que está sendo otimizado (precisa ser configurado previamente em "Application/QoS Maps"). Por fim, na aba "Conversation", podemos visualizar todos os detalhes referentes a cada tipo de tráfego (endereço de origem, destino, aplicação, porta, protocol, código DSCP e a quantidade de dados trafegados). Gráficos estatísticos também são gerados para, por exemplo, identificar os computadores que mais trafegam dados na rede (figura a seguir).

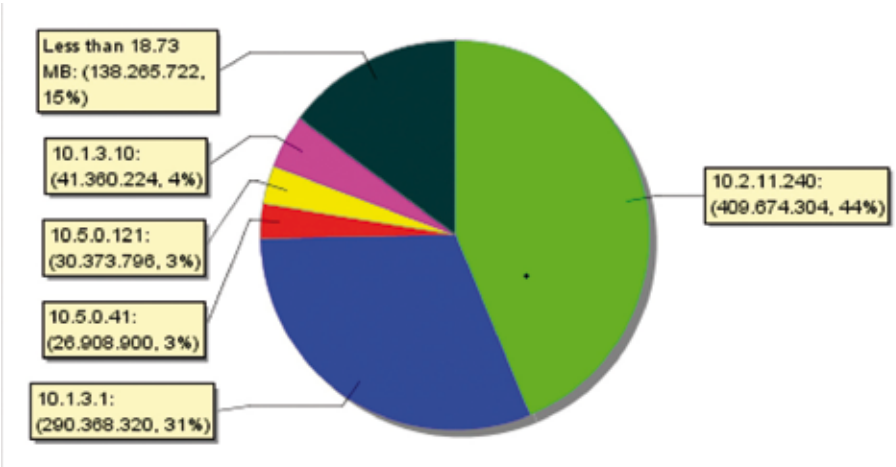


Figura 55 - Endereço IP dos *hosts* que mais trafegam dados
Fonte: ManageEngine - NetFlow Analyzer Professional [20--]

Uma vez que criamos todos os grupos IP, podemos criar contas de usuário para acesso ao NetFlow Analyzer com diferentes permissões de acesso. Os níveis disponíveis são:

a) administrador (todas as permissões);

b) operator (permissões para definir, alterar e remover alertas, criar contas de perfil guest, alterar a configuração dos dispositivos de que tem acesso, etc.);

c) guest (apenas visualizar gráficos e relatórios).

GERANDO FLUXOS NETFLOW COM LINUX

Além de configurar o envio de fluxos em roteadores e switches, existem algumas ferramentas disponíveis para serem instaladas em computadores, para que estes gerem os pacotes NetFlow, dentre eles o NDSAD, fprobe, nProbe e FlowProbe. Para a instalação do fprobe em um equipamento com Debian GNU/Linux (e derivados), utilizamos o comando "apt-get install fprobe". Durante a instalação, devemos informar qual a interface de rede será monitorada e o endereço (e porta) do servidor para envio dos fluxos. Após a instalação, o serviço entrará em execução, e os fluxos já estarão sendo enviados ao servidor. Terminamos aqui o estudo do NetFlow Analyzer. As tecnologias NetFlow, sFlow, JFlow, e cFlow, entre outras, são um avanço na forma como gerenciamos as redes. Até então, o administrador tinha à disposição o protocolo SNMP, além de agentes para ferramentas específicas. Além do NetFlow Analyzer, outras ferramentas também podem ser utilizadas, como o flow-tools, cflowd e o Ntop (do qual já foi falado, anteriormente).

SAIBA MAIS

Confira mais alguns sites onde você encontrará informações para complementar o seu estudo sobre as ferramentas de gerenciamento de rede.

Site da ManageEngine, com informações e documentos sobre as diversas ferramentas comercializadas, área para suporte comercial, fórum e download de versões de avaliação: <http://www.manageengine.com>.

Demonstração do NetFlow Analyzer, onde podemos avaliar o funcionamento da ferramenta sem a necessidade de realizar uma instalação: <http://demo.netflowanalyzer.com>.

Site do fprobe, onde é disponibilizado o código fonte para download: <http://fprobe.sourceforge.net>.

RECAPITULANDO

Neste capítulo você aprendeu a instalar, configurar e utilizar as principais ferramentas utilizadas para o gerenciamento e monitoramento de redes. Todas são ferramentas gratuitas, com exceção do NetFlow Analyzer que, apesar de ser paga, após o vencimento do período de avaliação, permite que seja utilizada de forma limitada, o que em algumas ocasiões é suficiente.

Você percebeu que, graças ao movimento Open Source, temos acesso a ótimos softwares? Isso é muito bom, não é mesmo? Podemos utilizá-los livremente, sem custos, ou se necessário, contratar um serviço de suporte comercial. Dependendo da maturidade da equipe de TI da empresa, esse pode ser dispensado.

Ainda nesse capítulo, você entendeu que, apesar de todas as ferramentas apresentadas serem utilizadas para o mesmo fim, cada uma tem características próprias. Essa situação faz com que muitos administradores optem por utilizar mais de uma ferramenta simultaneamente. Isso é interessante do ponto de vista dos recursos que estarão à disposição do administrador da rede, mas por outro lado, será preciso um tempo maior para a instalação e configuração de dois ambientes.

Com o uso de ferramentas open source, se tivermos o conhecimento da linguagem utilizada no seu desenvolvimento, podemos alterá-la para suprir as nossas necessidades. Outro recurso importante é o suporte a plugins, o que faz com que possamos entender as funcionalidades desta, desenvolvendo ou copiando aqueles criados pela comunidade. O seu aprendizado não acaba aqui. Continue lendo, pesquisando e se informando. Um bom profissional deve estar sempre atento às novidades e melhores práticas no mercado, por isso, mãos à obra, e sucesso na sua caminhada!

REFERÊNCIAS

ADD-ONS. ***Plugin* "Nagios Checker" para o Firefox.** [20--]. il. color. Disponível em: <http://addons.mozilla.org>. Acesso em: 04. Nov.2011

BARBOSA, Marcelo de M. Gráficos elegantes. **Linux Magazine**, São Paulo, n. 71, p. 48-50, out. 2010.

BENTHIN, Falko. O observador**. Linux Magazine**, São Paulo, n. 73, p. 72-77, dez. 2010.

CACTI. **Visualização dos gráficos no Cacti.** 2011. il. color. Disponível em: <http://www.cacti.net>. Acesso em: 04. Nov.2011

DCALA´S BLOG. **Visualização dos equipamentos em forma de mapa.** 2010. il. color. Disponível em: <http://dcala.wordpress.com>. Acesso em: 04. Nov.2011

DE LUCCA, J. E.; WESTPHALL, C. B.; SPECIALSKI, E. S.. Uma Arquitetura de Segurança para Gerência de Redes. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 12, 1994, Curitiba. **Anais...** Curitiba, 1994. p.467-485.

HABRAHABR. **Plugin Thold para o Cacti.** [20—]. il. color. Disponível em: <http://habrahabr.ru>. Acesso em: 04. Nov.2011

HARDWARE. **Relatórios detalhados gerados pelo NTOP.** [20--]. il. color. Disponível em: <http://www.hardware.com.br>. Acesso em: 04. Nov.2011

HEIN, Julian. O verdadeiro grande irmão. **Linux Magazine**, São Paulo, n. 31, p. 32-39, jun. 2007.

HONÓRIO, Marcelo. Ampla competência. **Linux Magazine**, São Paulo, n. 24, p. 66-67, out. 2006.

ICINGA. **Interface do Icinga.** [20--]. il. color. Disponível em: <http://web.demo.icinga.org>. Acesso em: 04. Nov.2011

KOCJAN, Wojciech. **Learning Nagios 3.0**. 1. ed. Birmingham, UK: Pack Publishing, 2008.

KUNDU, Dinangkur; LAVLU, Ibrahim. **Cacti 0.8 Network Monitoring**. 1.ed. Birmingham, UK: Pack Publishing, 2009.

LABORATORY OF INFORMATION TECNOLOGIES. **Gráfico diário gerado pelo MRTG.** [20--]. Il. color. Disponível em: <http://lit.jinr.ru>. Acesso em: 04. Nov.2011

LINUXARIA. **Ntop for Network Analysis.** 2010. il. color. Disponível em: <http://www.linuxaria.com>. Acesso em: 04. Nov.2011

MANAGE ENGINE, NetFlow Analyzer Professional Plus. **Seleção dos equipamentos e interfaces para monitoramento.** [20--]. il. color. Disponível em: <http://demo.netflowanalyzer.com>. Acesso em: 04. Nov.2011

_____. **Cadastrando um IP Group no NetFlow Analyzer.** [20--]. il. color. Disponível em: <http://demo.netflowanalyzer.com>. Acesso em: 04. Nov.2011

_____. **Gráfico de tráfego de entrada e saída da rede.** [20--]. il. color. Disponível em: <http://demo.netflowanalyzer.com>. Acesso em: 04. Nov.2011

_____. **Quantidade de tráfego por protocolo.** [20--]. il. color. Disponível em: <http://demo.netflowanalyzer.com>. Acesso em: 04. Nov.2011

_____. **Endereço IP dos *hosts* que mais trafegam dados.** [20--]. il. color. Disponível em: <http://demo.netflowanalyzer.com>. Acesso em: 04. Nov.2011

MARINO, Vinicius Andrade. Olheiro do Nagios. **Linux Magazine**, São Paulo, n. 48, p. 52-55, nov. 2008.

MEIER, Adriano Matos. De olho na rede. **Linux Magazine**, São Paulo, n. 74, p. 68-71, jan. 2011

_____. Monitorar é preciso. **Linux Magazine**, São Paulo, n. 33, p. 65-67, ago. 2007.

*MOZABY. **Aplicativo Zabbix para** smartphones**.** 2011. il. color. Disponível em: <http://www.mozaby.com>. Acesso em: 04. Nov.2011*

NETWORKING WITH OPENBSD. **Plugin Monitor.** 2010. il. color. Disponível em: <http://greendecx.blogspot.com>. Acesso em: 04. Nov.2011

NTOP. **Estrutura de funcionamento do NTOP.** [20--].il.color. Disponível em: http://www.ntop.org. Acesso em: 04. Nov.2011

OPENNMS. **Taxas de disponibilidade de cada item monitorado.** 2011. Disponível em: <http://demo.opennms.org>. Acesso em: 04. Nov.2011

_____. **Gráficos estatísticos OpenNMS.** 2011. Disponível em: <http://demo.opennms.org>. Acesso em: 04. Nov.2011

_____. **Gráficos sobre as conexões TCP em um host.** 2011. Disponível em: <http://demo.opennms.org>. Acesso em: 04. Nov.2011

OLUPS, Rihards. **Zabbix 1.8 Network Monitoring**. 1. ed. Birmingham, UK: Pack Publishing, 2010.

ORACLE. **Software Downloads**. Disponível em: <http://download.oracle.com>. Acesso em: 04. Nov.2011

SACKS, Matthew D. Imagem é tudo. **Linux Magazine**, São Paulo, n. 45, p. 60-64, ago. 2008.

SCHWARZKOPFF, Michael. Simple Network Management Protocol: Vista panorâmica. **Linux Magazine**, São Paulo, n. 20, p. 38-45, jun. 2006.

SEIFRIED, Kurt. Monitoramento eficiente. **Linux Magazine**, São Paulo, n. 76, p. 42-46, mar. 2011.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3 and, RMON1 and RMON2**. 3. ed. USA: Adisson Wesley, 1999.

UFCC CEEI, **MIB RMON.** [20--]. il. Disponível em: < http://www.dsc.ufcg.edu.br>. Acesso em: 04. Nov.2011

ZABBIX. **Equipe Zabbix.** 2011. Disponível em: <http://www.zabbix.com>. Acesso em: 04. Nov.2011

_____. **Uma das vantagens de se utilizar o Zabbix Proxy.** [20--]. il. color. Disponível em: <http://www.zabbix.com>. Acesso em: 04. Nov.2011

MINICURRÍCULO DO AUTOR

Adriano Matos Meier Tecnólogo em Redes de Computadores e pós-graduando em Gestão de Segurança da Informação pelo SENAI de Florianópolis/SC. Possui a certificação CCNA (*Cisco Certified Network Associate*). Atua na área de redes locais desde 1998 e na área de redes corporativas desde 2004. Atua também como instrutor nos cursos de Administração de Sistemas Linux e Administração de Redes Linux. Possui diversos artigos publicados nas áreas de gerenciamento, monitoramento, controle e serviços em redes de computadores. Atualmente, faz parte da equipe responsável pelo *datacenter* no Departamento Regional do SENAI de Santa Catarina. Tem interesse especial no sistema operacional GNU/Linux e em serviços para redes baseados em *software* livre.

ÍNDICE

SENAI - DN
UNIDADE DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA – UNIEP

Rolando Vargas Vallejos
Gerente Executivo

Felipe Esteves Morgado
Gerente Executivo Adjunto

Diana Neri
Coordenação Geral do Desenvolvimento dos Livros

SENAI - DEPARTAMENTO REGIONAL DE SANTA CATARINA

Simone Moraes Raszl
Coordenação do Desenvolvimento dos Livros no Departamento Regional

Beth Schirmer
Coordenação do Núcleo de Desenvolvimento

Caroline Batista Nunes Silva
Juliano Anderson Pacheco
Coordenação do Projeto

Gisele Umbelino
Coordenação de Desenvolvimento de Recursos Didáticos

Adriano Matos Meier
Elaboração

Juliano Anderson Pacheco
Revisão Técnica

Evelin Lediani Bao
Design Educacional

D'imitre Camargo Martins
Diego Fernandes
Júlia Pelachini Farias
Luiz Eduardo Meneghel
Ilustrações e Tratamento de Imagens

Priscila da Costa
Diagramação

Juliana Vieira de Lima
Revisão e Fechamento de Arquivos

Luciana Effting Takiuchi
CRB 14/937
Ficha Catalográfica

DNA Tecnologia Ltda.
Sidiane Kayser dos Santos Schwinzer
Revisão Ortográfica e Gramatical

DNA Tecnologia Ltda.
Sidiane Kayser dos Santos Schwinzer
Normalização

i-Comunicação
Projeto Gráfico

SENAI

Iniciativa da CNI - Confederação Nacional da Indústria

ISBN 978-85-7519-484-3