GESTÃO E MONITORAMENTO DE REDES DE COMPUTADORES

REDES DE ALTA DISPONIBILIDADE, VIRTUALIZAÇÃO E GERÊNCIA DE ROTEADORES

Autor: Me. Paulo Sérgio Pádua de Lacerda

Revisor: Rafael Rehm

INICIAR

Introdução

Cara(o) estudante, seja bem-vindo(a) à disciplina de Gestão e Monitoramento de Redes de Computadores! A proposta principal desta unidade é apresentar os fundamentos associados a redes de alta disponibilidade, virtualização e gerência de roteadores.

Com a internet, muitos serviços e produtos estão convergindo para o mundo digital, e a disponibilidade da rede é essencial para a continuidade do negócio. A virtualização é um serviço em crescimento nas empresas, pois permite diversos benefícios, como facilidade no aumento de capacidade de hardware. Nesse cenário de internet, o roteador tem papel fundamental na conexão das redes.

Em suma, você vai compreender e entender os fundamentos relacionados a alta disponibilidade, virtualização e aplicação do SNMP em roteadores. Vamos lá?

Arquitetura de Alta Disponibilidade

Na corrida das empresas para serviços e produtos convergindo para o mundo digital – a internet –, a inatividade dos servidores é um ponto crítico do negócio, pois eles devem funcionar plenamente. Todas as informações ficam armazenadas em servidores, de e-mail, arquivos, banco de dados, web, etc. (FOROUZAN, 2009).

Com o objetivo de não ocasionar perda de produtividade a negócios da empresa, a arquitetura de alta disponibilidade provê mecanismos que garantem o funcionamento pleno dos servidores de rede, pois permitem detecção de falhas, correção e monitoramento da rede, evitando a indisponibilidade dos serviços. Logo, manter disponibilidade do serviço permite diversos benefícios, como diminuição das e ações corretivas, suporte à expansão do negócio e minimização do impacto em caso de falhas ao negócio. Por isso, é fundamental a manutenibilidade da disponibilidade dos serviços na rede.

Disponibilidade

A disponibilidade é a garantia de que o serviço não fique fora do "ar", ou seja, não pare de funcionar. Vamos a um pequeno exemplo: vamos supor que a venda de ingressos para um determinado clássico seja totalmente on-line, e a abertura para as vendas seja na quinta-feira, sendo que o jogo será realizado no domingo, às 16h. Agora, imagine uma carga de tickets para 50.000 torcedores de ambos os times. Suponha que o sistema fique indisponível para a venda durante um período de 12 horas, da sexta às 18h até as 6h de sábado, e, somente após esse período, volte ao normal. Quanto de prejuízo a paralisação causa no negócio? Qual o impacto negativo com relação ao sistema ou à empresa que oferece o serviço para os times e também aos usuários? Qual o custo de retrabalho para colocar o sistema no "ar" novamente? Então, a alta disponibilidade se torna um ponto fundamental quando se trata de negócio via internet.

A disponibilidade pode ser calculada, segundo Ferreira e Santos (2005, p. 2, apud DANTAS, p. 58, 2008), pois "a disponibilidade é uma medida calculada como sendo a percentagem de tempo que um determinado componente da arquitetura (e.g. disco, servidor) está em funcionamento para o usuário final". Podemos quantificar esses valores através da fórmula:

Disponibilidade = **(Unidade de tempo total – downtime) / Unidade de tempo total** sendo que downtime é o tempo em que o servidor ficou indisponível.

A unidade de tempo total refere-se ao tempo de disponibilidade do servidor.

Agora, vamos ilustrar a fórmula com o seguinte cenário: vamos supor um serviço web de uma loja on-line (24x7) operando durante dez dias. Então, o servidor ficou disponível em um tempo total de 240 horas. Agora, suponha que o servidor tenha ficado em *downtime* total de 4 horas. Qual será a disponibilidade do servidor?

D = (240 – 4) / 240 = 0,98%.

Mas será que é o suficiente? Será que o sistema ficou parado justamente no momento de pico e causou um impacto financeiro ao negócio? Um ponto importante sobre alta disponibilidade é a gerência, pois manutenção

preventiva sempre é melhor do que a corretiva. Outro fato é que trabalhamos com produtos eletrônicos, discos rígidos, memórias, conectores, mas também com sistemas elétricos de alimentação etc., e esses sistemas podem falhar a qualquer momento, mesmo que os fabricantes garantam certa confiabilidade de operação.

Mas há um parâmetro de análise chamada regra dos noves (9), ou seja, quanto mais noves existir no percentual de resposta do cálculo da indisponibilidade, menos tempo de *downtime* ocorrerá. O Quadro 4.1 demonstra os números e o tempo de indisponibilidade, parada, de um servidor como exemplo.

Disponibilidade	Tempo parado por ano
99,999%	5,24 minutos
99,990%	52,42 minutos
99,950%	4,27 horas
99,900%	8,74 horas
99,000%	3,65 dias
90,000%	36,5 dias

Quadro 4.1 - Tempo de *parada* por ano
Fonte: Ferrigolo (2001, p. 9).

Entretanto, a garantia de uma alta disponibilidade em redes é determinada pela implantação de mecanismos, incluindo redundância, sistema em clusters etc.

Mecanismo de Alta Disponibilidade

O objetivo dos mecanismos de garantia de um sistema de alta disponibilidade é garantir ou minimizar ao máximo o tempo de *downtime* dos servidores e minimizar impactos ao negócio. Por isso, alguns mecanismos são implantados na rede que propicia essa disponibilidade de *uptime* (tempo de funcionamento dos servidores) em pleno funcionamento. Esses mecanismos são:

- **Redundância** : redundância em tecnologia da informação é sinônimo de duplicidade, pois os dispositivos mais importantes da rede, como o link principal ou servidor, podem ser duplicados com o objetivo de manter a continuidade do sistema. Pode-se, por exemplo, usar serviços de servidores em redundância para balanceamento de carga, ou seja, não criar overhead em servidores, criar redundância de armazenamento, como os mecanismos de sistemas de *Redundant Array of Intelligent or Inexpensive Disks* (RAID) ou mesmo criar redundâncias de links e fontes de alimentação de servidores.
- **Sistema de clusters** : são sistemas de aglomerado de computadores que estão ligados entre si, de modo que podem ser vistos como um único equipamento. Cada equipamento dentro de um cluster é um nó e, de forma transparente, quando um servidor falha, a requisição para esse servidor que falhou é transferida para outro nó do cluster de forma transparente ao usuário. O software de código aberto *Heartbeat* é uma ferramenta de criação de cluster de alta disponibilidade.

saiba mais

Saiba mais

Ficou curioso a respeito da ferramenta Heartbeat? Se deseja saber mais sobre o software, sua implantação e conceitos de operação, faça uma visita ao site Linux-ha.org e descubra como implantar o sistema de alta disponibilidade com Heartbeat. Sem dúvidas, na área de TI, é uma das melhores formas de obter conhecimento. Boa leitura e prática!

ACESSAR

- **Escalabilidade** : define-se como escalabilidade a capacidade do sistema de crescer de forma transparente, ou seja, ter a capacidade de suportar os serviços fornecidos em gerenciá-los em momento de aumento de requisições e tráfego.
- **Monitoramento** : monitorar e gerenciar a rede com métricas bem-definidas é fundamental para a garantia de um sistema de alta disponibilidade. Por isso, há a necessidade um bom planejamento e de quais equipamentos e serviços precisam ser gerenciados na rede, incluindo monitoramento de carga, logs, banco de dados, de sistema intrusos (malwares), recursos, erros, etc.

Segurança

“Tolerar as falhas” resume a segurança dos sistemas de alta disponibilidade,

pois todos os sistemas têm que ser tolerantes a falhas (*failover*), pois os projetistas de rede precisam garantir uma confiabilidade do sistema. Um sistema confiável é um sistema com poucas falhas ou com pouca indisponibilidade.

Mas como garantir uma tolerância a falhas? Uma das opções é a técnica de replicação. A réplica ativa (redundância) trabalha com dispositivos duplicados (primário e secundário), caso um dispositivo primário fique inoperante, o sistema configurado como secundário é ativado automaticamente, tornando-se primário. Ao contrário da réplica ativa, a passiva, por exemplo, faz uso de servidores de backup e uso de mecanismo de logging e checkpoint. Aplicativos como o HeartBeat podem ser usados na gerência de rede, embora seus *inputs* na rede possam aumentar o fluxo, eles podem ser usados com monitoramento dos estados dos servidores. Para fins didáticos do funcionamento de uma ferramenta de gerência de falhas, usaremos o Heartbeat. O aplicativo Heartbeat faz uso do protocolo *User Datagram Protocol* (UDP) para envio de mensagens (*keepalive*) entre os nós (servidores) no cluster. Caso um desses nós não receba a mensagem de *keepalive* no tempo determinado, há um conjunto de operações que tem a finalidade de transferir ações para os demais servidores e de forma transparente ao usuário final. Pois todos os serviços são aglomerados em um grupo de recursos, incluindo softwares de aplicações, endereços IPs, sistema de armazenamento, diretórios, etc. e designado por um *ResourceGroup* .

Esse recurso é configurado em todos os nós do clusters, porém ativo somente no nó principal. Porém, se existir uma falha do nó principal, o nó determinado como secundário passa a exercer todas as funções do nó principal. Essa transferência de funções é chamada de *takeover* . A Figura 4.1 ilustra uma situação de *takeover* .

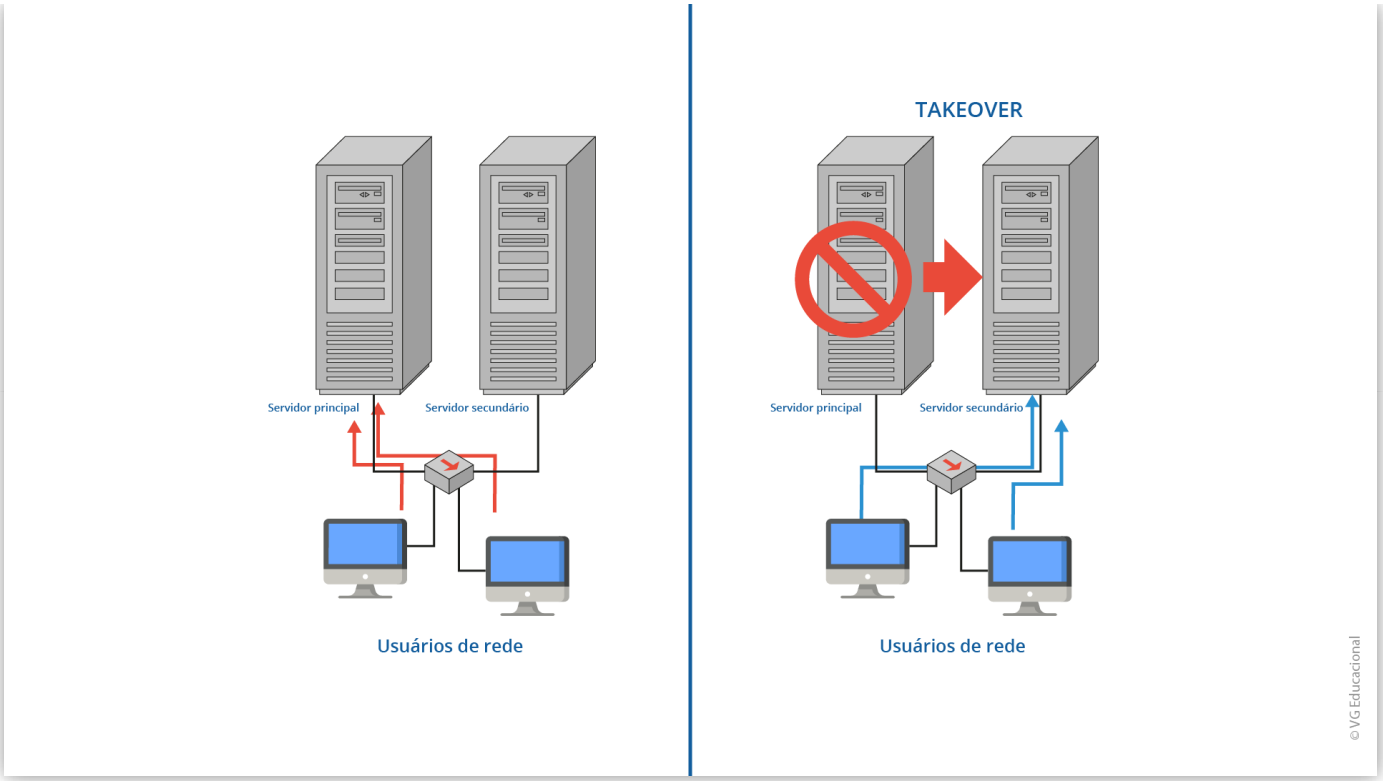


Figura 4.1 - Situação de takeover
Fonte: Elaborada pelo autor.

Todavia, há a compreensão de que existe um tempo e uma convergência da rede para que todos os nós entendam que os serviços passem a ser fornecidos pelo servidor secundário, mas não influenciem na indisponibilidade do negócio. Em suma, a arquitetura de alta disponibilidade precisa:

- Garantir minimização de falhas ou interrupções;
- Garantir não perda de informações;
- Garantir a continuidade do negócio através do funcionamento pleno da rede;
- Reduzir custos relativos a operações de *downtime* .

Porém, com o aumento dos serviços via internet, as empresas passam a comprar serviços de infraestrutura on-line ou em nuvem, assunto que será tratado no próximo tópico.

praticar

Vamos Praticar

Garantir a continuidade de negócio de empresas, às vezes, passa por implantação de sistema de alta disponibilidade. Serviços *on-line* estão diretamente associados a um desempenho de rede a pleno funcionamento. Garantir que o uptime da rede não tenha falhas depende da implantação de alguns mecanismos.

Assim, assinale a alternativa correta com relação à implantação de um mecanismo que atenda à alta disponibilidade da rede.

- **a)** Redundância somente das fontes de alimentação e dos servidores de rede.
- **b)** Monitoramento de todos os roteadores da rede e somente o servidor principal.
- **c)** Sistema de cluster com dois servidores, o principal e o secundário apenas.
- **d)** Escalabilidade nos momentos de maior exigência de requisições.
- **e)** Uso de softwares que fazem uso do protocolo de garantia de conexão TCP.

Virtualização e Implicações no Gerenciamento

O processo de virtualização está em crescimento na adoção pelos departamentos de Tecnologia da Informação nas empresas. Virtualizar um servidor é usar um aplicativo, seja VMware, Hyper-V ou VirtualBox, para criar servidores virtuais sob o mesmo host físico.

A virtualização é um processo que permite diversas facilidades, como customização, diminuição de preços, segurança, escalabilidade e integração. Diversas empresas oferecem o serviço de virtualização, como Infraestrutura como Serviço (IaaS), e permite pacotes que atendem à sua necessidade e que o pagamento seja com base na demanda solicitada.

Vamos a um exemplo de virtualização: suponha que uma determinada empresa tenha cinco servidores: e-mail, aplicação, web, firewall e autenticação. Esses servidores são físicos, porém internos na empresa. O processo de virtualização é criar Máquinas Virtuais (VM) usando um determinado produto de virtualização em uma única máquina e eliminar os hosts físicos. A Figura 4.2 ilustra esse cenário de um host com cinco VMs criadas.

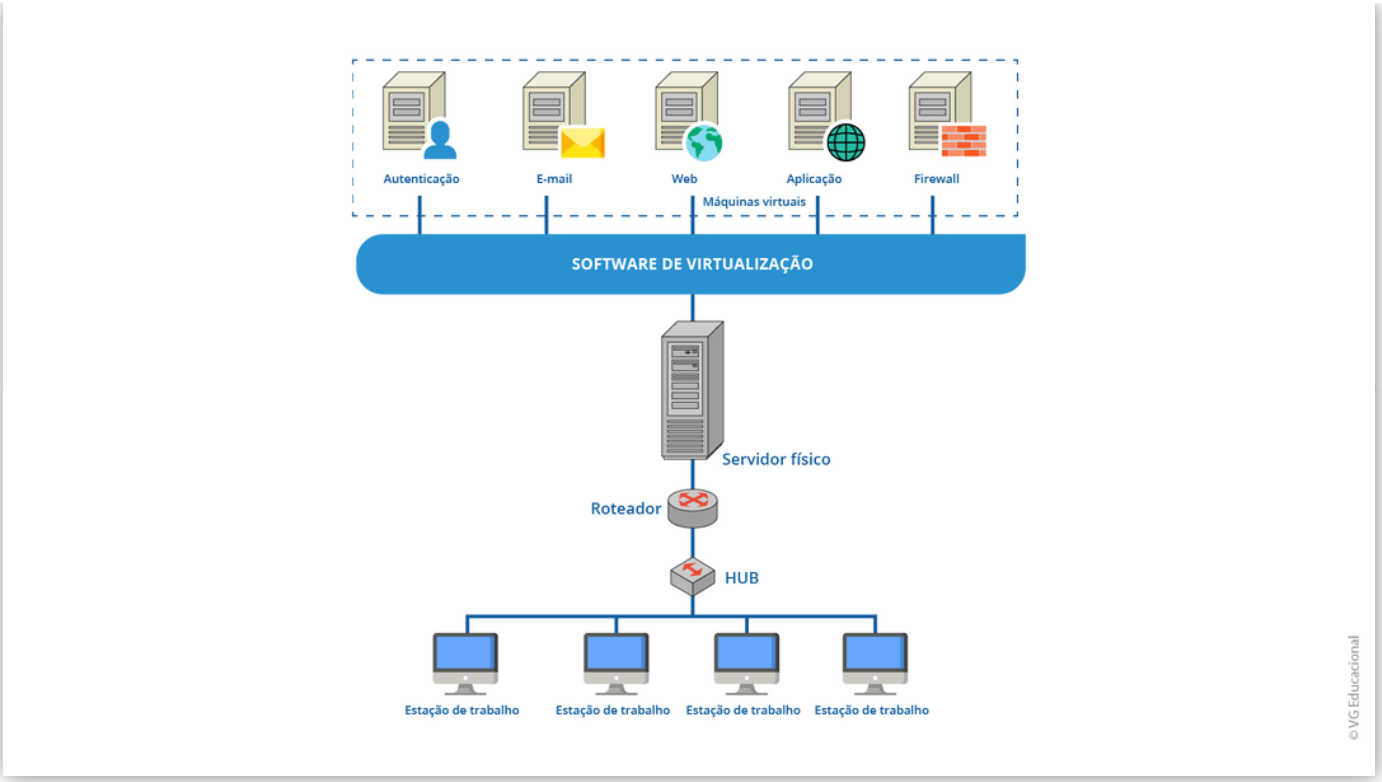


Figura 4.2 - Host com VMs
Fonte: Elaborada pelo autor.

Então, pode-se entender pela Figura 4.2 que tudo fica consolidado em um único servidor físico. OK! Você pode até pensar que o servidor principal fica indisponível, todos os serviços de rede param e a empresa para. Verdade, porém sabemos que, em uma infraestrutura de alta disponibilidade, um dos requisitos é a redundância de elementos críticos no caso, servidores com a mesma estrutura. Mas focamos somente o processo de virtualização e seus benefícios:

- Consolidação de servidores: todos os servidores em um único local;
- Espaço físico: diminui o espaço físico necessário para os servidores;
- Custo: diminui o número de elementos necessários para construir toda a infraestrutura de rede como racks, switches, cabeamento, consumo de energia elétrica, etc.;
- Facilidade de administração: um dos problemas relativos à manutenção de rede, ou seja, como tudo está integrado em um único local, com a virtualização, fica mais fácil administrar a rede, inclusive na integração de serviços menos utilizados;
- Criação de novos servidores: servidores físicos são mais custosos de serem criados, pois precisamos da máquina física e o sistema

operacional + software instalado para criação desse servidor. No caso da virtualização, novas máquinas são criadas em questão de alguns cliques a partir de configuração nova ou de um modelo preexistente, tornando o processo fácil e rápido.

- Maior confiabilidade e segurança do sistema: uma solução de virtualização adiciona uma camada de abstração entre a máquina virtual e o hardware físico subjacente;
- Escalabilidade: capacidade de expansão do hardware sem a necessidade de um hardware físico. Por exemplo, caso se queira aumentar a capacidade de memória de uma VM, será necessário somente aumentar a capacidade da memória existente na máquina virtual. A Figura 4.3 mostra a tela do software de virtualização VirtualBox que aumenta a capacidade de memória.

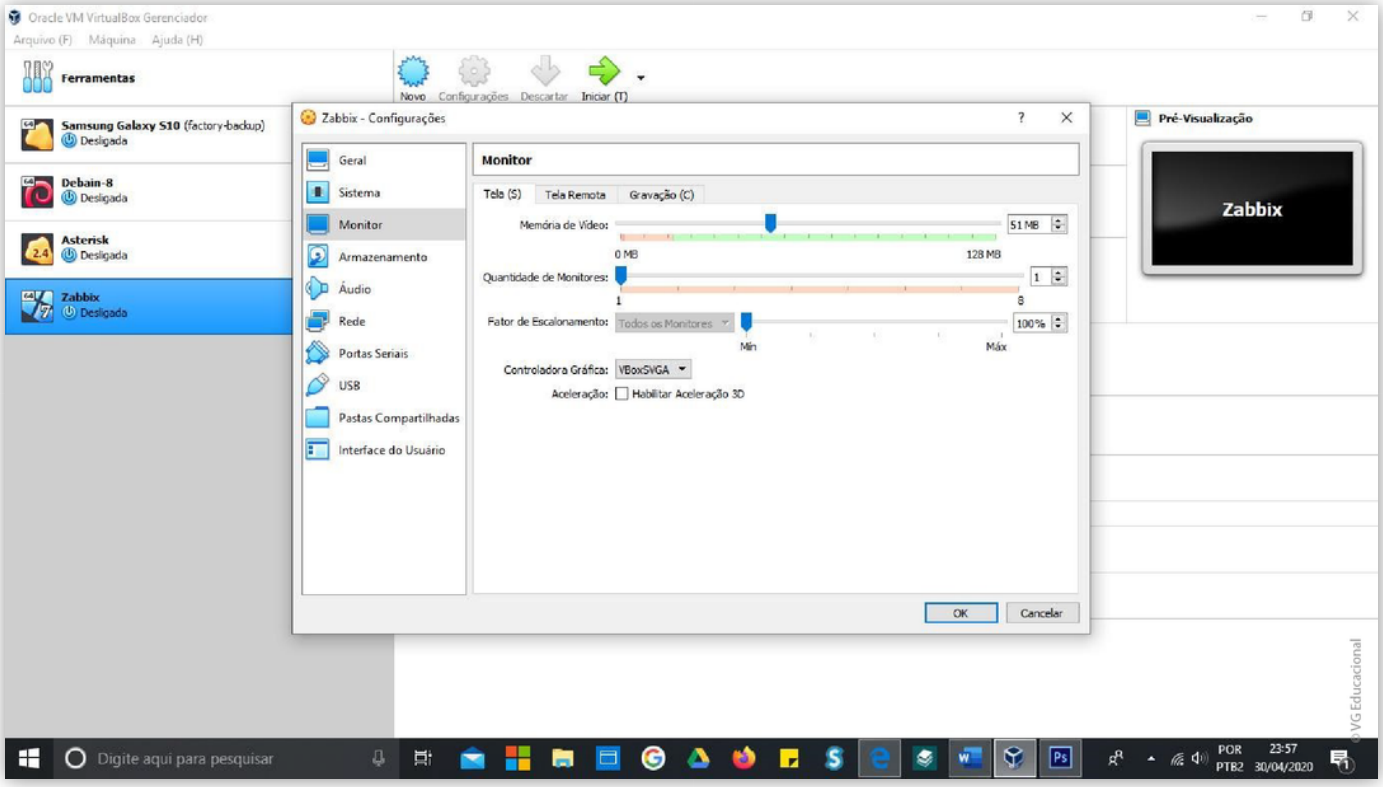


Figura 4.3 - Aumento da capacidade de memória no VirtualBox
Fonte: Elaborada pelo autor.

Em data center, por exemplo, existe o processo de virtualização em grande expansão, pois, além das características positivas descritas anteriormente, alguns outros benefícios também são garantidos, como:

- **Independência do sistema operacional** : a virtualização é tudo

sobre a criação de uma camada de abstração entre o hardware do host e um hardware virtual para os sistemas operacionais convidados em execução em cima da pilha.

- **Balanceamento dinâmico de carga** : lembre-se de que o balanceamento é dependente de políticas definidas. Todavia, à medida que as cargas de trabalho do servidor variam, a virtualização fornece a capacidade para máquinas que estão utilizando os demais recursos de um servidor, a ser movido para servidores subutilizados, com base nas políticas definidas.
- **Segurança** : há diversas opções de segurança para servidores, incluindo firewalls, software antivírus, monitoramento e proteção contra intrusão, etc.

Saiba mais

No mundo de Tecnologia da Informação, a Amazon é uma das grandes fornecedoras de serviços usados pela grande maioria das empresas, bem como criadora de novas tecnologias. O Serviço da Amazon Web Service e o serviço em Nuvem da empresa são providos de serviços como *Elastic Compute Cloud* (EC2). Vale a pena conferir os benefícios da virtualização através do EC2.

ACESSAR

Uma valiosa vantagem de serviços virtualizados, principalmente, em nuvem é a atualização do software, por contrato, pode-se garantir que o software sempre esteja atualizado. Esse ponto positivo é uma das premissas de optar por uma estrutura via IaaS do que física no ambiente interno. Por exemplo,

em caso de incidente na rede, as seguras irão contestar todos os firmwares da rede, se estão atualizados ou quando foi feita a última atualização.

Mas e para a gerência? Existem outros mecanismos que podem ser aplicados? A resposta é o assunto abordado que será abordado no próximo tópico.

Entidade e Padrões

Como já abordamos, a virtualização é um avanço na implantação de redes de computadores, porém, como quase tudo no universo de redes, há padrões. “Padrões são normas determinadas e aprovadas consensualmente pela maioria, ou por uma autoridade, que é usada como base para estabelecer uma comparação” (DICIO, p. 1, 2020).

A *Distributed Management Task Force* (DMTF), no domínio dos padrões de gerenciamento aberto, abrangendo diversas áreas em crescimento no universo de redes de computadores, desenvolve padrões para infraestrutura (DMTF, 2020). Esses padrões podem ser aplicados tanto a tecnologias tradicionais quantos a novas tecnologias como virtualização, nuvem, servidores e unidades de armazenamento. De forma colaborativa, membros e parceiros como *American National Standards Institute* (ANSI) e *Open System Interconnection* (OSI) contribuem para a melhoria da gestão na área da TI. Diretores de renomadas companhias associadas ao universo de TI fazem parte do conselho da DMTF, como Cisco, Hewlett Packard Enterprise, Intel Corporation, etc.

Reflita

No mundo há organizações sem fins lucrativos que são conhecidas por um nome como Cruz Vermelha. Mas essas entidades recebem um código, no caso da Cruz Vermelha, é 503(c)(3). Esse código é atribuído pela Receita Federal dos Estados Unidos. O DMTF também possui um código 501(c)(6). Essa homogeneidade de padrões não atrapalha o desenvolvimento e a evolução dos protocolos de rede?

Padrões como *Cloud Infrastructure Management Interface* (CIMI), Common Information Model (CIM) e Redfish são exemplos desenvolvidos pela DMTF. Então, a seguir, vamos compreender um pouco de cada padrão.

CIM

Entre os diversos problemas existentes no gerenciamento de uma rede de computadores, está a coleta de dados, mas associados à coleta estão a organização e o armazenamento. Logo, podemos exemplificar o problema por meio de uma comunicação entre duas pessoas – um funcionário do setor de TI e outro de setor de compras. Se o funcionário de TI pergunta: “O sistema está funcionando perfeitamente?”, a resposta do setor de compras pode vir de diversas maneiras, como “Ok”, “Está tudo bem”, “Funcionando”, “Em ordem”, ou seja, todas as respostas são entendidas como “tudo bem”. Mas já perguntou com relação ao computador? Como ele interpreta tal situação ou faz sua localização?

Como resposta, há uma necessidade de gerenciamento além das fronteiras de um simples coleta, é a necessidade de gerenciar a empresa por meio de processos e serviços. Nesse aspecto, o olhar é para a camada superior, e não a camada de nível de hardware, não é saber o porquê de determinada ventoinha parar de ventilar, mas entender qual serviço ficou indisponível ou o motivo de o processo não ter sido concluído. Hoje, o campo da gerência evoluiu e, precisamente, passa pelo monitoramento e pela análise de todos os elementos de rede, pois garante a continuidade dos serviços, mas, além disso, vai até a informação que determina o negócio.

O objetivo do CMI é relacionar os elementos que compõem uma rede de computadores e a própria rede que forma o sistema da empresa e a relação entre eles (CMI, 2010). O schema é um modelo que atende tanto ao gerenciamento de falhas, configuração, contabilidade, desempenho e segurança (FCAPS) quanto a serviços e operações relacionados a negócios.

Então, temos que o objetivo principal é a capacidade de criar um padrão (modelo) único de como tratar as informações de gerenciamento e também tratar a semântica de serviços, além de associar todos os elementos com relação ao modelo. Por meio de hierarquia de objetos, detalhes de camada inferior (hardware) e camada superior (serviços) são suportados. Todavia, há outros mecanismos em desenvolvimento pela DMTF, como o Redfish.

Redfish

Há tempos que o ambiente de redes é híbrido, principalmente com a chegada da internet. As tecnologias diferentes tendem a se convergir e, na proporção desse crescimento e dessa convergência, precisam de mecanismo para garantir a gerência de equipamentos, a rede de computação, o armazenamento, através de uma interface simples.

O Redfish é uma *Application Programming Interface* (API) que trabalha com padrões já definidos, como JSON (*Javascript Object Notation*), HTTP (*HyperText Transfer Protocol*), entre outros. Uma API é um objeto de programação que possui métodos padronizados que servem de “tradutor” de sistemas diferentes. Podemos entender uma API como o driver usado para instalação de alguns impressores ou plugins usados para pôr algumas aplicações.

Vamos a um exemplo de um pequeno objeto no formato JSON usado pelo Redfish:

```
{
"@odata.type": "#ComputerSystem.v1_10_0.ComputerSystem",
"Id": "437XR1138R2",
"Name": "WebFrontEnd483",
"SystemType": "Physical",
"AssetTag": "Chicago-45Z-2381",
"Manufacturer":  "Contoso",
"Model": "3500RX",
}
```

Notamos que o objeto é formado por chaves nominais, os termos antes do (:) e os valores, como @odata.type, determinam o tipo de recurso, nesse caso, o valor é #ComputerSystem.v1_10_0.ComputerSystem, ou a chave Name cujo valor é WebFrontEnd483.

Saiba mais

No passado, a linguagem denominada Extensible Markup Language (XML) era a linguagem usada para comunicação entre sistemas distintos. Porém, o JSON vem substituindo o XML nessa comunicação porque apresenta uma compactação melhor das informações bastante usada no universo da internet. Para saber do universo do padrão JSON, faça uma visita no site.

ACESSAR

Enfim, o ambiente de gerenciamento ultrapassa os limites do hardware, porém está estrategicamente posicionado ao lado da camada de negócios. Uma compreensão sobre o negócio da empresa auxilia no planejamento de monitoramento e gerenciamento da rede, mas também auxilia nas escolhas de ferramentas a serem implementadas nesse processo. Mesmo assim, o roteador ainda continua sendo um elemento fundamental na rede, portanto, no próximo tópico, vamos tratar sobre gerência de configuração em roteadores.

Vamos Praticar

Usando a ferramenta virtualbox, virtualização de host ou servidores, crie uma pequena rede interna, modo rede interna das placas de rede, com três máquinas virtuais: um servidor windows, um servidor linux e uma máquina com o Zabbix instalado. Crie uma tarefa no Zabbix para monitorar o status ativo (*on-line* ou *off-line*) dos servidores Windows e Linux. Vamos à prática!

Gerência de Configuração

Vamos tratar agora sobre os conceitos fundamentais da área da gerência de configuração. Lembramos que a OSI desenvolveu cinco áreas de gerenciamento de configuração, gerenciamento de falhas, gerenciamento de contabilização, gerenciamento de segurança e gerenciamento de desempenho (KUROSE; ROSS, 2013).

Neste tópico, vamos descrever os fundamentos do gerenciamento de configuração, especificado no RFC 3139, mas com relação ao equipamento roteador. Precisamos ressaltar que o roteador é o equipamento de rede da camada de rede tanto do modelo OSI quanto do TCP/IP que tem a finalidade de encaminhar ou fazer o roteamento dos pacotes IP da origem até o destino. Para tal finalidade, os roteadores fazem uso de algoritmo de roteamento por saltos como *Rounting Information Protocol (RIP)* ou por estado de link, como o *Open Shortest Path First (OSPF)* (TANENBAUM; WETHERRAL, 2011).

Outra valiosa característica dos roteadores é a capacidade de interligar redes diferentes. Isso é provido, principalmente, porque a internet é formada por redes heterogéneas, mas, na visão no usuário final, é uma única rede. Essa heterogeneidade da rede gera problemas de gerenciamento, pois diferentes

fabricantes podem gerar tipos diversos de serviços e comandos individuais do roteador, tornando complexo o gerenciamento.

Esse gerenciamento torna-se cada vez mais complexo, não só pelo crescimento do número de equipamentos, mas também pela diversidade de equipamentos conectados à rede. Esse crescimento crescente das redes gera uma maior dificuldade de gerenciamento, por exemplo, em relação ao tempo de configuração.

Hoje, gerenciar uma rede não passa mais por simplesmente configurar o roteador, mas pelo uso de políticas de alto nível, que determinam como as configurações devem acontecer nos dispositivos locais. Assim como qual política de alto nível, seja de topologia ou comportamento de serviço, deve ser aplicada em todos os equipamentos de rede que sustentam essa política.

saiba mais

Saiba mais

No passado, o gerenciamento de redes era baseado praticamente em três passos: o operador, a entidade responsável pela rede (ou engenheiro de rede) e o comportamento esperado. Hoje, há necessidade de aplicação de políticas. Mas você sabe o que significa políticas no gerenciamento de redes? O RFC 3060 especifica o significado de políticas, mas também como apresenta os grupos de políticas. Um excelente complemento a esse tópico. Boa leitura!

ACESSAR

Entretanto, o RFC 3139 determina alguns requisitos para o gerenciamento de

configurações, como:

a) ser capaz de interpretar a configuração local do dispositivo;

b) ser capaz de alterar dados do elemento de rede;

c) fornecer meios de configuração através de mecanismo com SNMP.

Com relação ao roteador, por exemplo, inúmeras tarefas podem ser planejadas e aplicadas ao equipamento, como o monitoramento de todo equipamento de rede, que deve ser feito com uma limitação de memória e, por essa razão, o gerenciamento dessa capacidade é fundamental, pois os roteadores com 100% de uso de memória podem gerar problemas de roteamento, principalmente no tempo de fila de processamento.

Outro fator importante com relação ao roteador é sua capacidade de execução das tarefas ou carga de processamento da CPU. Muitas vezes, o roteador está sobrecarregado de processamento devido à falta de balanceamento de carga da rede.

O processo de execução das tarefas em um equipamento de rede gera energia (calor), e essa energia aumenta a temperatura do equipamento. Esse aumento de temperatura, além de desgastar o equipamento ao longo do tempo levando ao defeito, pode também gerar falhas que prejudicam determinados processos.

Todo equipamento de rede, como roteadores e switches, são alimentados por energia elétrica e, por essa razão, devido a alguma falha na infra de energia elétrica, pode ficar com status de off-line. Outra métrica a ser usada no gerenciamento é o status de dispositivos de rede.

Como mencionado em unidades anteriores, gerenciar o link WAN sempre é um ponto favorável no gerenciamento de roteadores. Para entendimento do funcionamento de gerenciamento de um roteador, vamos usar o protocolo SNMP para gerenciamento de configuração para extrair informações sobre os dispositivos de uma rede de computação (STALLINGS, 1999). Vamos lembrar que um cenário de gerenciamento de redes é composto pela estação gerente

que contém um software de leitura das informações e os agentes gerenciáveis, que são módulos do software de gestão que fica armazenado nos dispositivos de redes, como roteadores e switches.

O Poder da MIB

Esses dispositivos gerenciáveis possuem uma base de informação de gerenciamento chamada de MIB. Essas MIB definem variáveis que podem ser lidas ou controladas por um software. Através do SNMP Get, pode-se, então, visualizar informações no equipamento da rede.

MIB representam cada objeto na rede que seja gerenciável. Mas, antes de detalharmos as MIBs, vamos conhecer um pouco do sistema de gerenciamento de redes (NMS). Esses sistemas devem ter em comum dois objetivos específicos:

a) Objeto: um objeto que representa cada recurso deve ser o mesmo a cada sistema.

b) Schema: um schema de representação que deve suportar a interoperabilidade.

Com isso, tem-se um padrão de representação que pode ser usado por ferramentas de gerenciamento. Uma outra questão relevante está relacionada à estrutura de informação de gerenciamento (SMI). Essa estrutura, especificada no RFC 1155, define, em termos gerais, como as MIBs devem ser definidas e construídas (STALLINGS, 1999). Vamos a um exemplo: o SMI define os tipos de dados de uma MIB e como os recursos são representados e nomeados. Os dados, por exemplo, podem ser do tipo integer (UNIVERSAL 2) ou *octetstring* (UNIVERSAL 4) e recursos, por exemplo, podem ser *networkaddress* (endereço de rede), *ipaddress* (endereço IP), etc.

O nome do objeto, recurso da rede, então, possui um padrão definido pela sintaxe ANS.1, que identifica cada recurso da rede. Esse padrão é denominado *Object Identifier* (OID). O OID, na verdade, é uma estrutura hierárquica que

especifica o recurso da rede. Lembre-se de que essa identificação é única, ou seja, não há duplicação de nomes. A estrutura hierárquica do OID é definida por uma sequência de números inteiros. Cada nó da estrutura hierárquica representa uma informação. A raiz do OID é definida por:

0: ITU-T

1: ISO

2: joint-iso-itu-t

Sendo que os nós subsequentes representam {iso.identified-organization.dod...}, ou seja, em sequência de inteiros {iso(1).org(3).dod(6)....} ou {1.3.6...}. A Figura 4.4 ilustra uma estrutura OID retirada de uma MIB usada para produtos Microsoft (*namespace* : 1.3.6.1.4.1.311) utilizando Ireasoning MibBrowser.

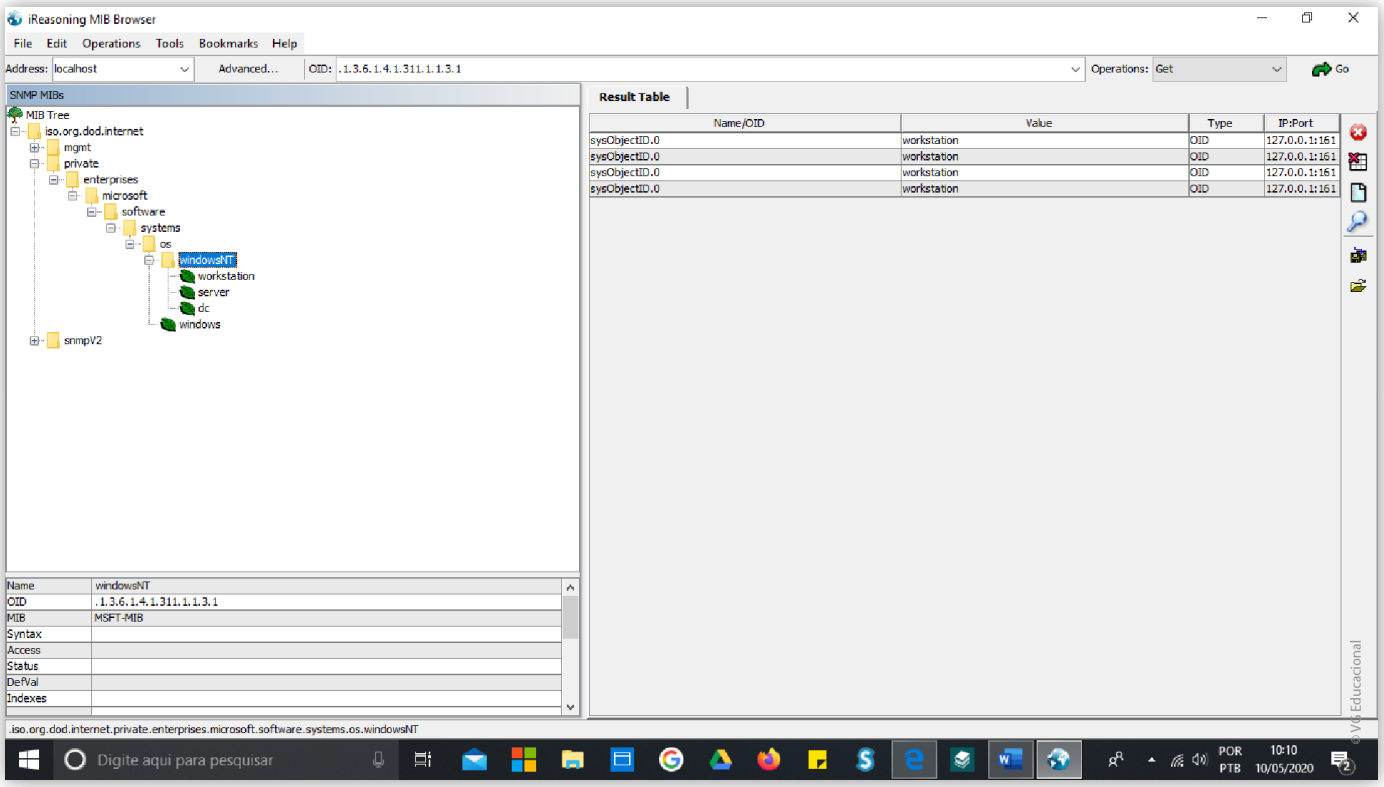


Figura 4.4 - Estrutura OID
Fonte: Elaborada pelo autor.

O SMI define quatro importantes grupos: *directory* , *mgmt* , *experimental* e *private* , todos debaixo do item “internet”. Entretanto, a Figura 4.5 ilustra o grupo mgmt especificando informações a respeito da tabela de entrada da

placa de rede em relação ao endereço físico.

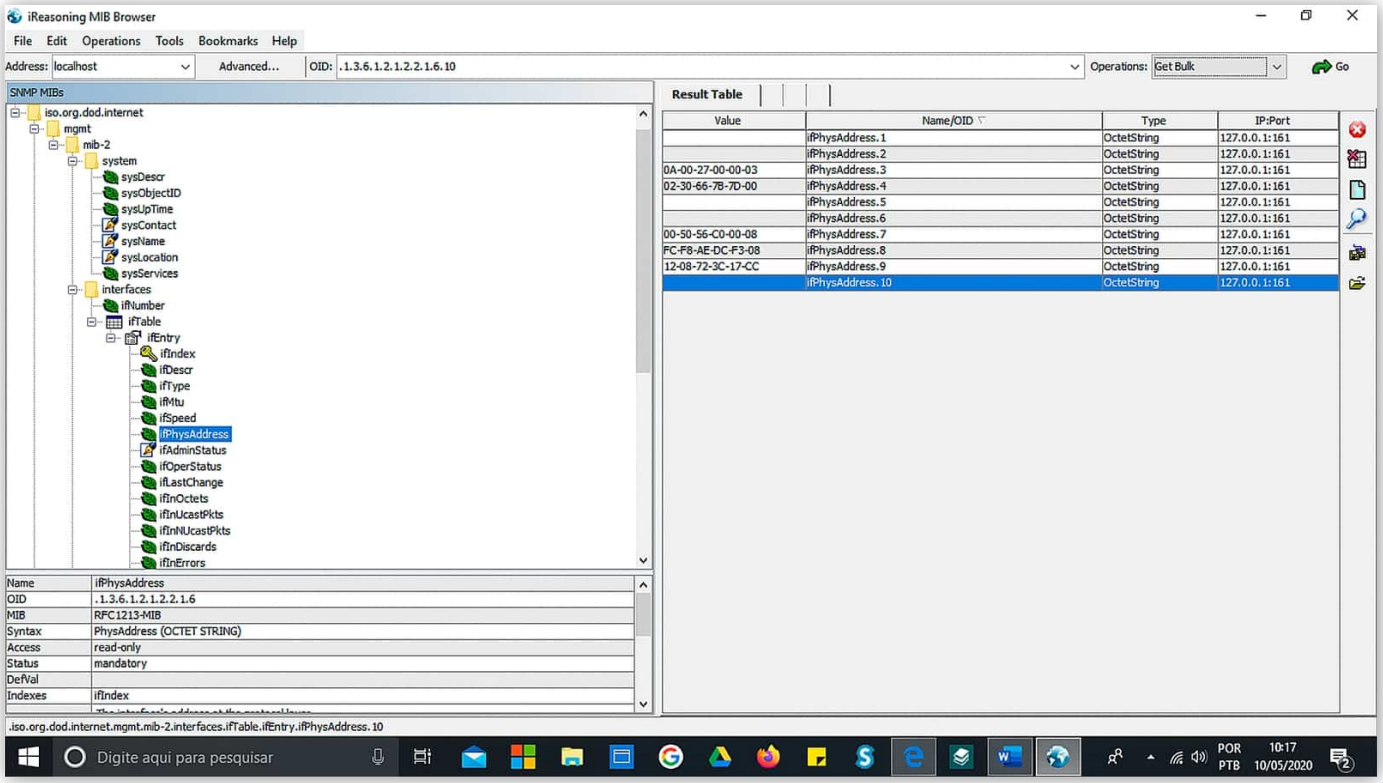


Figura 4.5 - Estrutura OID grupo mgmt
Fonte: Elaborada pelo autor.

Você pode observar na Figura 4.5 a estrutura da MIB(OID) hierárquica com nomes, detalhes de informações contidas no recurso, sequência numérica relacionada ao OID e valores relacionados à busca, como endereços físicos, tipo de dados e número de porta.

Lembre-se de que o RFC 1155 determina a especificação por padrão ANS.1. ASN.1 é uma sintaxe (notação) na descrição de dados enviados por protocolos, sem dependência de linguagem e representação de dados, podendo ser usado por aplicações complexas ou aplicações simples (STALLINGS, 1999). Um exemplo de escrita usando ANS.1 para definição de um objeto é:

tcpMxConn OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION “O limite total de conexões TCP que a entidade pode suportar. Em entidade que o número máximo de conexões é dinâmico, o objeto deve conter valor -1”.

As MIBs são divididas em duas versões MIB-I (RFC 1156) e MIB-II, sendo que a versão 2 (RFC 1213) é uma evolução da MIB-I com adições de novos grupos e objetos. A estrutura da MIB-II está representada na Figura 4.6, ilustrando a forma hierárquica das informações.

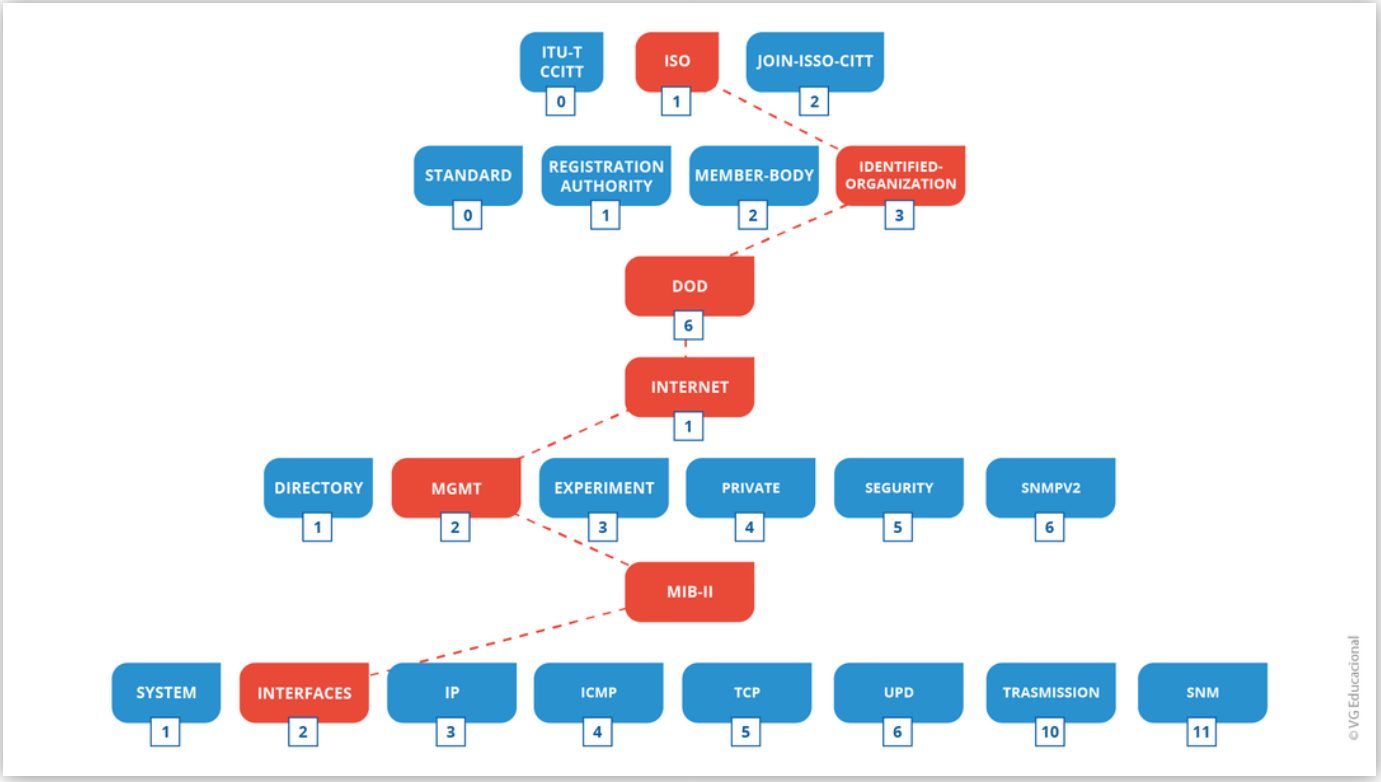


Figura 4.6 - MIB-II
Fonte: Elaborada pelo autor.

Como as MIB-II atuam associadas ao protocolo SNMP? Basicamente, o protocolo SNMP atua como um sistema cliente-servidor, pois os sistemas de gerenciamento enviam requisições aos recursos gerenciáveis da rede que retornam uma resposta. Então, essas mensagens oriundas de operações como GET são formadas por um cabeçalho e pelo PDU (*protocol data unit*). O cabeçalho detalha a versão do SNMP e a senha de conexão, denominada de comunidade (*community*). Já o PDU consiste em informações de acordo com a operação efetuada com GET, SET etc. Logo, podemos exemplificar com a

necessidade de monitorar o system uptime de um determinado computador, então, o OID seria 1.1.3.6.1.2.1.25.1.1.0 (MSFT-MIB.mib) através do arquivo de MIB do recurso da rede. A Figura 4.7 ilustra graficamente essa estrutura.

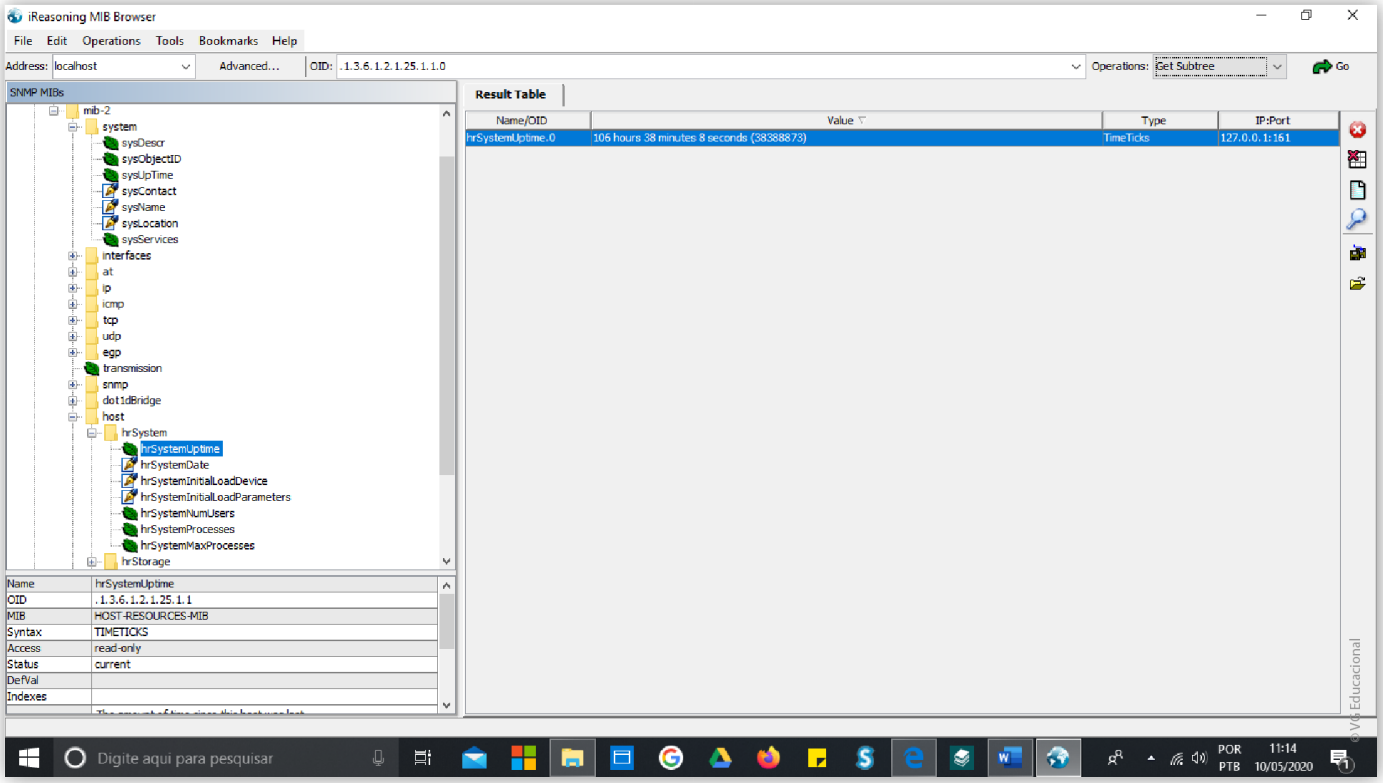


Figura 4.7 - System Uptime
Fonte: Elaborada pelo autor.

Então, você pode observar que o tempo do host de uptime surge como resposta à requisição de uma operação GET. Esse procedimento é usado pelas ferramentas de gerenciamento, porém mostrado em forma gráfica, através de dashboard.

praticar

Vamos Praticar

A virtualização é um processo já usado pelos departamentos de tecnologia da informação das organizações. Em data center, a virtualização é o ponto central, e uma virtualização pode ser realizada por meio de um software emulando sob um host, a exemplo tem-se o VirtualBox, ou instalando como um sistema operacional, a exemplo tem-se o VMware OS.

Com relação aos benefícios da virtualização, assinale a alternativa correta.

- **a)** A grande vantagem da virtualização são os agentes gerenciáveis.
- **b)** A grande vantagem da virtualização é a interconexão de redes.
- **c)** A grande vantagem da virtualização é a capacidade de coleta de informações na rede.
- **d)** A grande vantagem da virtualização é o custo.
- **e)** A grande vantagem da virtualização é a capacidade de atualização de softwares

As Ferramentas para uso em Rede

Outro recurso mais sofisticado que poderia ser usado para monitorar a gerência de configuração são os aplicativos Network Management System (NMS). Essas ferramentas são intensamente usadas para gerenciar todos os dispositivos existentes e gerenciáveis de uma rede, principalmente o roteador. Há um universo grande de ferramentas desenvolvidas para esse propósito. Entretanto, a Figura 4.1 ilustra um dashboard da ferramenta ManageEngine OpManager (OPMANAGER, 2020).

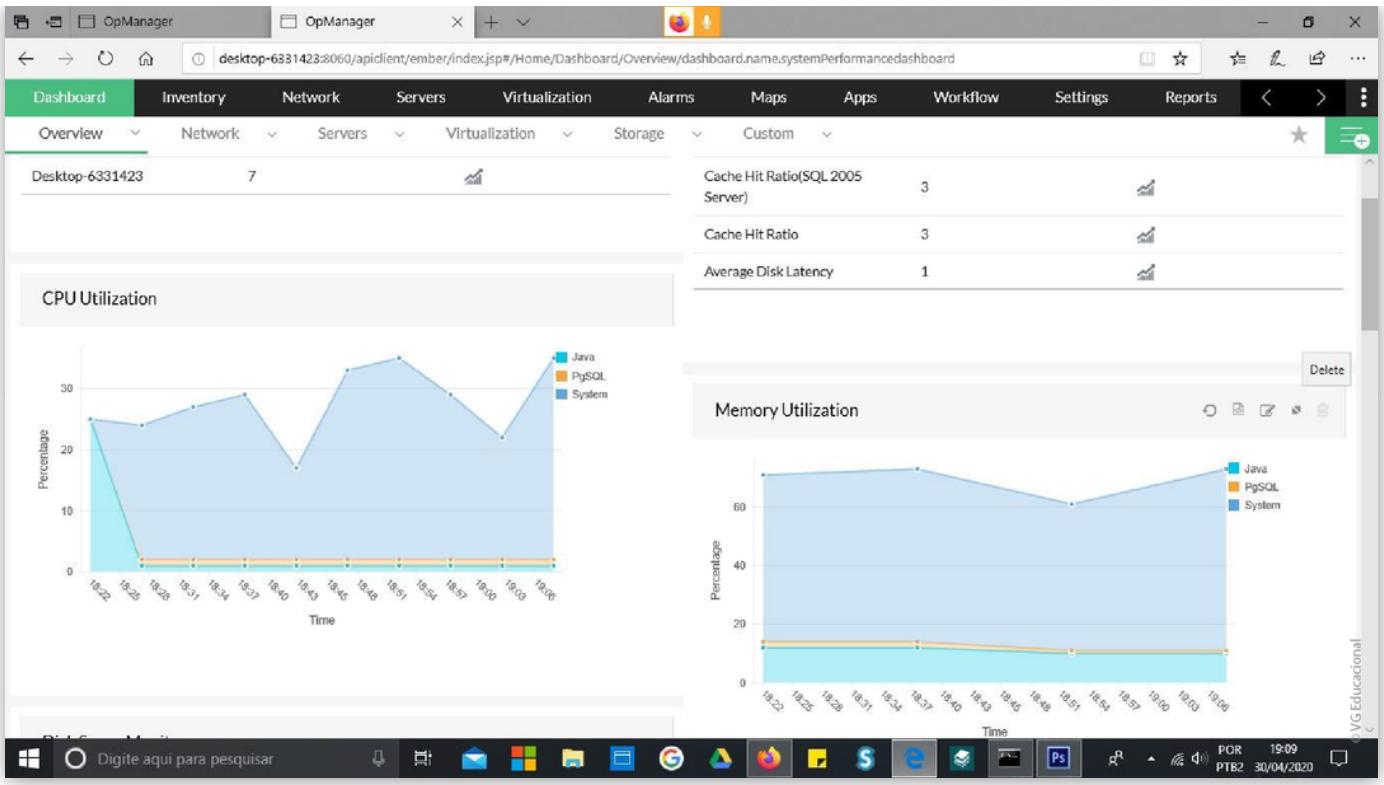


Figura 4.8 - OpManager
Fonte: Elaborada pelo autor.

Essa ferramenta tem um produto free que pode ser baixado diretamente do site e possui diversas funcionalidades de gerenciamento. Você pode, através da ferramenta, monitorar seu roteador de internet, seu computador, servidores instalados em máquinas virtuais e roteadores instalados em emuladores, como o *Graphical Network Simulator-3* (GNS3).

Porém, há o mundo de ferramentas gratuitas de gerenciamento, como o Nagios. Vamos lembrar que essas ferramentas de gerenciamento tiveram seu crescimento em grande parte devido à evolução da internet.

reflita

Reflita

A rede de internet geralmente chega à residência dos usuários via cabo conectado a um roteador? Esse roteador é configurado para gerar o acesso à internet a todos os equipamentos eletrônicos existentes naquele ambiente. Mas será que esse roteador é gerenciável? Quais são os recursos que precisam ser ativados? Você consegue responder?

O Nagios é uma ferramenta muito interessante, confiável e de código livre, que alerta o administrador sobre os eventos da rede, ou seja, monitorar servidores e outros dispositivos para analisar status de funcionamento. Além disso, Nagios pode aceitar informações de outros processos ou máquinas sobre seu status; por exemplo, um servidor web pode enviar informações para Nagios caso ele esteja sobrecarregado.

O propósito do monitoramento do sistema é detectar se algum sistema não está funcionando corretamente o mais rápido possível e notificar a equipe apropriada e, se possível, tentar resolver o erro – como reiniciando serviços do sistema. Basicamente, a ferramenta Nagios é dividida em dois grupos: hosts e serviços.

Os hosts representam um dispositivo físico ou virtual em sua rede (servidores, roteadores, estações de trabalho, impressoras, etc.);

Já os serviços são funcionalidades particulares, por exemplo, um servidor Secure Shell (SSH).

Outro ponto interessante na ferramenta Nagios é que ela oferece apenas quatro status: Ok, Aviso, Crítico e Desconhecido. Outra vantagem é que ele é baseado no quadro de plugins, permitindo que você desenvolva seu próprio plugin, isso mesmo, com um pouco de conhecimento de programação, você pode desenvolver seu próprio plugin de monitoramento.

Outra ferramenta para uso de monitoramento de código aberto é o Cacti. Essa ferramenta é usada para monitoramento do tráfego de uma rede. Faz uso do mecanismo *Round-robin Database* Tool (RRDtool) para armazenar os dados e, posteriormente, gerar os gráficos, além de coletar dados periódicos através de um conjunto de aplicativos que implementam SNMP denominado de NEY-SNMP.

saiba mais

Saiba mais

Como visto, as ferramentas de monitoramento e gerenciamento da rede são fundamentais para o administrador de rede. Mas você pode aprofundar seus estudos através de “mão na massa” utilizando essas ferramentas. A documentação do Cacti é uma excelente oportunidade para melhorar seu conhecimento. Boa leitura!

ACESSAR

Todavia, não podemos nos esquecer das ferramentas simples, porém úteis no cotidiano do administrador de redes, que são PING (teste de conectividade), TRACERT (traçar rotas), NETSTAT (análise sobre a porta do computador), TCPDUMP (captura e análise de tráfego), NMAP (análise/rastreio de um servidor, rede ou sub net), TOP (Processo de Monitoramento), HTOP (Linux

Process Monitoring), IOSTAT – Estatísticas de Input/Output entre diversas outras.

Enfim, o sucesso de um negócio está na capacidade de planejamento, por esse objetivo, a gerência de rede de computadores e todas as suas ferramentas, desde estudo de protocolos a ferramentas de monitoramento e gerência são objetos de muita análise e estudo.

praticar

Vamos Praticar

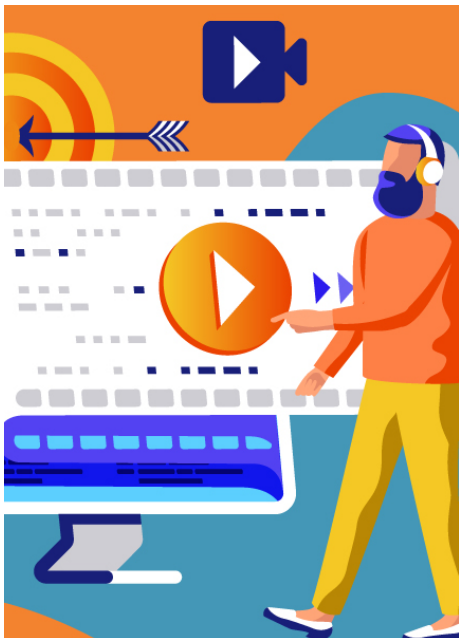
As ferramentas de monitoração são um instrumento que permite que o administrador possa controlar e gerenciar a rede. Mas esse universo é vasto e variado. Existem ferramentas pagas, não pagas e outras que acompanham o sistema o operacional e são tão importantes quanto as complexas NMS.

Assinale a opção correta com relação à ferramenta que permite ao administrador de rede fazer uma análise de conectividade entre dispositivos.

- **a)** PING.
- **b)** Netstat.
- **c)** Tracert.
- **d)** tcpdump.
- **e)** NMAP.

indicações

Material Complementar



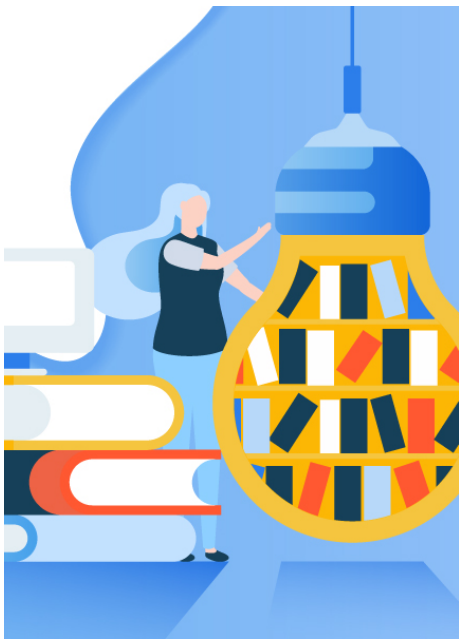
FILME

Nenhum Sistema está a Salvo

Ano : 2015

Comentário : Esse filme retrata ações de hacker a sistema de rede de computadores. Ele promove uma reflexão sobre a importância do bom planejamento de redes, pois, muitas vezes, falhas na configuração geram vulnerabilidades do sistema e podem ser exploradas por hackers, comprometendo o negócio.

TRAILER



LIVRO

Virtualização: Tecnologia Central do Data Center

Editora : Brasport

Autor : Manoel Veras de Sousa Neto

ISBN : 978-85-7452-761-1

Comentário : Este livro detalha em capítulos a importância da virtualização, ponto central de um data center, além disso, aborda assuntos como alta disponibilidade, gerência, software de virtualização, bem como os conceitos sobre gerência de infraestrutura e governança de TI. Um excelente livro para aquisição de conhecimento.

conclusão

Conclusão

Ao longo desta unidade, estudamos os conceitos sobre a alta disponibilidade de redes de computadores, assunto fundamental para as empresas do século XXI.

Nós observamos também que o processo de virtualização é presente e será o futuro nos departamentos da tecnologia da informação. A virtualização está presente nos data centers e permite os serviços de infraestrutura como serviços, os chamados IaaS.

Apresentamos os fundamentos da gerência de configuração e sua importância principalmente em roteadores, elemento-chave da interconexão de rede. Então, você teve a oportunidade de compreender os conceitos de alta disponibilidade, os princípios de sistema de virtualização e de padrões DMTF e detalhes sobre a gerência de configuração.

referências

Referências Bibliográficas

CMI. **Why CIM Overview Document_2010** . [2020] Disponível em:

https://www.dmtf.org/content/cim-overview-document . Acesso em: 27 abr. 2020.

DANTAS, J. R. Cluster de alta disponibilidade com arquitetura Heartbeat. **Revista Rios Eletrônica** , ano 2, n. 2, 2008.

DICIO. **Dicionário** . Disponível em: https://www.dicio.com.br/padrao/ . Acesso em: 27 abr, 2020.

DMTF. **Overview** . Disponível em: https://www.dmtf.org/education . Acesso em: 27 abr. 2020.

FERRIGOLO, R. M. O custo do downtime. *In* : CONGRESSO BRASILEIRO DE CUSTOS-ABC, 26. **Anais** ... Curitiba, 2001.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores** . AGH Editora, 2009.

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

NETO, M. V. S. **Virtualização** : Tecnologia Central do Data Center. Rio de Janeiro: Brasport, 2009.

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

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

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores** . 5. ed. Pearson, 2011.