

GESTÃO E MONITORAMENTO DE REDES DE COMPUTADORES MIB E FERRAMENTAS DE GERENCIAMENTO

Autor: Me. Paulo Sérgio Pádua de Lacerda

Revisor: Me. Rafael de Jesus Rehm

INICIAR

introdução

Introdução

Caro(a) estudante, seja bem-vindo(a) à disciplina de Gestão e Monitoramento de Redes de Computadores! A proposta principal desta unidade é apresentar os conceitos fundamentais sobre as Base de Informação de Gerenciamento, conhecidas como MIB, bem como a importância das ferramentas de gerenciamento utilizadas na gerência de redes.

O século XXI, em que os modelos de negócio *Bussiness-to-Bussiness* (B2B), *Bussiness-to-Client* (B2C) e Client-to-Client têm como infraestrutura básica de comunicação a Internet, monitorar e gerenciar os elementos que compõem uma rede torna-se um tarefa crítica, porque essa infraestrutura precisa ser de boa qualidade, transparente ao usuário e manter o modelo de negócio ativo, sem interrupções.

Nesse cenário, alguns conceitos sobre elementos usados na gerência de redes são essenciais para o seu administrador, assim como o entendimento de ferramentas de gerenciamento também são fundamentais. Portanto, compreender os fundamentos de Base de Informação de Gerenciamento, mas também o protocolo *Simple Network Management* (SNMP) são essenciais na gerência de redes de computadores. Em suma, você vai entender e compreender como aplicar MIB e uso de ferramentas na gerência de redes. Vamos lá?

MIB

Com visto em outro unidade, a gerência de redes é subdividida basicamente em três componentes: as estações de gerenciamento, os agentes gerenciáveis e os protocolos de gerenciamento, no caso, o *Simple Network Management Protocol* (SNMP).

Então, entre esses tópicos, as Base de Informação de Gerenciamento, conhecidas com MIB, são fundamentais. Porém, quem são as MIBs?, onde usá-las? e como usá-las? são questionamentos que vão ser decifrados ao longo deste tópico.

Vamos começar identificando quem são os agentes de uma rede de computadores. Um agente é todo elemento de rede de quem o administrador de rede deseja receber informação sobre seu status, como servidores de rede, roteadores, links, *switches* , placa de rede, *hotspot* , *hosts* , entre diversos outros elementos. Lembre-se sempre de que o processo de gerenciamento tem base em três primícias: análise e coleta dos dados, determinação do diagnóstico e providência de uma ação ou controle.

As MIBs são divididas entre MIB-I, o primeiro conceito a ser desenvolvido, e

MIB-II, especificada no RFC 1213 e que compreende a uma versão mais atualizada da MIB-I. Assim, um dos avanços foi o aumento de elementos gerenciáveis a cada produto utilizado na rede de computadores independente da marca (FOROUZAN, 2009). A MIB-II contém os objetos que são essenciais e não opcionais para um bom gerenciamento. A MIB-II é subdividida em grupos, e esses grupos são descritos as seguir (STALLINGS, 1999): system, interfaces, ip, at, icmp, tcp, udp, dot3, egp, transmission, snmp.

Entretanto, para cada objeto especificado, há um conjunto de outros objetos. Logo, podemos representar essa árvore de objetos hierárquicos pelo grupo *system*. Esse objeto possui 7 subelementos que representam informações gerais sobre o sistema que está ou será gerenciado.

Vamos representar o objeto system pela Figura 2.1. Pode-se entender que os objetos são subníveis de objeto *system* e a cada um objeto de informação, um número a ele está associado.

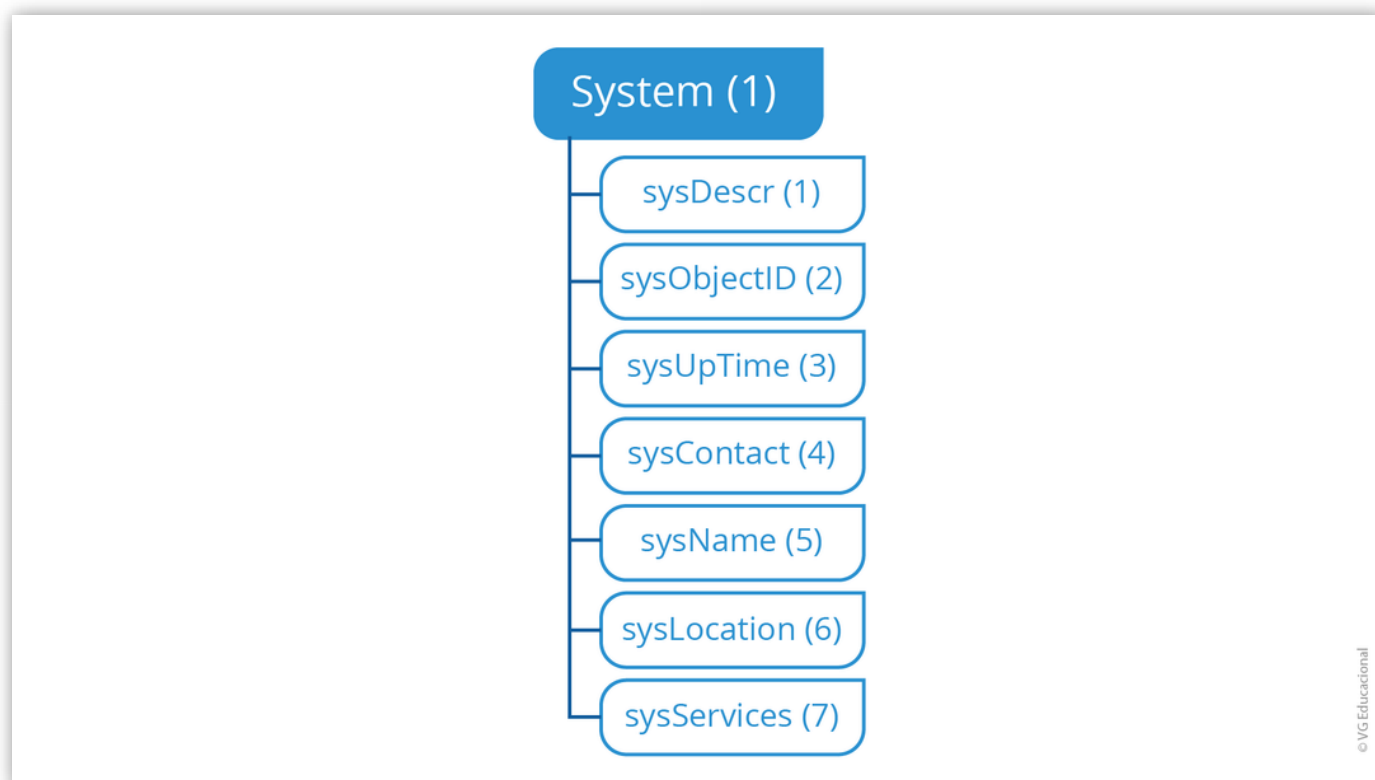


Figura 2.1 - Árvore do objeto system

Fonte: Elaborada pelo autor.

Nota-se pela Figura 2.1 que praticamente os subelementos são autoexplicativos, mas, para podermos compreender melhor, vamos, através

do subobjeto sysServices, descrever a sua finalidade dentro do grupo system. O grupo sysServices contém como valor uma faixa de 7 bits. Cada bit corresponde a um valor relativo a uma camada nos modelos de referência OSI e TCP/IP. Logo, podemos exemplificar a suíte TCP/IP no Quadro 2.1.

Camada	Funcionalidade
1	Camada física
2	Camada de enlace
3	Camada de Internet
4	Camada de transporte
7	Camada de aplicação

Quadro 2.1 - Modelo TCP/IP

Fonte: Elaborado pelo autor.

Nesse caso, o objeto sysServices apresenta valores em um range ou faixa entre 0 e 127 do tipo inteiro que representa um série de serviços básicos oferecidos pela entidade, por exemplo, se o protocolo TCP ou UDP está ativo. Cada subobjeto contém uma permissão de acesso, no exemplo do sysServices, RO, ou seja, *Read Only* ou somente para leitura, ao contrário do objeto sysContact, que tem a permissão RW, *Read Write*, leitura e escrita e contém informações de contato da pessoa responsável por aquele gerenciamento na rede.

Portanto, o identificador de Objetos (OID) na rede torna-se essencial para uso do gerenciamento, pois, através dele, o administrador de rede, pode, por exemplo, alterar informações de configuração na rede sem muita complexidade. Esses identificadores podem ser expressos, no caso da Figura 2.1, em relação ao sysService, com início da raiz no padrão ISO, teremos, 1(iso).3.(org).6(dod).1(internet).2(mgmt).1(mib-2). **1** (system). **7**

(sysServices), com relação ao sysContact, teremos 1(iso).3.(org).6(dod).1(internet).2(mgmt).1(mib-2). **1** (system). **4** (sysContact).

Bem, agora, que já entendemos como é a MIB e como ela pode ser representada por meio de OID, vamos utilizar uma ferramenta para ilustrar como é possível realizar ações e controle na rede, assunto para o próximo tópico.

MIB Browser

No intuito de diminuir a complexidade do gerenciamento de redes, ferramentas são utilizadas, a fim de proporcionar uma otimização para os administradores de rede, entre elas, os MIB Browsers.

Os MIB Browsers são aplicativos ou ferramentas que permitem configurar dispositivos de gerenciáveis em uma rede como roteadores e switches com protocolo de gerenciamento SNMP habilitado. Essas ferramentas coletam os dados dos dispositivos da rede, de forma que seja legível ao ser humano, tornando a tarefa mais simples, fácil e otimizada.

Embora haja diversos aplicativos no mercado para serem usados, para tal demonstração de como usar um MIB Browser para administrar o gerenciamento da rede, vamos a um exemplo com o simulador de redes da empresa Cisco, o cisco Packet Tracer, por ser fácil e excelente didaticamente. Porém, para que você possa acompanhar o exemplo, na prática, será necessário que você tenha o simulador instalado na sua máquina.

Antes, deixamos claro que não vamos explicar como criar e configurar o cenário apresentado, curso de fundamentos de redes básica, mas como criar o sistema para entender o uso do MIB Browser em um cenário essencial para o seu entendimento. No cenário apresentado na Figura 2.2, na qual constam dois roteadores e um host associado a uma rede 192.168.0/24, em que o host possui o endereço 192.168.0.1/24, o router 1, o endereço 192.168.0.2/24, e o router2, o endereço 192.168.0.3/24. No exemplo, o endereço de rede pode ser configurado por meio gráfico diretamente nas interfaces do host e dois

roteadores.

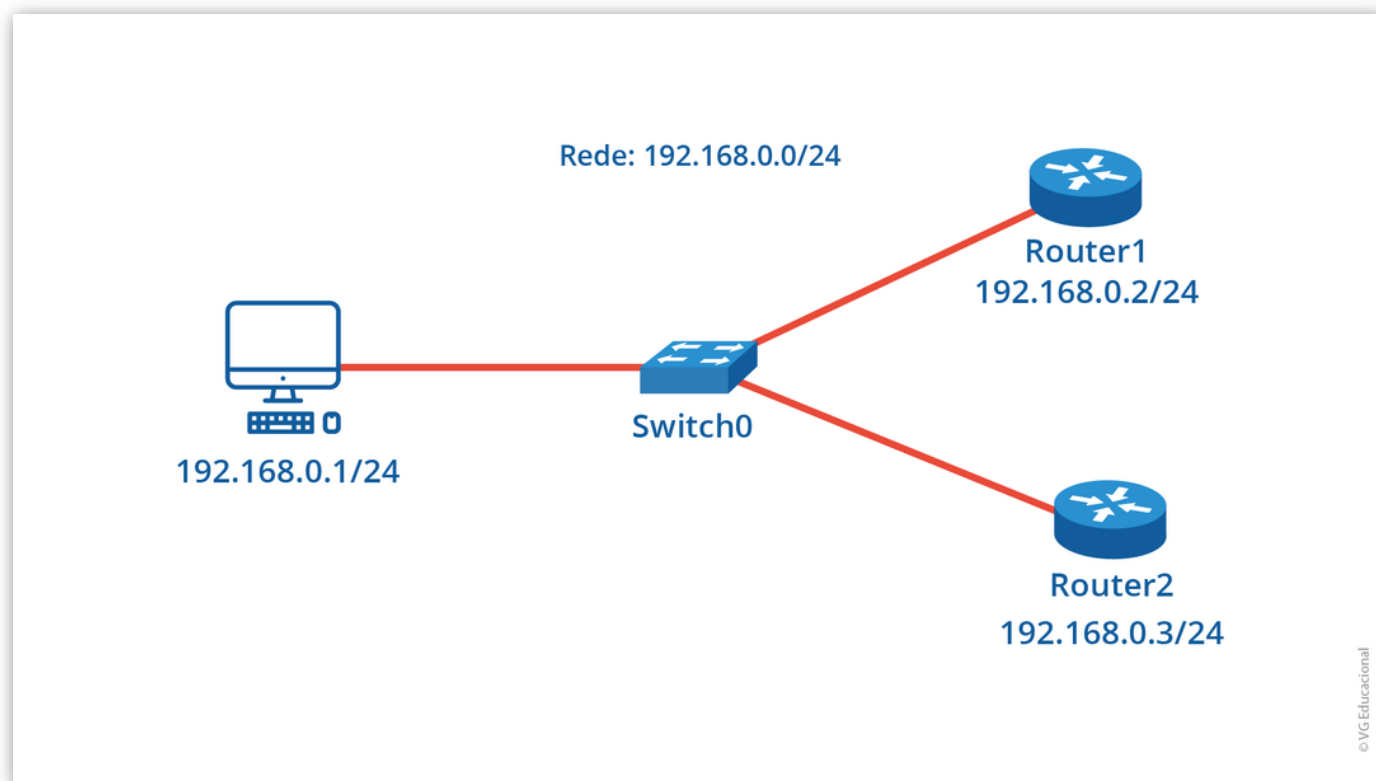


Figura 2.2 - Cenário da rede 192.168.0.0/24

Fonte: Elaborada pelo autor.

A partir do cenário em que a rede está configurada, é preciso ativar o protocolo SNMP e determinar como será a comunidade do protocolo e o tipo de acesso somente leitura ou escrita. A Figura 2.3 ilustra os passos dos comandos realizados na aba *Command line* (cli) do roteador identificado como router 1.

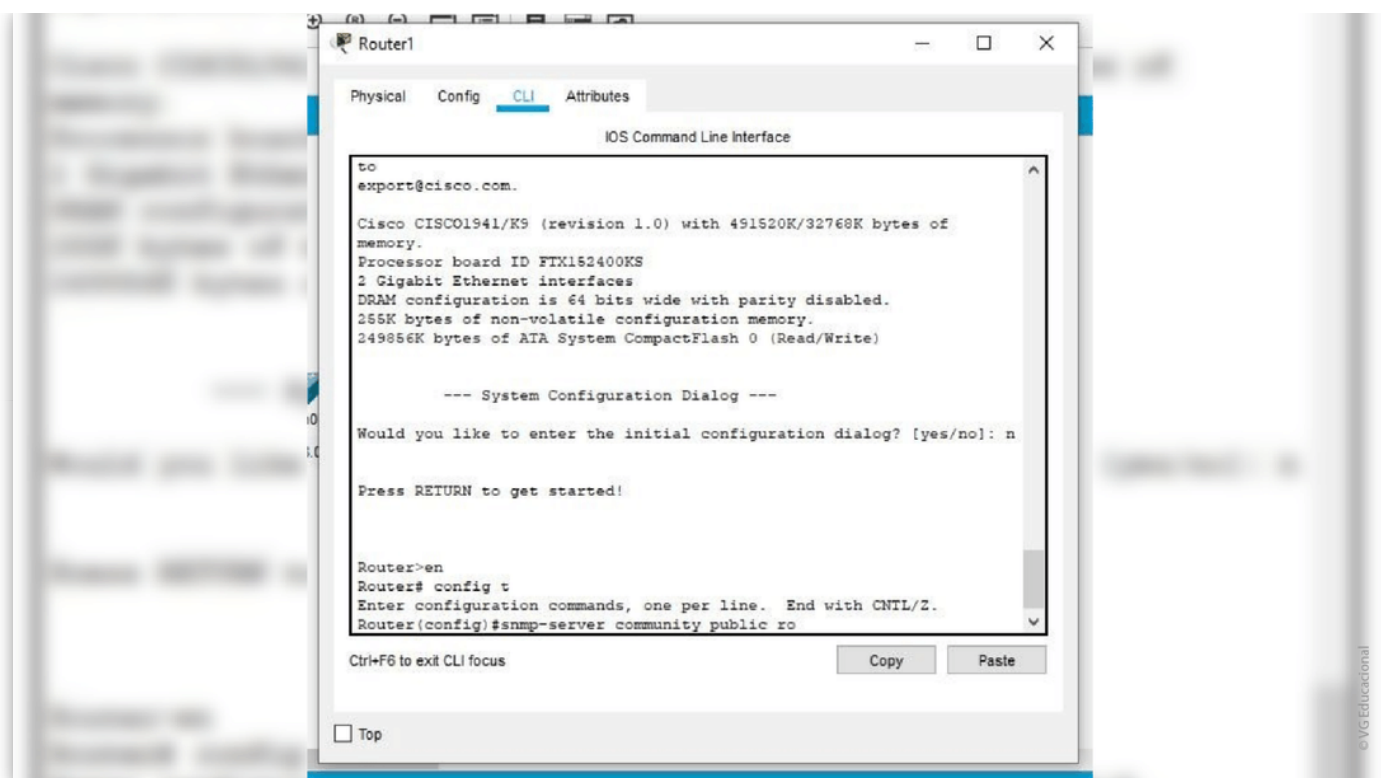


Figura 2.3 - Ativando o protocolo SNMP no roteador

Fonte: Elaborada pelo autor.

Agora que o roteador está com o protocolo SNMP ativo, vamos abrir o aplicativo MIB Browser do host para alterar, como exemplo, o nome do roteador. Notem que na Figura 2.3, o nome do roteador é R1. Então, vamos lá? Clique no host PC0, aba desktop e, em seguida, no aplicativo MIB Browser, conforme ilustrado na Figura 2.4.

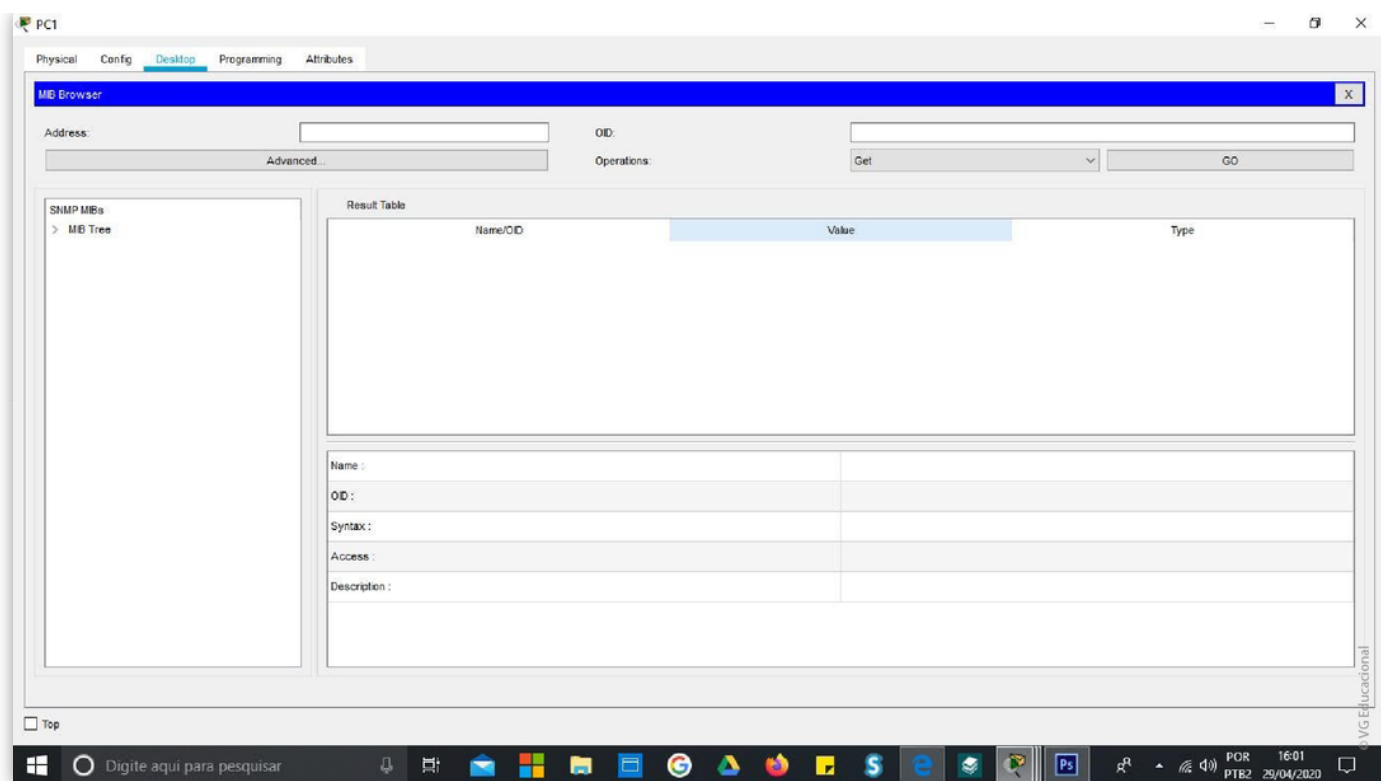


Figura 2.4 - MIB Browser

Fonte: Elaborada pelo autor.

Após ter executado o aplicativo MIB Browser, uma nova janela será aberta e algumas configurações precisarão ser realizadas para trabalhar com a ferramenta. Na caixa de texto *address*, digite o endereço do roteador a ser gerenciado, depois clique no botão *advanced*. Agora, precisamos configurar o acesso ao SNMP do roteador, então, configure a caixa *Read Community* para *read* e a outra caixa *Write Community* para *write*, conforme configuração no roteador e opte por SNMP v3, como está demonstrado na Figura 2.5.

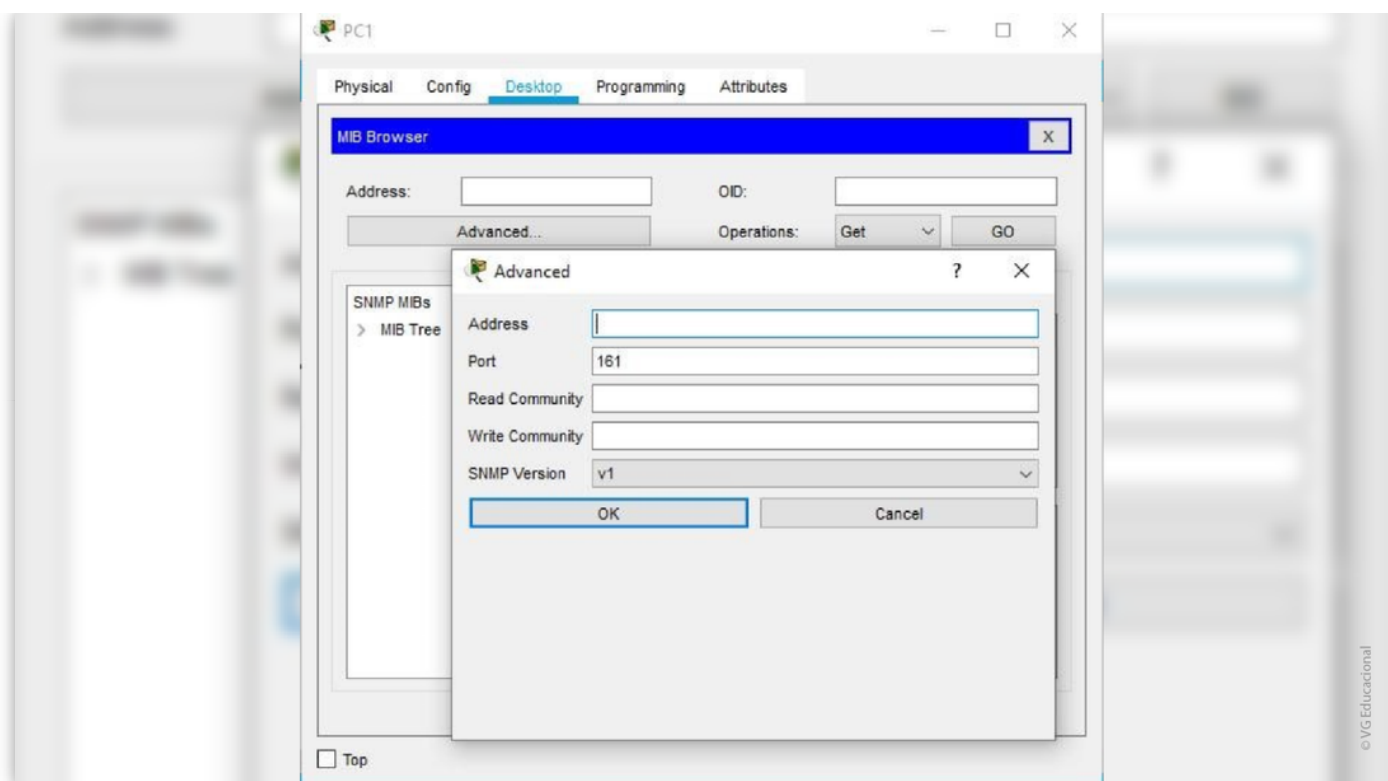


Figura 2.5 - Configurando o MIB Browser

Fonte: Elaborada pelo autor.

Pronto, agora você pode navegar pela estrutura de árvore do MIB Browser e verificar informações configuradas no navegador.

Temos uma demonstração de navegação para descobrirmos o nome atribuído ao roteador. Clique na opção *GO*, configurada para o método *GET* para receber informações do roteador. Essa demonstração é mostrada na Figura 2.6.

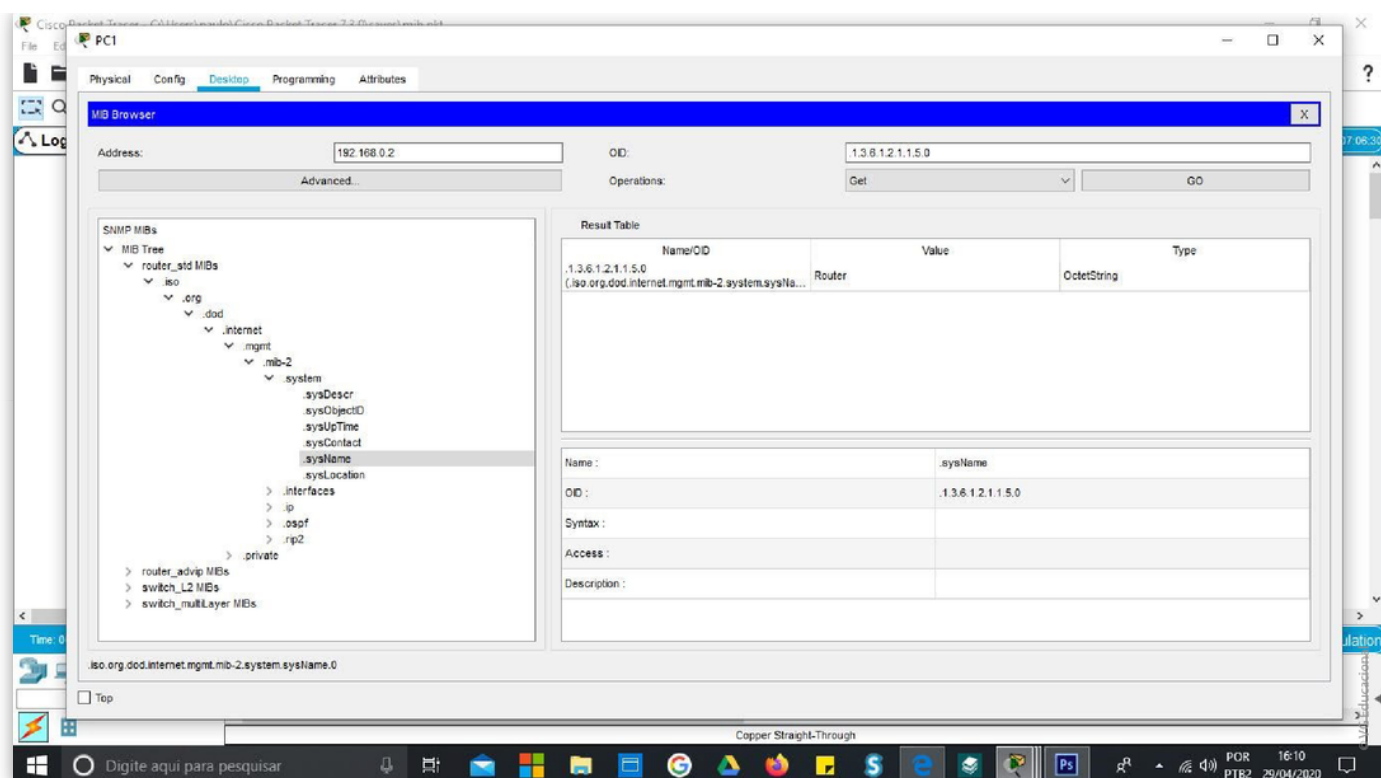


Figura 2.6 - Visualizando o nome do roteador no OID

Fonte: Elaborada pelo autor.

Por fim, precisamos mudar o nome do roteador para tal procedimento; altere o protocolo para *SET*, e uma nova pequena janela será aberta. Nessa janela configure um novo nome para o destino, opte pela opção *OctetString* e pronto. Agora, somente abra o roteador com o endereço 192.168.0.2/24 e clique na aba cli para verificar que o nome do roteador foi trocado.

Porém, há outros tipos de Mib Browser, como iReasoning Mib Browser apresentado na Figura 2.7.

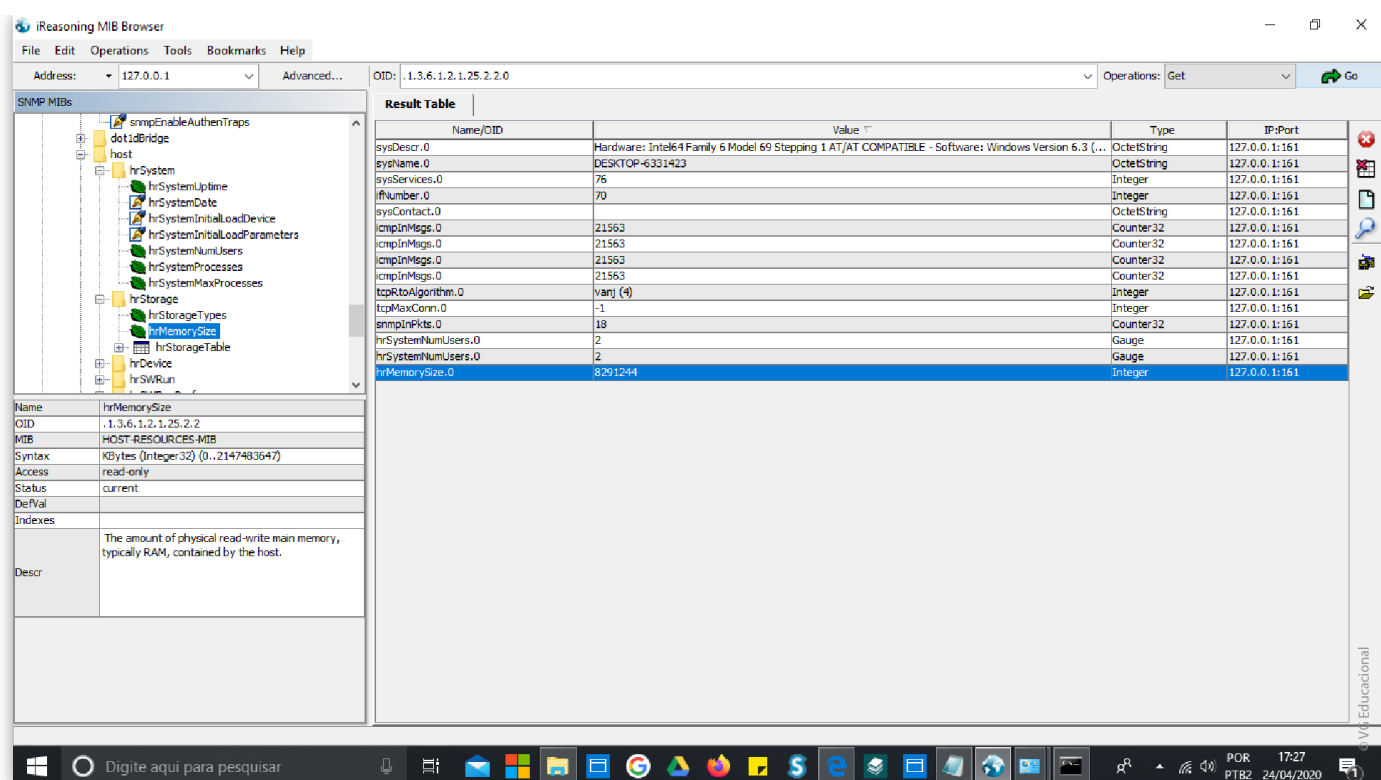


Figura 2.7 - Mib Browser iReasoning

Fonte: Elaborada pelo autor.

Na Figura 2.7, foi habilitado o SNMP para Windows 10 e configurada a TRAP (INTERRUPÇÕES) para uma comunidade SNMP public somente leitura (*read-only*). Uma observação importante no Windows 10 é que o protocolo SNMP tem que ser instalado via *Power Shell* .

Saiba mais

Você pode fazer um estudo do protocolo SNMP em sua máquina, o sistema operacional Windows 10, bastando seguir os passos do tutorial do site TheITBros. Você poderá usar o MIB Browser IReasoning ou outro qualquer para acessar as informações através do arquivo de MSFT-MIB.mib para equipamentos Windows. Vale a pena conferir! Você pode encontrar o tutorial no link a seguir.

[ACESSAR](#)

Observe que algumas informações foram recuperadas com o comando GET, como, por exemplo, a quantidade de memória (8Gbytes), em destaque na figura. No canto esquerdo, está a estrutura da MIB e, abaixo, informações sobre o objeto a ser lido. Em destaque, o hrMemorySize, seu OID .1.3.6.1.2.1.25.2.2.0, sua sintaxe KBytes (Integer32) (0..2147483647) e tipo de acesso read only. Como arquivo MIB para acesso às informações, foi utilizada a MSFT-MIB.mib.

Porém, o protocolo SNMP possui comandos que podem ser usados para análise também dessas informações, como os comandos SNMPWALK e SNMPGET. Esses comandos são os assuntos abordados no próximo tópico.

Comando SNMPWALK e SNMPGET

Nesse mundo da Internet, o modelo TCP/IP é o referenciado, e nesse padrão

temos o protocolo SNMP. Com recursos de comandos do protocolo, pode-se obter informações gerenciais da rede semelhantes ao uso de um MIB Browser, porém através de linhas de comando.

Temos, então, o comando `SNMPWALK`, que é um comando presente em um sistema de gerenciamento de segurança (SMS) que atua através de requisições `SNMPGETEXT` com o objetivo de obter informações sobre uma agente gerenciável na rede. Então, podemos utilizar o comando para obter informações passando um OID como referência, uma busca em todos os níveis da estrutura de árvore abaixo do referenciado será realizada e o resultado, retornado ao usuário.

O comando pode ser usado tanto em ambiente Windows quanto em ambientes Linux, mas, para efeito de ilustração de aplicação, vamos demonstrar o comando sendo aplicado a um servidor local Linux. Vale a pena lembrar que não é o objetivo a configuração do ambiente, mas a aplicação e o resultado do comando.

A sintaxe básica do comando é: *snmpwalk -v 1 -c public endIP (opcional OID)* , e como exemplos de comando, temos:

```
snmpwalk -v 1 -c public 192.168.0.2 .1.3.6.1.2.1.1
```

```
snmpwalk -v 1 -c public localhost system
```

```
snmpwalk -v 2c -c public localhost
```

onde `-v` é a versão (1, 2c, 3) do protocolo snmp, `-c` determina a string e comunidade, nos exemplos, `public`, o agente gerenciável, nesse exemplo, o servidor representado por `localhost` ou `endIP` (192.168.01) e, por fim, o OID pelo nome `system`.

Vamos ilustrar, pela Figura 2.8, o uso do protocolo `snmpwalk`, para buscar as informações no servidor linux:

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux appliance 4.18.0-147.8.1.el8_1.x86_64 #1
SNMP Thu Apr 9 13:49:54 UTC 2020 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (753) 0:00:07.53
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/sn
mp.local.conf)
SNMPv2-MIB::sysName.0 = STRING: appliance
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.7 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.8 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatchin
g.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for th
e SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
```

© VG Educacional

Figura 2.8 - Comando snmpwalk

Fonte: Elaborada pelo autor.

Observe que a imagem é um recorte de todas as informações sobre o host servidor linux, mas pode-se especificar com OID as informações que se deseja visualizar. O Quadro 2.2 demonstra o comando e o retorno da informação encontrada no servidor linux.

Comando	Descritivo	Resposta
snmpwalk -v 2c -c public localhost iso.3.6.1.2.1.1.1	Obtendo dados do servidor	iso.3.6.1.2.1.1.1.0 = STRING: 'Linux teste-VirtualBox 5.3.0-46-generic #38~18.0.4.1-ubuntu SMP Tue Mar 31 04:17:02 UTC 2020 x_86_64"
snmpwalk -v 2c -c public localhost iso.3.6.1.2.1.1.7	Obtendo o tipo de serviço	iso.3.6.1.2.1.1.7.0 = INTEGER : 72
snmpwalk -v 2c -c public localhost iso.3.6.1.2.1.1.5	Obtendo o nome do servidor	iso.3.6.1.2.1.1.5.0 = STRING: "teste-VirtualBox"

Quadro 2.2 - Exemplo de comando snmpwalk e resposta

Fonte: Elaborado pelo autor.

Compreende-se pelo quadro nome do servidor, especificação da versão do sistema 18.0.4.1, o tipo Linux Ubuntu. Outro dado interessante é que o sistema foi instalado em um ambiente virtual, VirtualBox, e usado para arquitetura 32 e 64 bits.

Porém, quando precisamos obter informações de um objeto gerenciável de rede, fazemos uso do comando SNMPGET. O protocolo SNMO usa requisições SNMPGET para solicitar informações de um roteador, impressora, servidor, passando como parâmetro o OID do objeto. O comando SNMPGET faz uso de um ou mais OIDs como passagem de parâmetros de comando de linha.

A sintaxe genérica do comando SNMPGET é snmpget [options] [community string/authentication information] [host name/address] [object Identifier]. Logo, podemos exemplificar o uso do comando por meio de algumas linhas de aplicação descritas a seguir:


```
snmpget -v 1 -c public localhost iso.3.6.1.2.1.1.5.0
```

```
snmpget -v 1 -c public localhost iso.3.6.1.2.1.1.7.0
```

```
snmpget -v 1 -c public localhost iso.3.6.1.2.1.1.5.0 iso.3.6.1.2.1.1.7.0
```

O retorno do comando será o valor setado na variável do identificador de objetos (OID). Nos exemplos expostos, no comando `snmpget -v 1 -c public localhost iso.3.6.1.2.1.1.7.0`, o valor do retorno seria INTEGER: 72.

Bem, como apresentado, os recursos de gerenciamento de redes são extensos, cheios de detalhes e merecem um planejamento de uso. Todavia, precisamos entender como esse fluxo de informações ocorre dentro do sistema, ou seja, como é o processo de comunicação no uso do protocolo SNMP. O próximo tópico vai explorar esse assunto.

praticar

Vamos Praticar

Usando uma ferramenta de leitura de MIB, faça um teste de gerenciamento em um host Windows e Linux. Utilize o aplicativo VirtualBox para criar a máquina virtual Windows e Linux, habilite o protocolo snmp em ambas as máquinas e faça a troca do nome do host pela ferramenta de leitura de MIB. Vamos praticar.

A Comunicação do Protocolo SNMP

Como já visto, o modelo de gerenciamento de redes com referência ao modelo TCP/IP, arquitetura da Internet, faz uso do protocolo SNMP, protocolo que fora adotado como um padrão de gerenciamento. Entretanto, vamos entender como a comunicação é realizada por esse protocolo para a gerência da rede.

Como já vimos no tópico anterior, o protocolo SNMP possui três elementos básicos que são a estação gerência com o sistema de gerenciamento e os agentes que são daemons que ficam executando e enviando informações à estação gerente dos dispositivos gerenciáveis por meio de requisições e respostas. Esse processo é muito similar a requisições cliente-servidor.

O protocolo SNMP pode fazer conexão via dois protocolos TCP e o UDP, mas seu padrão é o UDP. Ambos os protocolos são de camada de transporte e uma das principais diferenças entre eles é o tipo de orientação que esses protocolos utilizam, pois o TCP só envia a informação quando há um conexão realizada entre a origem e o destino, mas o protocolo UDP não precisa dessa conexão para que os dados sejam enviados.

Saiba mais

Se você ficou interessado em se aprofundar a respeito da arquitetura do protocolo SNMP, uma excelente leitura sobre qualquer protocolo são os Request For Comments. Leia a RFC 3411 que detalha com profundidade a arquitetura do protocolo SNMP. Boa leitura! Você pode encontrar o texto da RFC 3411 no link a seguir.

ACESSAR

O termo *handshake* é utilizado na conexão TCP para expressar a comunicação entre a origem e o destino no envio de dados, ou seja, o método utilizado para configurar uma conexão TCP na Internet (TANENBAUM; WETHERAL, 2011). Essa técnica de conexão faz uso de mensagens SYN (**SYN** *chronize*), ACK (**ACK** *nowledgement*) +SYNC, ACK para estabelecer a conexão.

O processo começa quando a origem (A) envia uma mensagem de sincronismo de envio de pacotes (SYN) para o destino (B) em seguida, e o destino recebe a mensagem (SYN) e responde à origem (A) com uma mensagem de conhecimento+sincronismo (SYN+ACK). Então, a origem (A) lê a mensagem enviada pelo destino, e envia um ACK ao destino (B). Somente após todos esses passos, a conexão é estabelecida (KUROSE; ROSS, 2013).

A partir desse ponto, a estação gerente através do protocolo SNMP utilizando o método *get-request* solicita informações ao agente que responde a estação gerente com uma resposta pelo SNMP utilizando o método *get-response* .

Como visto, o processo de envio e recebimento das informações do protocolo SNMP via TCP é totalmente dependente de uma conexão. Caso a conexão não

seja estabelecida, o gerenciamento não será realizado, ou melhor, não haverá comunicação entre os elementos estação gerente e agente gerenciável.

Por esse motivo, o protocolo TCP não é adequado ao protocolo SNMP, por depender de uma conexão; todavia, o protocolo SNMP, por padrão, faz uso do protocolo UDP, pois o protocolo UDP não precisa da conexão, ou seja, não precisa que haja uma conexão entre a estação gerente e o agente gerenciável, tornando o processo de comunicação mais rápido.

O processo de comunicação do protocolo SNMP, utilizando os protocolos TCP e UDP é mostrado na Figura 2.9, em que o item a ilustra o *handshake* feito primeiramente pelo protocolo TCP (orientado a conexão) e o item b ilustra o uso do protocolo UDP (não orientado a conexão).

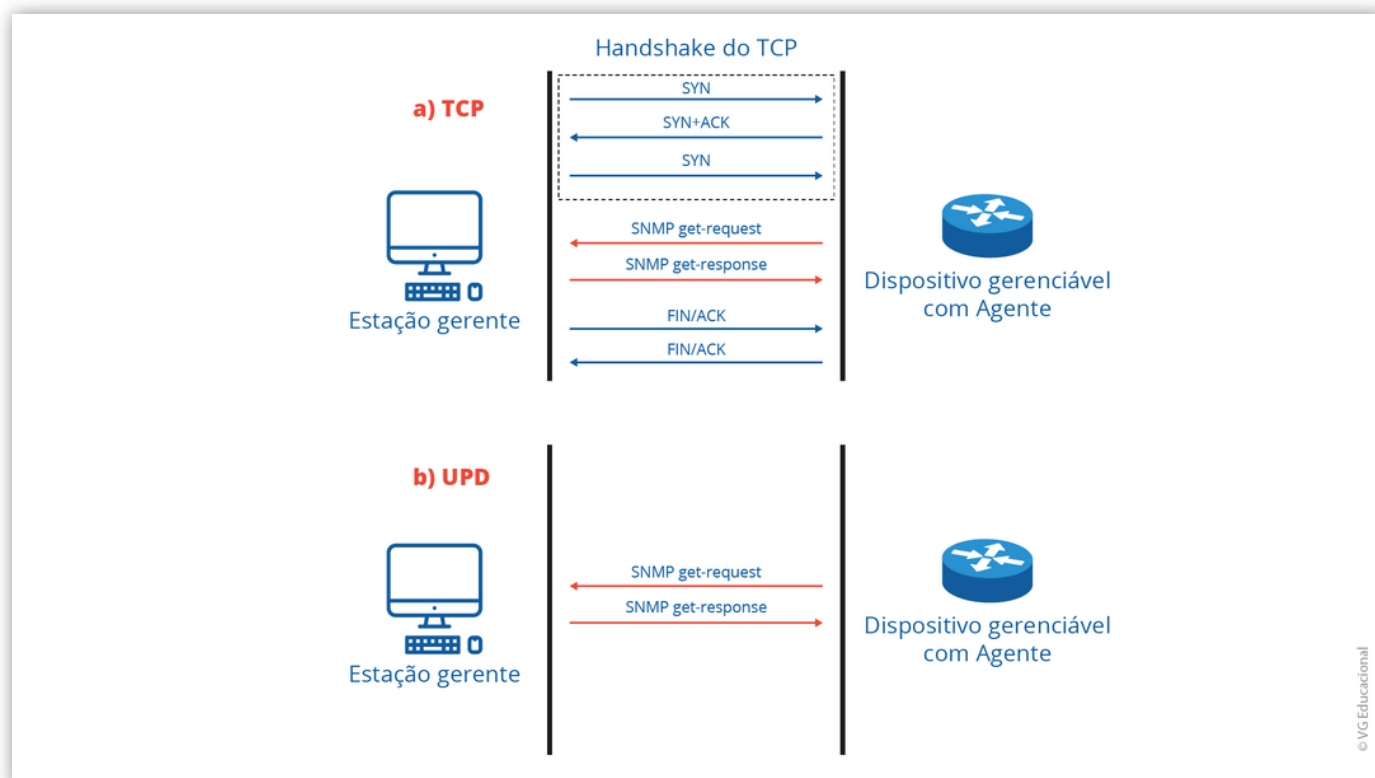


Figura 2.9 - Comunicação do protocolo SNMP, handshake. a) TCP, b) UDP

Fonte: Elaborada pelo autor.

Pode-se notar, pela Figura 2.9, item a, que há ainda um sinal de comunicação (mensagem) utilizada pelo protocolo TCP para encerramento (*FIN*alize) do processo de comunicação entre os elementos. Nota-se também uma similaridade com o sistema cliente-servidor em relação aos métodos *get-request* e *get-response* , pois na Internet, ao navegarmos, sempre o usuário

está requisitando uma página (*request*) e o servidor respondendo a essa requisição (response).

Logo, existe um cenário complexo de entendimento dos mecanismos de funcionamento da gerência de uma rede de computadores, porém, ferramentas são desenvolvidas com base nesses mecanismos com a finalidade de melhorar o monitoramento e gerenciamento dos elementos em uma rede que será nosso assunto do próximo bloco.

Vamos Praticar

O protocolo SNMP faz a comunicação via requisição e resposta. Durante o processo para estabelecer uma comunicação, o protocolo de gerenciamento utiliza diversos métodos, como métodos de sincronismo, de confirmação, entre outros. Assinale a alternativa correta que especifica o método e a respectiva definição correta de uma solicitação de uma estação gerente através do protocolo SNMP.

- ☐ **a)** GET-REQUEST.
- ☐ **b)** SYN, método usado para comunicação entre a estação gerente e o objeto gerenciável.
- ☐ **c)** ACK, método usado para comunicação entre a estação gerente e o objeto gerenciável.
- ☐ **d)** SYN+ACK, método usado para comunicação entre a estação gerente e o objeto gerenciável.
- ☐ **e)** GET-RESPONSE.

Ferramentas de Gerenciamento

Com o avanço das tecnologias, diversos softwares são usados para otimização de processos dentro de diversas áreas. No universo do gerenciamento de redes não é diferente, pois diversas ferramentas podem ser usadas como software de controle e gerenciamento da rede.

Diversas ferramentas são utilizadas para gerenciamento e monitoramento de redes de computadores, e para uma melhor compreensão, vamos apresentá-la em categorias, mas lembre-se de que todas, no entanto, podem ser úteis na gerência de redes.

Vamos começar com um registro de alguns comandos que são úteis e às vezes usados como ações por essas ferramentas, destacados a seguir (COMER, 2015):

- Ping: comando usado para verificar a conectividade entre origem e destino.
- Traceroute: comando utilizado para verificar os saltos entre a origem e o destino.
- Netstat: ferramenta utilizada para exibir estatísticas de conexão TCP,

UDP, protocolo de rede, interfaces e tabela de roteamento.

- Nmap: software que realiza varredura de portas.
- Nslookup: obtenção de informações sobre Domain Name Server de um determinado domínio.

Essas ferramentas podem ser usadas em Linux e alguns em Windows como o caso do *ping*, ilustrado pela Figura 2.10.

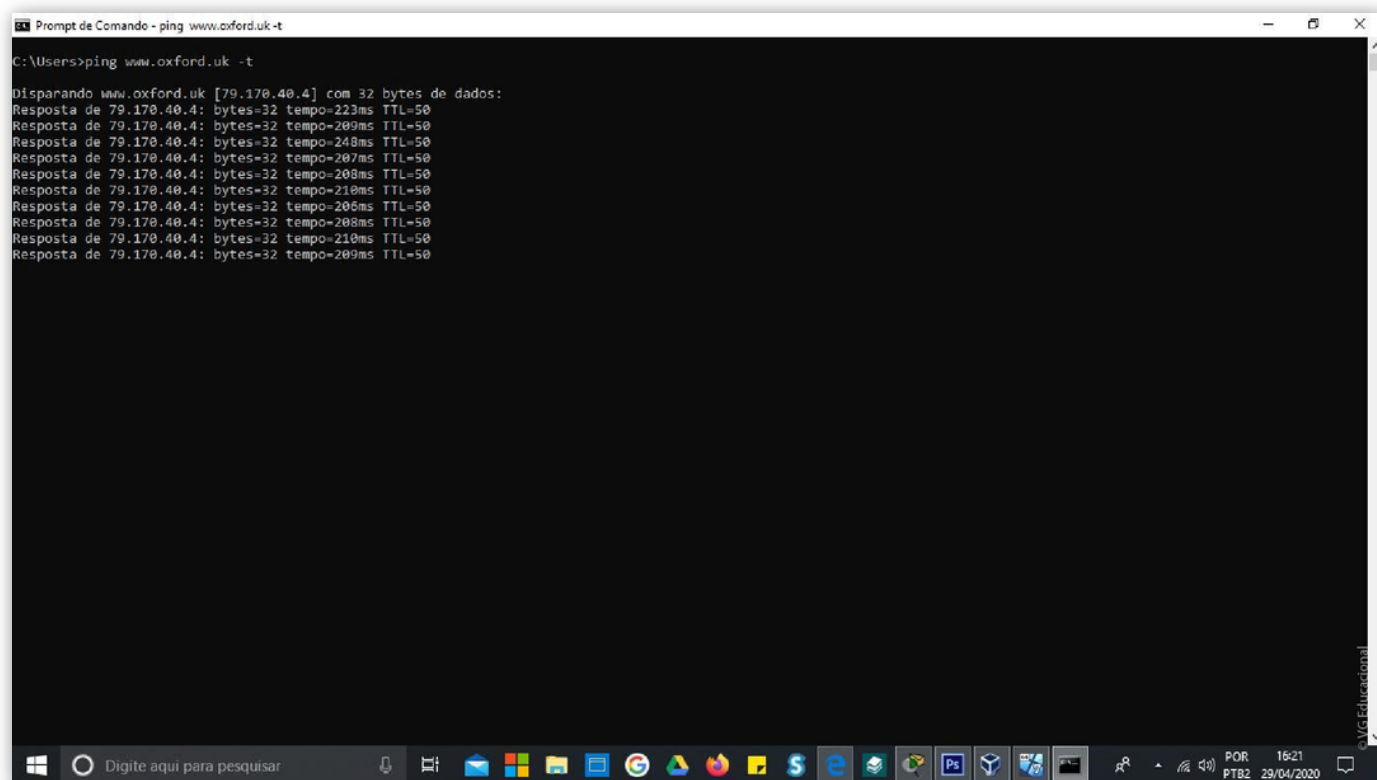


Figura 2.10 - Uso do ping via comando

Fonte: Elaborada pelo autor.

A Figura 2.10 ilustra o teste de conectividade via prompt do Windows ao site

Oxford Uk; a opção *-t* especifica tempo indefinido. O ping usa o protocolo *Internet Control Message Protocol* (ICMP), e são esses tipos de protocolos que podem ser analisados por ferramentas de análise de protocolos (COMER, 2015).

Ferramentas de Análise de Protocolos

Ferramentas analisadoras de protocolo têm a finalidade de analisar o fluxo de dados através de uma interface e podem ser úteis na gerência de rede, por exemplo, o tcpdump (Linux e Windows) e o software Wireshark (Windows e Linux).

Reflita

A questão de segurança é muito crítica em redes, principalmente quando o meio é a Internet. Hackers fazem uso de programas específicos para capturar senhas de usuários. Entretanto, será que é possível capturar senhas de usuários através de software que analisa protocolo?

Tanto o tcpdump quanto o Wireshark são analisadores de protocolos e pode-se ilustrar: Uma análise mais detalhada de centenas de protocolos; Captura ao vivo e análise off-line; Dados de rede capturados podem ser navegados através de uma gráfica.

Porém, outras ferramentas que agrupam todas essas funcionalidades, monitorar e gerenciar, de forma mais gráfica com facilidades de uso e entendimento do administrador de rede, são chamadas de ferramentas de gerenciamento de redes, destaque do próximo tópico.

Softwares de Gerenciamento

A área de gerenciamento e monitoramento de redes é dinâmica, pois, devido ao fato de a rede se tornar um sistema crítico para o negócio, empresas do

ramo procuram desenvolver soluções de softwares para atender as necessidades do gerenciamento, um mundo vasto de aplicativos e soluções ofertados por diversas empresas.

Nesse cenário constituído de várias aplicações, a escolha mais adequada é uma tarefa árdua para o administrador de Tecnologia da Informação ou de redes, pois algumas variáveis devem ser estudadas antes da aquisição e implantação do software de gerenciamento, como, por exemplo, custo de aquisição (licença), tempo de atividade/inatividade, alarmes ou alerta e como esses alertas são enviados, portabilidade, acesso fácil por diversas plataformas, customização da ferramenta, mapeamento da rede, utilização do protocolo SNMP, tipos de equipamentos que pode gerenciar, facilidade de uso, etc.

Essa decisão é altamente dependente do planejamento realizado pela equipe de Tecnologia da Informação baseada nos requisitos levantados e modelo de negócio da empresa. A equipe de TI dispõe de um universo de software ou ferramentas de gerenciamento e, dentro desse universo, existem as ferramentas pagas, que são aquelas que precisam de licença para serem usadas, e as ferramentas não pagas, gratuitas (sem licenciamento), mas também as chamadas *open source*, código aberto, relacionadas à licença *General Public Licence* (GPL).

O monitor PTRG da empresa Paessler é uma ferramenta paga que possui recursos avançados de gestão de redes de computadores. Essa ferramenta possui como ponto forte monitoramento de software, tráfego, dispositivo de forma gráfica e apresentação de forma hierárquica. Faz uso de diversas tecnologias em seu monitoramento, como SNMP, WMI, HTTP, entre outros (PRTG, 2020). Com relação ao custo, a ferramenta é cobrada por meio de planos diferenciados. Já o ManageEngine OpManager é uma outra solução de monitoramento e gerenciamento de redes que controla dispositivos, servidores, tráfego, falhas e possui templates pré-configurados e preço de aquisição em dólar (OPMANAGER, 2020).

Agora, vamos mostrar três outras ferramentas, porém não pagas, que também podem ser usadas no monitoramento e gerenciamento de redes de

computadores: o Nagios, o Icinga e o Zabbix.

Vamos começar pela ferramenta Icinga, que pode ser contratada por modelos de pacote desde um pacote básico a pacotes chamados *enterprise*, mais completos. Possui módulo *cloud* com suporte *Amazon Web Service* (AWS) e Microsoft Azure, além de gerar relatórios ao administrador e remotamente o monitoramento, podendo ser feito por tablet ou smartphone (ICINGA, 2020).

O Nagios é uma ferramenta usada para monitoramento de rede de classe empresarial, desenvolvida para ser estável e muito robusta e rápida. O software Nagios é instalado em ambientes Linux e pode fazer o monitoramento e gerenciamento de dispositivos em plataforma tanto Linux quanto Windows. A ferramenta Nagios tem suporte a monitoramento de rede, do servidor, de aplicativos, ferramentas de monitoramento, dispositivos Windows. Esse aplicativo faz parte da categoria de aplicativos de código aberto (*open source*). O Nagios monitora tanto os serviços quanto os hosts e alerta o administrador de redes quando há um problema bem como alerta quando esse problema é resolvido. Logo, protocolos de rede do modelo TCP/IP, incluindo SMTP, POP3, HTTP, NTP, ICMP, SNMP, entre outros, possuem suporte no Nagios (NAGIOS, 2020).

A ferramenta Zabbix também é uma ferramenta de monitoramento e gerenciamento de redes com base em código aberto (*open source*). Pode monitorar inúmeros parâmetros e uma solução de monitoramento distribuído de classe empresarial, uma ferramenta que permite que o administrador de redes possa ter uma visão completa dos recursos de rede pela emissão de relatórios e visualização de dados com base nos dados armazenados, portanto, recurso fundamental para a análise do planejamento de capacidade (UYTTERHOEVEN; OLUPS, 2010).

O Zabbix possui uma interface de usuário de plataforma Web, ou seja, seus recursos são configurados via interface web, permitindo uma acessibilidade de qualquer local. A escalabilidade do software Zabbix é grande, pois pode ser usada tanto em pequenas redes quanto redes de inúmeros equipamentos. Possui suporte a inúmeros protocolos da arquitetura TCP/IP. Sendo assim, o Zabbix será a ferramenta explorada no próximo tópico.

praticar

Vamos Praticar

Com o intenso aumento e expansão das redes de computadores, principalmente a integração com a Internet, diversas ferramentas são utilizadas para controlar e gerenciar o comportamento de servidor, roteadores, links etc. Muitas são pagas, outras são gratuitas ou livres, ou seja, não precisam de licença ou a *General Public Licence* (GPL).

Com base no descritivo anterior e em conceitos aprendidos, assinale a alternativa que apresenta uma ferramenta proprietária paga.

- ☐ **a)** Nagios.
- ☐ **b)** Zabbix.
- ☐ **c)** PTRG.
- ☐ **d)** Icinga.
- ☐ **e)** Traceroute.

Fundamentos da Ferramenta Zabbix

Agora que já fomos apresentados tanto ao protocolo de gerenciamento de redes e seus métodos quanto a ferramentas que nos ajudam na gerência de redes. Nesse tópico, vamos explorar um pouco mais a ferramenta Zabbix.

A ferramenta Zabbix permite diversas formas de fazer o gerenciamento e monitoramento de diferentes aspectos da sua infraestrutura de TI e, de fato, quase qualquer dispositivo de rede que deseja conectar a rede e ligar a ferramenta. Possui uma arquitetura semidistribuída e com Gestão centralizada. Embora muitas instalações tenham um único sistema central, é possível o uso de monitoramento distribuído com proxies, e a maioria das instalações será usar agentes Zabbix (UYTTERHOEVEN; OLUPS, 2010).

Algumas funcionalidades estão disponíveis no Zabbix para uso. Vamos a algumas delas:

- possui uma interface web centralizada e fácil de usar;
- existe um servidor que é executado na maioria dos sistemas operacionais semelhantes ao UNIX, incluindo Linux, AIX, FreeBSD, OpenBSD e Solaris;

- há agentes nativos para a maioria dos sistemas operacionais semelhantes ao UNIX e Microsoft (Versões do Windows);
- possui a capacidade de monitorar diretamente o SNMP (SNMPv1, SNMPv2c e SNMPv3) e dispositivos IPMI;
- tem a capacidade de monitorar diretamente as instâncias do vCenter ou vSphere, usando o VMware API;
- tem capacidade de incorporar gráficos e outros recursos de visualização;
- permite alertas e notificações com fácil integração com outros sistemas;
- possui facilidade de customização, incluindo templates;
- permite detecção de baixo nível (LLD) e capacidade de gerar itens, gráficos e gatilhos (entre outros) de forma automatizada.

Por gráfico, é possível compreender melhor a arquitetura do Zabbix, e essa arquitetura é mostrada na Figura 2.11. Nela, pode-se notar que o servidor Zabbix permite monitorar elementos diretamente conectados à rede principal, mas quando o monitoramento é realizado remotamente, o Zabbix faz uso de agente proxy para obter a informação.

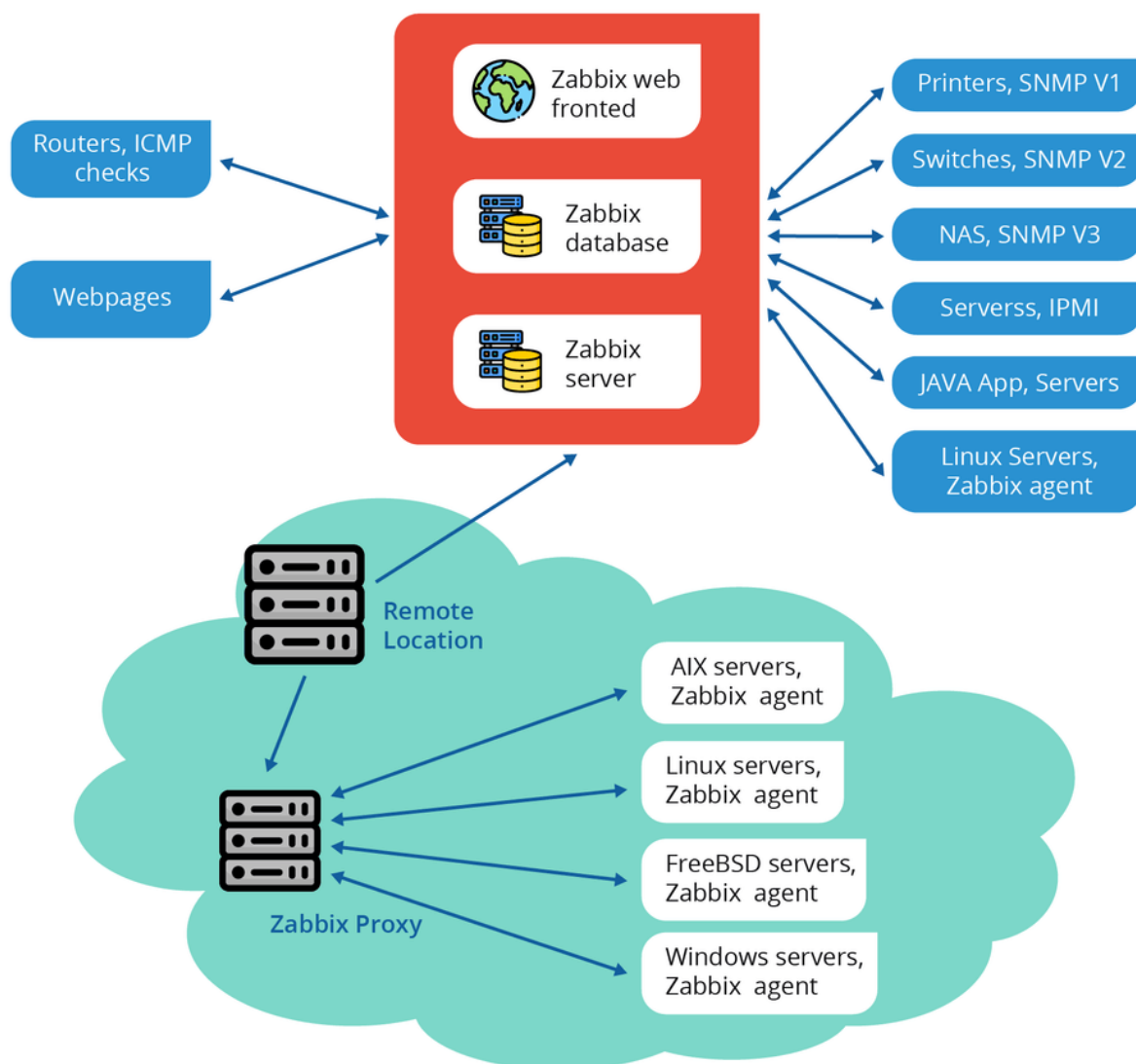


Figura 2.11. x - Zabbix, infraestrutura

Fonte: Uyterhoeven e Olups (2010, p. 50).

Então, podemos verificar que o Zabbix suporta um banco de dados e também acessa as suas configurações por meio de um front-end Web. As informações de acesso e configuração ficam armazenadas no banco de dados e, por isso, tanto o acesso local ou via web precisarão de acesso ao banco.

Como dito, o Zabbix é acessado por uma interface do usuário via plataforma web, logo, no próximo tópico, vamos abordar os principais menus dessa interface.

A Interface do Zabbix

Neste tópico, vamos apresentar os principais menus da Ferramenta Zabbix, mas lembre-se de que a ferramenta já está instalada e configurada em um ambiente virtual, pois o propósito é apresentado na interface web.

Como já visto, o acesso ao Zabbix é via interface Web. Essa interface não é muito complexa, pois apresenta um conjunto de cinco principais menus, e cada item do menu principal, um conjunto de submenus. A Figura 2.12 ilustra a interface do Zabbix.

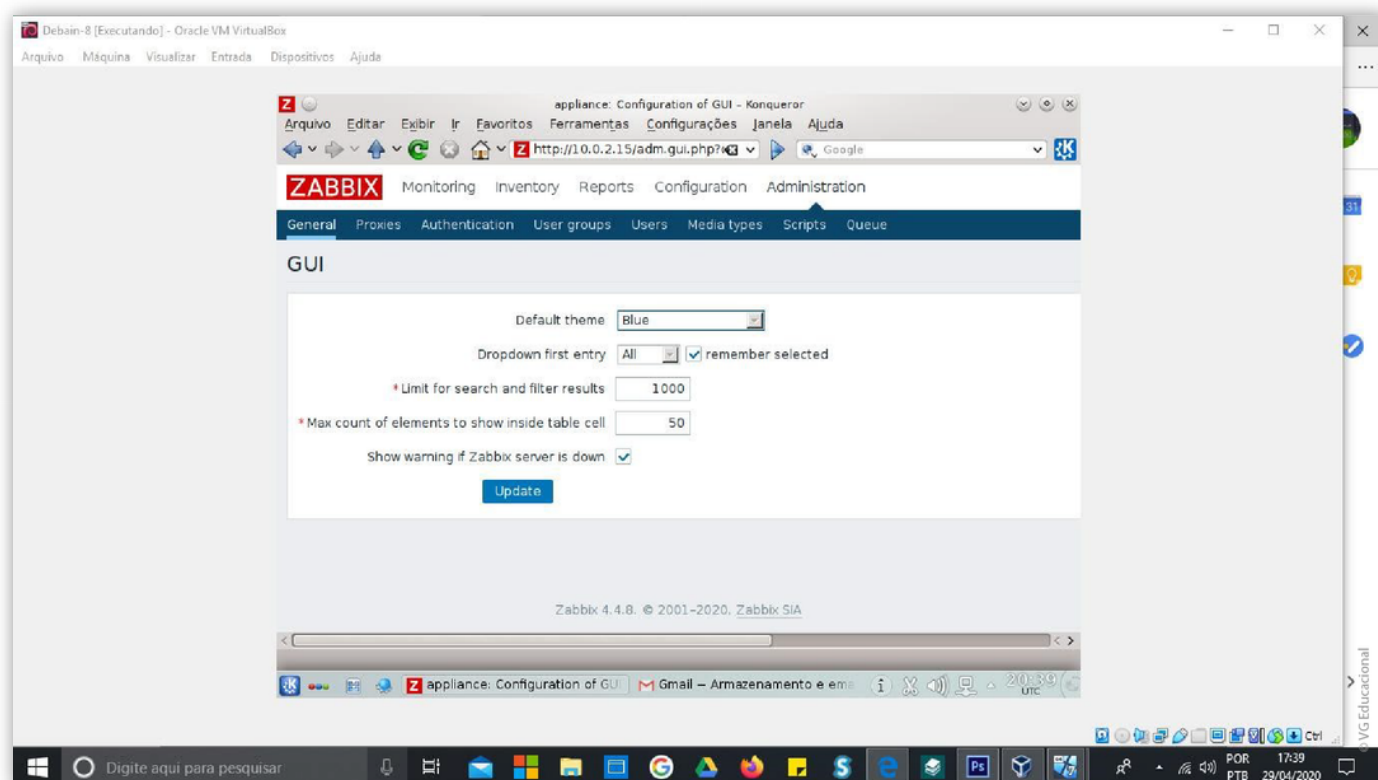


Figura 2.12 - Interface do Zabbix

Fonte: Elaborada pelo autor.

Pode-se notar pela Figura 2.12 os cinco menus principais: administração, monitoramento, inventário, relatório e configuração. Cada menu possui um conjunto de outros submenus. Como visto na figura, a aba administração está ativa e abaixo dessa aba estão ativos outros submenus, como geral, proxies e autenticação.

Então, vamos descrever os objetivos de cada menu:

Administração: como o próprio menu faz referência, nessa seção do Zabbix, algumas configurações gerais da ferramenta poderão ser configuradas como usuários, autenticação desses usuários, aspectos gerais da ferramenta como o

tema da interface, filas que mostram os tempos de atualização dos scripts, scripts que são ações executadas pelo Zabbix, entre outras.

Configuração: talvez seja a parte mais importante do Zabbix, pois nessa seção serão configuradas as ações de monitoramento, como host, template e manutenção.

Relatórios: exibe relatórios gerenciais sobre o sistema.

Inventário: esse menu tem a finalidade de mostrar inventário sobre o sistema, por exemplo, mostra as ações realizadas no sistema, por quem e quando.

Monitoramento: nesse menu, por meio de gráficos ou não, o administrador de redes poderá entender o que está acontecendo na rede.

Contudo, para um bom entendimento da ferramenta, há necessidade de prática, um entendimento teórico e muita experiência na área, porém, simulações podem ser feitas para a compreensão de como age a ferramenta. No próximo tópico, será mostrado como criar um monitoramento usando Zabbix.

Saiba mais

Se você deseja se aprofundar mais na prática do Zabbix, então não perca tempo. Instale a estrutura e comece a praticar. Você poderá encontrar como baixar e fazer toda a instalação do Zabbix, mas também informações mais detalhadas da aplicação no site do aplicativo na área de documentação. Boa prática! Você pode encontrar tudo sobre a instalação no link a seguir.

[ACESSAR](#)

Habilitando um Gerenciamento

O gerenciamento serve para analisar o comportamento da rede pelo administrador para que possa corrigir falhas e ser notificado de problemas corrigidos e serve também para analisar capacidade da rede para futuras expansões. Para tal cenário, a ferramenta Zabbix permite que o administrador de rede construa seu próprio modelo de gerenciamento e visualização do mesmo.

Antes de começarmos a criar um novo gerenciamento com a ferramenta, é necessário entender o processo de criação. O Zabbix possui template já prontos, mas o que são os template? Templates são um conjunto de aplicações a serem monitoradas, protocolos, alarmes, hosts etc. que já vêm pré-configurados, mas o administrador pode criar um customizado.

Vamos, então, construir um template. Para isso, clique no menu configuração,

submenu template e no botão criar. Na janela de criação de template, há necessidade de determinar um nome para o template, um nome visível, e um grupo. O grupo é um nome dado a um conjunto de aplicações com servidores Linux ou Windows. Preenchidas todas as caixas, clique em atualizar e seu template será criado.

Cada template criado possui aplicações a serem monitoradas, itens a serem ativados, triggers, que são os alarmes disparados, gráficos, que são as telas de monitoramento que determinam janelas a exibir informações, além de descoberta de web. Entretanto, os itens necessários para criação são aplicações, itens, gráficos e triggers.

Após a criação do template, há necessidade de criar o item. Um item é um processo que se deseja monitorar. No exemplo da Figura 2.13, é o servidor Apache, e algumas configurações podem ser setadas, como nome do processo, tempo de monitoração, tipo do agente e intervalo de atualização.

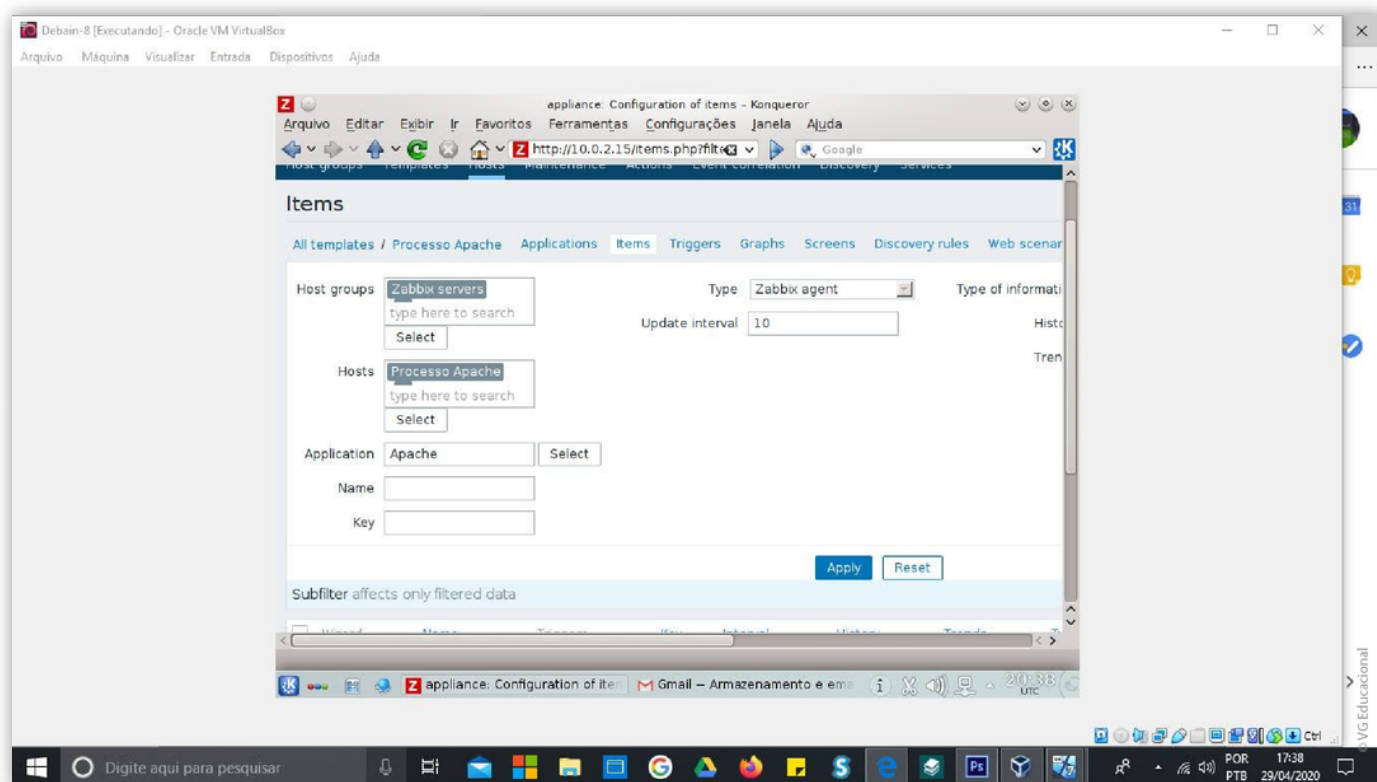


Figura 2.13 - Item, servidor apache

Fonte: Elaborada pelo autor.

Ok! Item criado, agora é necessário criar um trigger. Um trigger é um gatilho que se configura no Zabbix a respeito de um processo a ser monitorado.

Pode-se determinar no trigger a criticidade do processo, bem como criar expressões de monitoramento. A Figura 2.14 mostra uma configuração básica de um trigger.

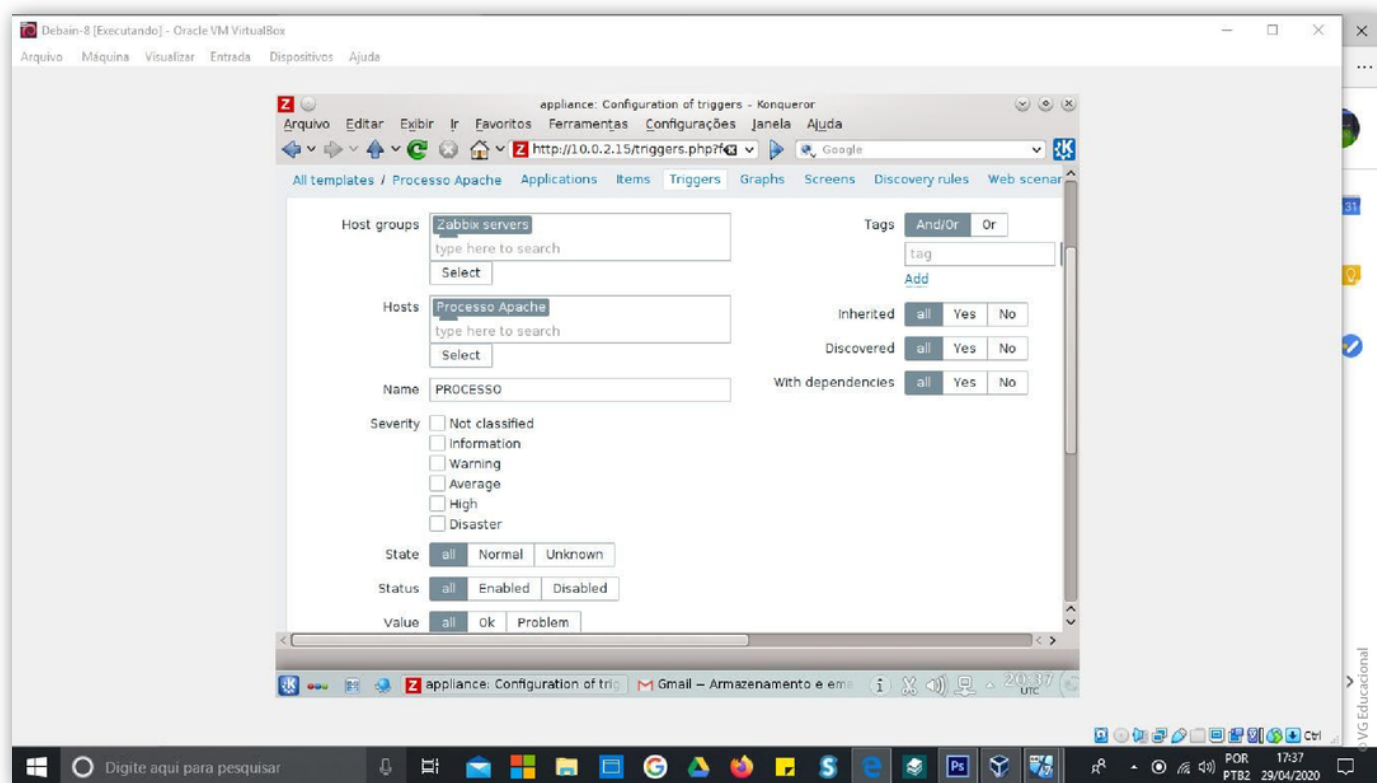


Figura 2.14 - Trigger

Fonte: Elaborada pelo autor.

O trigger bem como o item estão na subárvore de opções template, ou seja, fazem parte do mesmo template. No trigger da Figura 2.14, é mostrada uma expressão que é o identificador do template, o processo identificado por uma chave ({\$APACHE_PROCESSO}) e valores representados pelo número zero. O próximo passo é construir um host e aplicar ao *host* o *template* para que o processo de monitoramento seja ativado.

Lembre-se de que alguns erros podem ocorrer, por exemplo, se o trigger não estiver ativo, algum problema com a chave item, ou se o agente Zabbix não estiver ativo, verifique o *hostname* no arquivo de configuração do agente Zabbix. Se tudo estiver correto, o *host* precisa ser criado. Na sua criação, é necessário somente determinar um nome visível, o grupo a que ele pertence, como por exemplo Linux Server, e um template.

A partir desse momento, o Zabbix começa a monitorar o sistema e esse

monitoramento pode ser visualizado pelos gráficos. A Figura 2.15 mostra o monitoramento em forma de gradiente do servidor Apache no uso de memória.

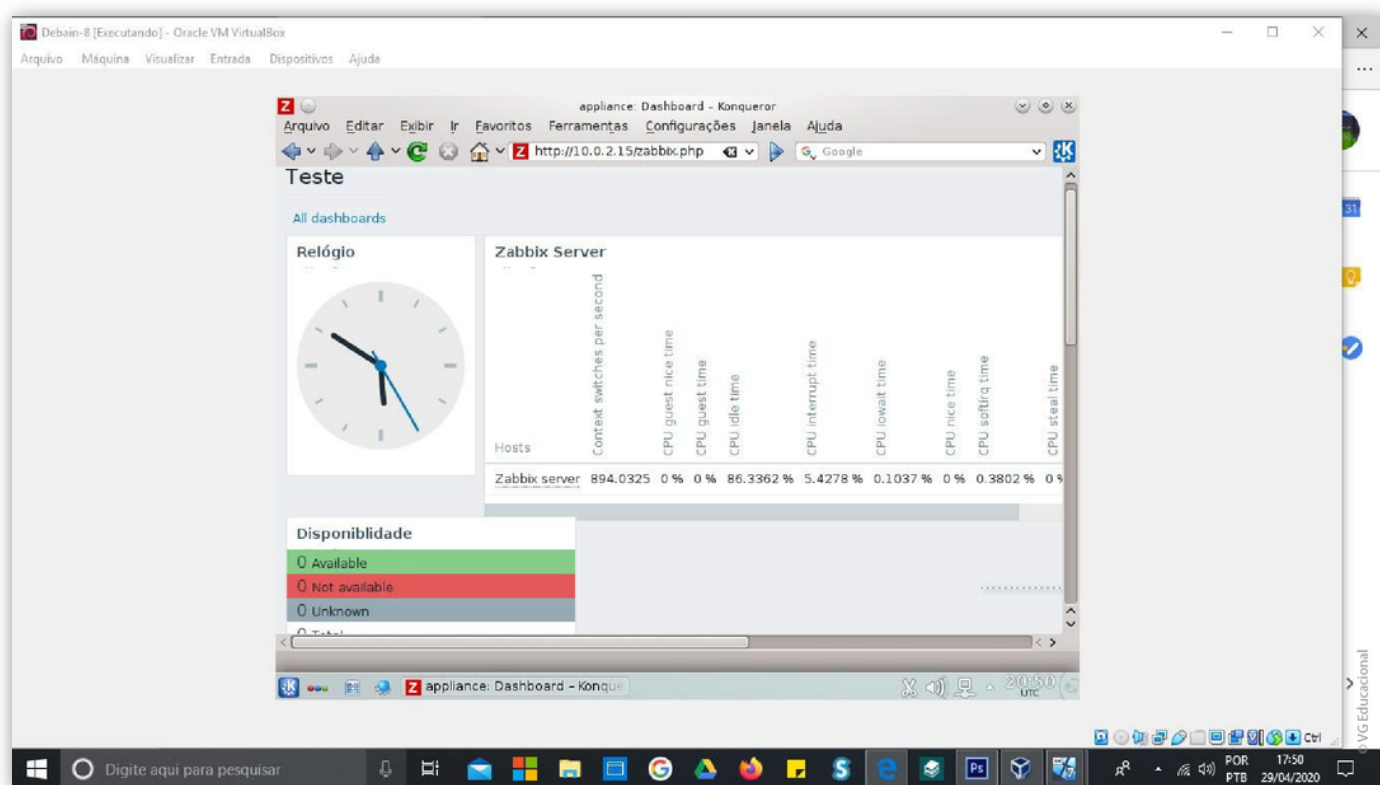


Figura 2.15 - Dashboard de monitoramento

Fonte: Elaborada pelo autor.

Note que a disponibilidade do servidor é expressada pelo número zero, indicando disponível, e caso esteja indisponível, indica 1, sinônimo de binário (0,1). Note que a ferramenta possui outros variados recursos de gerenciamento de redes, permitindo um melhor controle do administrador de rede.

praticar

Vamos Praticar

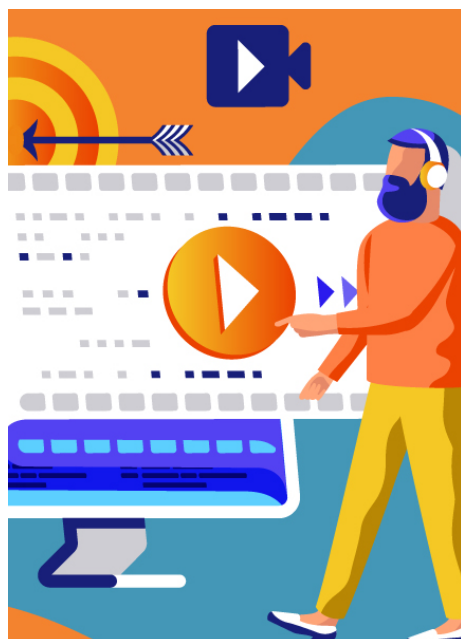
Há no mercado de gerenciamento de rede inúmeras ferramentas de monitoramento e gerenciamento de redes. O Zabbix é uma dessas ferramentas de código aberto, possui suporte a diversos protocolos como HTTP, SNMP, TCP, entre outros, e pode ser implementado em pequenas e grandes redes.

Assinale a alternativa que apresenta uma afirmação correta com relação às configurações do Zabbix.

- ☐ **a)** Um trigger é um template usado para mapear protocolos no Zabbix.
- ☐ **b)** Um item é um gráfico que pode ser usado para visualizar as informações.
- ☐ **c)** Templates são construídos com base nas configurações gerais.
- ☐ **d)** Hosts são os elementos predefinidos aplicados ao template e usados na monitoria.
- ☐ **e)** Gráficos podem ser customizados no Zabbix para exibição de informações.

indicações

Material Complementar



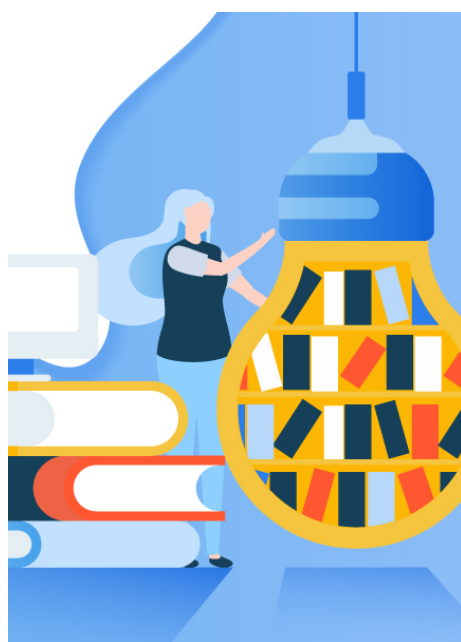
FILME

Tron

Ano: 2010

Comentário: Por se tratar de um tema moderno, realidade virtual, mostra intrinsecamente barreiras e desafios que serão enfrentados pelo administrador de redes. Futuro é a realidade virtual e também o futuro do universo de gerenciamento e monitoramento de redes. Então, esse filme traz uma ótima reflexão sobre o futuro do gerenciamento de monitoramento de redes. Para conhecer mais sobre o filme, acesse o trailer a seguir.

TRAILER



LIVRO

De A Zabbix: Aprenda a monitorar e gerenciar aplicações e equipamentos de redes com o Zabbix

Editora: Novatec

Autores: Adail Spínola Horst, Aécio dos Santos Pires, André Luis Boni Déo

ISBN: 978-85-7522-416-8

Comentário: Este livro explica o uso do Zabbix, desde a instalação ao monitoramento de serviços. Dê uma

atenção especial ao capítulo 12, pois é reservado especialmente ao protocolo SNMP. Esta é uma excelente leitura que enriquecerá seus conhecimentos a respeito da gerência de rede.

conclusão

Conclusão

Ao longo desta unidade, estudamos os conceitos sobre métodos do protocolo de gerenciamento SNMP, mas também conhecemos algumas ferramentas usadas para gerenciamento e monitoramento das redes de computadores.

Observou-se também que a comunicação se realiza pelo protocolo SNMP através da rede entre as estações gerente e os agentes, o chamado *handshake* . Por fim, apresentamos a ferramenta de código aberto Zabbix usada para monitoramento e gerência de redes. Nesta unidade, você teve a oportunidade de: entender como o protocolo SNMP faz a sua comunicação, analisar os métodos de linha de comando,

conhecer algumas ferramentas de mercado e entender o uso da ferramenta Zabbix.

referências

Referências Bibliográficas

COMER, D. E. **Computer Network and Internet** . New York: Addison-Wesley Professional, 2015. ISBN 0133587932.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. Porto Alegre: AMGH Editora, 2009.

ICINGA. **Documentação**. Disponível em: <https://icinga.com/>. Acesso em: 17 abr. 2020.

KUROSE, J.; ROSS, K. W. **Redes de computadores e a internet: uma abordagem top-down**. 6. ed. São Paulo: Pearson, 2013. ISBN 9788581436777.

NAGIOS. **Documentação**. Disponível em: <https://www.nagios.com/>. Acesso em: 17 abr. 2020.

OPMANAGER. **Documentação**. Disponível em: <https://www.manageengine.com>. Acesso em: 17 abr. 2020.

PRTG. **Documentação**. Disponível em: <https://www.paessler.com>. Acesso em: 17 abr. 2020.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3, and RMON1 and 2**. 3. ed. Massachusetts: Addison-Wesley, 1999. ISBN 0201485346.

TANENBAUM, A. S.; WETHERAL, D. **Redes de Computadores**. 5. ed. São Paulo: Pearson, 2011. ISBN 9788576059240.

UYTTERHOEVEN, P.; OLUPS, R. **Zabbix 4 Network Monitoring**. 3. ed. São Paulo: Packt Publishing, 2010.