

Gestão e monitorização de redes

A gestão e monitorização de redes tem novas dimensões estando a mais importante relacionada com o consumo energético dos equipamentos. Por um lado, já são patentes as preocupações dos fabricantes em evidenciar os níveis de consumo. Por outro, aparecem formas padronizadas de medir esses consumos, e para o final do ano esperam-se importantes novidades, como a apresentação de uma metodologia padrão. Há ainda novos padrões Ethernet e novas funcionalidades como a Virtual Ethernet Port Aggregation, ou VEPA. As redes continuam em crescente complexidade, cada vez mais numa base IP. Exigem ferramentas de monitorização e gestão cada vez mais sofisticadas para manter uma visão clara sobre o estado da rede e abordar os problemas à medida que vão surgindo. E o equipamento tem de estar sempre pronto a aceitar tráfego.

Fotolia.com

➔ Redes tornam-se mais ecológicas e fazem poupar dinheiro

O equipamento de rede pode representar até 15% da energia consumida. Mas ao contrário dos servidores que têm controlos de consumo de energia, o equipamento de rede precisa de estar sempre ligado e pronto a funcionar.

Pág. 2

➔ Novos padrões Ethernet podem reduzir "dores de cabeça"

Vários padrões de IEEE Ethernet poderão contribuir para reduzir as dores de cabeça na gestão dos centros de dados. O principal enfoque dos mesmos é nos problemas ligados à virtualização.

Pág. 4

➔ Os maiores erros na gestão de rede

Quando se olha para as piores brechas de segurança nas empresas, torna-se claro que os gestores de rede continuam a repetir erros, muitos deles, fáceis de evitar.

Pág. 6

➔ Otimize a gestão de rede de Wi-Fi

Baseada no relatório "Wireless LAN 2009", a consultora Aberdeen elaborou um conjunto de medidas a tomar num processo de optimização das redes de Wi-Fi.

Pág. 8

Redes tornam-se mais ecológicas e fazem poupar dinheiro

O equipamento de rede pode representar até 15% da energia consumida. Mas ao contrário dos servidores que têm controlos de consumo de energia sofisticados, o equipamento de rede precisa de estar sempre ligado e pronto a suportar tráfego de várias origens e feitios.

A infra-estrutura de redes não pertence à mesma classe dos servidores ou do armazenamento, em termos de consumo de energia. Mas o equipamento de rede pode representar até 15% da energia consumida.

Ao contrário dos servidores que têm controlos de consumo de energia sofisticados, o equipamento de rede tem de estar sempre ligado e pronto a aceitar tráfego. E nas racks o consumo de energia do equipamento de rede é relevante. Um gabinete de 13W gera mais calor do que muitas racks de servidores, o suficiente para merecer uma atenção especial de arrefecimento.

Por comparação, a maioria dos centros de dados atingem máximos de consumo de energia entre os 8kW e os 10kW para os servidores de racks, diz a Gartner. O gabinete médio de hoje em dia consome cerca de 4kW, diz Peter Gross, vice-presidente e director-geral da HPCritical Facilities Services.

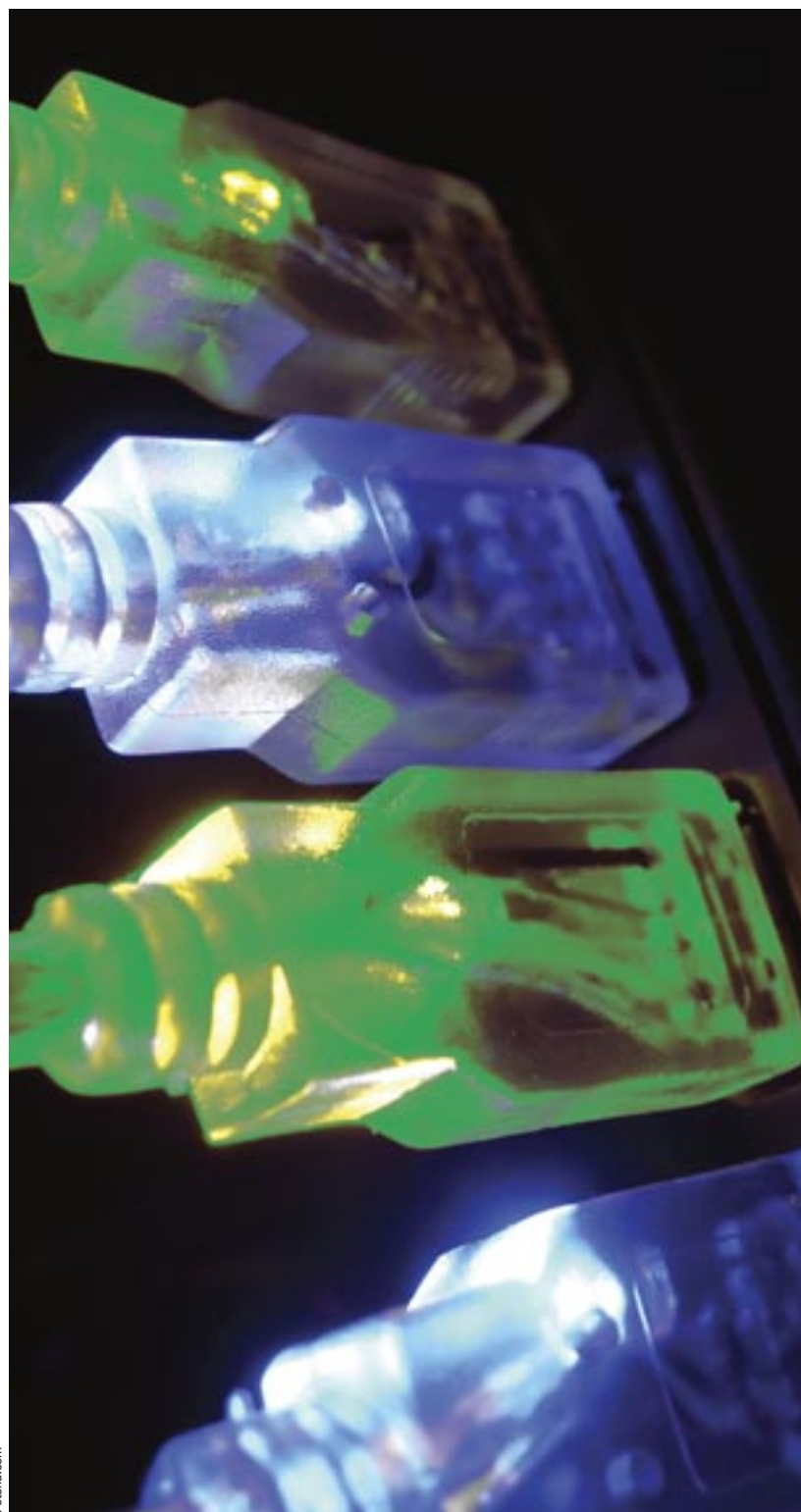
Alguns fabricantes já adoptaram algumas funcionalidades de energia, tais como fontes de energia altamente eficazes e ventoinhas de velocidade variável. Mas em relação aos switches há um limite para o que é possível fazer na área da gestão de consumo de energia. A maior parte dos switches consome 40% a 60% da energia máxima disponível. Qual-

quer coisa abaixo dos 40% compromete o desempenho. Há contudo muitas inovações a emergir, incluindo tecnologia mais eficiente.

As melhorias de tecnologia capazes de favorecer a eficiência energética estão a evoluir gradualmente em várias áreas, e à medida que são implementados novos equipamentos, as inovações vão entrando em utilização.

O funcionamento a temperaturas mais altas, por exemplo 130 graus, pode resultar em armários com equipamento de apenas um fabricante. Mas os fabricantes terão de trabalhar melhor a questão da multiplicidade de tecnologias e equipamentos instalados em cada armário, antes de se poder ter a certeza de que é possível permitir essa temperatura – especialmente nas racks. "Ninguém sabe ainda como o networking e outros tipos de equipamento deverão reagir quando estiverem encostados a servidores, que produzem mais calor" diz Drue Reeves, analista do Burton Group.

Outro enfoque são as melhorias na monitorização de consumo de energia, e com controlos mais granulares. A monitorização do consumo e da temperatura é um aspecto chave para qualquer centros de dados, e essencial para a gestão do crescimento. O software de gestão pode ser configu-



rado para identificar equipamento específico na rede, tais como telefones de tecnologia IP, usando o protocolo Link Layer Discovery. O software pode desligar automaticamente da corrente Power-over-Ethernet os dispositivos VoIP, em determinado período do dia ou quando o PC associado estiver desligado.

Os switches de terminal são normalmente ligados a dois routers para efeitos de redundância durante o dia, mas a rede pode ser configurado de forma a que um router entre em modo de repouso, à noite. O segundo router deverá ser reanimado só quando for necessário.

Este tipo de aplicações representa uma enorme oportunidade para haver poupanças.

Melhores especificações e padrões

Os padrões emergentes podem rapidamente ajudar a poupar energia quando as redes não estão a ser usadas e deverão permitir que as TI comparem a eficiência de produtos concorrentes.

Ethernet eficiente

O esboço do padrão emergente IEEE P802.3az Energy Efficient Ethernet (EEE) pode resultar no maior impacto de eficiência, no processo de poupança de energia, no consumo do equipamento de rede, quando a utilização é fraca. Hoje os dispositivos Ethernet transferem energia entre si, mesmo quando o tráfego se encontra estagnado. O equipamento de suporte ao padrão EEE deverá enviar um impulso periodicamente, mas manter-se inactivo durante o resto do tempo, reduzindo o consumo de energia mais de 90% durante este último período.

Numa rede grande, isso pode representar um consumo assinalável que pode ser evitado.

O padrão deverá permitir a escolha de outros modos de operação. Num switch de 10 Gbit, por exemplo, as portas individuais que estão a suportar apenas um volume de 1Gbit vão poder reduzir o consumo de energia, para o nível adequado, para suportar essa carga, poupando energia até a actividade ser retomada.

Os produtos desenvolvidos para suportar o padrão EEE deverá começar ter maior adesão por volta de 2011.

Últimas novidades tecnológicas

- **Desenhos de circuitos integrados específicos para aplicações (ASIC) que possibilitam aos switches desligar os componentes não utilizados, desde luzes de LED do painel, a tabelas em memória.**
- **Avanços na tecnologia da utilização de silício deverão minimizar as fugas de energia e promover a eficiência de energia com cada uma das novas gerações de chips. Há analistas que prevêem a possibilidade de reduzir o consumo de certos equipamentos para 10% do que consomem hoje em dia.**
- **O desenvolvimento de software mais eficiente capaz de consumir menos ciclos de CPU – e menos energia.**
- **Desenhos de equipamentos que os tornam capazes de correr a temperaturas mais altas, para reduzir custos de arrefecimento.**



NIC virtuais

Outra tecnologia emergente, o Multi-Root I/O Virtualization do PCI-SIG, oferece servidores numa rack com acesso a um repositório partilhado de placas de interface. Isto acontece através de um canal PCI Express, alargando essencialmente esse canal para fora do servidor. "Em vez de uma NIC em cada servidor, terá acesso a um banco de NIC numa rack, e podem associar-se porções de largura de banda de um desses NIC a um servidor", diz Reeves do Burton Group.

As poupanças de energia deverão emergir da crescente utilização da rede – alcançada com a repartição da largura de banda em cada "NIC virtual" – e a necessidade de menos portas NIC de switch. Reeves prevê que surjam produtos conformes a este padrão por volta de 2012.

Eficiência classificada

Finalmente, começaram a surgir medidas padronizadas de eficiência energética em alguns equipamentos de rede. A Juniper Networks por exemplo inclui uma classificação de consumo de energia – Energy Consumption Rating (ECR) – nas fichas de alguns dos seus produtos. A ECR é um esboço de especificação criado pela iniciativa do concórcio ECR. A Lawrence Livermore Labs, Ixia e a Juniper desenvolveram a especificação, que mede o desempenho de equipamentos de rede e telecomunicações, por unidade de energia.

Tanto a Cisco como a Juniper estão a apoiar especificação da Alliance for Telecommunications Industry Standards', Telecommunications Energy Efficiency Rating (TEER), apresentada no ano passado.

Contudo, nenhuma das especifica-

ções foi universalmente aceite. A Juniper suporta a ECR mas não inclui a classificação em todas as suas fichas de produto.

A HP diz que não adoptou nenhum dos padrões nas fichas porque os utilizadores não percebem as métricas. O que lhes interessa é o número de watts usados pela solução.

Outra crítica apontada às especificações pela HP é que lhes falta detalhe e abertura na metodologia de classificação. Isso significa que os fabricantes podem escolher metodologias capazes de se adaptarem melhor às suas necessidades.

EPA tem padrão na agenda

O tipo de especificação verdadeiramente aberta não deverá surgir antes do final do corrente ano quando a classificação Energy Star, da EPA, for lançada.. (A EPA desenvolveu uma especificação – Energy Star Small Network Equipment – em Dezembro, mas a maior parte do equipamento de redes será coberto pela especificação Large Network Equipment, que está a ser preparada.

De acordo com a EPA, a organização tenciona anunciar um esboço para os centros de dados em Junho de 2010, e no final do ano, para o equipamento de redes de centro de dados. A nova especificação que deverá cobrir componentes como as fontes de alimentação e chips internos, Energy Efficient Ethernet e todo o consumo dos dispositivos, será o padrão essencial, acredita a HP.

A maneira mais fácil para os gestores de redes incrementarem a eficiência energética hoje é comprar um novo equipamento. Mas será um processo gradual porque os gestores devem ponderar a idade do equipamento, face aos potenciais ganhos de eficiência.

Embora um corte de 15% nos custos de energia acaba por ganhar uma dimensão muito assinalável quando aplicado a um conjunto de milhares de servidores, em menos racks de switches, o total de poupanças é muito mais pequeno.

Para uma única rack, as poupanças por kilowatt habitualmente não justificam uma actualização. De acordo, com o Burton Group a maior parte das empresas não sentirá que vai poupar o suficiente, para suportar a actualização. ■



Novos padrões Ethernet podem reduzir “dores de cabeça”

Vários padrões de IEEE Ethernet poderão contribuir para reduzir as dores de cabeça na gestão dos centros de dados.

O principal enfoque dos mesmos é nos problemas ligados à virtualização

A HP, a Cisco e outros fabricantes de equipamento de redes estão a alimentar uma batalha épica para ganhar controlo sobre centro de dados das empresas. Ao mesmo tempo estão a juntar esforços para fazer vingar novos padrões tecnológicos de Ethernet, capazes de melhorar significativamente a gestão dos nervos computacionais cada vez mais virtualizados. As especificações IEEE 802.1Qbg e 802.1Qbh são desenhadas para tentar resolver questões de gestão muito sérias e emergentes pela explosão de máquinas virtuais nos centros de dados. Resumidamente, os standards emergentes eliminarão volumes significativos de processamento de políticas, segurança e gestão, de switches virtuais, em placas de interface de rede – ou

seja, network interface cards (NIC) –, e servidores blade, e colocam-nos outra vez nos switches Ethernet físicos, que ligam os recursos de armazenamento e computação. Os esboços dos padrões a serem preparados promovem uma funcionalidade denominada Virtual Ethernet Port Aggregation (VEPA), uma extensão para switches físicos e virtuais concebidos para eliminar o grande número de elementos de switching, com necessidade de serem geridos num centro de dados.

A adopção das especificações deverão tornar a gestão mais fácil tanto para os gestores de servidores, como para os gestores de redes, ao exigir menos elementos para gerir e menos instâncias elementares como tabelas de endereçamento, políticas de se-

gurança e de serviço, além de configurações – para gerir. "Precisam de ser uma forma de comunicar entre o hypervisor e a rede", diz Jon Oltsik, um analista do Enterprise Systems Group. "Quando se considera a complexidade associada à gestão de dúzias de máquinas virtuais, num servidor físico, a sofisticação do switching dos centros de dados, tem de existir."

Mas ao adicionar a sua inteligência para o hypervisor ou sistema hospedeiro, acrescentaria por sua vez um overhead de processamento de rede significativo para o servidor, diz Oltsik. Também duplicaria a tarefa de gerir as tabelas de gestão e controlo de acesso aos suportes, alinhando políticas e filtros a portas, e ou, máquinas de virtuais, e por aí diante.

"Se os switches já tivessem a inteligência com eles, porque haveríamos de o fazer noutra sítio?", pergunta Oltsik.

A VEPA cumpre a sua obrigação permitindo a colaboração entre uma estação terminal com um switch externo para suportar a ligação entre múltiplas estações terminais virtuais e máquinas virtuais, e redes externas. Isso deveria aliviar a necessidade de se ter switches virtuais em servidores blade, para armazenar e processar todas as funcionalidades – como a segurança, as listas de políticas e controlo de acessos (ACL) – residentes no switch externo exterior ao centro de dados.

O esboço em detalhe

Juntas, as especificações 802.1Qbg

e bh são desenhadas para alargar as capacidades de switches e NIC das estações terminais numa centro de dados virtual, especialmente com a proliferação e movimento das máquinas virtuais. Citando dados da Gartner, os responsáveis envolvidos no trabalho por detrás do IEEE na bg e bh, diz que 50% dos volumes de trabalho de todos os centros de dados serão virtualizados até 2012.

Alguns dos outros fabricantes envolvidos no bg e bh incluem o 3Com, Blade Network Technologies, Brocade, Dell, Extreme Networks, IBM, Intel, Juniper Networks e QLogic. Embora não sejam as primeiras especificações IEEE a endereçar os centros de dados virtuais, o bg e a bh são correcções à especificação IEEE 802.1Q para redes LAN virtuais e estão sob a supervisão dos grupos de trabalho da organização, o 802.1 Data Center Bridging e o Interworking. Os padrões bg e bh deverão ser ratificados durante 2011, de acordo com aqueles envolvidos no esforço da IEEE, mas os produtos já conformes aos esboços do standard, podem surgir no mercado este ano.

O bg está mais focado nas conexões virtuais dos extremos: um ambiente onde uma estação física terminal contém múltiplas estações terminais virtuais, participantes numa rede LAN conectada. A VEPA permite que uma conexão externa, ou switch, faça o reencaminhamento em modo "hairpin" de imagens entre máquinas virtuais, uma coisa que as conexões de 802.1Q, ou switches não estavam concebidas para fazer.

"Numa conexão, se a porta sobre a qual é necessário enviar uma imagem for a mesma em que veio, normalmente um switch acaba por deixar para trás o pacote," diz Paul



Congdon, CTO na HP ProCurve, e vice-presidente do grupo de trabalho IEEE 802.1 e autor do VEPA. "Mas a VEPA permite o modo "hairpin" para permitir que a imagem seja reencaminhada pela porta por onde entrou. Permite que dê a volta e prossiga." O VEPA não modifica o formato da imagem Ethernet mas apenas o comportamento dos switches, diz Congdon. Em si mesmo, o padrão foi limitado nas suas capacidades. Portanto a HP combinou a sua proposta de VEPA com a proposta de VN-Tag da Cisco, para o reencaminhamento e gestão nos servidores e de switch, de forma a suportar a capacidade de correr múltiplos switches virtuais e múltiplos VEPAs simultaneamente no terminal. Isto exigiu um esquema de canalização para o bg, baseado numa especificação VN-Tag, criada pela Cisco e pela VMware, para uma política seguir uma máquina virtual à medida que se move. Esta capacidade multicanal anexa uma etiqueta à imagem que identifica sobre que máquina virtual a imagem entrou. Mas outra extensão foi necessária, para permitir que os utilizadores implementassem switches remotos, em

vez dos que estavam adjacentes ao rack de servidores – tal como a política que controla os switches para o ambiente virtual. É neste aspecto que o 802.1Qbh se torna pertinente: permite que as conexões virtuais de extremos repliquem imagens, sobre múltiplos canais virtuais para um grupo de portas remotas. Isto deverá permitir que os utilizadores abram portas sucessivamente para um desenho de rede flexível, e faça um uso mais eficaz da largura de banda para fazer difusão de imagens em modo multicast, broadcast e unicast. A capacidade de extensão de portas de bh permite aos administradores escolher o switch ao qual querem delegar políticas, ACLs, filtros, QoS e outros parâmetros às máquinas virtuais. Os extensores de portas deverão residir na parte de trás da rack ou em blades individuais, e funcionarão como uma placa de linha do switch controlador, diz Joe Pelissier, director técnico da Cisco. "Reduz bastante o número das coisas que é necessário gerir e simplifica a gestão porque o switch controlador estará a fazer todo o trabalho," argumenta Pelissier. O que ainda está a faltar do

bg e do bh é uma protocolo de descoberta para conseguir fazer auto-configuração, diz Pelissier. Alguns no grupo do 802.1 estão mais inclinados a usar o protocolo Logical Link Discovery Protocol (LLDP), enquanto outros, incluindo a Cisco e a HP, estão mais interessados em definir um novo protocolo para a tarefa. "O LLDP está limitado em termos de quantidade de dados que poderá transportar e com que rapidez pode carregá-la," considera Pelissier. "Precisamos de alguma coisa que carregue dados em volumes de dezenas a centenas de kilobytes e seja capaz de enviar dados mais rapidamente do que uma imagem de 1,500 bytes, por segundo. O LLDP também não tem capacidade de fragmentação. Queremos ser capazes de repartir a quantidade de dados pelas múltiplas imagens."

Complementares ou concorrentes

A Cisco e a HP dizem que as suas propostas de VEPA e VN-Tag de extensão multicanal e multi-portas são complementares apesar de relatórios de que são concorrentes a competir para obter a mesma coisa: reduzir o número elementos de centros de dados geridos; e a definirem uma linha clara de demarcação entre NIC, gestores de servidores e switches quando monitorizarem as comunicações de máquinas virtuais. Embora Congdon reconheça que inicialmente propôs a VEPA como uma alternativa à técnica VN-Tag da Cisco, as duas juntas são "uma arquitectura bem implementada, baseada numa na outra onde os switches virtuais e a VEPA formam a camada mais básica de implantação, e é possível evoluir até às soluções mais complexas com a VN-Tag." ■

COMPUTERWORLD

PROPRIEDADE  workmedia

RUA GENERAL FIRMINO MIGUEL, Nº 3 TORRE 2 - 3º PISO 1600-100 LISBOA EDITOR: JOÃO PAULO NÓBREGA jnobrega@computerworld.workmedia.pt DIRECTOR COMERCIAL E DE PUBLICIDADE: PAULO FERNANDES pfernandes@computerworld.workmedia.pt
TELEF. 210 410 329 – FAX 210 410 303 DIRECTOR DE ARTE: JOSÉ TEIXEIRA zteixeira@workmedia.pt TODOS OS DIREITOS SÃO RESERVADOS.



O Computerworld, detém um acordo de licenciamento com a IDG, o líder mundial em media, estudos de mercado e exposições na área das tecnologias de informação (TI). Fundada em 1964, a IDG possui mais de 9.000 funcionários em todo o mundo. A IDG oferece o mais vasto leque de opções de media, os quais atingem consumidores de TIs em mais de 90 países, os quais representam 95% dos gastos mundiais em TIs. O portfolio de produtos e serviços abrange seis áreas chave: publicações impressas, publicações online, exposições e conferências, estudos de mercado, formação, e serviços de marketing globais. Mais de 90 milhões de pessoas lêem uma ou mais das 290 revistas e jornais da IDG, incluindo as pertencentes às principais famílias -Computerworld, PC World, Network World, Macworld e Channel World. A IDG Books Worldwide é o editor de livros de informática com mais rápido crescimento a nível mundial, com mais de 700 títulos em 38 línguas. Só a série "... For Dummies" tem mais de 50 milhões de cópias em impressão. Através da IDG.net (<http://www.idg.net>), a IDG oferece aos utilizadores online a maior rede de sites Internet especializados em todo o mundo. Esta compreende mais de 225 sites Internet em 55 países. A International Data Corporation (IDC) é o maior fornecedor mundial de informações sobre TIs, de análise e consulta, possuindo centros de pesquisa em 41 países e mais de 400 analistas em todo o mundo. A IDG World Expo é um produtor de primeira linha de mais de 168 conferências e exposições com marca própria, abarcando 35 países e incluindo a E3 (Electronic Entertainment Expo), Macworld Expo, ComNet, Windows World Expo, ICE (Internet Commerce Expo), Agenda, DEMO, and Spotlight. ExecuTrain, a subsidiária de formação da IDG, é a maior empresa do mundo na área da formação em informática, com mais de 230 instalações em todo o mundo e 785 cursos. A IDG Marketing Services ajuda empresas de topo na área das TIs a construir uma imagem reconhecida internacionalmente. Para isso desenvolve programas globais de marketing integrado, através das exposições e das suas publicações impressas e online. Pode encontrar mais informações do grupo IDG no site www.idg.com.

➔ Os erros de gestão de rede mais estúpidos

Quando se olha para as priores brechas de segurança nas empresas, torna-se claro que os gestores de rede continuam a repetir erros, muitos deles, fáceis de evitar.

É admirável como as brechas e segurança são o resultado de esquecimentos dos gestores de rede, que não tomam as medidas de segurança óbvias para dar segurança aos seus sistemas, particularmente em servidores não críticos.

➔ 1. Esquecer-se de mudar as passwords por defeito em todos os dispositivos de rede.

A maior parte dos CIO pensa que este problema nunca vai acontecer na empresa em que trabalham. Contudo é inacreditável a frequência com que as empresas têm um servidor, switch, router ou appliance de rede com uma password de fábrica — por vezes “password” ou “admin”, ainda em vigor. Para evitar este problema é necessário fazer um rastreio de vulnerabilidades a cada dispositivo na rede com um endereço IP, não só nos sistemas críticos ou expostos à Internet. Depois é necessário mudar as passwords de fábrica encontradas. Mais de metade dos registos comprometidos durante o ano passado foram resultado da utilização de uma password de fábrica num dispositivo de rede segundo um estudo da Verizon.

➔ 2. Usar a mesma password nos mesmos dispositivos.

Os departamentos de I usam frequentemente a mesma password em múltiplos servidores e várias pessoas sabem a password. Pode ser uma boa password, mas quando é partilhada entre os vários sistemas, estes sistemas estarão todos em risco.

Por exemplo, uma das pessoas que sabem as passwords, pode mudar de empresa e reutilizar a password, na nova organização. Ou um fornecedor de outsourcing que gere um sistema não crítico como um sistema de arrefecimento de centro de dados pode usar a mesma senha em todos os sistemas que controla para todos os seus clientes. Em todo o caso, se a password for descoberta por um hacker, este pode entrar em muitos servidores e fazer mais estragos.

Será necessário um processo, automatizado ou manual, para assegurar que as passwords de servidores não sejam partilhadas entre múltiplos sistemas, são mudadas regularmente e são mantidas seguras. É tão simples como manter as actuais passwords escritas em cartões guardados num cofre controlado por uma pessoa.

➔ 3. Falhar na detecção de erros de código de SQL

O ataque mais comum — representa 79% de todos os registos comprometidos — é contra as bases de dados ligadas a um servidor de Internet. A porta por onde os hackers entram nos sistemas é usando um comando SQL com um formulário baseado na Web. Se o formulário for bem escrito em termos de programação, não deve aceitar comandos SQL. Mas às vezes os programadores criam acidentalmente o que se denominam erros de injeção de SQL.

A forma mais fácil de prevenir estes erros é correr uma firewall aplicacional em modo “learn”, de forma a que possa monitorizar como os utilizadores inserem dados num campo e depois colocar a firewall em modo operacional, de uma forma que impeça os comandos de serem injectados num campo.

O problema da programação está bastante difundido. Se uma empresa testar 100 servidores, vai provavelmente encontrar um problema de injeção de SQL em 90 deles.

É vulgar as empresas corrigirem apenas os erros de injeção de SQL nos seus servidores críticos, esquecendo-se que a maioria dos hackers entra nas redes, através de sistemas de menor nível crítico. É recomendável que os gestores de redes segmentem as suas redes usando listas de controlo de acessos para restringir a comunicação dos servidores com dispositivos que não são essenciais. A medida impedirá o hacker de ganhar um acesso generalizado aos dados através de uma erro de código de SQL.

➔ 4. Configurar mal as suas listas de controlo de acessos

Segmentando a sua rede ao usar listas de controlo de acessos é a forma mais simples de assegurar que os sistemas comunicam apenas com os sistemas com os quais devem comunicar. Por exemplo, ao permitir que os parceiros de negócio acedam a dois servidores na sua rede através da VPN, deve ser usada a lista de controlo de acessos, para se assegurar que estes parceiros de negócio tenham acesso a apenas estes dois servidores.

Se um hacker entrar na sua rede através da abertura para os parceiros de negócio, o hacker pode apenas chegar aos dados nestes dois servidores. É muito frequente um criminoso entrar na rede através da VPN e ter acesso a tudo.

Ter listas de controlo de acesso devidamente configuradas teria protegido 66% dos registos comprometidos durante o ano passado. A razão pela qual os CIO não tomam este passo simples é que envolve a utilização dos routers como firewalls, e muitos gestores de rede não pretendem seguir essa estratégia.

➔ 5. Permitir a instalação de software de gestão ou acesso remoto

Uma das formas mais populares de os hackers entrarem na rede é usarem um pacote de software de gestão e acesso remoto, como o PCAnywhere, Virtual Network Computing (VNC) ou Secure Shell (SSH). Vulgarmente, a estas aplicações falta-lhes as medidas de segurança mais básicas, tais como boas passwords.

A forma mais simples de descobrir este problema é fazer um rastreio externo a todo o campo de endereços IP para procurar pelo PCAnywhere, VNC ou tráfico SSH. Uma vez encontradas estas aplicações, tome medidas extraordinárias de segurança nelas como tokens ou certificados, além das passwords. Outras opções passam por rastrear os dados de Netflow dos routers com exposição externa e perceber se tem algum tráfico de gestão remota na rede.

➔ 6. Esquecer vulnerabilidades básicas em aplicações não críticas

Quase 80% dos ataques de hacking são o resultado de brechas de segurança em aplicações web, de acordo com vários estudos. Os gestores de redes sabem que a sua maior vulnerabilidade está nas aplicações Web, portanto colocam todo o seu esforço no teste dos sistemas críticos e expostos na Internet.

O problema é que a maioria dos ataques não estão a testar aplicações não expostas na Internet. Todas as aplicações devem ser rastreadas à procura de vulnerabilidades básicas.

As pessoas foram ensinadas a darem prioridade ao que é mais crítico. Mas os criminosos não sabem o que é mais crítico. Entram por onde for mais fácil. Depois de entrarem na rede, podem instalar o seu software e depois monitorizar o tráfego da organização.

➔ 7. Não proteger adequadamente os servidores contra o malware

O software nocivo nos servidores chega aos 38% de todas as brechas de segurança. A maior parte do malware é instalado por um atacante remoto e é usado para captar dados. Tradicionalmente, o malware não é descoberto pelos antivírus. Uma forma de os gestores de redes descobrirem malware como leitores de teclados ou spyware, é correrem um software de detecção de intrusões em todos os servidores e não só nos servidores críticos. Uma sugestão: feche os servidores de forma a que nenhuma aplicação nova possam correr nelas. Os gestores de rede não gostam de fazer isto, porque podem querer acrescentar novo software, mais tarde. O melhor é “abrir” o servidor, instalar o software novo e depois “trancar” o servidor outra vez.

➔ 8. Falhar na configuração dos routers para proibir tráfego externo prescindível

Uma das formas mais populares de malware é abrir uma “porta” na retaguarda das defesas do servidor, ou criar um escudo de comando no servidor. Uma maneira de prevenir isto é usar listas de controlo de acessos. Assim previne-se que os servidores enviem tráfego que não deviam enviar. Por exemplo, o servidor só deve enviar tráfego de correio, e não tráfego SSH.

Outra opção será usar os routers para negar por defeito as filtragens não autorizadas, que bloqueiam o tráfego de saída excepto aquilo que pretende que saia da sua rede. Muito poucas empresas fazem isso.

➔ 9. Deixar de saber onde estão alojados os dados de cartão de crédito e outros dados de cliente.

A maior parte das empresas consideram saber onde estão os dados críticos como a informação de cartão de crédito, números de segurança social ou outra informação pessoal. Naturalmente reforçam os servidores com os mais altos níveis de segurança.

Mas muito frequentemente estes dados estão alojados noutra sítio da rede, como um site de backup ou no departamento de desenvolvimento de software. São estes servidores secundários, pouco críticos que muitas vezes são atacados e levam à maioria das brechas de segurança. Um forma fácil de descobrir onde estão os dados é fazer uma exploração da rede. Coloca-se um sniffer na rede e vemos onde os dados devem estar e onde está além desses sítios.

➔ 10. Não seguir as recomendações PCI DSS

O PCI DSS é um conjunto de 12 medidas de controlos para proteger dados de titulares de cartões. Mas a maior das empresas nem sequer tenta estar em conformidade com os padrões PCI. Por vezes, uma organização segue as recomendações para os servidores, onde sabe que estão informações de cartões de crédito armazenadas.

Mas não segue a mesma política para os servidores secundários onde estão alojadas informações com dados críticos. Mesmo que 98% dos registos comprometidos envolva dados de pagamento por cartão, apenas 19% das organizações com brechas na sua segurança, seguiram os padrões habituais de protecção.

SLAs e Reporting - A Qualidade de Serviço apercebida e os processos de melhoria contínua

José Luis Neves Viegas
Gestão Produto PT Prime

As Organizações dependem hoje, mais do que nunca, de redes e serviços de comunicações que sejam fiáveis, flexíveis e seguros, capazes de assegurar um desempenho com elevado nível de exigência, num panorama cada vez mais competitivo e globalizado.

O nível de desempenho dos sistemas constitui assim um factor crítico indispensável para o sucesso dos negócios.

A pressão nas Organizações é constante no sentido de otimizar custos e focar no seu core business. Estar permanentemente ligado à sua Organização, ter acesso seguro em qualquer local às aplicações de negócio, correio electrónico, telefone e Internet, mais do que uma moda tecnológica, é uma necessidade imperiosa.

Na actual realidade já não existe separação entre as tecnologias de informação, networking e os serviços de voz. De facto, a voz (VoIP) não é mais do que uma aplicação suportada na mesma rede. Como tal, também a convergência fixo-móvel tem importância e conveniência acrescidas.

A Qualidade na equação

As Organizações procuram soluções cada vez mais integradas e a oferta por parte dos operadores já não pode limitar-se ao simples fornecimento de circuitos, VPN ou Internet. Para ir ao encontro das necessidades actuais do tecido empresarial, é imprescindível dispor de um vasto leque de produtos e serviços geridos, como o fornecimento de equipamento, operação, manutenção e gestão, ligações internacionais, VSAT, serviços avançados em data center, disaster recovery e business continuity, só para citar alguns exemplos.

Tendo em linha de conta a interdependência cada vez maior do negócio das Organizações com a qualidade dos serviços que são contratados a um operador, é natural que o tema dos SLAs seja cada vez mais uma exigência dos Clientes.

A necessidade de estabelecer e conhecer com rigor os critérios que definem os níveis de qualidade e as condições em que o serviço é prestado, torna-se uma questão fundamental que determina a confiança no prestador de serviço.

O que é um SLA?

Um SLA (Service Level Agreement) é, em primeira análise, um contrato entre um Cliente e um fornecedor. Contém, nomeadamente, obrigações e contrapartidas técnicas e comerciais a serem assumidas de parte a parte, com um foco na qualidade global do

fornecimento de um serviço crítico para o Cliente.

O Ciclo da Melhoria Contínua

Um fornecedor que assume sem rodeios os seus SLAs, deve encarar os desafios decorrentes desta oferta como oportunidades para afinar processos internos, com base num Ciclo de Melhoria Contínua.

Como ponto de partida, é fundamental definir (ou redefinir), continuamente, a oferta comercial e otimizar os processos internos associados ao fornecimento dos seus produtos e serviços, de modo a ir ao encontro das metas (KPIs) estabelecidas / exigidas.

Reporting: Medir e Comprovar

Indicar a existência de SLAs é um aspecto. Uma outra questão é saber medir e comprovar a sua efectiva aplicação.

Um dos principais desafios é o factor escala. Na PT Prime, e considerando apenas o nível da WAN, o número de equipamentos geridos aproxima-se de 100.000.

De igual forma, é necessário ter em linha de conta a diversidade de estruturas de comunicações, que combinam

o legacy com as mais recentes ofertas e protocolos.

No caso dos Clientes com contratos de Outsourcing, são alocados recursos humanos e plataformas técnicas dedicadas, como por exemplo, o CA Unicenter. Para os restantes Clientes, a PT Prime optou por uma abordagem de desenvolvimento in-house, através de uma plataforma de monitorização que permite uma elevada customização, fornecida pela PT Sistemas de Informação (empresa do Grupo PT).

Vantagens para o Cliente

A plataforma de monitorização de serviços geridos, designada PT Service Monitor, está dimensionada de modo a lidar com os desafios que são colocados pelas Organizações.

Dado que as redes e os sistemas de comunicação são realidades dinâmicas, a disponibilização da informação em tempo real, baseada em informação georreferenciada com interface web, é um dos requisitos endereçados. Igualmente relevantes são a disponibilização de informação de parque de serviços, o acesso a ferramentas de teste em tempo real (SNMP/ ICMP) e a consulta on-line do status de cada um dos trouble tickets.

Supervisão e Monitorização

Corrigir os casos concretos e prevenir situações de risco (reactiva ou proactivamente) são também acções que fazem parte do processo de melhoria contínua.

Nesta vertente, existem na PT Prime equipas diferenciadas que se dedicam a duas funções complementares:

- **Event Management Team:**
A supervisão proactiva é das actividades mais importantes em termos de intervenção para problemas associados a equipamento gerido (usualmente routers). A utilização de plataformas-padrão, reconhecidas como líderes de mercado, foi uma escolha natural. No sentido de uma detecção célere e eficaz, os períodos de observação definidos são muito curtos (ex: 5 minutos).
- **Service Level Management Team:**
A análise do SLA, detecção de casos recorrentes, trend analysis, prevenção de casos futuros e propostas de evolução fazem parte das tarefas de gestão dos SLAs, sendo suportada na plataforma PT Service Monitor.

E o futuro?

Temos assistido, ao longo destes últimos anos, a um crescente grau de exigência em termos de SLAs por parte das Organizações.

A PT Prime endereça por completo qualquer requisito a este nível. Dos SLAs baseados em trouble ticketing, passamos para o apuramento de métricas de rede como delay, jitter e packet loss (por classes de serviço).

Com a evolução da oferta para soluções integradas de networking e sistemas de informação (por exemplo, o cloud computing), os critérios de análise têm que considerar também o desempenho das aplicações na rede.

Tendo como cerne a sua plataforma PT Service Monitor, a PT Prime tem dado e continuará a dar uma resposta plena e inovadora aos novos desafios que se perfilam em termos de SLA e reporting para os Clientes Empresariais.

Lista de acrónimos utilizados:

ICMP - Internet Control Message Protocol (RFC 792);
KPI - (SLA) Key Performance Indicator;
SLA - Service Level Agreement;
SNMP - Simple Network Management Protocol (RFC 1157 entre outras);
VPN - Virtual Private Network;
WAN - Wide Area Network.



Optimize a rede de Wi-Fi

O Aberdeen Group partiu do seu extenso relatório "Wireless LAN 2009" e elaborou uma série de recomendações e de medidas a tomar num processo de optimização das redes de Wi-Fi. Estão agrupadas em três conjuntos, correspondendo a estádios de evolução.

1º Grupo

- Comece por fazer uma avaliação profunda da segurança e do desempenho; do inventário, compre as ferramentas básicas para diagnóstico, análise e planeamento.
- Procure a ajuda que precisar: melhore as competências de TI e do help desk de Wi-Fi, avalie serviços de suporte em outsourcing.

* Implemente mecanismos de segurança na sua rede sem fios.

2º Grupo

- Se ainda não o fez, mude para uma abordagem centralizada de gestão e monitorização da rede Wi-Fi, incluindo a implementação de actualizações.
- Comece a medir: vai precisar de ferramentas para poder ver dentro da rede WLAN, para perceber o que está a acontecer e porquê.
- Faça uma hierarquia de prioridades de largura de banda para determinadas aplicações, e para utilizadores, incluindo visitantes da organização. Segundo o relatório, 75% das empresas neste grupo não tomou nenhuma destas medidas.

3º Grupo

- Faça análises de custos e benefícios para actualizações de largura de banda para perceber se valem a pena; e depois meça-as para tentar perceber se está a obter o que devia.
- Use projectos piloto para instalar novos equipamentos, para descobrir problemas de incompatibilidades e de desempenho.
- Estabeleça métricas do que é o desempenho "normal" das aplicações de Wi-Fi, e certifique-se de que a rede sem fios está em conformidade com essas métricas.

Dê as boas vindas aos smartphones na empresa

Actualmente os trabalhadores das empresas querem usar os seus iPhones, Androids e outros dispositivos além dos Blackberries. Se não liderar a gestão dessa adopção pode ter problemas

Não vale a pena resistir: o iPhone venceu, e depois virão outros, como os dispositivos equipados com o Android. Pode tentar barrar o uso dos mais recentes smartphones na rede empresarial, que mais tarde ou mais cedo eles vão entrar e ligar-se aos sistemas de TI. Com efeito, muitos CIO e CSO já desistiram. Concentram agora as suas energias noutros objectivos, como descobrir a melhor forma de integrar a sua presença, e aproveitá-los como dispositivos de negócio. Estes são muito pessoais, mas constituem também ferramentas cada vez mais capazes de satisfazer as necessidades de gestão e segurança das empresas. A revolução dos PC tornou difusa a distinção entre a informática pessoal e a de negócio, já há vinte anos. Agora é altura de procurar aproveitar o melhor possível a revolução dos smartphones.

Há centenas se não milhares de smartphones e telemóveis com aplicações. Mas a maioria não têm interesse para a utilização empresarial, que implica a visualização de e-mails, agendas, contactos, tarefas a executar, aplicações e acesso a dados. O conjunto dos mais interessantes incluem o iPhone, o (iPod Touch e o iPad), os dispositivos Google Android OS 2.x devices, Microsoft Windows Mobile, os dispositivos Nokia Symbian (como o S60 e o E71), e os BlackBerry.

Dada a importância do e-mail nesses dispositivos torna-se importante considerar plataformas como o IBM Lotus Domino/Notes, Microsoft Exchange, e o Novell GroupWise. Mas pode fazer sentido adicionar alguns produtos de gestão de mobilidade. É necessário ter consciência de que a maioria desses dispositivos não acrescentam verdadeiras capacidades de segurança. Alguns facilitam o provisionamento das capacidades nativas de segurança. Mas a maioria estão focadas na monitorização e gestão da despesa com as redes celulares, na monitorização dos dispositivos como activos, e dando às TI informação básica dos dispositivos para serviços de suporte. Mas em vez de adicionar mais uma ferramenta de gestão, pode querer desistir do



provisionamento de smartphones, o que resolve as questões ligadas à gestão de contas, para o qual estas plataformas de gestão foram concebidas.

Tenha em mente que a mobilidade... está sempre a mudar. Por exemplo, há mudanças a ter em conta. O iPhone OS 4.0 deverá ser disponibilizado no Verão deverá aumentar as capacidades corporativas do iPhone, assim como tornar mais fácil a gestão destes dispositivos por ferramentas de terceiras partes – da mesma maneira que o RIM's BlackBerry Enterprise Server gere os BlackBerry.

Outras novidades esperadas têm a ver com o lançamento da versão beta do Data Synchronizer Mobility Pack, uma adição ao GroupWise 8 que inclui serviços do Exchange ActiveSync (EAS). Com esse software será possível gerir dispositivos compatíveis com o EAS - como o iPhone e o Windows Mobile, tal como era possível com o Microsoft Exchange Server. Finalmente a Microsoft diz que o Windows Phone 7 OS, deverá estar disponível no Natal e deverá ter as mesmas capacidades de gestão da plataforma Windows Mobile. ■ CW

Considerações sobre a adopção de uma plataforma de gestão de redes

Quando se tenciona investir em tecnologias de monitorização ou de gestão, há uma série de factores a considerar.

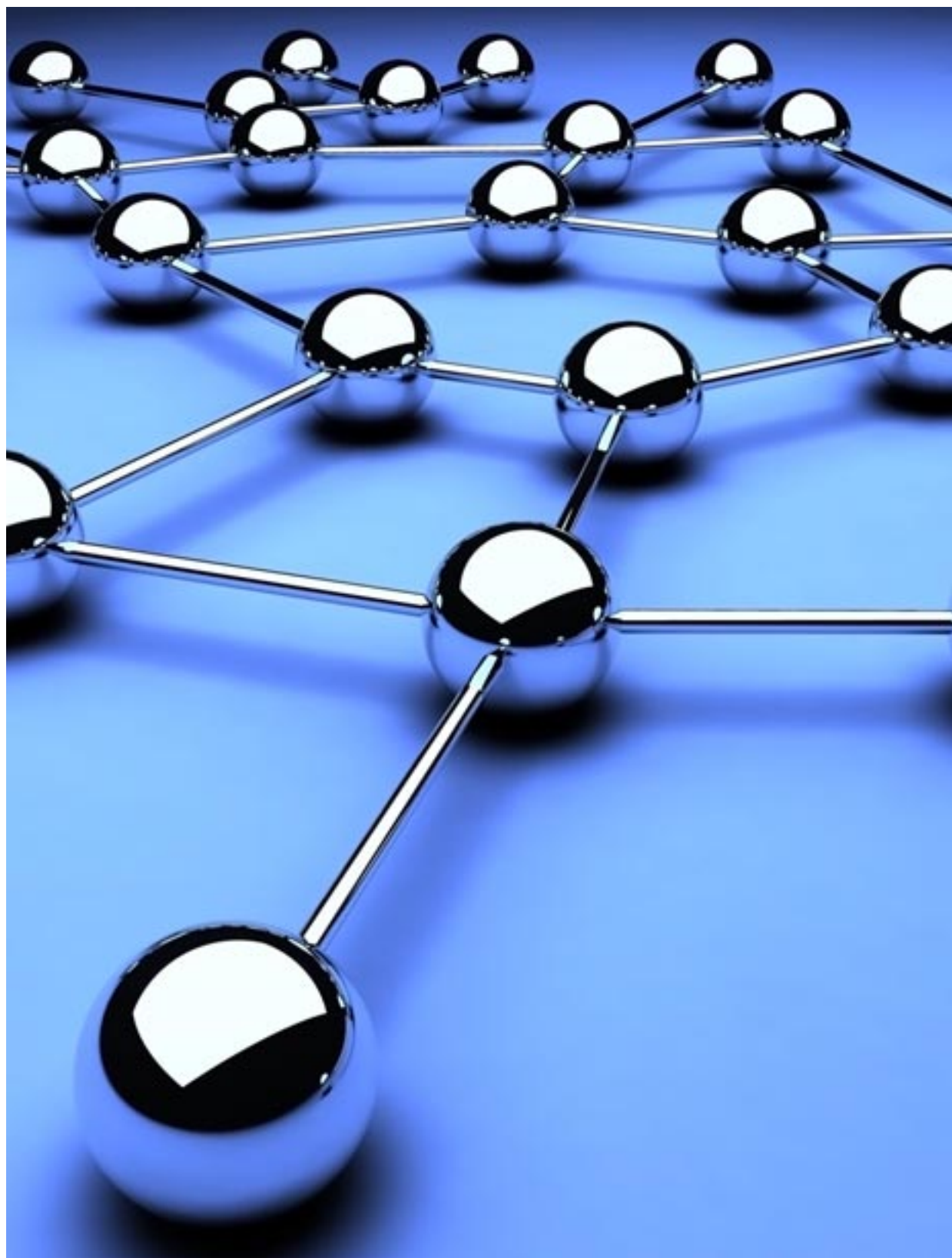
FRAMEWORK vs. PRODUTO INDIVIDUAL: Os quatro grandes fabricantes de gestão oferece muitas características inseridas em suites, mas há quem argumente que o tempo de implementação e os custos são demasiado altos.

Precisa de considerar o que se pretende gerir e quais as características mais críticas. Embora o termo "framework" supostamente esteja morto, muito fabricantes oferecem suites de capacidades que os clientes podem misturar e conjugar. Produtos individuais podem oferecer um ponto de impacto negativo a um preço baixo.

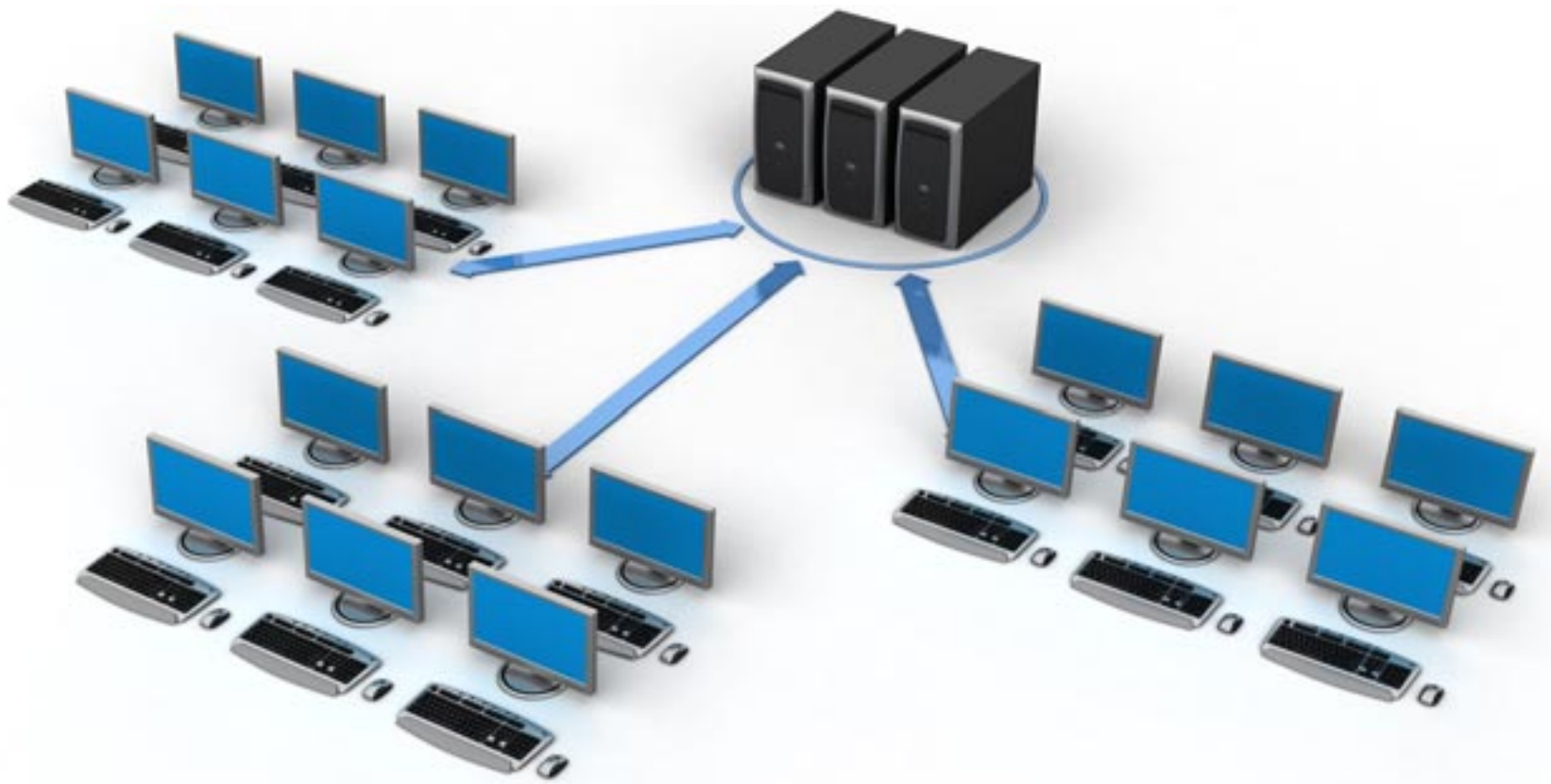
O benefício de escolher um fabricante com múltiplos produtos é o nível de integração, e a desvantagem é a incorporação de mais ferramentas do que realmente precisa.

Pese as necessidades do ambiente face às capacidades e considere a possibilidade de expandir a utilização dos produtos para futuras necessidades da rede.

ACTIVOS OU PASSIVOS: Se pretender ser capaz de configurar o software para assumir acções automatizadas, deverá investir em tecnologias activas. As capacidades activas possibilitam ao software reiniciar as máquinas ou serviços nos dispositivos. As características exigem maiores esforços de configuração no início, e muitas vezes implicam instalar agentes em dispositivos de gestão. Contudo as capacidades activas podem



Fotolia.com



Fotolia.com

►►► ajudar a automatizar tarefas repetitivas. As tecnologias activas também são tidas como grandes consumidoras de capacidade de processamento, além de espaço nos dispositivos onde residem, mas a maior parte das tecnologias ocupa muito pouco espaço.

As tecnologias passivas são frequentemente usadas para monitorizar tráfego e tempos de resposta nos dispositivos. As ferramentas podem funcionar em tempo real para alertar os responsáveis de TI, sobre volumes perdidos ou problemas de desempenho, mas vulgarmente não têm qualquer acção. Ferramentas passivas também envolvem a monitorização não intrusiva de tráfego, a qual não exige a instalação de agentes ou dispositivos geridos. Recolhem informação e armazenam-a para diversos propósitos, incluindo a identificação de tendências, a gestão de registos ou de conformidade, ou requisito de auditoria.

AGENTE OU BASEADO EM AGENTES: no que se refere a agente de software, a maioria dos gestores de TI preferem lidar com pequenos "gremlins" nas suas máquinas do que optar pela alternativa. As pequenas peças de código funcionam com o software de gestão de rede para recolher informação dos dispositivos geridos, e desenvolver acções sobre

eles. Mas configurar, implementar e actualizar milhares de agentes em sistemas servidores e clientes não é apelativo. Em alguns casos, o desempenho e a segurança degrada-se quando as máquinas ficam sobrecarregadas com software de agentes de vários fabricantes.

Mas sem agentes, seria necessário visitar fisicamente desktops e servidores para realizar tarefas simples como a actualização de software.

Foi por isso que a maioria dos gestores de TI escolhem a instalação alguns agentes seleccionados em máquinas geridas, reduzindo o esforço manual e ajudando a proteger a máquina com ferramentas de antivírus. "Há riscos em colocar muitos agentes em qualquer dispositivo, portanto tive de estabelecer limites sobre quantos agentes deviam ser enviados para os terminais," diz William Bell, director de segurança da informação na CWIE, uma empresa de alojamento de conteúdos na Internet em Tempe (Ariz). "Algumas pessoas dirão que os agentes são botnets à espera de que algo aconteça, mas se alguma vez tentou fazer correcções em milhares de máquinas sem agentes, saberá que os agentes têm o seu lugar."

RELATÓRIOS EM TEMPO REAL OU HISTÓRICOS: muitos produtos oferecem ambas as capacidades, mas

precisa de determinar como quer que o produto de gestão de rede deverá reportar sobre os dados que recolhe. As ferramentas que reportam em tempo-real fazem-no na detecção de problemas e remediação. O relatório em tempo real, não é bem em tempo real: é quase; e deverá ajudar a resolver problemas de desempenho, talvez antes de os utilizadores perceberem a degradação de serviços ou uma falha nos mesmos. Os relatórios históricos são mais frequentemente usados para detectar tendências de utilização e planear futuras capacidades.

Os dados recolhidos ao longo do tempo podem fornecer informação valiosa sobre padrões de desempenho. Tais informações podem ajudar a afinar aplicações para melhores desempenhos em redes ou alocar recursos diferentemente para suportar a procura.

CONFIGURAÇÃO: Talvez mais do que qualquer outra área tecnológica, é necessário configurar as ferramentas para endereçar especificamente as necessidades de um ambiente em particular. Estas tecnologias não funcionam com configuração de fábrica. É necessário estabelecer parâmetros, de validação de dados nos dispositivos e nos sistemas e configurar máquinas e sistemas para, ou enviar dados, ou permitir às ferramentas de

gestão que retirem dados dos registos de dispositivos e dos sistemas. Ao mesmo tempo que os tempos de instalação outrora comuns no passado já não são toleráveis, as ferramentas de monitorização e gestão ainda exigem que os seus recursos humanos configurem o produto para trabalhar no seu ambiente.

PROCESSOS: Adoptando boas práticas como as de ITIL permitirá manter-se em cima da gestão ao longo de grandes ambientes. Como parte da gestão da manutenção quotidiana, os processos deverão equipar a empresa com as ferramentas para suportar as condições actuais e adoptar mais facilmente novas tecnologias sem impactos negativos nas operações normais do ambiente. Por exemplo, processos – tais como a gestão da mudança e de configurações – deverá ajudar a empresa a prevenir desvios das configurações ou a ocorrência de mudanças não autorizadas, que podem causar questões de conformidade e tempo de indisponibilidade, respectivamente.

"Estas matrizes ajudam as empresas a padronizar as operações de TI, a gestão de processos, e as práticas – baixar os custos ao reduzir a necessidade de trabalho não planeado, tornando mais fácil adoptar e implementar tecnologias de redução de custos," diz Forrester Research. ■

Como funcionam as plataformas

As tecnologias de monitorização e gestão têm de ser capazes de reunir dados para análise de forma a que possam reportar o estado da rede a qualquer hora.

As ferramentas são normalmente ou baseados em agentes não usam agentes. Os fabricantes que fornecem a sua tecnologia como software, exigem frequentemente agentes, pequenas partes de código que residem em dispositivos geridos ou em servidores perto dos dispositivos geridos, para recolher os dados. Os agentes podem também ser configurados para desempenharem acções, como reiniciar um dispositivo, se residirem no dispositivo gerido. Os dados recolhidos dos agentes são então processados por um motor de correlação e procedimentos de análise são aplicados para determinar o que os eventos significam para a rede no seu todo. As funcionalidades de reporte fornecem dados recolhidos, em gráficos ou tabelas e por vezes em painéis de controlo customizados.

A gestão de desempenho move a gestão de rede, do mundo a preto e branco da indisponibilidade e disponibilidade, para um mundo de cinzentos subtis.

À medida que as falhas de dispositivos se tornam menos comuns, os gestores de redes dependem mais em gestão de desempenho para manter os ambientes a funcionarem sem sobressaltos. Em vez de esperar pelas falhas, as ferramentas de gestão de desempenho podem monitorizar coisas como a degradação de tempos de resposta, capazes de contribuir para serviços de rede que caíam abaixo dos limites pre-estabelecidos.

Esses limites estão determinados antecipadamente por gestores de redes que calculam que tempos de resposta, que latência de redes e que degradação de desempenho estão dispostos a tolerar. Por exemplo, um servidor de internet capaz de suportar uma aplicação crítica seria de maior preocupação do que um servidor de back-end a suportar uma aplicação pouco usada.

Os produtos de gestão de rede fazem análises profundas ao nível da raiz quando mais de um dispositivo ou elemento está envolvido na disponibilização de um serviço. Com múltiplos dispositivos, é necessário determinar onde uma falha ocorreu. Tais esforços de gestão trazem

a gestão padronizada de dispositivos para outro nível de gestão: a gestão de níveis de serviço ou Service Level Management (SLM). Esta prática monitoriza o desempenho do serviço de uma rede inteira ou aplicação de negócio, que engloba múltiplos componentes de rede, sistema, armazenamento e aplicações. Dados recolhidos por agentes instalados em várias máquinas são agregados para perceber onde degradações de desempenho ocorrem ao longo do serviço.

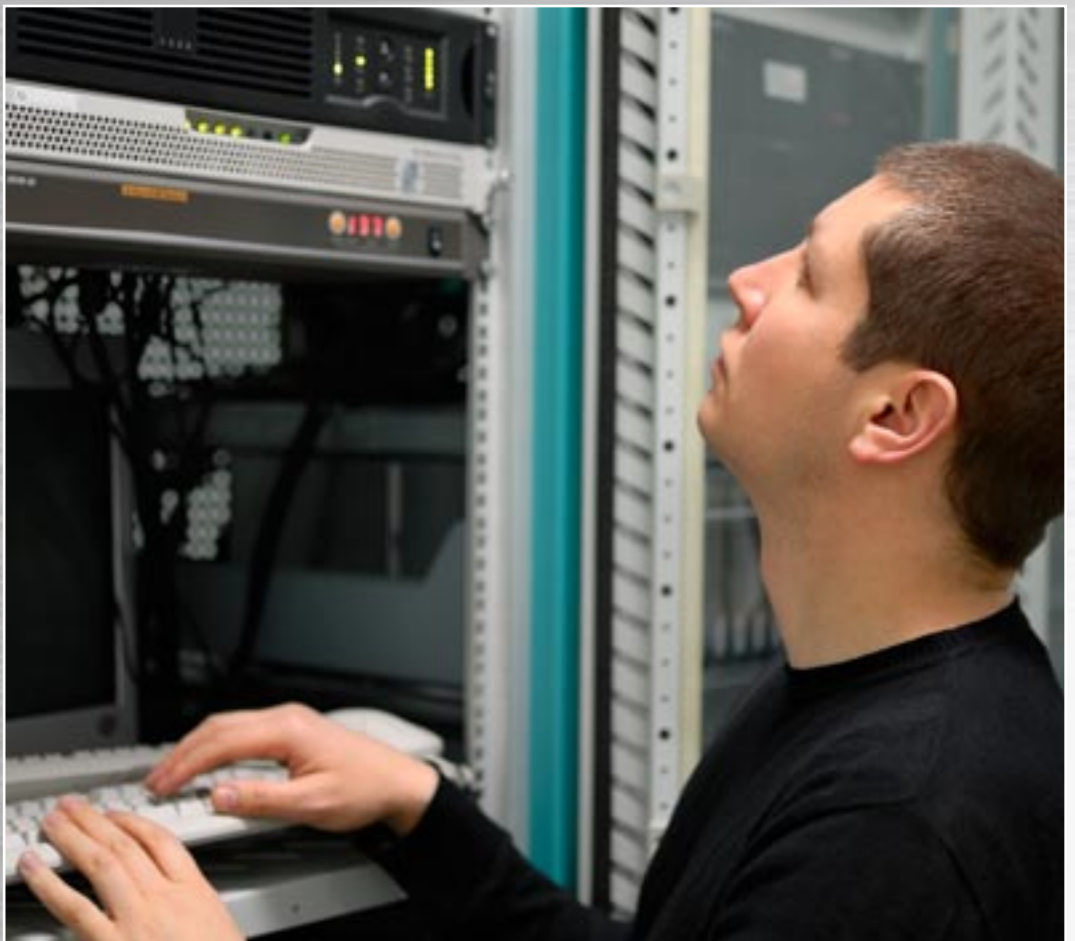
As ferramentas sem agentes são normalmente usados mais frequentemente na monitorização de disponibilidade de dispositivos de rede e sistemas.

Muitos fabricantes actualizaram as suas ferramentas sem agentes com suporte para protocolos como o Windows Management Instrumentation (WMI) e o Secure Shell (SSH) para capacitar o software para conseguir reunir mais dados de um dispositivo ou sistema sem ter de instalar um agente.

As tecnologias sem agente também funcionam bem na descoberta de rede e sistemas de in-

ventariação de, mas a tecnologia torna-se limitada quando é necessária informação mais profunda. As ferramentas de gestão de rede com enfoque em análise de tráfego podem, disponibilizar uma visão do tipo e do volume de tráfego na rede em qualquer altura. Alertam quando os padrões de tráfego se desviam do comportamento normal, que pode indicar um problema de desempenho ou um problema de segurança.

Os fabricantes de análise de tráfego podem usar também métodos sem agents para recolher dados sobre padrões de tráfego e identificar os protocolos mais usados na rede. Os produtos desta área abrangem desde dispositivos móveis para resolver problemas específicos a agentes instalados num ponto fixo que monitoriza tendências de tráfego em períodos longos. Os dispositivos conseguem identificar quando um servidor está a mandar demasiados pedidos, que pode ser um problema de segurança, ou quando um utilizador final está a entrar numa rede de partilha P2P.



INVISTA NO SEU NEGÓCIO. A PT INVESTE POR SI NA TECNOLOGIA.

A informação da sua empresa vai ficar à prova de tudo. Com os Data Centers PT a sua empresa pode alojar sistemas de informação com total segurança, beneficiando de ganhos em eficiência, produtividade e rentabilidade para o seu negócio. A PT disponibiliza uma rede de Data Centers entre Lisboa, Porto e Ilhas, que possibilita o fornecimento das soluções acertadas para a protecção do principal activo da sua empresa: a informação.

Para mais informações contacte o seu Gestor de Cliente ou consulte o site www.ptempresas.pt

