Monitoramento de infraestrutura com Zabbix | Acompanhe a saúde de sua infraestrutura

infra MAGAZINE

Cloud computing e o mercado
Como a nuvem vai afetar os profissionais de TI

Gerenciamento de Alta Disponibilidade em Serviços de TI
A administração dos serviços de TI com garantias de continuidade

Edição 05 - Ano 01

DevMedia

Backup
planejando seu sistema



Redes IP Multicast
Conheça e domine as Redes IP Multicast

Antivírus Corporativo
A escolha correta para sua organização

Especial

Linux e Windows: isso dá Sambta | Integrando o mundo não Windows com o Windows



TENHA ACESSO ILIMITADO A TODO CONTEÚDO DO SITE DEVMEDIA

SEJA UM ASSINANTE MVP!

Tenha acesso garantido a qualquer tema que você possa necessitar!

VIDEOS -AULAS

O assinante MVP acessa todas as vídeo-aulas do site DevMedia. Nenhum outro produto dá essa possibilidade. São mais de **7.000 video-aulas.**

CURSOS

Nosso site possui atualmente **+ de 250 cursos online** com a qualidade que você já conhece e confia. Com o MVP você terá acesso a todos eles.

REVISTAS

Assinante MVP acessa todas as nossas revistas na versão digital, incluindo todas as edições anteriores. Quando pintar aquela dúvida você terá mais de **3.500 artigos para consultar!**

ASSINATURA MVP MOST VALUABLE PROFESSIONAL

A assinatura MVP te dá a oportunidade de aumentar seu conhecimento em diversos assuntos, com qualidade e economia.

Invista na sua carreira se torne um profissional ainda mais completo!

POR APENAS R$59,90 POR MÊS

DevMedia

Acesse: www.devmedia.com.br/mvp

Sumário

Olá, eu sou o **DevMan**! Desta página em diante, eu estarei lhe ajudando a compreender com ainda mais facilidade o conteúdo desta edição. Será um prazer contar com sua companhia! Confira abaixo o que teremos nesta revista:



Infra

06 – Gerenciamento de Alta Disponibilidade em Serviços de TI
A administração dos serviços de TI com garantias de continuidade
[*André Leon S. Gradvohl*]

Infra, Web

08 – Cloud computing e o mercado
Como a nuvem vai afetar os profissionais de TI
[*Alberto Oliveira*]

Infra

11 – Linux e Windows: isso dá Samba
Integrando o mundo não Windows com o Windows
[*Thiago Pirola Ribeiro*]

Infra

20 – Salve seus dados com Bacula
Backup centralizado utilizando uma ferramenta open source – Parte 1
[*Flávio Alexandre dos Reis e Eduardo Pagani Julio*]

Infra

28 – Redes IP Multicast
Comunicação multiponto: gerenciamento dos grupos de usuários e roteamento de pacotes IP multicast
[*André Koide da Silva*]

Segurança, Infra

36 – Monitorando servidores com collectd
Deixe o monitoramento ser seus olhos
[*Thiago Nache*]

Segurança, Infra

44 – Monitoramento de infraestrutura com Zabbix
Como usar esta ferramenta para monitorar a saúde de sua infraestrutura
[*Mário de Mello Bittencourt Neto*]

Segurança, Infra

53 – Antivírus Corporativo
A escolha correta para sua organização
[*Roberto Henrique de Sousa*]

[Infra] Artigo que apresenta tecnologias relacionadas a questões de Infraestrutura.

[Segurança] Artigo dentro do contexto de Segurança: redes, servidores, sistemas operacionais, infraestrutura em geral.

[Web] Artigos sobre ou que envolvam tecnologias de infraestrutura para WEB.

infra MAGAZINE

Ano I • Edição 05 • 2012

Edição

Editor

Eduardo Spínola (*eduspinola@gmail.com*)

Produção

Jornalista Responsável Kaline Dolabella - JP24185

Atendimento ao leitor

A DevMedia possui uma Central de Atendimento on-line, onde você pode tirar suas dúvidas sobre serviços, enviar críticas e sugestões e falar com um de nossos atendentes. Através da nossa central também é possível alterar dados cadastrais, consultar o status de assinaturas e conferir a data de envio de suas revistas. Acesse **www.devmedia.com.br/central**, ou se preferir entre em contato conosco através do telefone 21 3382-5038.

Publicidade

publicidade@devmedia.com.br – 21 3382-5038

Anúncios – Anunciando nas publicações e nos sites do Grupo DevMedia, você divulga sua marca ou produto para mais de 100 mil desenvolvedores de todo o Brasil, em mais de 200 cidades. Solicite nossos Media Kits, com detalhes sobre preços e formatos de anúncios.

Fale com o Editor!

É muito importante para a equipe saber o que você está achando da revista: que tipo de artigo você gostaria de ler, que artigo você mais gostou e qual artigo você menos gostou. Fique a vontade para entrar em contato com os editores e dar a sua sugestão!

Se você estiver interessado em publicar um artigo na revista ou no site Easy Java Magazine, entre em contato com o editor, informando o título e mini-resumo do tema que você gostaria de publicar:

Eduardo Spínola - Editor da Revista
eduspinola@gmail.com

DevMedia

Editorial

Alguma vez você já perdeu arquivos por não fazer backup? Já teve algum HD queimado e não conseguiu recuperar seus dados? Caso positivo, você sabe o trabalho que esta situação pode proporcionar. Caso negativo, não é difícil de imaginar os problemas enfrentados. Agora, ao invés de pensar em seu computador pessoal, imagine as proporções deste problema se o mesmo acontecer em sua empresa. Esta não é uma boa situação que devemos vivenciar para aprender. Previna-se! Para auxiliar nesta tarefa, como capa desta edição, faremos um rico estudo sobre backup.

Salve seus dados com Bacula tem como objetivo demonstrar a importância do uso de ferramentas de backup para qualquer administrador que zele pela segurança de seus dados. Nessa primeira parte do artigo serão abordados conceitos básicos, mitos, tipos e métodos utilizados para cópia de dados. Será demonstrado como elaborar uma rotina de backup adotando várias tecnologias de armazenamento.

Gerenciamento de Alta Disponibilidade em Serviços de TI descreve os principais objetivos associados à alta disponibilidade, bem como os controles e métricas para atingir tais objetivos. Em seguida, associam-se os cinco estágios do ciclo de vida dos serviços propostos pelo ITIL aos objetivos associados à alta disponibilidade.

Cloud computing e o mercado fala de um assunto bastante atual e que, eventualmente, gera polêmica ao ser comentado: o que será dos profissionais de TI, em um momento onde as empresas procuram levar seus serviços para cenários de utilização de recursos em nuvem?

O artigo **Linux e Windows: isso dá Samba** apresenta a instalação e configuração do servidor Samba nas distribuições Debian e Ubuntu, utilizando-se de modo texto e modo gráfico para a configuração do mesmo.

Redes IP Multicast relata as principais características das redes IP multicast. Estas suportam as comunicações multiponto, demandadas pelas novas aplicações da Internet, tais como: IPTV, videoconferência, ensino a distância, entre outras. Para tanto, serão examinados os protocolos de gerenciamento de grupos de usuários e os algoritmos de roteamento utilizados para o encaminhamento dos pacotes IP multicast.

Já **Monitorando servidores com collectd** destaca aspectos do monitoramento de servidores Linux utilizando as principais ferramentas do mercado, ampliando a visão do administrador e possibilitando ações preventivas no ambiente, como alertar seu cliente que o consumo de recursos está aumentando e que em breve ele poderá ter problemas.

Em um ambiente de TI com vários sistemas operacionais, servidores e serviços, saber como eles estão se comportando e ser avisado preventivamente ajuda a intervir antes que problemas maiores se apresentem. Este é o conteúdo abordado em **Monitoramento de infraestrutura com Zabbix**.

Para finalizar, **Antivírus Corporativo** retrata as principais razões para a adoção de um sistema de antivírus corporativo e quais as implicações que uma organização pode sofrer por não seguir as melhores práticas de segurança contra ameaças virtuais.

Eduardo Oliveira Spínola
eduspinola@gmail.com
twitter.com/Java_Magazine



Seu **conhecimento vale muito** na DevMedia

Publique artigos e vídeos gratuitamente no site e participe do programa **PayContent.**

Sua participação pode ser premiada: quanto mais você postar, mais chances de ganhar.



Para saber mais acesse:
www.devmedia.com.br/paycontent

DevMedia

Gerenciamento de Alta Disponibilidade em Serviços de TI

O gerenciamento dos serviços de TI com garantias de continuidade

André Leon S. Gradvohl

O artigo anterior abordou os conceitos de Alta Disponibilidade (*High Availability* – HA) e Recuperação de Desastres (*Disaster Recovery* – DR). Naquela ocasião, destacou-se uma série de definições pertinentes aos conceitos e mostraram-se algumas topologias para implementá-los. Contudo, o tema é muito vasto e, por isso, este artigo complementará as informações, considerando as questões de gerenciamento de alta disponibilidade nos serviços de TI.

Para ter um gerenciamento de HA efetivo, o primeiro passo é compreender e documentar os requisitos de disponibilidade da instituição ou do cliente. Importa destacar que nem todos os serviços prestados pela instituição devem atender aos critérios de alta disponibilidade (99,9% de disponibilidade ou mais) e, quanto maior o número de serviços com características de HA, maior será o investimento. Por isso, a implementação do gerenciamento de disponibilidade com sucesso depende de uma clara compreensão dos requisitos de disponibilidade do cliente e dos negócios da instituição.

Objetivos e controles associados à Alta Disponibilidade

Os quatro principais objetivos associados à HA são: (i) maximização do tempo de serviço disponível ou redução do tempo médio entre falhas de serviço; (ii) eliminação ou redução do impacto dos incidentes relacionados ao serviço; (iii) minimização do tempo de manutenção do serviço não planejado ou não agendado; e (iv) redução do tempo de manutenção planejado ou agendado. Esses objetivos estão ligados a três conceitos importantes: *reliability* (confiança do serviço), *maintainability* (facilidade de manutenção do serviço) e *serviceability* (tempo planejado de manutenção).

Uma vez determinados os objetivos, o próximo passo é determinar os controles necessários para o gerenciamento de HA. Os principais controles são os seguintes: planos de disponibilidade, tanto no nível empresarial, quanto no nível do serviço (incluindo todos os serviços que possuem HA); identificação dos recursos críticos de TI, especialmente os discos e processadores; manutenção dos planos de disponibilidade; políticas de segurança; níveis de acordo de serviço (*service level agreement* – SLA) e níveis de acordo de operações (*operations-level agreement* – OLA); uma estratégia de TI; e um catálogo de serviços. Esses controles são documentos essenciais para o gerenciamento de sistemas com alta disponibilidade.

Resumo DevMan

De que se trata o artigo:

O artigo trata do gerenciamento de alta disponibilidade de serviços. No artigo são descritos os principais objetivos associados à alta disponibilidade, bem como os controles e métricas para atingir tais objetivos. Em seguida, associam-se os cinco estágios do ciclo de vida dos serviços propostos pelo ITIL aos objetivos associados à alta disponibilidade.

Em que situação o tema é útil:

O tema é de suma importância aos analistas de infraestrutura que desejam incorporar os conceitos de alta disponibilidade aos serviços prestados pela instituição a que pertencem. O artigo indica algumas métricas que devem ser observadas por esses analistas para acompanhar e certificar que seus serviços atendem aos critérios de alta disponibilidade.

Gerenciamento de Alta Disponibilidade em Serviços de TI:

O artigo aborda o conceito de gerenciamento de alta disponibilidade, incluindo os objetivos e controles associados a este gerenciamento. Além disso, apresentam-se as principais métricas a serem observadas para garantir serviços com alta disponibilidade. Por fim, estabelece-se uma relação entre o ciclo de vida dos serviços descrito pelo Information Technology Infrastructure Library e os objetivos da alta disponibilidade.

Além dos controles, é preciso ter métricas que possam medir o desempenho de um sistema de gerenciamento de disponibilidade. Tais métricas podem sinalizar alguns aspectos que devem estar presentes nos controles mencionados. Entre tais aspectos estão os esforços, custos financeiros e quantidade de tempo dedicados às tarefas, por exemplo. A seguir, apresentam-se algumas das métricas mais comuns:

- Duração de tempo, esforço humano e custos requeridos para desempenhar as atividades do processo de gerenciamento de disponibilidade, e.g. planejamento e execução dos planos de disponibilidade;
- Porcentagem, duração, frequência, impacto e custo dos incidentes que afetaram a disponibilidade;
- Quantidade e porcentagem de:
  - Planos de disponibilidade aprovados, financiados e executados;
  - Componentes de TI críticos e serviços com acordos de HA (atualizados e não atualizados); e

– Componentes de TI críticos e serviços com critérios de recuperação.

• Tempo decorrido desde a última:

– Auditoria de disponibilidade;

– Atualização do plano de disponibilidade; e

– Avaliação do plano de disponibilidade.

Alta Disponibilidade e o ciclo de vida dos serviços

Não se pode comentar sobre ciclo de vida de serviços sem relacioná-lo com o que preconiza o *Information Technology Infrastructure Library* (ITIL), em sua versão 3, lançada em maio de 2007. O ITIL documenta as boas práticas que devem ser aplicadas na operação, manutenção e infraestrutura de serviços TI.

A versão 3 do ITIL identifica cinco estágios no ciclo de vida de serviços, conforme ilustrado na **Figura 1**, a saber: (i) gerenciamento da estratégia de serviços; (ii) projeto de serviços; (iii) transição de serviços; (iv) operação dos serviços; e (v) melhoria contínua do serviço. Esses cinco estágios estão relacionados aos quatro objetivos da HA descritos a seguir.

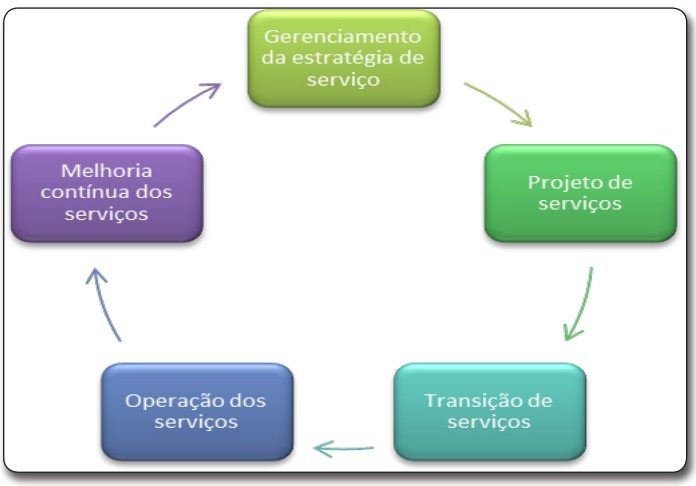


Figura 1. Ciclo de vida dos serviços, segundo a ITIL

No estágio (i), o gerenciamento da estratégia de serviço ajuda na definição dos requisitos de disponibilidade e na racionalização dos investimentos para melhorar a disponibilidade do serviço. Isso é feito ao se detalhar a relação entre o serviço e as estratégias funcionais e do negócio.

Na fase (ii), o projeto do serviço inclui a determinação e documentação dos requisitos do serviço, inclusive aqueles ligados às questões de disponibilidade, bem como a adição de um conjunto de requisitos funcionais e não funcionais. Convém ressaltar que o gerenciamento de disponibilidade é um processo de TI e, como tal, é parte do estágio de projeto do serviço.

Na transição de serviços, ou seja, no estágio (iii), o serviço muda para o modo operacional, e isso envolve o desenvolvimento de uma base de informações de configuração relacionada ao serviço. Essa base de informações contém a documentação da arquitetura do serviço, os procedimentos operacionais e outras documentações específicas. Nesse estágio também se incluem testes, avaliação e validação do serviço em ambiente de produção. Portanto, também é necessário incluir os testes de HA.

Na fase (iv), operação do serviço, várias atividades operacionais devem ser observadas. Entre elas estão aquelas ligadas às medidas antes citadas, a saber: gerenciamento de eventos e incidentes, com vistas às coletas dos dados relativos aos quatro objetivos associados à HA; auditorias de configuração pós implantação, incluindo auditoria de disponiblidade; e auditorias de operação, com o objetivo de direcionar manutenções preventivas em hardware e software.

Por fim, no estágio (v), o melhoramento do serviço inclui o desenvolvimento e implementação dos planos de melhoria da disponibilidade. Esses planos são baseados na análise da arquitetura, observando os pontos de fragilidade do serviço implantado e que impactam na sua disponibilidade.

Conclusão

São três as ações fundamentais da atividade de gerenciamento: organizar, planejar e executar. Sendo assim, um sistema de alta disponibilidade, bem gerenciado, prescinde da organização de requisitos claros que estabeleçam os critérios de negócios e de serviços. Em seguida, esse sistema precisa de um bom planejamento que considere esses requisitos e garanta a continuidade dos serviços, especialmente na presença de incidentes. Depois, por ocasião da sua execução, o sistema deve atender os requisitos de robustez previstos no seu plano original. Essas ações fazem parte de um ciclo que se renova a cada atualização dos serviços. Cabe aos analistas responsáveis pela infraestrutura uma visão crítica de todo o processo, a auditagem da situação e a indicação das melhorias a serem implementadas no próximo ciclo.



André Leon S. Gradvohl

gradvohl@ft.unicamp.br

É doutor em Telecomunicações, mestre e bacharel em Computação. Atua como professor e pesquisador da Faculdade de Tecnologia (FT) da Universidade de Estadual Campinas (Unicamp). Também é membro do Laboratório de Simulação e Computação de Alto Desempenho (LaSCADo) e do Grupo de Engenharia da Informação e Conhecimento (GEICon), ambos sediados na FT/Unicamp. É responsável pelo projeto "Metalinguagem para processamento de alto desempenho em arquiteturas híbridas" financiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP - 2011/00861-0).

Livro "An Introductory Overview of ITIL V3", Escrito por Alison Cartlidge et al. Editora itSMF Ltd., 2007.

http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf

Livro "Business Continuity and Disaster Recovery Planning for IT Professionals". Escrito por Susan Snedaker. Editora Syngress, 2007.

Normas ISO/IEC 27001 (Information Security Management System) e ISO/IEC 27002 (Information Technology - Security Techniques)

http://17799.standardsdirect.org

Cloud computing e o mercado

Como a nuvem vai afetar os profissionais de TI

Alberto Oliveira

Nos últimos meses recebemos uma enxurrada de informações relacionadas a provedores de serviços na nuvem. Soluções, parceiros, fabricantes. Parece que todos resolveram aderir a esse tipo de cenário.

A migração para a nuvem pode ser bastante atrativa para vários modelos de negócio, por várias razões. Economia com recursos computacionais, espaço físico, resfriamento do datacenter, manutenção e suporte são alguns dos motivos pelos quais as corporações vêm adotando mais e mais as soluções de cloud.

Corporações de vários tamanhos irão achar atraente a possibilidade de não precisar mais manter uma estrutura de equipamentos cara, bem como os contratos de suporte relacionados aos serviços suportados pela mesma e necessários ao negócio. E-mail corporativo, anti-spam, filtro de conteúdo, portal de colaboração, software para vídeo conferência são alguns exemplos de serviços tão comumente utilizados nos dias de hoje e que possuem opções de utilização na nuvem, com menor custo de aquisição e diversos benefícios de escalabilidade e manutenção.

Resumo DevMan

De que se trata o artigo:

O artigo fala de um assunto bastante atual e que, eventualmente, gera polêmica ao ser comentado: o que será dos profissionais de TI, em um momento onde as empresas procuram levar seus serviços para cenários de utilização de recursos em nuvem?

Em que situação o tema é útil:

O tema aborda o cenário atual de Cloud Computing e pode auxiliar os profissionais que desejam um direcionamento sobre as oportunidades que existem no mercado de trabalho, com base nas novas soluções de Cloud Computing.

Cloud computing e o mercado:

Nesse artigo discutimos, de forma breve, as soluções de Cloud Computing existentes no mercado e o seu impacto na vida dos profissionais de TI, bem como as oportunidades geradas pelo novo modelo de negócio.

Como tudo começou?

O conceito de nuvem não é recente. Já utilizamos recursos armazenados ou "hosteados" há bastante tempo. E-mail gratuito, blogs, aluguel de espaço em provedores para colocar servidores e hosting de sites web estão entre as opções mais conhecidas. Entretanto, com a evolução das tecnologias e links de acesso, provavelmente muitos fabricantes pensaram: porque eu preciso "vender" o meu software/hardware se eu posso "alugar" e garantir minha sustentabilidade, além de propor um modelo de utilização bastante atrativo para todos os tamanhos de organização? E assim nasceu a mais nova onda da informática, como tantas outras que já tivemos (linguagens visuais, por exemplo): o Cloud Computing.

Existem, hoje, várias siglas associadas ao modelo de computação na nuvem. Citaremos três, em específico, onde existe uma tendência de que gerem as maiores demandas de oportunidades de trabalho e negócios, baseadas já nesse novo cenário. O mercado está em plena mudança de conceitos, inclusive, e a forma como trabalhamos já começou a mudar. Tempos atrás era impensável prestar suporte a um serviço onde não houve "deploy". Como eu vou suportar algo que não foi instalado ou configurado? Hoje, temos a possibilidade disso, bem como a de desenvolver e customizar aplicações que não se encontram no ambiente físico do cliente. Vejamos, então, as principais possibilidades de serviços em Cloud Computing:

- **PaaS – Plataforma como serviço:** Utilizamos este termo para definir o uso de recursos de plataforma na nuvem. Quando pensamos em plataforma, lembramos do que usamos comumente em nossos ambientes. Servidores web, Active Directory, servidores SQL. O consumo desse tipo de serviço caracteriza o PaaS;
- **IaaS – Infraestrutura como serviço:** Utilizamos este termo para definir o uso de percentuais, ou "pedaços" de servidores hospedados que tenham a capacidade de responder a uma necessidade específica da corporação, em termos de processamento e recursos;
- **SaaS – Software como serviço:** Talvez o modelo mais conhecido de todos, o SaaS pode ser definido como o modelo que permite o uso de um determinado software como se o estivéssemos alugando, isto é, pagando para utilizá-lo. Um bom exemplo é o pacote BPOS da Microsoft (futuramente Office365) ou o Google Apps, da Google, onde você pode "alugar" caixas postais, criar portais corporativos, dentre outras possibilidades, sem investimento em infraestrutura. Outro exemplo, você utiliza o Exchange como servidor de correio (Microsoft), tem acesso a todos os recursos que o mesmo provê, mas não precisou

comprar o produto ou montar uma estrutura interna para usar o serviço. Você utiliza o serviço que a Microsoft fornece.

Para onde estamos indo?

Utilizar recursos de nuvem pode ser bastante tentador. Existem inúmeras vantagens no modelo de prestação do serviço, tais como SLA agressivo, custo de aquisição "inexistente", redução expressiva no custo de manutenção, uso por demanda, dentre outras, representando, muitas vezes, uma economia real. Você consegue acesso a recursos que possuem redundância e alta-disponibilidade em termos geográficos, suporte 24x7 mundial com alto valor agregado como solução e baixo custo para utilização. Num exemplo clássico desse cenário, vamos falar sobre anti-spam na nuvem.

Hoje, estatisticamente falando, 70% a 80% das mensagens que chegam ao servidor de correio são SPAM, ou seja, serão descartadas. Isso acarreta custo com processamento de servidor para eliminar as mensagens; link de internet; compra, manutenção e atualização do software anti-spam; espaço físico para colocar o servidor (ou a máquina virtual); ar condicionado para resfriar o ambiente e muito mais custos que nem sempre conseguimos visualizar. Então, porque não receber apenas os 20% de mensagens que interessam ao invés de manter todo esse aparato para simplesmente eliminar o indesejável?

Existem, da mesma forma, restrições nos serviços que devem ser observadas. Vamos falar sobre recuperação de mensagens em caixas postais. Suponha que, inadvertidamente, você apague uma mensagem importante de sua caixa postal. Os provedores de nuvem, em geral, limitam o tempo em que mantêm essa informação passível de recuperação, antes da deleção completa. Se você identificar rapidamente que realizou a ação, não há maiores problemas. Basta abrir um chamado e recuperar a mensagem. Mas e se você se der conta disso após o período de salvaguarda do provedor? Sua mensagem será perdida em definitivo, infelizmente. Existem outros agravantes. Algumas empresas necessitam, por questões de regulamentação, armazenar e recuperar dados por mais tempo do que os provedores oferecem atualmente. Na média, o padrão é de 14 dias. Empresas que aderem a Sarbanes-Oxley (veja a **Nota DevMan 1**), por exemplo, necessitam guardar dados por cinco anos. Para essas corporações, a adoção de recursos na nuvem poderá ser mais lenta ou, num primeiro momento, indesejada.

Entretanto, existe uma verdade única e absoluta: as empresas SEMPRE irão procurar formas de ter melhores serviços, gastando menos. Neste cenário, a nuvem é uma realidade e não teremos como "fugir" disso. Então, o que nos resta? Quais as oportunidades que teremos com as empresas migrando seus serviços para a nuvem?

O Futuro e as oportunidades

Diante deste cenário, o profissional de infraestrutura, como conhecemos hoje, tende a "morrer". Uma vez que não haja serviços dentro das corporações, o que restará de trabalho para nós? Felizmente, muita, muita coisa. Da mesma forma que passamos por uma mudança em termos de modo de operação de nosso trabalho, novas opções se tornam viáveis e reais. Por exemplo: quantas empresas você conhece que prestam consultoria para adoção de soluções em nuvem? Quantas outras procuram prover treinamento de usuários para utilização dos novos serviços? Oportunidades existem e precisamos estar atentos às mesmas.



Nota do DevMan 1

Sarbanes-Oxley

A lei Sarbanes-Oxley, apelidada de Sarbox ou ainda de SOX, visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo ainda regras para a criação de comitês encarregados de supervisionar suas atividades e operações, de modo a mitigar riscos aos negócios, evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrerem, garantindo a transparência na gestão das empresas. (Fonte: Wikipédia).

Vejamos algumas possibilidades dentro do cenário que se desenha:

- **Nuvem privada:** Nem todos os ambientes estão aptos à adoção de nuvem, conforme discutimos anteriormente. Sendo assim, um novo nicho que se expande é o de ambientes virtualizados internos (nuvens privadas), de alta disponibilidade, para fornecimento de serviços de média e alta complexidade. É bem verdade que nem todas as empresas adotarão esse modelo, mas é certo que muitas o farão e, com isso, teremos bastantes oportunidades no setor. E como se preparar para isso? Estudando as tecnologias de virtualização existentes hoje e estando antenados com as mudanças do mercado;
- **Plataforma como serviço:** Utilizando serviços na nuvem, tais como servidores de banco de dados, continuamos a ter a figura do DBA presente, tanto durante a migração da estrutura interna para a nuvem, quanto na manutenção e estruturação das bases em si. Desenvolvimento agregado a soluções de nuvem é uma das grandes (e boas) possibilidades dentro deste nicho;
- **Infraestrutura como serviço:** Mais e mais provedores de serviço irão surgir, tentando, cada um, ter a sua "fatia" do bolo dos novos serviços. Esses provedores certamente irão precisar de profissionais qualificados e capacitados para manter seus serviços disponíveis. Os consultores com conhecimentos em infra e segurança serão, cada vez mais, assediados por essas empresas. É preciso estar com o conhecimento em dia e alinhado com as novas necessidades e modelos de negócio;
- **Software como serviço:** No processo de utilização de softwares "hospedados", capacitação é um item que merece atenção, pois os usuários, e administradores, passarão por um processo de readequação na forma de trabalho. Consultorias para adoção de nuvem pode ser um excelente negócio, tanto no momento de migração, quanto no suporte ao ambiente em produção.

Conclusão

Existem inúmeras outras possibilidades de negócios envolvendo a nuvem. Diante de tudo isso, o que sobra para os profissionais que cuidam da infraestrutura das corporações? Os tão conhecidos administradores da rede?

Toda novidade traz novas possibilidades. Numa visão mais objetiva, podemos entender que haverá uma aproximação desses profissionais da área de negócios da empresa. O papel deles será fundamental na consultoria e no apoio à implantação da melhor solução de nuvem para o negócio da empresa.

Isso incorrerá em uma quebra de paradigma, visto que o envolvimento do administrador da rede passará a ser direcionado ao andamento do negócio e das opções de otimização do mesmo, ao invés do antigo foco técnico em implementar e manter soluções. É uma forma de trabalhar diferente e precisaremos nos adequar a ela. Como em toda grande mudança, haverá resistência. Ser ágil e procurar a capacitação necessária fará toda a diferença para o futuro de cada profissional.



Alberto Oliveira
Alberto.oliveira@truesec.com.br
É consultor de segurança da informação e atua no mercado há mais de 10 anos. Já realizou diversos projetos envolvendo tecnologias de segurança Microsoft e de outros fabricantes. É sócio fundador da TrueSec Soluções, empresa de consultoria e treinamentos localizada em Recife-PE. É MVP em Forefront desde 2006 e possui as seguintes certificações: CISSP, CompTIA Security + MCSA/MCSE: Security, MCT, MCTS, MCITP e ITIL. Já realizou diversas palestras pelo Brasil e webcasts Microsoft, sendo palestrante oficial do TechEd em três oportunidades: sobre segurança da informação, ISA Server e TMG, e contribui nos fóruns técnicos da Microsoft e listas de discussão (MCPdx/MCT Brasil). Twitter: @_AlbertoOliveir. Blog: http://oliveiraalberto.wordpress.com.

Artigo: Cloud Computing: Entenda este novo modelo de computação
http://idgnow.uol.com.br/computacao_corporativa/2008/08/13/cloud-computing-entenda-este-novo-modelo-de-computacao/

Artigo: Redes Sociais e Cloud Computing transformarão a área de TI
http://computerworld.uol.com.br/tecnologia/2008/04/09/gartner-multicore-redes-sociais-e-cloud-computing-transformarao-ti/

Artigo: O que é Cloud Computing (computação nas nuvens)?
http://www.infowester.com/cloudcomputing.php

DÊ UM SALTO EM CONHECIMENTO!



Acesse o maior portal para desenvolvedores da América Latina!

17 mil posts

280 mil cadastrados

5 milhões de page-views por mês

Linux e Windows: isso dá Samba

Integrando o mundo não Windows com o Windows

Thiago Pirola Ribeiro

Resumo DevMan

De que se trata o artigo:

Este artigo apresenta a instalação e configuração do servidor Samba nas distribuições Debian e Ubuntu, utilizando-se de modo texto e modo gráfico para a configuração do mesmo.

Em que situação o tema é útil:

O conteúdo apresentado neste artigo auxiliará os usuários que necessitam de locais específicos para compartilhar arquivos e impressoras, criando uma estrutura centralizada e de fácil manutenção e gerenciamento.

Linux e Windows: isso dá Samba:

Este artigo apresenta o servidor Samba, que permite o compartilhamento de arquivos e impressoras do Linux com o ambiente Windows. Ao término do artigo, o leitor terá um servidor Samba em pleno funcionamento.

O Samba é um serviço disponibilizado em sistemas operacionais Unix e seus derivados para o compartilhamento de arquivos e impressoras entre esses sistemas e o sistema operacional Windows. Essa interação é feita pelo protocolo Netbios utilizado pelo Windows e interpretado pelo Samba, realizando uma tradução, e com isso inserindo as máquinas Unix na rede do Windows.

Antes do surgimento do Samba, o mundo Unix era exclusivo de servidores de grande porte, aos quais eram conectados os terminais e seus arquivos eram compartilhados apenas entre outros Unix. Com o desenvolvimento do Linux e suas melhorias e facilidades, inúmeros usuários adotaram este sistema, porém sempre encontravam problema em compartilhar arquivos ou mesmo uma impressora com um computador que estava trabalhando com Windows. Atualmente em algumas distribuições Linux, o Samba já vem instalado e em pleno funcionamento, porém muito subutilizado por não se ter uma ferramenta de configuração adequada.

Este artigo será focado na instalação e configuração do servidor Samba, apresentando a configuração através do terminal e, também, através de dois programas gráficos que utilizam o navegador como interface de configuração.

Histórico

O Projeto do Samba nasceu da necessidade de Andrew Tridgell acessar uma área de um disco em um servidor Unix utilizando-se de um PC com DOS (sistema operacional da Microsoft anterior ao Windows e sem janelas). Através de engenharia reversa e análises do protocolo NETBIOS da Microsoft, Andrew conseguiu fazer com que o servidor Unix aparecesse para o DOS, como se fosse outro PC com DOS. Atualmente pode-se fazer esse tipo de acesso a servidores Unix através de clientes NFS (*Network File System* – Sistema de Arquivos para Rede).

Andrew publicou o código do protocolo desenvolvido em 1992, porém o nome Samba para o servidor originou-se das letras do protocolo desenvolvido SMBServer (nome patenteado pela empresa Syntax) e, conforme descrito no histórico do próprio Samba, iniciou-se uma busca por uma palavra que continha as letras S, M e B, nessa ordem. Após a busca, encontrou-se a palavra SAMBA, que foi adotada como o nome do servidor e é utilizada até os dias de hoje.

O Samba é mais comumente utilizado para compartilhamento de arquivos, diretórios e impressoras entre os sistemas operacionais Microsoft e não-Microsoft, sendo que nestes são incluídos Unix, Linux, Mac OS, BSDs, entre outros.

Atualmente o Samba está na versão estável 3.6.3 e é oferecido através de pacotes para diversas distribuições Linux.

Instalação

Neste artigo serão utilizadas as distribuições Linux Debian e Ubuntu, sendo que recomendo para a utilização em servidores de produção, o Debian e o Slackware.

Pode-se instalar o Samba mais facilmente através dos pacotes que já vêm nas próprias distribuições ou através do binário encontrado no próprio sítio do Samba. Muitas vezes os pacotes disponibilizados nas distribuições não são os da última versão do sítio do Samba, porém é uma versão estável e já testada, para o Debian, e com isso não se terá problemas de conflitos e/ou incompatibilidades. Nas duas distribuições apresentadas aqui, pode-se utilizar a versão em testes ou ainda a instável, contudo para um servidor que estará em produção, com usuários acessando, isso não é recomendado.

A instalação através dos pacotes nas duas distribuições pode ser feita utilizando-se do terminal, que pode ser encontrado no Ubuntu (na versão clássica), ou no Debian, acessando-se o menu *Aplicativos* > *Acessórios* > *Terminal*. Já na versão do Ubuntu com *Unity* (versões mais recentes), clique no logotipo do Ubuntu e digite **terminal** para encontrar o programa.

Dentro do terminal, execute o comando:

```
sudo apt-get install samba
```

No Debian, aparecerá uma janela na instalação solicitando o nome do grupo de trabalho que será inserido no servidor Samba. Assim, informe o grupo de trabalho e clique em *Ok*. Após o término da instalação, o Debian já iniciará os serviços do Samba e importará os usuários locais para a base local do Samba.

No caso do Ubuntu, nada será solicitado na instalação, sendo que o mesmo também converterá os usuários do sistema para o Samba.

No Ubuntu, nas versões acima da 9.04, ainda se pode instalar o Samba pelo *Ubuntu Software Center*, que se encontra no menu *Aplicativos*, para a versão clássica da interface gráfica ou na interface *Unity*, na própria barra do menu abaixo do logo do Ubuntu.

Após iniciar o *Ubuntu Software Center*, na caixa de pesquisa apresentada na **Figura 1** (a), digite **samba** e tecle *Enter*. O retorno da busca será exibido na janela logo abaixo da caixa de pesquisa, aparecendo uma linha com Samba e o botão *Install*, **Figura 1** (b). É só clicar em *Install* que o Ubuntu baixará os pacotes necessários para a instalação e, ao término, instalará os pacotes e o Samba.

Independente de qual método de instalação for utilizado, alguns itens básicos serão inseridos no sistema e alguns *daemons* (processos em *background*) serão iniciados. Os processos que podem aparecer após a instalação e inicialização do Samba são:

- **nmbd**: Este *daemon* é o primeiro a ser iniciado e manipula todas as solicitações de registro e resolução de nomes, interagindo com as requisições baseadas no protocolo UDP, sendo este o protocolo base dos serviços de DNS;
- **smbd**: Este *daemon* deve ser iniciado imediatamente após a inicialização do **nmbd**. Ele manipula os serviços baseados em conexões que utilizam o protocolo TCP/IP, necessário para realizar as comunicações entre servidor/cliente e trocas de arquivos e gerenciamento de impressão, além do gerenciamento da autenticação local no Samba;
- **winbindd**: Este *daemon* deve ser iniciado quando o Samba é membro de um domínio, como o Active Directory, e também é necessário quando o Samba tem relações de confiança com outro domínio. Essas relações de confiança são muito utilizadas entre domínios, pois se um domínio confia no outro, os arquivos que serão entregues/compartilhados entre os usuários desses domínios são confiáveis e não precisarão de uma nova autenticação para que as transações ocorram. Para compartilhamentos do Samba fora de um domínio, ou seja, compartilhamentos básicos, este *daemon* não será iniciado.

Configuração

A configuração do Samba pode ser feita através da edição do arquivo de configuração ou através de interfaces gráficas. A segunda opção é muito utilizada, principalmente por usuários inexperientes ou na primeira vez em que se está configurando o servidor. Após instalar e configurar algumas vezes o Samba, nota-se que há pouca alteração de uma instalação para outra. Como exemplo cita-se alguns itens que podem ser alterados, como: o nome do grupo de trabalho e o nome do servidor Samba. Desta forma, administradores mais experientes, normalmente substituem o arquivo de configuração instalado originalmente por um arquivo de configuração que já foi utilizado e configurado em outra instalação.

O arquivo de configuração é o *smb.conf*, sendo que ao ser instalado, a distribuição já insere um *smb.conf.default* ou *smb.conf-sample* para auxiliá-lo no primeiro contato com esse arquivo. O conteúdo mínimo do *smb.conf* é apresentado na **Listagem 1**.

Listagem 1. Arquivo básico smb.conf.

```
[global]
  workgroup = grupo_de_trabalho
  netbios name = Minha_Maquina

[temporario]
  path = /tmp
```

O arquivo de configuração é todo separado por sessões, como é o caso da sessão **[global]**. Com essa organização fica mais fácil a manutenção posterior de itens específicos.

No caso da configuração apresentada anteriormente, a sessão **global** conterá todas as configurações globais necessárias para o funcionamento do serviço.

No item **workgroup** deverá ser colocado o nome do grupo de trabalho que é utilizado em sua rede. Deve-se atentar para o fato de não poder utilizar-se de espaços nos nomes, pois muitas vezes o serviço não funciona por esse simples espaço.

Em **netbios name** deve-se inserir o nome da máquina, sendo que este nome identificará o servidor Samba para os outros sistemas operacionais.

A sessão **temporario** é criada para que a pasta *tmp* possa aparecer como compartilhada ao acessar a máquina e com isso os usuários poderão acessar os arquivos e pas-

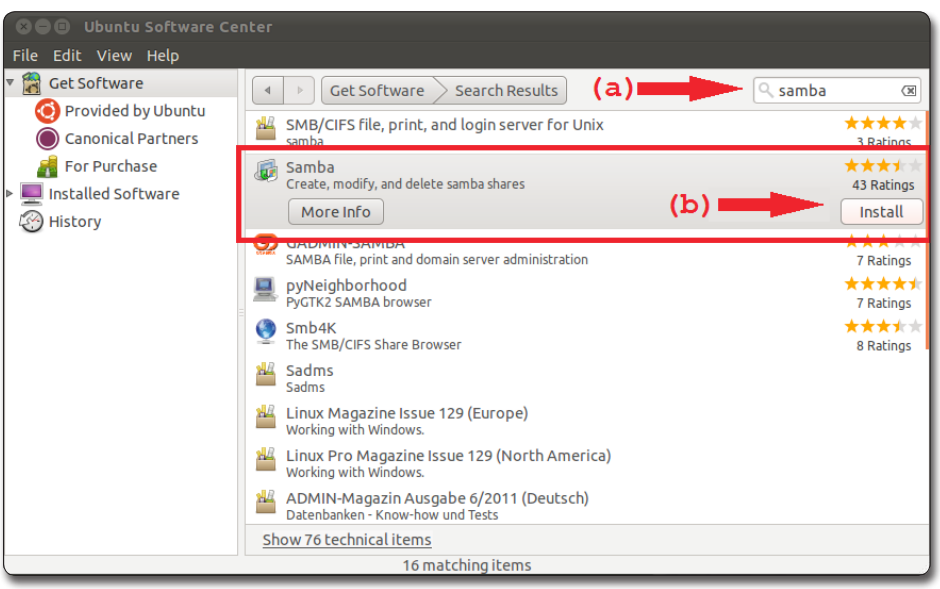


Figura 1. Janela do software Ubuntu Software Center: (a) campo de pesquisa e (b) botão para instalar

tas dentro de */tmp*. Essa sessão pode ser criada com qualquer nome, *Arquivos_do_Thiago*, *Material_Aulas*, no lugar do **temporario** utilizado no exemplo, porém lembrando-se de evitar espaços no nome.

O arquivo de configuração deverá ser editado em seu local específico, ou seja, o local onde a distribuição o instalou. Por padrão, nas distribuições abordadas neste artigo, o arquivo de configuração será colocado em */etc/samba*.

No arquivo *smb.conf*, o que estiver com **;** ou **#** é tido como comentário e a linha é desconsiderada pelo Samba.

Caso necessite testar a configuração das **Listagens 1** ou **2**, ainda é preciso realizar um outro passo no Debian: criar os usuários e senhas para acessar o compartilhamento.

A criação de usuários e senhas é realizada pelo comando **smbpasswd** e seu funcionamento é simples. Esse comando tem suas particularidades, pois é ele que adicionará os usuários ao Samba. As opções básicas do comando são apresentadas a seguir, porém existem 19 opções ao todo:

```
smbpasswd [-a] [-x] [-e] [-d] [usuario[%senha]]
```

No comando **smbpasswd**, as opções apresentadas são:

- **-a**: caso queira adicionar um usuário;
- **-x:** excluirá o usuário do Samba;
- **-d**: utilizada quando se tem um usuário ativo no Samba e o mesmo não deverá mais acessar os compartilhamentos do servidor.

Listagem 2. Arquivo de exemplo comentado do smb.conf.

```
[global]
# Os parâmetros passados para essa seção
# definem o comportamento do Samba

 workgroup = WORKGROUP
 # Nome do grupo de trabalho

 server string = %h server (Samba %v)
 # Fornece uma descrição do servidor Samba
 # que será visível a todas as máquinas Windows;

 log file = /var/log/samba/log.%m
 # Define a localização e nome do arquivo
 # de log a ser gerado

 max log size = 1000
 # Especifica o tamanho máximo em Kb
 # do arquivo de log a ser gerado

 syslog only = no
 # Os logs ficarão somente no syslog (yes)
 # ou também no log do samba (no);

 syslog = 0
 # As informações menos importantes serão
 # escritas no syslog, o restante vai para /var/log/samba/

 panic action = /usr/share/samba/panic-action %d
 # Caso o nmbd e o smbd travarem por
 # algum motivo, executa-se o comando do panic action

 ; security = user
 # Necessário para controle de acesso por domínio,
 # uma vez que é utilizado o controle de acesso
 # local usando usuários e grupos locais.

 encrypt passwords = yes
 # Senhas criptografadas. Utilizar p/ Windows
 # superiores ao Windows 95

 guest account = nobody
 # Conta que será utilizada para
 # usuários não autenticáveis.

 invalid users = root, admin
 # Usuários que não poderão utilizar o Samba.

 unix password sync = no
 # As senhas do Unix e do Samba
 # deverão estar sincronizadas.

 passwd program = /usr/bin/passwd %u
 # Programa que será utilizado para a mudança de senhas

[homes]
# São definidas as permissões padrão para os diretórios
# de usuários quando montados a partir de computadores
# em rede para usar os recursos de compartilhamento

 comment = Home Directories
 # Comentários sobre o compartilhamento.

 browseable = no
 # Apresenta o compartilhamento na lista
 # de compartilhamentos visíveis para o Windows

 writable = no
 # Permite escrita na pasta

 create mask = 0700
 # Especifica as permissões do que será criado
 # dentro da pasta compartilhada

 directory mask = 0700
 # Especifica as permissões da pasta compartilhada

 [printers]
 # Definições de permissão de acesso às
 # impressoras compartilhadas pelo servidor Samba

 comment = All Printers
 browseable = no
 writable = no

 path = /tmp
 # Diretório para impressão

 public = no
 # Necessidade de senha para acesso caso não seja público

 printable = yes
 # O cliente manda a impressão para o spool em um diretório


[publico]
# Compartilhamento criado como exemplo
 comment = Diretório Público
 path = /home/data
 public = yes
 writable = yes
 printable = no
```

Nesse caso, essa opção desativa o usuário, mas não apaga;

• **-e**: caso o usuário possa novamente acessar os compartilhamentos após ter sido desativado, essa opção ativa o usuário. Isso ajudará na administração do servidor, uma vez que não será necessário apagar o usuário e, posteriormente ter que cadastrá-lo novamente;

• **%senha**: insere a senha do usuário via comando. Porém, se não for informada a senha, o comando *smbpasswd* a solicitará na próxima linha.

Interfaces Gráficas

Inúmeros usuários ainda não têm muita familiaridade ou mesmo não estão habituados com linhas de comandos e preferem configurar os serviços de um modo visualmente mais fácil. Com isso utilizam-se de programas que, através de um navegador, exibem as configurações para serem selecionadas por botões e caixas de texto. No sítio do Samba [2] existe uma relação de diversas interfaces para auxiliá-los nas configurações, e dentre elas, foram selecionadas o Webmin e o SWAT por serem as mais utilizadas, porém nada impede que se teste as outras opções.

Webmin

O Webmin é uma interface, via navegador, que auxilia na configuração de praticamente todos os serviços do Linux, permitindo criar usuários, configurar o Samba, DNS, LDAP, dentre outros. Mesmo sendo útil para inúmeros usuários, foi retirado do repositório padrão do Debian e do Ubuntu, e com isso, para instalar o Webmin, este deverá ser baixado do sítio do Webmin [3]. No caso das distribuições utilizadas nesse artigo, o arquivo a ser baixado contendo a instalação do Webmin deverá ter a extensão *.deb*.

A instalação é um pouco diferente da instalação do Samba, pois o comando **apt** baixaria os pacotes e os instalaria, mas como o pacote *.deb* já contém o programa que será instalado. O comando **dpkg** (*debian package* – gerenciador de pacotes do Debian) auxiliará na instalação dos pacotes baixados manualmente.

Para instalar o Webmin, faça:

```
sudo dpkg -i webmin_1.580_all.deb
```

Ocorrerão alguns erros durante a execução do comando anterior, pois a instalação do Webmin depende de diversos outros serviços e pacotes que já deveriam estar instalados, como as bibliotecas *libnet-ssleay-perl* e *libio-pty-perl*. Felizmente não é preciso se preocupar com os pacotes e serviços faltantes, pois no Debian e no Ubuntu o comando **apt** resolve o problema de pacotes que estão faltando e instalações incompletas. Para que o Webmin termine de ser instalado, após o **dpkg**, execute o comando:

```
sudo apt-get -f install
```

O comando anterior pode ser utilizado para qualquer pacote *.deb* que tenha sido instalado através do **dpkg** e, como no caso do Webmin, não haviam todas as dependências previamente instaladas.

Executado os dois passos, o Webmin estará instalado e funcionando. Para acessá-lo da própria máquina onde foi instalado, abra o navegador e no endereço coloque:

```
https://127.0.0.1:10000
```

Muitas vezes, em servidores em produção, não é instalada a interface gráfica e com isso a utilização do Webmin deverá ser feita através de outro computador com qualquer sistema operacional que tenha um navegador e esteja conectado na mesma rede da máquina onde foram instalados o Webmin e o Samba. Nesse outro computador, deverá ser colocado na barra de endereços do navegador o endereço IP do servidor o qual se quer acessar. Nota-se que o acesso deverá ser feito através de *https* que utiliza o protocolo de segurança SSL, o mesmo utilizado para acessar o *Internet Banking*, na comunicação criptografada entre as máquinas.

A primeira tela que aparecerá é a de login, conforme a **Figura 2** ilustra. No caso da instalação ter sido feita no Debian, o usuário que deverá ser utilizado é o *root* e a senha é a mesma definida para acessar o Linux com este usuário. No caso do Ubuntu, utiliza-se o usuário criado na instalação do Ubuntu, pois não é permitido o acesso a comandos e serviços através do usuário *root*.

No caso da perda da senha de acesso do Webmin, esta poderá ser alterada executando-se o comando seguinte no terminal:

```
/usr/share/webmin/changepass.pl /etc/webmin usuário novasenha
```

O programa *changepass*, feito em Perl, faz parte do pacote do Webmin e auxiliará na alteração da senha perdida. Os parâmetros do comando a serem utilizados para essa alteração são:

• **/etc/webmin**: pasta onde estão os arquivos de configuração do Webmin;

• **usuário:** nome do usuário do Samba que se quer alterar a senha;

• **novasenha:** a nova senha para o usuário.

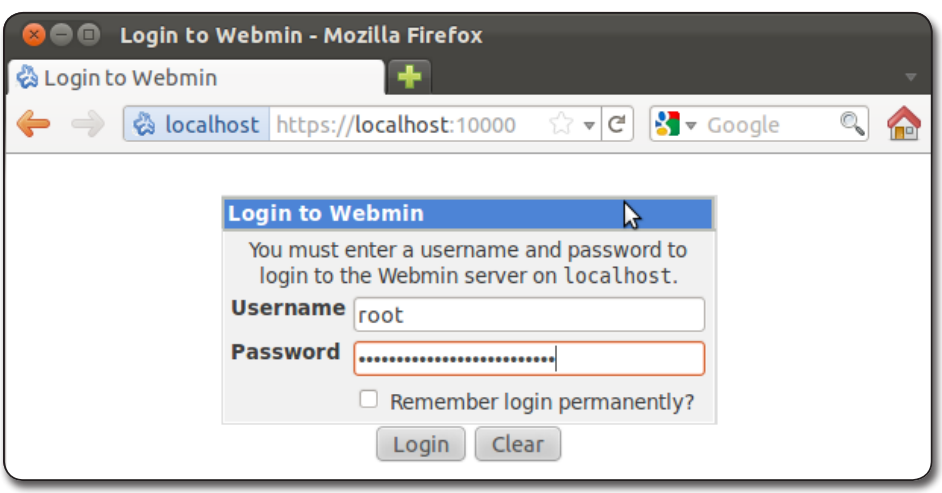


Figura 2. Tela de Login do Webmin

Feito o login, a tela inicial do Webmin apresentará as informações do sistema além de um menu lateral de opções, conforme ilustra a **Figura 3**.

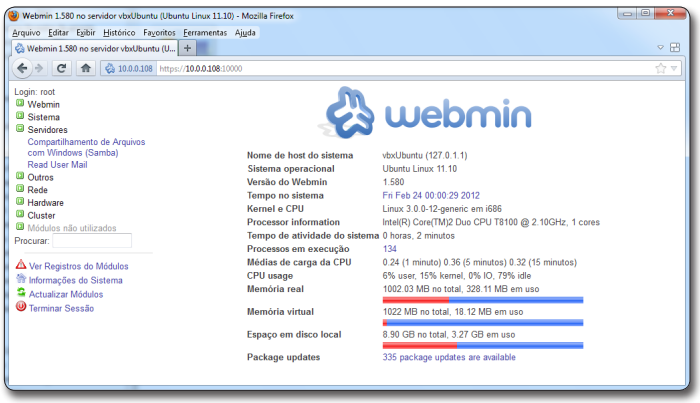


Figura 3. Tela inicial do Webmin

As configurações do servidor Samba estão no menu lateral esquerdo, acessando *Servidores > Compartilhamento de Arquivos com Windows (Samba)*. Ao ser selecionado esse item, aparecerão à direita as configurações do Samba, conforme a **Figura 4**.



Figura 4. Tela principal de configuração do Samba

A explicação da configuração completa do Samba através do Webmin resultaria em um novo artigo, pela quantidade de opções que se encontram para cada item apresentado no menu de configuração. Porém, aqui serão apresentados os principais itens que auxiliarão nas configurações básicas.

A **Figura 5** apresenta esses itens de configuração básicos. Um exemplo desses itens é o grupo de trabalho, que por padrão é Workgroup, porém caso seja necessário inserir o servidor Samba em um grupo de trabalho que não seja o padrão, insira o nome do grupo na caixa de texto. Ao término da configuração, é obrigatório selecionar o botão *Salvar* no final da tela, pois sem isso as configurações não serão adicionadas/alteradas do arquivo *smb.conf* atual.

Para compartilhar um arquivo através do Webmin é bem simples, pois como é ilustrado pela **Figura 6**, escolhe-se o nome do compartilhamento e o local a ser compartilhado. Caso não se saiba o caminho completo, o botão [...] ajudará com a lista de pastas e subpastas.

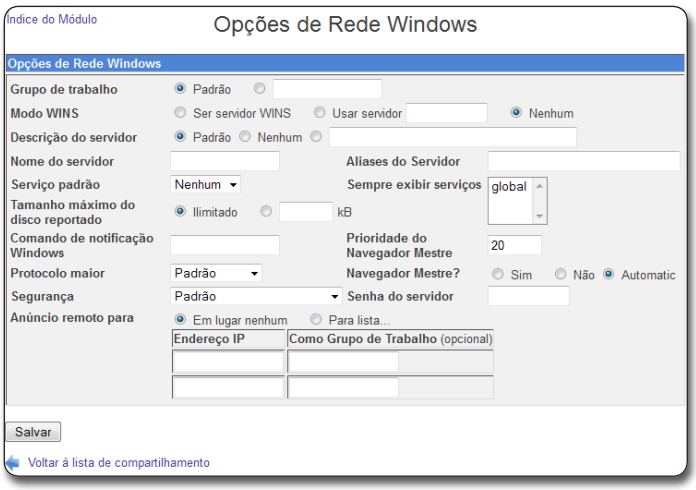


Figura 5. Tela com as configuração que o Samba apresentará à rede Windows



Figura 6. Configurando o compartilhamento de uma pasta

Impressoras também são simples de serem compartilhadas, uma vez que as mesmas já estejam corretamente instaladas no servidor onde o Samba está. A **Figura 7** ilustra a tela de configuração de compartilhamento de impressoras, sendo que no item *Impressora Unix* aparecerá a lista de impressoras instaladas no seu sistema.

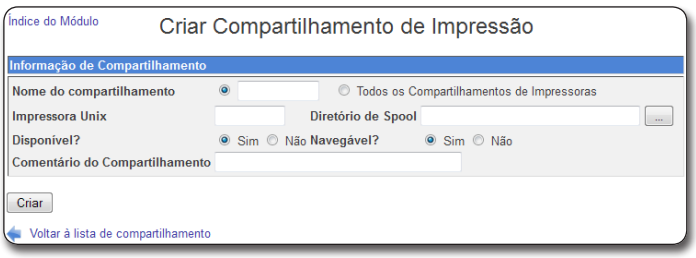


Figura 7. Configurando o compartilhamento de uma impressora

Após configurar alguns compartilhamentos, esses aparecerão na tela principal de configuração do Samba, conforme a **Figura 8**.

Ao selecionar um compartilhamento, este será aberto para edição, como ilustra a **Figura 9**. Na edição poderão ser especificados os usuários que terão acesso e o tipo de acesso e políticas de escrita/

leitura, além de poder visualizar as conexões ativas para esse compartilhamento.



Figura 8. Tela inicial com os novos compartilhamentos



Figura 9. Edição de compartilhamentos.

Uma parte não menos importante na configuração do serviço é a configuração dos usuários. Essa configuração poderá ser feita através dos ícones que aparecem no final da tela inicial. A **Figura 10** apresenta a parte inferior da tela inicial de configuração do Samba através do Webmin.

Seis itens de configuração de usuários são apresentados por esta figura. O item *Editar usuários e senhas do Samba* apresentará uma lista dos usuários já importados pelo Samba na instalação. Caso algum novo usuário tenha sido criado posteriormente à instalação do Samba, pode-se inserí-lo nesse item. No entanto, se forem diversos usuários, recomenda-se a utilização da opção *Converter usuários do Unix para usuários do Samba*. A opção *Configurar sincronização automática de usuários do Unix e Samba* também é apresentada, e com ela, cada usuário criado no Linux será automaticamente adicionado ao Samba. Muitos acharão uma ótima escolha, porém não se recomenda a utilização da mesma, pois se o servidor for invadido e criado um usuário de acesso livre, este também será adicionado ao Samba.

Na **Figura 10** também podem ser observados dois botões que permitem reiniciar ou parar o servidor Samba sem a necessidade de nenhum comando mais complexo através do terminal. Caso o servidor esteja parado, o botão de *Iniciar Servidores do Samba* aparecerá, e ao clicá-lo, os serviços necessários para o funcionamento do Samba serão iniciados.



Figura 10. Parte inferior da tela inicial mostrando as configurações de usuários e botões de acionamento dos servidores Samba

SWAT

O SWAT (*Samba Web Administration Tool* – Ferramenta de Administração do Samba via Web) é muito difundido entre os usuários, pois oferece uma interface simplificada e direta, porém os tópicos não são divididos em telas, e sim em uma longa lista em uma mesma tela.

Apesar da simplicidade, com essa ferramenta consegue-se configurar tranquilamente o Samba para quase todas as necessidades específicas de um ambiente.

A instalação do SWAT é simples, e quase todas as distribuições Linux têm o pacote de instalação em seus repositórios. No caso deste artigo, a instalação será feita através do comando no terminal:

```
sudo apt-get install swat
```

No caso do Ubuntu, ainda se tem a opção da instalação pelo *Ubuntu Software Center*. Assim, basta proceder a pesquisa por SWAT e clicar em *Install*, do mesmo modo como foi feito na instalação do Samba, **Figura 1**.

O acesso ao SWAT é feito através do navegador, do mesmo modo que o Webmin, porém em outra porta, podendo-se ter as duas ferramentas instaladas e rodando simultaneamente. Para acessar o SWAT, utilize o endereço:

```
http://127.0.0.1:901
```

Esse serviço de configuração utiliza a porta 901, sendo configurada no arquivo *inetd.conf* do sistema. O inetd é um *daemon* que verifica as portas de comunicação do Linux e, ao ser solicitado algo na porta 901, o SWAT será chamado para atender à solicitação.

A primeira tela será a janela de *login*, conforme a **Figura 11** apresenta. Novamente, caso esteja utilizando o Debian, o usuário a ser utilizado é o *root* e a senha é a mesma utilizada para acessar o Linux. No caso do Ubuntu, o usuário *root* é desabilitado por padrão, porém será necessário ativá-lo, pois qualquer outro usuário do Ubuntu que utilizar o SWAT não terá privilégios para configuração, apenas terá opções de listagens.

Para ativar o usuário *root* do Ubuntu, deve-se inserir uma senha para este usuário, e essa ação pode ser feita através do terminal com o comando:

```
sudo passwd root
```

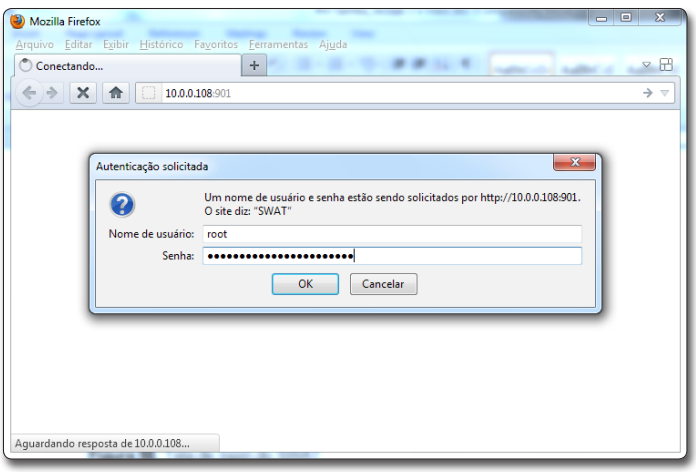


Figura 11. Tela de login do SWAT

Após o *login*, a tela inicial do SWAT é apresentada, conforme pode ser observado na **Figura 12**. Logo abaixo dos ícones, são apresentados *links* para um manual local do SWAT.

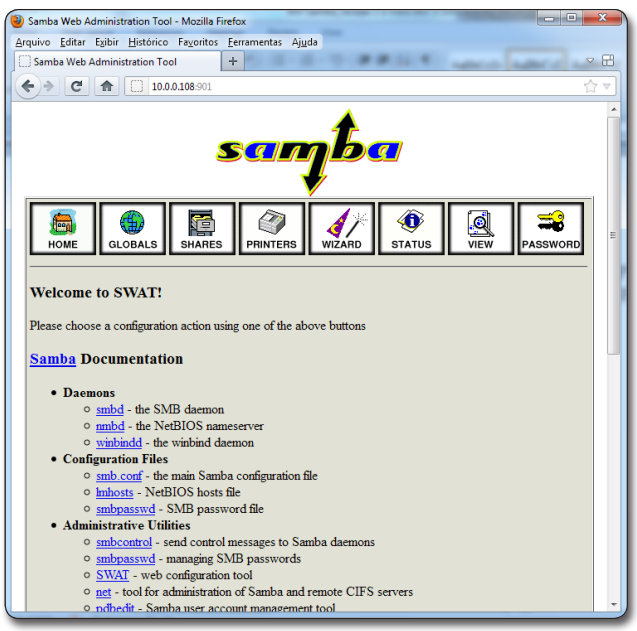


Figura 12. Tela inicial do SWAT

No item **Globals** são apresentados os itens de configuração global do servidor Samba (observe a **Figura 13**), como o **workgroup**, **netbios name**, dentre outros.

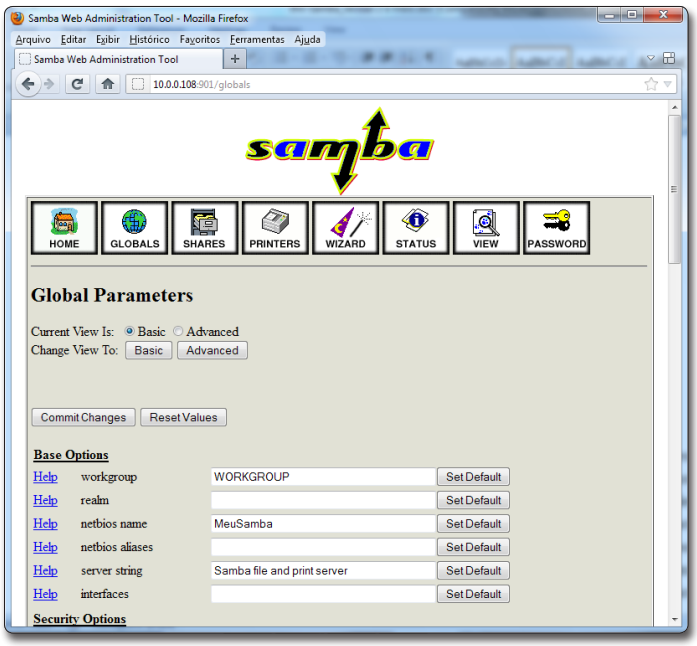


Figura 13. Tela de configurações dos parâmetros globais básicos do Samba

Em todas as telas de configuração do SWAT serão apresentados os botões *Basic* e *Advanced*, sendo normalmente selecionado o *Basic*. Nesse caso os itens básicos de configuração são apresentados, porém, caso a necessidade de configuração para um determinado local não seja contemplada nesse item, ao selecionar *Advanced*, serão exibidos todos os itens de configuração permitidos para o momento (veja a **Figura 14**). Note a diferença visual na barra de rolagem entre as **Figura 13** e **14**. Isso acontece pela quantidade de itens de configuração que são disponibilizados no modo avançado.

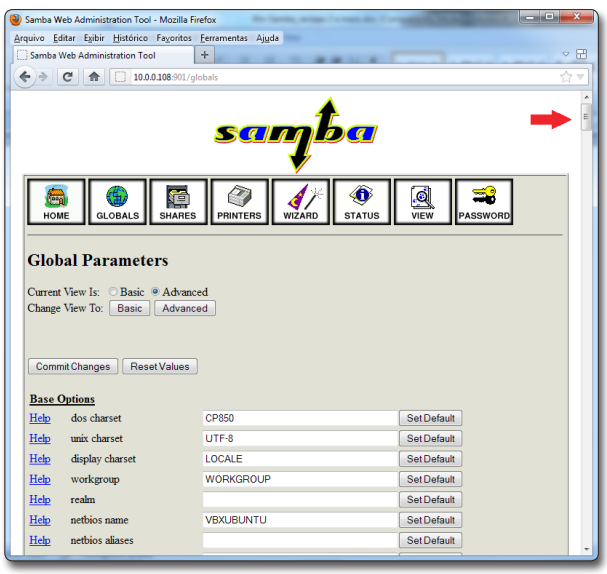


Figura 14. Tela de configurações dos parâmetros globais avançados do Samba

A configuração de compartilhamento, ilustrada pela **Figura 15**, apresenta os itens que podem ser editados ou mesmo criados e suas opções de configuração. Para se criar um compartilhamento, é necessário inserir o nome do compartilhamento no campo de texto à frente do botão *Create Share*. E logo em seguida, clicar no próprio botão. Serão abertos diversos campos de configuração logo abaixo, conforme mostra a **Figura 15**, e, no mínimo, o *path* deverá ser preenchido com o caminho da pasta que será compartilhada.

Para salvar as alterações que foram feitas, clica-se no botão de *Commit Changes*.

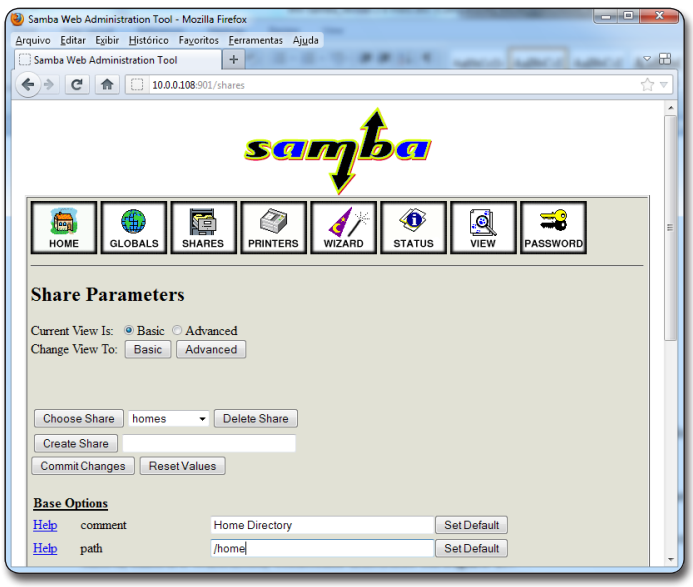


Figura 15. Tela de configurações dos parâmetros de compartilhamento básico do Samba

Caso seja necessário parar ou iniciar o servidor Samba, através do ícone (*Status*) do menu superior do SWAT, serão apresentados botões para gerenciar o **smbd**, **nmbd** e **winbindd**, conforme ilustrado na **Figura 16**.

Além dos botões de gerenciamento, nessa mesma tela são apresentadas as conexões ativas no servidor, os compartilhamentos ativos e até mesmo os arquivos que estão sendo utilizados.

A parte de usuários e senhas, apresentada na **Figura 17**, é mais simples que a do Webmin, porém cumpre o que promete: inserir e modificar usuários, ativando-os e desativando-os.

A parte superior é destinada ao gerenciamento de usuários locais do Samba, e na parte inferior é feito o gerenciamento dos usuários do Samba em sistemas remotos, tendo que explicitar a máquina remota em que será alterada a senha do usuário.

Conclusão

O servidor Samba é amplamente utilizado em diversos ambientes de redes que necessitem compartilhar arquivos e impressoras de um sistema Linux com máquinas Windows e, de certo modo, é de simples configuração.

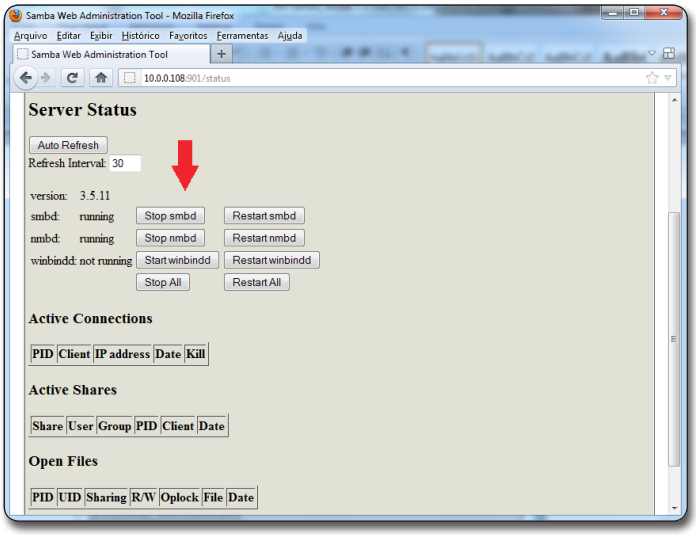


Figura 16. Tela de status do servidor Samba, com destaque para os botões de controle

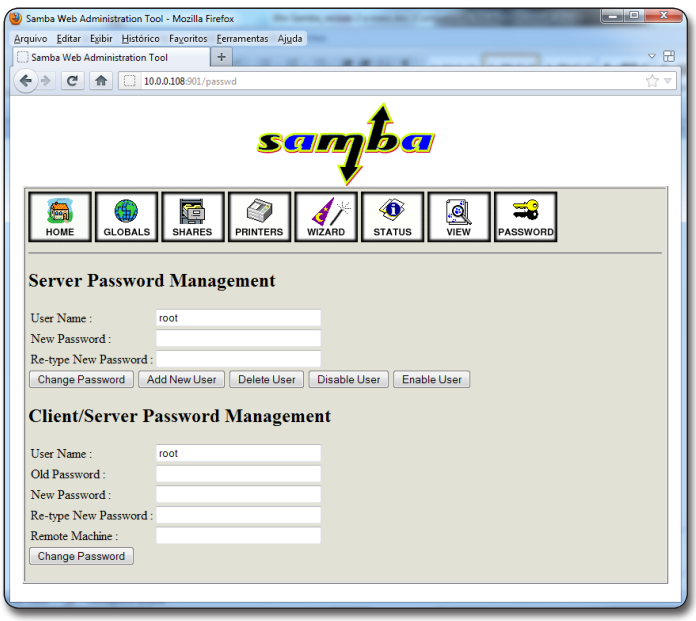


Figura 17. Tela de configuração de usuários e senhas

As ferramentas gráficas para configuração do Samba auxiliam a usuários sem muita afinidade com o mundo Unix, como também àqueles que já têm certa experiência, abrindo um leque de opções de configurações avançadas.

Por sua vez, diversas melhorias e implementações de novas funcionalidades são prometidas para a versão 4 do Samba, dentre elas: servidor LDAP interno com a semântica de Active Directory, Suporte ao Active Directory na parte de logon e administração, melhoria na escalabilidade de pequenas e grandes instalações, arquitetura de banco de dados flexível (LDB – *LDAP-like embedded database* – banco de dados embarcado do tipo LDAP)[8], entre outras. Mesmo com todas essas novidades sendo implementadas desde 2005, até o momento a versão 4 não se tornou oficial. Mesmo assim, vale a espera.



Thiago Pirola Ribeiro
thiagopirola@gmail.com
Atua como pesquisador e professor da Universidade Federal de Viçosa -UFV- na área de Computação. É bacharel em Análise de Sistemas e mestre em Ciência da Computação. Tem experiência na área de Computação, com ênfase em Processamento de Imagens, Linguagens de Programação, Software Livre, Redes de Computadores, Sistemas Operacionais e Servidores.

[1] Sítio Oficial do Samba
http://www.samba.org

[2] Interfaces Gráficas de Configuração
http://www.samba.org/samba/GUI/

[3] Webmin
http://prdownloads.sourceforge.net/webadmin/webmin_1.580_all.deb

[4] Samba-3 by Example
http://www.samba.org/samba/docs/Samba3-ByExample.pdf

[5] The Official Samba-3 HOWTO and Reference Guide
http://www.samba.org/samba/docs/Samba3-HOWTO.pdf

[6] Página de Manuais do Samba
http://www.samba.org/samba/docs/man/manpages-3/

[7] Capítulo sobre Swat do Livro - Learning Debian GNU/Linux
http://oreilly.com/openbook/debian/book/ch10_03.html

[8] LDB
http://ldb.samba.org/

FÓRUM
DEVMEDIA
O lugar perfeito para você ficar por dentro de tudo o que acontece nas tecnologias do mercado atual



No novo Fórum da DevMedia você vai encontrar canais específicos de Delphi, ASP.NET, Java, Banco de Dados e Engenharia de Software; além de ter contato com profissionais qualificados da área para troca de informações, sugestões e muito mais.

ACESSE AGORA
www.devmedia.com.br/forum

DevMedia

Salve seus dados com Bacula

Backup centralizado utilizando uma ferramenta open source – Parte 1

Flávio Alexandre dos Reis e Eduardo Pagani Julio

Em Tecnologia de Informação (TI), cópia de segurança (*backup*) é uma cópia de dados de um dispositivo de armazenamento para outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Alguns meios difundidos de backup incluem CD-ROM, DVD, disco rígido, disco rígido externo (compatíveis com USB), fitas magnéticas (LTO) e também uma cópia de segurança externa (*online*). Esta última pressupõe o transporte dos dados por uma rede, como a *Internet*, para outro ambiente, geralmente para equipamentos mais sofisticados, de grande porte e alta segurança fornecidos por empresas especializadas.

Outra forma de cópia de segurança pouco difundida é feita via rede, que é o tema abordado neste artigo. Na própria rede local de computadores, o administrador ou o responsável pela cópia de segurança grava os dados, processa e distribui as partes constituintes da cópia nos computadores da rede. Isto tudo de forma segura, incluindo dados criptografados (para não haver extração ou acesso aos dados na forma original por pessoas não autorizadas) e o procedimento ser oculto.

Neste contexto, este artigo tem como objetivo demonstrar a importância do uso de ferramentas de backup para qualquer administrador que zele pela segurança de seus dados. Conheceremos alguns conceitos básicos, mitos, tipos e métodos utilizados para cópia de dados. Além disso, será demonstrado como elaborar uma rotina de backup adotando várias tecnologias de armazenamento. Começaremos por alguns conceitos básicos.

O *backup* consiste na cópia de dados específicos (redundância) para serem restaurados no caso da perda dos originais. A cópia pode ser realizada para o mesmo computador, para um dispositivo de armazenamento ou, ainda, em outro prédio ou localidade. Neste último caso, temos a vantagem de também proteger os dados contra acidentes que possam acometer fisicamente a estrutura.

Independente de como os dados possam ser perdidos (apagamentos acidentais, corrupção dos dados, etc.), um *backup* eficiente consiste naquela política em que se minimizam os impactos desta perda possibilitando a restauração do arquivo ou serviço no menor tempo possível e com o mínimo de defasagem em termos de alteração das informações.

O *backup* pode variar de acordo com a natureza dos arquivos, com as necessidades empresariais e com a infraestrutura disponível. Além disso, existem algumas métricas que devem ser observadas: tempo de execução das cópias (conhecido como janela de *backup*), a periodicidade, a quantidade de exemplares das cópias armazenadas, o tempo que as cópias devem ser mantidas, a capacidade de armazenamento, o método de rotatividade entre os dispositivos, a compressão e encriptação dos dados. Todos esses fatores devem ser avaliados pela equipe responsável pela execução do processo de cópia.

Quanto à topologia, os *backups* podem ser classificados como centralizados ou descentralizados. No primeiro caso, geralmente há um servidor que comanda a realização de cópias de segurança conferindo uma maior praticidade na administração e economia pelo armazenamento dos dados em poucos dispositivos, ocorrendo aí um ganho pela escalabilidade. Geralmente é realizado pela noite para que haja mínima possibilidade de impacto aos serviços utilizados em horário administrativo. No segundo caso, cada setor fica responsável pela cópia de segurança, mantendo a mesma em sua posse (caso não aconselhável).

Resumo DevMan

De que se trata o artigo:

Este artigo tem como objetivo demonstrar a importância do uso de ferramentas de backup para qualquer administrador que zele pela segurança de seus dados. Nessa primeira parte do artigo serão abordados conceitos básicos, mitos, tipos e métodos utilizados para cópia de dados. Será demonstrado como elaborar uma rotina de backup adotando várias tecnologias de armazenamento.

Em que situação o tema é útil:

Este serviço é usado quando o administrador precisa manter uma cópia de arquivos de banco de dados, arquivos de configuração, diretórios compartilhados, diretórios de e-mails, máquinas virtuais e demais serviços utilizados pela organização. A centralização de backup com o Bacula visa facilitar a administração e identificação de falhas no processo de cópia.

Salve seus dados com Bacula:

O Bacula é uma solução de backup multiplataforma desenvolvida sob a licença GPL. É robusta, cheia de recursos e modular, se adapta a redes de qualquer tamanho e em qualquer topologia. Com essa solução não há mais a necessidade de altos investimentos em licenças de software para backup.

Tipos de Backup

A seguir serão apresentados os tipos de backup que normalmente são encontrados no dia a dia das organizações. Ao final da lista, é apresentada uma tabela com exemplo de implementação de backup *full* e diferencial.

• **Completo (*Full*)** – este tipo de backup faz cópia de todos os arquivos definidos na configuração da ferramenta, independente dos arquivos terem sido alterados ou não. Geralmente é realizado quando o servidor passa por backup pela primeira vez, ou no início de cada ciclo de *backups* (ex.: uma vez por semana). Como é um backup mais longo, geralmente é iniciado na sexta-feira ou sábado para que tenha a janela do final de semana para ser realizado. Este tipo de *backup* se mostra extremamente caro para ser realizado diariamente, principalmente pela excessiva quantidade de espaço em disco que será utilizada levando em consideração o tamanho do diretório ou arquivo a ser armazenado;
• **Diferencial** – este tipo de backup faz a cópia apenas dos arquivos modificados a partir do último *backup Full*. Por exemplo: um *backup Full* ocorreu no sábado; um *backup* diferencial realizado na segunda só conterá os dados alterados ou criados na segunda; se na terça-feira for gravado outro *backup* diferencial, ele novamente vai gravar os arquivos alterados ou criados desde que se gravou o *backup Full*, isto é, os arquivos de segunda e terça. Assim, este tipo requer menos capacidade de armazenamento e resulta em *backups* mais rápidos. Em contrapartida, a restauração fica mais complexa, pois necessita sempre de pelo menos dois volumes de backup (um *full* e possivelmente o último diferencial). Observe na **Tabela 1** um cronograma de *backup* utilizando a cópia completa e diferencial;
• **Incremental** – este tipo de backup faz a cópia apenas dos arquivos modificados a partir do último *backup* diferencial. Ao contrário do diferencial, se for feito um *backup* Incremental após outro Incremental, o segundo *backup* não irá conter os dados do primeiro. Apesar de ser o tipo mais rápido de *backup*, tende a deixar a restauração demasiadamente complexa uma vez que pode exigir vários volumes (o *full* e todos os demais incrementais);
• **Cópia** – cópia secundária ou complementar de determinado volume de *backup* (redundância). Muito utilizada para *backup off-site*. O volume copiado é mantido intacto. Pode ser feito via *RAID* (veja a **Nota DevMan 1**);
• **Migração** – os dados de determinado volume são migrados para outro, sendo que o primeiro deixa de existir. Pode ser útil quando há suspeitas de erros de leitura e/ou gravação em determinada mídia de armazenamento (ex.: fita, HD, etc.) e, dessa forma, os dados precisam ser movidos para um meio "saudável" antes que a mídia pare de funcionar.

Mitos sobre cópias de segurança

A partir de agora conheceremos três mitos associados à execução de backups bastante difundidos na comunidade de TI.



Nota do DevMan 1

RAID: Redundant Array of Independent Drives (Conjunto Redundante de Discos Independentes) é um meio de se criar um subsistema de armazenamento composto por vários discos individuais com a finalidade de ganhar segurança e desempenho.

Mito 1 – Gerenciamento do Ciclo de Vida da Informação

Backup não pode ser confundido com o Gerenciamento do ciclo de vida da Informação (ILM – *Information Lifecycle Management*). Alguns desenvolvedores de ferramentas para *backup* têm advogado no sentido de que este seria um dos papéis deste tipo de ferramenta. Ocorre que o ILM consiste em um processo que abrange muito mais elementos, como: auditoria, indexação, criação, atualização, deleção, aspectos de armazenamento e de acesso.

Ao invés disso, na verdade o backup estaria dentro de uma subdisciplina do ILM, que seria o ILP (*Information Lifecycle Protection* – ou Proteção do Ciclo de vida da Informação), que também conteria uma série de outros fatores:
• Proteção proativa contra a perda de dados – que pode constituir em antivírus ou outros aspectos em nível de aplicação, por exemplo;
• Alta disponibilidade;
• Redundância de sistemas;
• E se mesmo assim houver perda na informação, a restauração dos dados previamente armazenados pelo serviço de *backup* seria executada.

Mito 2 – Ferramentas de *backup* nativas

O segundo mito nos diz que as ferramentas de *backup* nativas dos sistemas operacionais seriam suficientes e/ou mais confiáveis que as ferramentas específicas para este serviço. Os *softwares* nativos dos sistemas operacionais carecem de uma qualidade essencial quando o assunto é *backup*: interoperabilidade. Dessa maneira, seria impossível ou excessivamente difícil realizar cópias de segurança de vários servidores em apenas um *storage*, o que representa uma enorme economia com recursos de armazenamento. Além disso, haveria um maior custo pela manutenção e administração descentralizada de aplicações heterogêneas de *backup*.

Mesmo as ferramentas proprietárias de cópias de segurança são consideradas mais eficientes quando comparadas com as nativas, e em relação à confiabilidade, não estariam a anos no mercado se não tivessem esta qualidade. O mesmo, analogamente, vale para

Dia	Segunda	Terça	Quarta	Quinta	Sexta	Sábado	Domingo
Tipo	Diferencial	Diferencial	Diferencial	Diferencial	Diferencial	Diferencial	FULL
Comentário	Contém os dados modificados a partir do backup full no domingo	Contém os dados modificados a partir do backup full no domingo	Contém os dados modificados a partir do backup full no domingo	Contém os dados modificados a partir do backup full no domingo	Contém os dados modificados a partir do backup full no domingo	Contém os dados modificados a partir do backup full no domingo	Backup Completo

Tabela 1. Agendamento de backup FULL e Diferencial

as soluções livres. Além disso, existem outras funcionalidades importantes que dificilmente são encontradas em ferramentas nativas, a saber:

• Possibilidade de cópias e restaurações cruzadas (ou seja, através da rede – de uma estação para outra diversa);
• Restaurações rápidas utilizando apenas as mídias necessárias para o trabalho;
• Catálogo para indexar os arquivos gravados, facilitando a busca pelos arquivos gravados;
• Manipulação de robôs-de-fitas;
• Ferramentas de recuperação de desastres (*disaster recovery*).

Mito 3 – *Scripts* substituindo ferramentas

O terceiro mito nos diz que *scripts* bem elaborados para backup podem suprir a necessidade de uma ferramenta específica (exemplo de *shell script* e *rsync*). A elaboração desses códigos para *backup* consiste em um retrabalho, visto que já existem aplicações bastante maduras desenvolvidas sob licenças livres. Além disso, o uso de scripts trata-se de uma solução única, utilizada apenas no ambiente no qual se encontra em produção. Isto dificulta bastante a possibilidade de termos suporte externo ou compartilhamento de experiências em outros cenários. A continuidade da solução também estaria prejudicada se não houvesse uma detalhada documentação interna, bem como os custos para o aprendizado seriam mais elevados do que com uma ferramenta comum.

Mídias de Backup

Há no mercado uma vasta quantidade de mídias de armazenamento que podem ser utilizadas para fins de *backup*. A seguir serão descritas algumas delas, tanto quanto algumas de suas especificações. É importante destacar aqui que o Bacula possui suporte a todos os tipos citados abaixo.

Fita magnética

Fitas magnéticas geralmente trazem a capacidade no seguinte formato: não-compactado/compactado (por exemplo: 20/40 Gb). Esta é uma compactação via *hardware* realizada pelo próprio *drive*, e deve ser privilegiada em relação à compressão via software.

A quantidade de dados compactados gravados varia de acordo com a natureza original das informações (ex.: arquivos já compactados como .mp3, .jpg, .zip, etc.).

A título de exemplo, abaixo temos alguns modelos de fita:

• *Digital Data Storage* (DDS) – as capacidades mais recentes são DDS-4 (20/40GB e 3.2 MB/s de gravação/leitura), DDS 72 (36/72GB, com mesma taxa de transmissão) e DDS 160 (capacidade: 80/160GB e "throughput" de 6.9MB/s);
• *Digital Linear Tape* (DLT) – capacidades: 40, 300 e 800 GB, com taxas de 6, 36 e 60 MB/s respectivamente;
• *Linear Tape-open* (LTO) – capacidades recentes: 200/400GB (LTO-2), 400/800GB (LTO-3) e 800/1.6TB (LTO-4), com taxas de transmissão de 40, 80 e 120 MB/s.

Mídia óptica

São todas as mídias que armazenam os dados por reflexão ou marcação. Entram nessa categoria as fitas perfuradas, que usam leitura óptica como mídia de marcação e os DVDs e CDs, como mídias de reflexão.

As mídias que usam reflexão (CD-R, CD-RW e DVD-R), são classificadas em duas categorias diferentes: regraváveis e de gravação única.

As principais vantagens da mídia óptica são: durabilidade e imunidade a campos magnéticos. A desvantagem está no pouco espaço de armazenagem (os gravadores de hoje ainda não gravam mais de uma camada do DVD, o que o limita a cerca de 8.7 GB).

Convém ressaltar ainda que, atualmente, não são usadas mídias de marcação para procedimentos de backup. A falta de uma capacidade, durabilidade e confiabilidade ampliadas, fizeram com que esse tipo de mídia não fosse tão utilizada para fins de *backup*.

Disco rígido

O fato dos discos rígidos estarem sempre acessíveis para o sistema operacional, aliado a diminuição no custo por gigabyte e aumento de confiabilidade, fizeram com que aumentasse a aplicabilidade dos HDs para o armazenamento dos backups. Atualmente, eles se mostram uma boa opção para pequenas e médias empresas, já que o investimento inicial é baixo (ao contrário dos robôs de fita).

Além disso, o uso de discos rígidos é escalável na medida em que basta a aquisição de mais discos para que seja ampliada a capacidade de armazenamento. A facilidade de operação também é um dos pontos fortes. Enquanto com robôs-de-fita só é possível ler ou escrever em uma fita por *drive* de cada vez, em um disco rígido é possível fazer a leitura e gravação simultânea de todos os seus volumes (ex.: *backup* e *restore* simultâneo).

No caso dos discos, é recomendável a criação de vários volumes dentro de um mesmo disco (no mínimo 04) para otimizar seu uso (evitar a perda de espaço ocioso). Outra boa prática é alternar o *schedule* de maneira a utilizar os diferentes discos (no mínimo 02) de maneira alternada para que a perda de um dos discos não represente a perda de todas as informações de *backup* já gravadas.

Classificação quanto ao local de armazenamento

Também podemos classificar os backups quanto ao seu local de armazenamento. Esta classificação pode ser feita da seguinte forma:

• **Backup on-site:** Neste caso, os dados ficam armazenados no mesmo prédio de origem (servidor). Assim, a ocorrência de catástrofes físicas (ex.: incêndio) poderia afetar não apenas o dado original, mas também a cópia de segurança. O *backup on-site* é aceitável quando há uma existência de cofres antichamas para armazenamento das mídias;
• **Backup off-site:** Oposto do *backup on-site*, os dados ficam armazenados em localidade diferente dos dados originais. É uma das características do *backup em nuvem* (ler **Nota DevMan 2**).



Nota do DevMan 2

Backup em Nuvem: Um servidor de backup em nuvem fornece ao usuário a possibilidade e flexibilidade de acessar seus dados de qualquer lugar que tenha acesso a Internet. Um exemplo desse serviço é o Dropbox, fundado em 2007 por Drew Houston e Ferdowsi Arash. O Dropbox fornece aos usuários 2 GB de espaço gratuitamente e oferece planos para quem necessita de mais armazenamento.

Projetando um sistema de backup

Utilizando alguns fundamentos da Gerência de Projetos, pode-se planejar (e executar) a instalação de um sistema de *backup*. Neste contexto, a elaboração de uma política de *backup* trata-se de um documento normativo que trará as diretrizes para os sistemas de *backup* da empresa. A seguir serão apresentados itens de suma importância para que um projeto de backup possa ser elaborado.

O que será protegido

Nessa atividade será necessário equilibrar a padronização (de agendamentos, níveis, retenções, etc.) em relação às diferentes necessidades da organização. Um ambiente muito complexo pode trazer dificuldades na administração dos *backups*. É importante também verificar seu SLA (*service level agreements* / acordo de níveis de serviço) para saber a periodicidade adequada dos *backups*, além do prazo pactuado para restauração de arquivos. Além disso, é fundamental verificar se existem rotinas especiais que precisam ser seguidas para a realização de um *backup* confiável (exemplo: dump de um banco de dados que não suporta *backup on-line*). A maioria das aplicações traz em sua documentação quais arquivos ou como deve se proceder para efetuar cópias de segurança.

Sistemas operacionais envolvidos

Infelizmente, nem todas as soluções de *backups* são como o Bacula, cuja gratuidade de licença e compatibilidade entre módulos para diferentes sistemas operacionais dispensa uma maior precisão nesta etapa da migração.

No caso das ferramentas proprietárias, a compra de uma licença para *backup* de máquina GNU/Linux, por exemplo, não serve para *backup* de uma estação *Windows* (e vice versa). Isso faz com que seja necessário um planejamento muito mais preciso para adquirir licenças de um serviço tão dinâmico quanto cópias de segurança. Os módulos podem não ser compatíveis entre si, impossibilitando *backup* cruzado, ou modelo centralizado.

O cerne da questão aqui consiste em saber se a solução de *software* a ser adquirida suporta todos os sistemas operacionais de sua empresa (ou ao menos a maioria), de preferência com módulos compatíveis. Além disso, é fundamental verificar se a ferramenta faz *backup* de arquivos abertos (nas soluções proprietárias, geralmente é cobrado um alto valor por esta funcionalidade adicional).

Gerência de Capacidade

As necessidades de *backup* crescem em média, segundo estudos, entre 20 e 25% ao ano. Entretanto, um bom planejamento se mostra importante para que não seja adquirida uma solução de software que fique rapidamente obsoleta. Além disso, é importante também estarmos atentos para não desperdiçarmos recursos na compra de um *storage* superdimensionado às necessidades reais de armazenamento.

Nesse ponto entra o Gerenciamento de Capacidade, conceito trazido pelo ITIL (ler **Nota DevMan 3**). O gerenciamento de capacidade trata de assegurar que a capacidade da infraestrutura de TI está adequada às demandas do negócio conforme a necessidade e o tempo. Boas alternativas são soluções baseadas em disco rígido, e que podem ser modularizadas. Um exemplo está no uso de *disk-arrays* serial-ata e *hot-swap*, que permitem inclusive configuração de RAID – caso não considere o uso de LVM (*Logical Volume Manager*) ou BOF (*bunch of disks*) suficientemente segura.



Nota do DevMan 3

ITIL: Information Technology Infrastructure Library foi criada em 1989 pelo CCTA, hoje incorporado pelo Office of Government Commerce, um órgão independente do governo britânico. Constitui-se de uma descrição coerente e integrada de práticas de gerenciamento de serviços de TI. Estas práticas ajudam a implantar e manter um gerenciamento de serviços de TI focando em pessoas, processos, tecnologia e parceiros que são usados na entrega de serviços que atendam às necessidades dos clientes. A versão atual, a ITIL V3, foi lançada em junho de 2007. Junto com o lançamento da ITIL V3, também foi lançado um novo esquema de qualificação profissional.

Se o administrador optar por drives de fita singulares (ou seja – sem alimentação automática), tenha certeza que seu *backup* dificilmente irá requerer multivolume (mais de uma fita para o *backup full*). Caso contrário, será trabalhosa a atividade de troca das fitas.

No caso de robôs de fita, a grande preocupação reside no *throughput* de seus drives, na medida em que a quantidade de fitas por *backup* não é tão importante, pois não requer intervenção manual. A quantidade de fitas de seu esquema pode aumentar muito caso necessário, mas sua janela de *backup* não.

Alguns robôs suportam a instalação posterior de *drives* adicionais. Além disso, para *backups* centralizados ou cruzados (ou seja, que importem em tráfego de rede), verificar a capacidade de transferência de dados bem como estações críticas nas quais o *download* dos dados possa causar impacto ao usuário é um fator importante. Neste caso, uma alternativa seria a instalação de uma placa de rede adicional.

Realocação de equipamentos

Algumas vezes, encontramos tesouros perdidos no parque computacional de TI: um drive DDS, com sorte um DLT. Somados, ou seja, como se fossem um conjunto de *storage*, podem fornecer uma boa capacidade de armazenamento e gravação para seus *backups*. O mesmo ocorre com os HDs. Vale salientar que, no caso de mídias antigas, é importante verificar o MTBF (ou validade) das mesmas. Também tenha certeza do conteúdo das mesmas antes de reciclá-las.

Escolha do software

Além dos aspectos já mencionados, o suporte ao hardware de armazenamento é fundamental não só pela ferramenta a ser adquirida, mas também pelo sistema operacional hospedeiro. As distribuições GNU/Linux costumam prover uma farta e estável compatibilidade com sistemas de fita, disco rígido, aliada à flexibilidade do *shell script*, configurando-se como ótima escolha para hospedar um servidor de *backups*.

É necessário um cuidado com a operação de *autochangers* (robôs de fitas) no que se refere aos tempos entre os comandos de operações (carga, descarga de fitas). Se este tempo (utilizado pela solução de *backup*) for menor do que o necessário, podem ocorrer desagradáveis travamentos. E se a ferramenta não permitir a modificação destes parâmetros, tudo indica que a integração entre as soluções será inviável.

Não se pode esquecer também que notificações por *e-mail* facilitarão, e muito, a vida do administrador e operadores de *backups*. Além disso, a opção por uma ferramenta proprietária pode ocasionar um aprisionamento tecnológico, não podendo mudar de solução posteriormente sem ter de renovar as licenças para poder restaurar o legado.

Hardwares de armazenamento e servidor de backup

Este ponto é um dos últimos passos em um planejamento de *backup*. É interessante observar que para realizar esta atividade, a maioria das informações que subsidiarão esta escolha já foram identificadas. O administrador deverá ter em mente que a solução adquirida deverá permanecer por, no mínimo, 5 ou 7 anos (quando então já estará obsoleta, com dificuldade para adquirir suprimentos ou peças de reposição).

Soluções definitivas nunca serão uma opção. As opções mais usuais são o *drive* de fita manual (para soluções de até 1.2 Terabytes – LTO4), o robô de fitas (mais caros e, portanto, para capacidades superiores) e sistemas baseados em discos rígidos (que atendem a todas as necessidades de armazenamento, independente do tamanho). Os dispositivos ópticos, apesar de muito promissores, ainda se mostram muito limitados em termos de capacidade, podendo ser utilizados apenas para pequenos projetos.

Preservação do legado de backup

A maneira mais usual para se preservar determinado legado de *backup* (ou seja, *backup* realizado por solução que não está mais em produção na empresa) consiste em manter um conjunto alternativo (*software* e *hardware*) para restauração de arquivos antigos.

Entretanto, podem ser utilizados outros métodos: coexistência de soluções em uma mesma estação (compartilhando o *hardware* de *backup*, de maneira sempre alternada), ou ainda, a transferência de dados da solução antiga para a atual através de *restores* e novos *backups*. Esta última, apesar de econômica em termos de ocupação de *hardware*, pode gerar um grande trabalho manual e comprometer a integridade dos dados. Por ser tão problemática, a migração de sistemas de *backup* deve sempre ser planejada com cautela, inclusive evitando as diversas limitações impostas pelas licenças de *software* proprietário.

Políticas e boas praticas de backup

A existência de uma política de *backup* em uma organização é essencial e está dentro do considerado como melhores práticas. Ela consiste em um documento que deverá conter os princípios de como ocorrerão os *backups* e *restores*, bem como o papel das partes interessadas, o tempo máximo para a resolução das ocorrências e a estratégia. Entretanto, o documento deve ser genérico o suficiente para permitir liberdade de escolha das ferramentas utilizadas, bem como as soluções de hardware utilizadas. Pode-se especificar que o *backup* será feito, preferencialmente, em mídia magnética e de maneira automatizada, mas nunca especificar fabricantes, modelos, referências. Vale salientar que é importante estar de acordo com os SLA ou OLA existentes para não gerar divergência entre a política e os contratos.

A seguir são apresentadas algumas boas práticas para políticas de *backup*:

- Ter estratégia condizente com a natureza dos dados armazenados;
- Efetuar testes de *restore* com periodicidade;
- Efetuar auditorias periódicas, inclusive com gerência de capacidade do sistema;
- Operador de fitas, administrador de backup e administrador de *restore* devem ser sempre pessoas diferentes;
- Constante documentação (inclusive banco de soluções);
- Alta disponibilidade;
- Efetuar planejamento e simulações de *disaster recovery*;
- Exigir *ticket* para *restore*;
- Desejável *ticket* para cada dia de realização dos *backups* para que seja informado se foram concluídos corretamente;
- Deve haver um procedimento formal de descarte das mídias não mais necessárias (ex.: trituração, incineração, etc.);
- Adequação à norma ISO 27002.

Sistema centralizado de backup

Nessa seção são apresentadas características de um sistema de *backup* de forma centralizada. Com esse procedimento há uma economia de fitas na medida em que é minimizada a quantidade de espaço subutilizado. Seguem alguns pontos que caracterizam sua valorização:

- Facilidade na administração, correção de erros, troca e controle de fitas;
- Economia de hardware (*storages*);
- Maior agilidade (*time sharing*);
- Facilidade no *restore* (catálogo único).

No contexto de um sistema de *backup*, pode-se aplicar algumas técnicas que em conjunto podem trazer benefícios ao serviço em questão. O primeiro item é conhecido como Esquema GFS (*Grandfather-father-son backup*). Ele se refere ao mais comum esquema de rotação de mídias para as cópias de segurança. Originalmente concebido para o *backup* em fitas, funciona bem para qualquer

estrutura de *backup* hierárquico. O método básico consiste em criar três conjuntos, sendo um diário, um semanal e outro mensal. Para melhor entendimento podem ser associados da seguinte forma. Os diários ou filhos serão rotacionados a cada dia com um semanal (ou pai) a cada semana; o semanal é rotacionado, em bases semanais, com um mensal (ou avô).

Ocasionalmente, um volume pode ser removido do esquema para estabelecer um marco, ou para fins de *disaster recovery*. Os administradores de rede consideram o GFS como o método mais simples e efetivo de rotação de fitas.

Há ainda de se considerar os benefícios dessa técnica. Um exemplo seria a proteção de seus arquivos com um número mínimo de fitas. Normalmente apenas uma ou duas são necessárias para o *restore* de um servidor, reciclando algumas fitas e arquivando outras. Pode-se ainda reduzir o desgaste das fitas ou outros dispositivos ligados ao *storage*. Tem-se ainda como benefício a facilidade na localização de arquivos armazenados devido à sistematização dos *backups*.

A estratégia de rotação GFS é baseada em uma agenda de 7 dias (Domingo – Sábado), na qual é feito ao menos um *backup full* a cada semana. Nos demais dias são feitos *backups* diferenciais (diários). O *backup full* a ser realizado durante a semana (por exemplo, na sexta-feira à noite), será sempre considerado como *backup* semanal. Então, as fitas diárias podem ser recicladas depois de 7 dias e as semanais após um mês.

Na terminologia GFS, o backup diário é o filho e o semanal, o pai. O último *backup full* de cada mês será considerado o *backup mensal* ao invés de semanal. Este é o avô. Os *backups* mensais devem ser armazenados por um período maior (meses, ou até anos) de acordo com a política de *backup* existente na organização.

Um ponto importante que precisa ser ressaltado é a reciclagem das fitas. Por padrão, o *backup* reutiliza as fitas diárias semanalmente (ou seja, uma mesma fita sempre vai fazer o backup nomeado de segunda-feira). Um exemplo das fitas semanais é que elas deverão ser reutilizadas, tomando como base a fita de sexta-feira, na segunda sexta-feira do mês. Seguindo o exemplo, haverá uma proteção de 1 ano de *backups*, utilizando 4 fitas diárias, 4 semanais, e 12 mensais. Obviamente, este número pode aumentar em caso de *backups* multivolumes, ou se o tempo de retenção (reciclagem) for menor que o padrão.

Sabendo que *backups* diferenciais diários ocupam um menor volume, ao invés do uso de quatro fitas necessárias no padrão GFS comum (gerando assim a necessidade de troca das mídias diariamente), pode ser implementada outra proposta:

• Semana 1: (fita A) para todos os *backups* diferenciais diários é utilizada uma mesma fita, com retenção de uma semana;

• Semana 2: (fita B) uma segunda fita é inserida, e será utilizada durante toda esta segunda semana, a não ser para realização do *backup full* semanal. Atenção, esse será feito em uma fita específica;

• Semana3: (fita A) agora se recicla a fita A, que receberá os *backups* diários da semana em questão;

• Semana 4: (fita B) e dá-se sequência no ciclo de *backup*.

A grande vantagem deste esquema é que o risco de danos à fita é diminuído, pois menos trocas de fitas são necessárias. Entretanto, as fitas são gravadas e regravadas em um ritmo mais acelerado.

Conhecendo o Bacula

A partir de agora passaremos a analisar o Bacula, que é um conjunto de ferramentas que permitem administrar as rotinas de *backup*, restauração e verificação dos dados de computadores em uma rede de sistemas variados. Em resumo, o Bacula é um programa de *backup* em rede. Ele é formado pelos seguintes componentes (módulos), que podem trabalhar de maneira independente em máquinas variadas, inclusive com sistemas operacionais diferentes:

• ***Director Daemon***: serviço responsável pela administração de todos os processos de *backup*, *restore*, verificação e arquivamento. O administrador de sistema usa o *Director Daemon* para efetuar agendamentos de *backup* e recuperar arquivos;

• ***Console Manager***: programa que auxilia o administrador ou o usuário a se comunicar com o *Director Daemon*. Pode ser executado em qualquer computador da rede e em sistemas operacionais diferentes. Atualmente existem três versões do *Console Manager*:

- Texto puro (*TTy*);
- Interface gráfica (GUI) usando bibliotecas do "*Gnome*";
- Bibliotecas "*wxWidgets*" (tanto em formato "*Unix*" quanto em "*Windows*").

• ***File Daemon***: é o software (serviço ou programa cliente) que é instalado na máquina que vai ser protegida pelo *backup*, ou seja, ele vai ser responsável por enviar os arquivos solicitados pelo *Director Daemon* pela rede. Também é responsável por administrar a gravação dos arquivos de restauração comandados pelo *Director Daemon*. Existem versões do *File Daemon* para diferentes sistemas operacionais: GNU/Linux, *BSD, Unix, Windows Macintosh;

• ***Storage Daemon***: serviço que consiste em administrar a gravação e restauração dos dados e atributos dos *backups* fisicamente em mídias apropriadas. Estes podem ser volumes de dados gravados diretamente no disco rígido ou em alguma mídia removível;

• ***Catalog***: é o programa responsável por manter uma indexação de todos os arquivos que são armazenados no *backup* e gerar uma base de dados dos volumes gerenciados pelo *Director Daemon*. O *Catalog* agiliza a busca de um arquivo no *backup* na hora que o administrador de sistema necessita efetuar uma restauração. Como ele mantém uma base de indexação dos arquivos gravados, a busca por um arquivo no meio dos volumes é mais rápida.

Na **Figura 1** pode-se ter uma ideia geral de como é o funcionamento dos módulos no *Bacula*. Conforme podemos observar, o *Director* é o coração do Bacula. Ele recebe os comandos do administrador via *Console* (modo texto, GUI, web) e se comunica com os clientes (*file daemons*). Esses clientes entram em contato com a *Storage Daemon*, que posteriormente fará as gravações dos arquivos no disco (*Physical Media*), e ela, em seguida, troca informações com o *Director*, como autorizações, índices e atributos que ficam gravados no *Catalog SQL*.

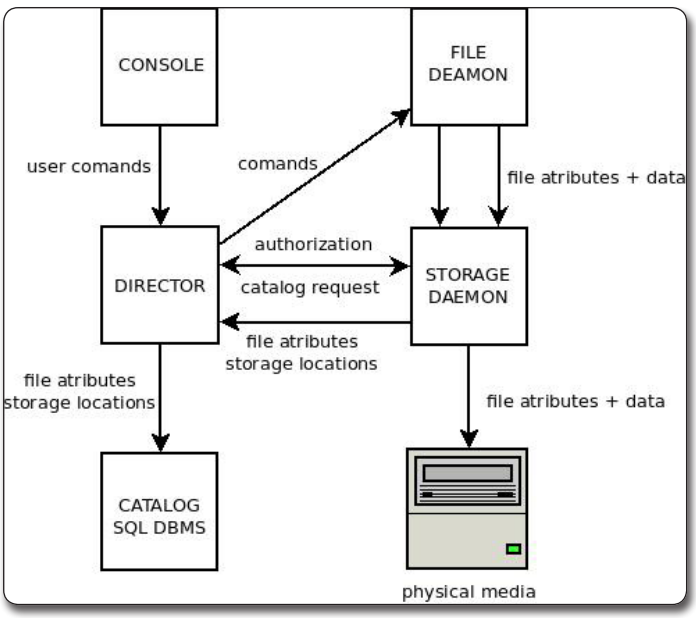


Figura 1. Módulos do Bacula

Para esclarecer ainda mais o entendimento dos módulos no Bacula, a **Figura 2** apresenta de forma sucinta como ocorre a interação desses agentes no Bacula. Conforme podemos observar, o administrador (*admin workstation*), através de uma console de comandos ou *wxWidgets Console* (interface gráfica), faz consultas, envia comandos para o Servidor Bacula (*Director*), este escutando na porta 9101. A aplicação roda em segundo plano autenticando as conexões e controlando as operações de backup. O administrador (*admin workstation*) ao mesmo tempo faz um monitoramento do cliente Bacula (*File Daemon*) na porta 9102, e da *storage* que armazena todos os dados pela porta 9103. O *Director* se comunica com os clientes ordenando as rotinas de backup para a *storage*, que por sua vez grava na mídia de armazenamento. Durante todo esse processo o *Director* está em contato com o servidor de banco de dados, aqui o MySQL na porta 3306, para armazenar e consultar os Índices.

Características do Bacula

Agora que já sabemos como funciona o Bacula e seus agentes, seguem abaixo algumas de suas principais características:

- Estrutura cliente/servidor;
- Estrutura modular independente (*director*, *client*, *database*, console de administração);
- GPL – economia de custos com licenças, conhecimento e possibilidade de customização da ferramenta;
- Inúmeros canais de suporte pela comunidade (*mailing lists*, *forums*, *IRC channel*);
- Grande documentação disponível na Internet;
- Portabilidade (compatibilidade entre os módulos para diferentes sistemas);
- Várias opções para a customização de *backups*;
- 100% compatível com o esquema GFS;
- Ferramenta de "backup" multi-banco de dados;
- Possui baixos requisitos de *hardware*.

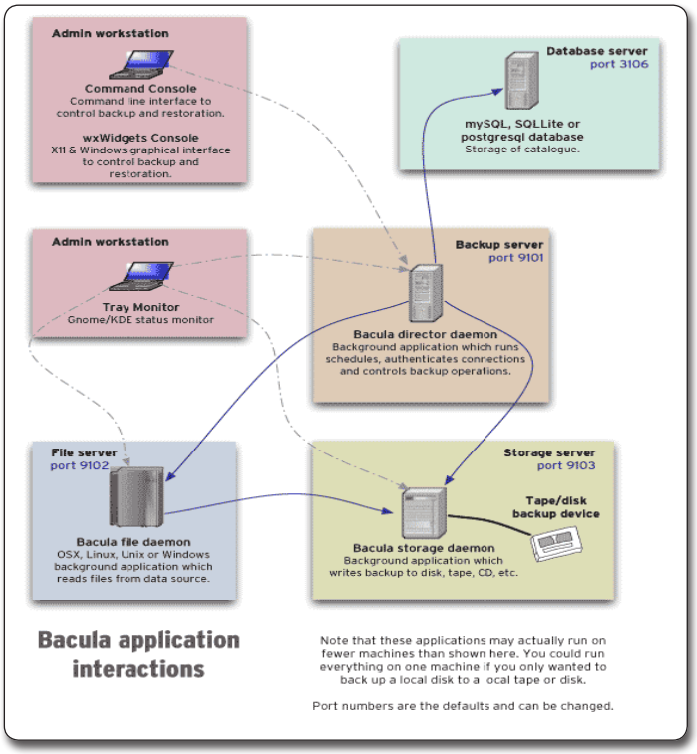


Figura 2. Interação dos módulos no Bacula

Além dessas características, o Bacula possui uma funcionalidade que permite a execução de *scripts* (ou executáveis) antes ou depois do início de trabalhos (*backup/restore*), tanto no cliente quanto no servidor. Tais operações podem ser efetuadas via linha de comando (modo texto) ou GUI (interface gráfica).

Um destaque especial pode ser dado também para as ferramentas de administração via *web*. O *webacula* e o *bacula-web* são ferramentas de visibilidade gerencial, sendo que a primeira ainda possibilita operações de *backup* e *restore*.

O Bacula tem suporte para a maioria dos dispositivos de *storage* do mercado (inclusive mídias ópticas). Um ponto fundamental é o envio de mensagens de log. Esta é uma funcionalidade importante tanto para os trabalhos de *backup/restore* quanto para fornecer instruções para operadores de diferentes perfis.

Pelo fato de ser livre, o Bacula permite o desenvolvimento de uma série de *addons* potencializando os recursos da ferramenta (veja a **Nota DevMan 4**). Inclusive, já existe *plugin* para o *Nagios*, ferramenta de monitoração.

O Bacula pode ainda substituir as ferramentas proprietárias mais comuns no mercado de TI (como exemplo, o *ArcServe* da *Computer Associates* e o *TCM*, da IBM).

Por fim, uma grande vantagem do Bacula consiste no fato de que, por possuir variante da licença GPL, ele é distribuído gratuitamente pela Internet. Além da economia gerada, a distribuição gratuita não impede que o administrador implemente o backup em um servidor, simplesmente porque ainda não tem comprada a licença do software. Para uma área tão crítica e dinâmica como é a das cópias de segurança, esta é uma característica chave.



Nota do DevMan 4

Addons: Conjunto de plugins que agregam funcionalidades a uma determinada aplicação.

Outras ferramentas de backup

Para finalizar, apresentaremos nesta seção algumas opções de ferramentas disponíveis para trabalharmos com backup:

• **Amanda**: Ferramenta livre, acrônimo para *Advanced Maryland Automatic Network Disk Archiver*, trata-se de um sistema que permite a configuração de um servidor mestre para realização de *backups* de múltiplos clientes numa rede com a possibilidade de armazenamento em fita, disco ou dispositivo. Ela usa o dump nativo do UNIX ou a ferramenta GNUtar e pode realizar *backups* de uma grande quantidade de máquinas rodando diferentes sistemas UNIX, com possibilidade de uso do Samba ou *Cygwin* para o *backup* de sistemas *Microsoft Windows*. Esta foi por muito tempo a mais popular ferramenta livre para realização e gerenciamento de *backup*;

• **Arcserve**: Ferramenta proprietária, muito interessante uma vez que suporta diversos sistemas operacionais, assim como o Bacula. Entretanto, a licença para um sistema só serve para aquele em específico, causando um aprisionamento tecnológico. O console de administração do *Arcserve* requer uma máquina possante e uma boa largura de banda na rede para que o desempenho operacional seja satisfatório. O licenciamento do *Arcserve*, além de possuir um custo elevado, é dividido por módulos e por funcionalidades, ou seja, cada vez que houver necessidade de um novo recurso, será necessário adquirir um novo módulo. No final do projeto, seu custo se torna demasiadamente alto;

• **TSM**: ferramenta proprietária, trata-se de uma ferramenta com bastantes recursos e, em certo ponto, é similar ao Bacula. A maior desvantagem fica na falta de documentação aberta, resultando em maior necessidade de treinamento e dificuldade na solução de problemas/*bugs*. De forma semelhante à ferramenta anterior, possui todas as demais desvantagens em se adotar uma ferramenta proprietária. O TSM costuma ser fornecido gratuitamente para quem adquire um *storage* da IBM, o que consiste em uma venda casada. No momento que o usuário começa a utilizar o TSM, cria um legado de *backups* difícil de ser migrado posteriormente. A renovação da licença e do suporte após o primeiro ano e para todos os demais passa a ser praticamente obrigatória, gerando um aprisionamento tecnológico.

Conclusão

Toda organização que se preze deverá ter um bom capítulo sobre *backup* na sua Política de Segurança da Informação. Conforme mencionado, há vários aspectos a serem avaliados quando um serviço de cópias de segurança é implementado. Nessa primeira parte do artigo sobre o Bacula apresentamos uma introdução sobre a importância do uso de cópias de segurança assim como suas formas.

Além disso, conhecemos o Bacula e seus principais componentes. Vimos que com ele ganhamos em flexibilidade de personalização de políticas e hardware, e obtemos uma redução de custos com licenças de uso.

Na próxima edição será apresentada de forma prática a instalação, configuração e uso do Bacula em um sistema operacional baseado em kernel Linux.



Flávio Alexandre dos Reis
reis.falexandre@gmail.com – www.reisfa.eti.br
Especialista em Segurança da Informação – FMG/JF, Pós Graduando em Redes de Computadores – CES/JF. Certificado LPIC-1, CLA. Atualmente professor em Instituições de Ensino Superior da Região de Juiz de Fora em disciplinas ligadas a Redes de Computadores e Sistemas Operacionais.



Eduardo Pagani Julio
epagani@gmail.com
Doutorando e Mestre em Computação pela Universidade Federal Fluminense. Atualmente professor do curso de Ciência da Computação da Universidade Federal de Juiz de Fora em disciplinas ligadas a redes.

Source Forge
http://sourceforge.net/projects/bacula/files/#files

Source Force - Download
http://sourceforge.net/projects/bacula/files/bacula/5.2.3/bacula-5.2.3.tar.gz/download

Software Livre
http://softwarelivre.org/bacula

Dicas-L
http://www.dicas-l.com.br

Bacula
http://www.bacula.org/en/

Bacula-br
http://www.bacula.com.br/?p=367

Viva o Linux
http://www.vivaolinux.com.br

Amanda
http://www.amanda.org/

TSM
http://www-01.ibm.com/software/tivoli/products/storage-mgr/

ARCServe
http://www.arcserve.com/us/support/ca-arcserve-backup.aspx

FARIA, M.H. Bacula – Ferramenta Livre de Backup. Editora Brasport.

Redes IP Multicast

Comunicação multiponto: gerenciamento dos grupos de usuários e roteamento de pacotes IP multicast

André Koide da Silva

O serviço IP multicast pode ser caracterizado como um conjunto de protocolos e mecanismos que tornam possível o envio de mensagens simultâneas para um grupo de usuários em uma rede de dados IP. Esseserviço tem sido requisitado pelas aplicações multimídia emergentes da Internet, viabilizadas principalmente pelo aumento da disponibilidade de redes com alta capacidade e alto desempenho. Entre outras vantagens da comunicação multiponto, destaca-se o melhor uso dos recursos da rede, pois os fluxos de dados são otimizados, sobretudo quando comparados à transmissão ponto-a-ponto (unicast).

Neste artigo, serão detalhadas a alocação dos endereços IP, sua organização em classes distintas e o subconjunto reservado às redes multicast. Também será relatada a arquitetura genérica deste serviço, contextualizada em duas partes com funções distintas. A primeira parte tratará do gerenciamento de grupos de usuários, com a apresentação dos protocolos responsáveis pelas ações relacionadas à composição dos grupos, tais como: a manipulação de informações dos participantes, a inclusão e a exclusão de seus usuários. Já a segunda parte, descreverá a infraestrutura de distribuição de pacotes, na qual serão expostos os protocolos de roteamento IP multicast, que coordenam os recursos de processamento e comunicação; são esses protocolosque tornam possível o encaminhamento de mensagens entre os servidores e os consumidores do conteúdo multicast.

Introdução ao IP multicast

As redes surgiram a partir da necessidade da troca de dados entre pessoas e computadores, possibilitando o acesso a documentos, imagens, planilhas, arquivos de áudio e vídeo, entre outros. Em setembro de 1981 foi publicada a especificação do protocolo IPv4 (*Internet Protocol version 4*), doravante designado simplesmente IP. Desde o início,esse protocolo se caracterizou pela simplicidade de implantação, interoperabilidade e robustez, sendo atualmenteo padrão adotado nas comunicações pela Internet.

Nas redes IP, cada dispositivo conectado (desktops, notebooks, celulares, servidores etc.) utiliza um identificador denominado endereço IP. Composto por 32 bits (4 octetos), cada byte usualmente é representado na forma decimal (0 a 255), separado por pontos, embora também possa ser adotada a notação binária, conforme ilustrado na **Figura 1**.

Inicialmente, o conjunto total de endereços IP (pouco mais de 4 bilhões) foi agrupado em cinco categorias distintas, com a finalidade de atender às necessidades das redes de computadores com diferentes tamanhos(**Tabela 1**). Destarte, endereços de classe A foram utilizados por grandes empresas, com até 16,7 milhões de dispositivos; já aquelas com até 65 mil, empregaram endereços de classe B.A classe C atendeu pequenas organizações, com cerca de 250 equipamentos. Por fim, os endereços de classe D e E foram reservados, respectivamente, para aplicações multicast e pesquisas.

Resumo DevMan

De que se trata o artigo:

Neste artigo serão apresentadasas principais características das redes IP multicast. Estas suportam as comunicações multiponto, demandadas pelas novas aplicações da Internet, tais como: IPTV, videoconferência, ensino a distância, entre outras. Para tanto, serão abordados os protocolos de gerenciamento de grupos de usuários e os algoritmos de roteamento utilizados para o encaminhamento dos pacotes IP multicast.

Em que situação o tema é útil:

Os tópicosabordados serão fundamentais para a compreensão dosconceitos básicos relativos à manutenção e à operação das redes IP multicast. Estas possuem características distintas das transmissões unicast, comumente observadas em aplicações de correio eletrônico e navegação na web. Portanto, podem servir tanto para oembasamentoteórico visando à implantação deste recurso nas redes das organizações, quanto à análise e avalição do funcionamento de serviços já em produção.

Redes IP Multicast:

O suporte ao recurso de comunicação multiponto está se tornando cada vez mais comum nas redes de dados modernas, especialmente porque este tipo de transmissão faz o melhor uso de seus recursos e reduz o consumo de banda nos enlaces entre os segmentos de rede. Entretanto, a implementação e a manutenção deste serviço requer conhecimentos específicos de sua arquitetura de operação, que envolve protocolos de gerenciamento de grupos usuáriose de roteamento de pacotes multicast. Além disso, são fundamentais os conceitos sobre a hierarquização e a alocação dos endereços IP, possibilitando o desenvolvimento de projetos segundo as diversas recomendações e normalizações existentes.


```
Notação binária: 11001000 11001000 10101000 00000001
Notação decimal: 200.200.168.1
```

Figura 1. Possíveis representações de um endereço IP

Categoria	Endereço inicial	Endereço final	Número total de dispositivos endereçáveis
Classe A	1.0.0.0	126.255.255.255	16.777.214
Classe B	128.0.0.0	191.255.255.255	65.534
Classe C	192.0.0.0	223.255.255.255	254
Classe D	224.0.0.0	239.255.255.255	Reservado para multicast
Classe E	240.0.0.0	255.255.255.255	Uso experimental

Tabela 1. Categorias dos endereços IP

Diferentes formas de comunicação podem ser adotadas para a transmissão dos pacotesIP (denominação atribuída aos dados encaminhados por intermédio das redes de computadores).Em cada uma delas, classes específicas de endereçamentopodem ser aplicadas:

• **Broadcast:** nesta forma de comunicação, os dados são encaminhados para todos os dispositivos. Por convenção, o último endereço IP de cada rede é designado endereço de broadcast (seja da classe A, B ou C). No exemplo ilustrado na **Figura 2**, ao remeter um pacote para 10.0.0.255, a estação Aenviará uma cópia deste aos dispositivos conectados à rede(10.0.0.11, 10.0.0.12, 10.0.0.13, 10.0.0.14 e 10.0.0.15), sem a necessidade de identificá-los individualmente;

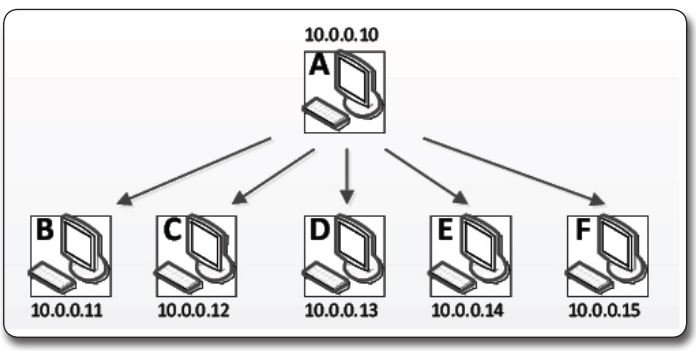


Figura 2. Comunicação broadcast (difusão) entre dispositivos conectados à rede

• **Unicast:**é uma transmissão ponto-a-ponto, ou seja, de um emissor aum destinatário, por meio de seu endereço de classe A, B ou C. No exemplo a seguir (**Figura 3**), o dispositivo A envia um pacote diretamente para B, através de seu endereço IP 10.0.0.11.

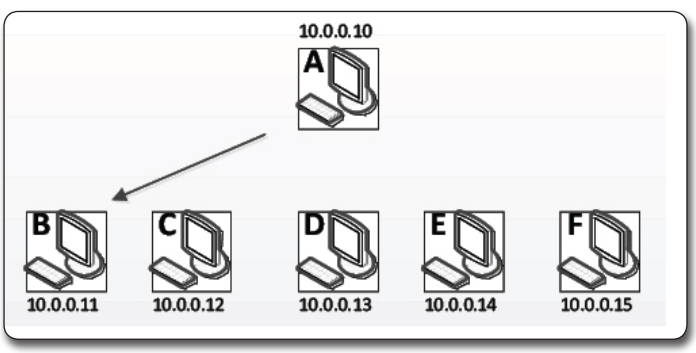


Figura 3. Comunicação unicast (ponto-a-ponto) entre dispositivos conectados à rede

• **Multicast:** neste método, os pacotes são enviados para um grupo de dispositivos (multiponto) identificado porum endereço IP da classe D. Deste modo, caso os usuários B e F desejem receber asmensagens de A, estes devem demonstrar seu interesseafim de que o emissor as encaminhe (**Figura 4**). É importante observar que a principal diferença entre um pacote multicast e os demais, é a presença do endereço IP declasse D (designação do grupo), ao invés de um da classe A, B ou C.

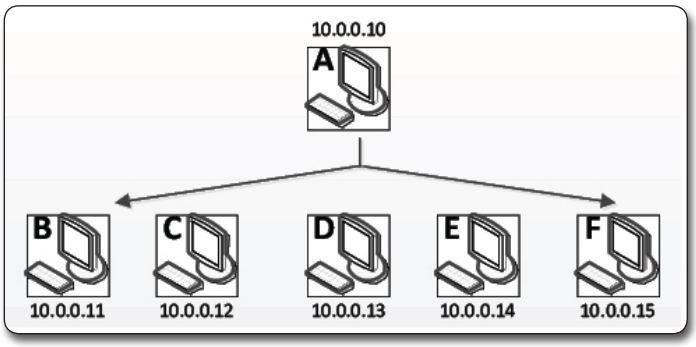


Figura 4. Comunicação multicast (multiponto) entre dispositivos conectados à rede

Atualmente, diversas aplicações emergentes da Internet, como o IPTV (*Internet Protocol Television* – tecnologia de transmissão dos sinais televisivos para aparelhos digitais por intermédio do protocolo IP), ensino a distância,videoconferência e computação distribuída, necessitam de suporte à comunicação multiponto. Essas aplicações se diferenciam do tradicional envio de mensagens de correio eletrônico ou mesmo da navegação em páginas na WWW (*World Wide Web*), pois podem ter mais de um emissor do conteúdo, além de diversos receptores, podendo chegar a alguns milhões, no caso da IPTV. Conforme será apresentado nas seções a seguir, o IP multicast suporta essas novas aplicações por intermédio do gerenciamento dos grupos de usuários e da implementação de protocolos de roteamentode pacotes multicast – responsáveis pela determinação do melhor caminho entre dois ou mais dispositivos (**Figura 5**).

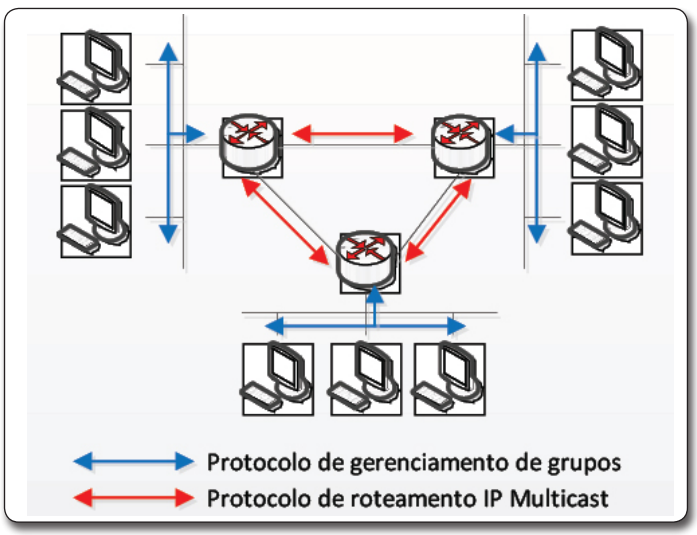


Figura 5. Serviços implementados pelo IP Multicast

Características gerais

Segundo Luís Henrique M. K. Costa e Otto Carlos M. Bandeira Duarte, em seu artigo *Roteamento multicast na Internet*, o modelo de serviço IP multicast especifica um grupo como uma comunicação aberta, onde:

- qualquer dispositivo conectado à rede pode participar, sem a necessidade de autorização do remetente;
- não há limitação quanto ao número de grupos aos quais um usuário pertença, ou seja, este pode receber o conteúdo de um ou mais grupos simultaneamente;
- não há obrigatoriedade do originador de tráfego fazer parte do grupo;
- os dispositivos podem entrar ou sair a qualquer instante, portanto o grupocaracteriza-se por sua natureza dinâmica;
- os participantes não são conhecidos, nem pelo remetente, nem pelos demais receptores.

Os grupos multicast são identificados por intermédio de um endereço IP da classe D, entre224.0.0.0 e 239.255.255.255. A partir dessa identificação, o IANA (*Internet Assigned Number Authority*), órgão internacional responsável pela alocação de endereços IP na Internet, determinou propósitos especiais para partes deste conjunto. A lista a seguir destaca as principais faixas reservadas:

- **224.0.0.0 a 224.0.0.255:** corresponde aos endereços que não são encaminhados pelos roteadores a outras sub-redes, ficando restritos à rede local. São utilizados para compartilhamento de mensagens de controle por diversos protocolos. A **Tabela 2** ilustra alguns exemplos;
- **233.0.0.0 a 233.255.255.255:**faixa reservada àatribuiçãoautomática de endereços aos sistemas autônomos (SA).Um SA é uma coleção de blocos de endereços IP e equipamentos de rede sob o controle de uma mesma organização, a qual é identificada por um número inteiro com 16 bits (0 a 65535). O método para determinação dos endereços é conhecido como GLOP (curiosamente esta sigla não é um acrônimo, mas a própria designação da técnica) e tem como mecanismo básico a inclusão do número do sistema autônomono endereço multicast. O exemplo ilustrado na **Figura 6** pressupõe uma empresa com SA 5662. Considerando que este númerotambémpode ser representado em notação binária com 16 bits, basta convertê-lo e associá-lo ao segundo e terceiro octetos do endereço multicast. Assim, a empresa com SA 5662 poderá usar a faixa de endereços 233.22.30.0 a 233.22.30.255;

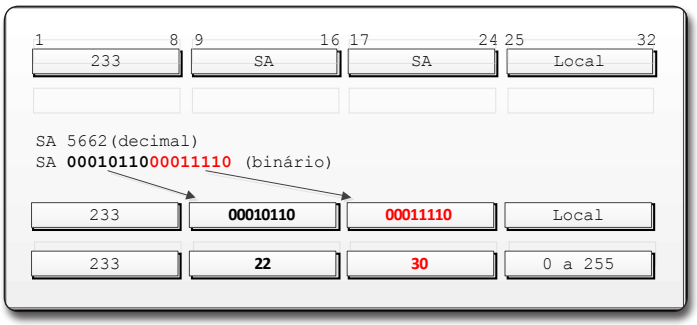


Figura 6. Faixa de endereçamento multicast baseado no número do sistema autônomo de uma organização

- **239.0.0.0 a 239.255.255.255:** conjunto de endereços alocado paraconfiguração local nas organizações, não encaminhado à Internet (privado).

Os demais endereços podem ser atribuídos dinamicamente pelas aplicações. Desta forma, como não existe um controle similar àquele feito aos endereços IP unicast, há o risco de diversos remetentesde tráfego multicast elegeremum mesmo endereço de grupo, ou seja, os clientes podem receber mensagens de outras aplicações, gerando inconsistências e informações corrompidas. Visando o controledo escopo dos pacotes multicast, as aplicações frequentemente utilizam o campo TTL (*Time To Live*) do cabeçalho IP. Este foi criado com o intuito de evitar que, principalmente em decorrência de problemas de roteamento, um pacote fosse transmitido indefinidamente pela rede.Portanto, o valor do TTL é decrementado em uma unidade, em cada roteador pelo qual o pacote atravessa, sendo descartado ao atingir o valor zero. Dependendo do valor definido aos pacotes multicast, estes podem ter escopo restrito à rede local, ao site da organização, à região, entre outros (**Figura 7**).

Os servidores de pacotes multicast devem atribuir o valor do TTL conforme a localização dos clientes. Entretanto, com o intuito de assegurar o escopo da transmissão, especialmente nos casos em que não é possível definir o número de roteadores entre o emissor e o receptor, é possível definir um valor limite (*threshold*) para o encaminhamento do tráfego multicast, nos roteadores que delimitam a rede da organização. Estes dispositivos, além de decrementar o valor do TTL, descartam o pacote quando o valor

Endereço	Descrição
224.0.0.1	Todos os dispositivos na rede.
224.0.0.2	Todos os roteadores na rede.
224.0.0.9	Utilizado pelo protocolo de roteamento dinâmico RIPv2 (Routing Information Protocol version 2) para a atualização das tabelas de rotas.
224.0.0.13	Utilizado pelo protocolo de roteamento multicast PIM (Protocol Independent Multicast) para o compartilhamento de informações da topologia.
224.0.0.18	Utilizado pelo protocolo de redundância de VRRP (Virtual Router Redundancy Protocol) para prover a redundância entre roteadores em uma mesma rede local.
224.0.0.102	Utilizado pelo protocolo de redundância de HSRP (Hot Standby Router Protocol), proprietário da Cisco Systems, para prover a redundância entre roteadores em uma mesma rede local.

Tabela 2. Exemplos de endereços reservados na faixa 224.0.0.0 a 224.0.0.255

obtido for inferior ao *threshold*, garantindo que o mesmo não seja propagado para outras redes (**Figura 8**).

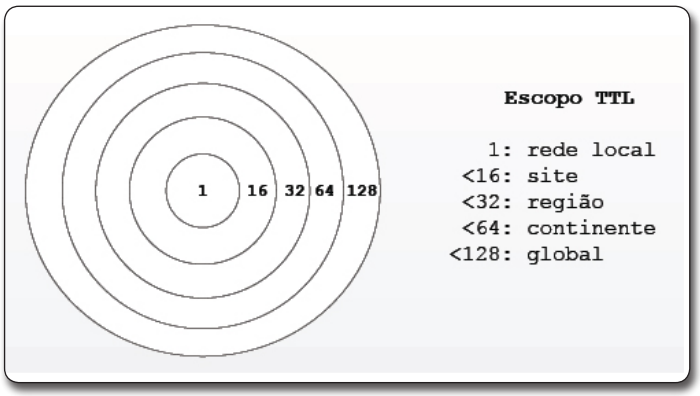


Figura 7. Restrição de escopo dos pacotes IP multicast segundo o TTL configurado

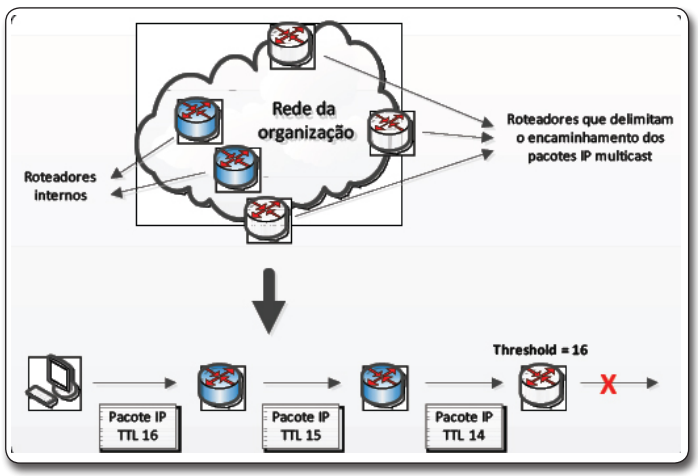


Figura 8. Controle do escopo utilizando o TTL threshold nos roteadores que delimitam a rede de uma organização

Segundo Chuck Semeria e Tom Maufer, em seu artigo *Introduction to IP Multicast Routing*, o IANA também reservou uma faixa de endereços MAC (*Media Access Control*) para o serviço IP multicast com o objetivo de aperfeiçoar a transmissão dos pacotes nas redes locais, quando empregada a tecnologia Ethernet (visto que esta igualmente possui suporte às comunicações ponto-a-ponto, broadcast e multicast). O MAC é um endereço físico com 48 bits utilizado na identificação das interfaces de conexão às redes de computadores. Para tanto, foi desenvolvido um procedimento com a finalidade de mapear os endereços IP da classe D para endereços MAC: este consiste basicamente na justaposição entre um prefixo de 25 bits e os 23 bits menos significativos do endereço IP multicast. Desta maneira, anexa-se o valor 00000001-00000000-01011110-0 (01-00-5e, em representação hexadecimal) aos 23 bits finais (contados a partir da direita para esquerda) do endereço IP, conforme ilustrado na **Figura 9**.

É importante notar que, caso estejam em uso endereços IP da classe D que se diferenciam apenas pelos bits mais significativos, estes resultarão em MAC duplicados. Nestas ocorrências, os clientes do tráfego multicast precisam ratificar se o endereço IP pertence ao grupo correto; caso contrário, devem descartar o pacote recebido.

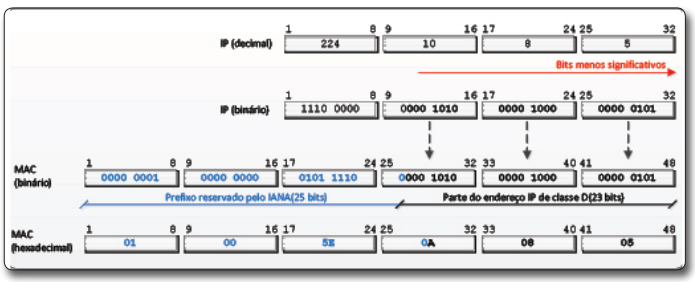


Figura 9. Mapeamento entre endereços de classe D e MAC

Vantagens e desvantagens da trasmissão IP multicast

Entre as principais vantagens da comunicação multicast, está o menor consumo de banda entre o servidor e os clientes.Suponha o cenário descrito na **Figura 10**, no qual um servidor de IPTV está atendendo os clientes A, B, C, D e E, por intermédio de fluxos unicast com aproximadamente 1 Mbps de largura de banda. Neste cenário, o enlace entre o servidor e o roteador R1 deve suportar ao menos 5 Mbps (somatória dos fluxos); já a conexão entre R1 e R2 consumirá 3 Mbps e, por fim, os enlaces entre R2 e R4, e entre R1 e R3, cerca de 2 Mbps (cada um). Observe que os roteadores R1, R2, R3 e R4 precisam encaminhar múltiplos fluxos de dados exatamente iguais. Imagine agora uma rede com centenas de milhares de usuários recebendo a mesma transmissão de um programa através da IPTV. Qual seria a largura de banda necessária entre os servidores de conteúdo e seus roteadores de acesso à Internet?

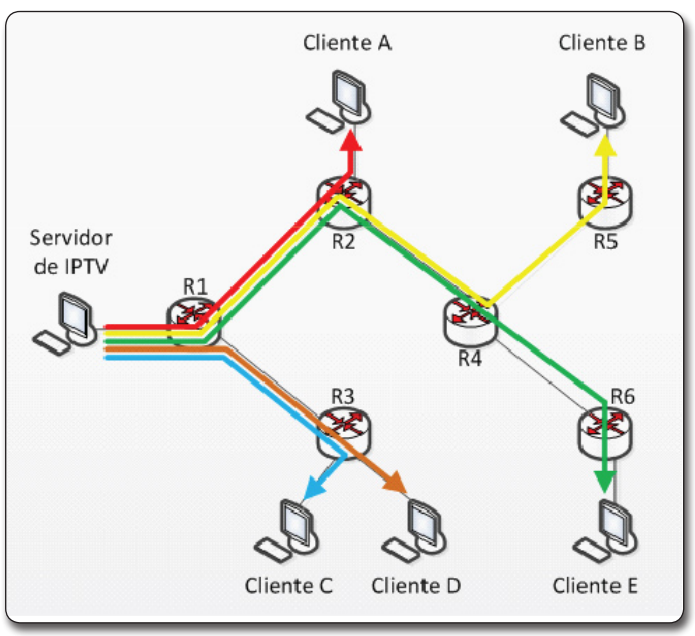


Figura 10. Fluxos unicast entre um servidor de IPTV e seus usuários

A **Figura 11** ilustra o mesmo cenário anterior, porém usando a infraestrutura de IP multicast para as transmissões multipontos.

Por meio do gerenciamento de grupos e do roteamento multicast, é possível que, independentemente do número de usuários interessados no conteúdo, um único fluxo atravesse a rede. Desta maneira, será utilizado cerca de 1 Mbps (neste exemplo) em todos os enlaces de comunicação.

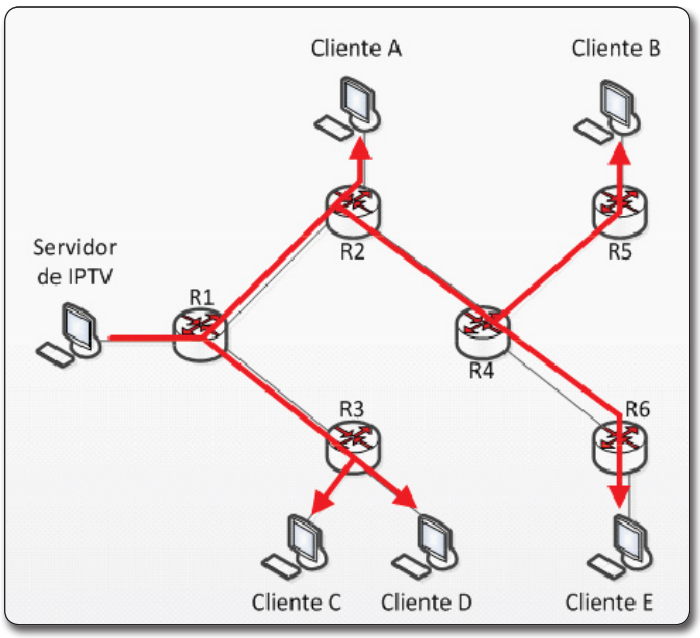


Figura 11. Fluxos multicast entre um servidor de IPTV e seus usuários

Além da redução do tráfego e do uso eficiente da largura de banda da rede, destacam-se as seguintes vantagens do serviço IP multicast:

• Os servidores e os clientes suportam a configuração desta funcionalidade sem a necessidade daaquisiçãode novossoftwares, pois todos os sistemas operacionais atuais disponibilizameste recurso;

• Não são necessários investimentos na infraestrutura da rede, já que os equipamentos modernos possibilitam o encaminhamento de pacotes multicast e a implantação dos protocolos de roteamento;

• Redução do processamento nos dispositivos de rede (desktops, servidores, roteadores, entre outros), resultante da redução do número de pacotes propagados pela rede.

Por fim, a lista a seguir apresenta os principais pontos negativos do IP multicast:

• O remetente não conhece a identidade e sequer o número de clientes que estão recebendo o conteúdo;

• Atacantes podem explorar facilmente a segurança de redes com este recurso, pois a associação e a desassociação dos usuários no grupo ocorre de maneira anônima;

• A necessidade de treinamento e capacitação dos profissionais que suportam a infraestrutura deIP multicast, pois envolve conceitos e protocolos diferentes daqueles habitualmente conhecidos, principalmente por aqueles que trabalham exclusivamente com a comunicação unicast.

Gerenciamento de grupos de usuários

O *Internet Group Management Protocol* (IGMP) é responsável por informar aos roteadores de um segmento de rede local sobre a presença de usuários interessados em participar de um grupo, gerenciandosua inclusão e exclusão. Uma analogia pode ser feita com a função do controle remoto em um aparelho televisor, o qual permite ligar ou desligar a recepção dos sinais de um determinado canal (similaridade com a participação em um grupo multicast).

Sendo assim, suponha uma aplicação que deseja se registrar em certo grupo, doravante denominado *G*;para tanto, esta deve enviar uma mensagem *IGMP Join* para a rede local, notificando sobre seu interesse em receber os pacotes destinados a *G*. Caso existam múltiplos roteadores neste segmento, o protocolo IGMP elegerá um deles, que será denominado*Designated Router* (DR) e terá a função exclusiva de processar todas as mensagens multicast trocadas pelos dispositivos (**Figura 12**). Daniel Barroso Monteiro, no artigo *Protocolos de Roteamento Multicast*, destaca que o DR encaminha apenas uma cópia do pacote na rede local. Desta forma, todos os solicitantes devem monitorá-la por intermédio do endereço MAC do grupo *G*.

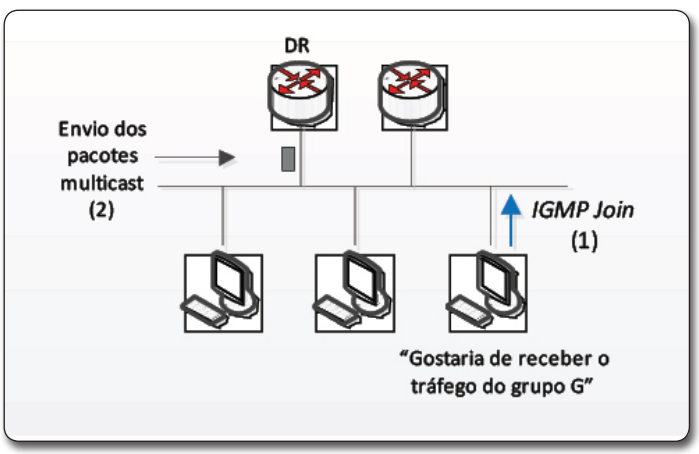


Figura 12. Mensagem de inclusão do participante no grupo G

Periodicamente, os roteadores também enviam mensagens *IGMP Membership Query*, inquirindo os dispositivos conectados à rede sobre o interesse em participar de algum grupo. Ao recebê-las, os usuários respondem em quais grupos desejam participar, por intermédio do *IGMP Membership Report*. Veja a **Figura 13**.

Existem três especificações diferentes do IGMP, a saber:

• **IGMP v1:** proposta inicial do protocolo, publicada em agosto de 1989;

• **IGMP v2:** nesta segunda versão, disponibilizada em novembro de 1997, a principal mudança foi a implementação de um mecanismo de exclusão do grupo, onde os clientes podem notificar explicitamente o remetente, avisando que não desejam mais receber os pacotes;

• **IGMP v3:** a alteração mais significativa nesta variante, anunciada em outubro de 2002, foi a inclusão do suporte à filtragem do tráfego, possibilitando ao solicitante determinar quais remetentes terão seus pacotes aceitos.

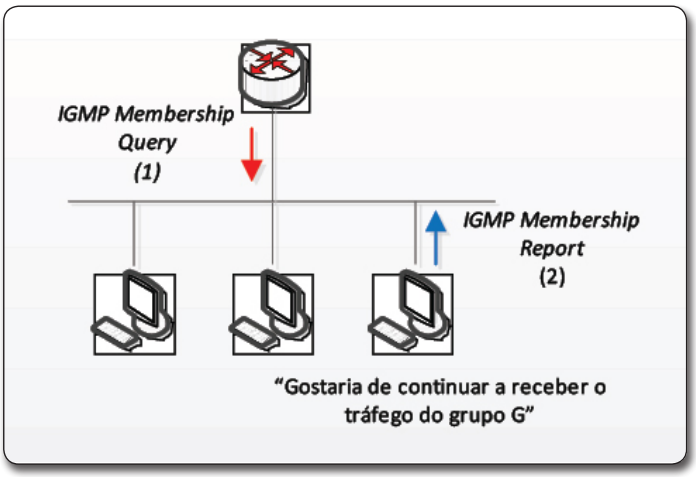


Figura 13. Mensagens enviadas para confirmar o interesse no conteúdo do grupo G

Portanto, no IGMP v1, o tráfego multicast é enviado até que o registro do grupo *G* expire (*timeout*). Somente quando o roteador não receber resposta às suas mensagens *IGMP Membership Query*, para um grupo *G*, este poderá excluí-lo de sua tabela de roteamento.

Já no IGMP v2, devido ao suporte à mensagem*IGMP Leave*, o receptor do conteúdo pode notificar ao remetente seu interesse em abandonar o grupo *G*, possibilitando ao roteador removê-lo imediatamente. Caso não existam outros dispositivos interessados, o grupo também poderá serretirado. Neste caso, o roteador envia uma mensagem denominada *IGMP Membership Group-Specific Query*, para o grupo G. Se não houver resposta, o grupo será excluído (**Figura 14**).

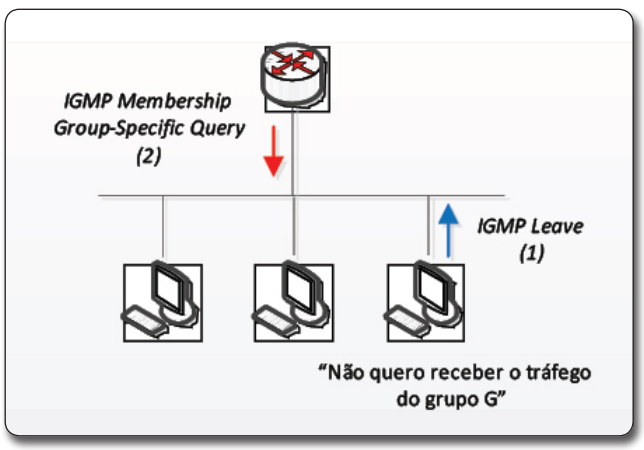


Figura 14. Mensagens para exclusão explícita do grupo (IGMP v2).

A versão mais recente do protocolo IGMP (v3) suporta a filtragem dos remetentes. Consequentemente, as aplicações usuárias podem determinar quais os emissores terão seus pacotes aceitos (por exemplo, servidor A e B), ou quais serão bloqueados (exceto os servidores C e F, todos os demais podem enviar). Desta maneira, os roteadores podem identificar quais pacotes não precisam ser encaminhados, por não serem aceitos pelos destinatários, mesmo que pertençam ao grupo.

Independentemente da versão, o protocolo IGMP trata a comunicação entre os clientes e o roteador no segmento local de rede. Para que o conteúdo gerado pelos remetentes seja encaminhado aos solicitantes, é necessária a criação de uma árvore de distribuição, através dos protocolos de roteamento multicast, conforme será exposto na próxima seção.

Protocolos de roteamento multicast

Segundo Daniel Barroso Monteiro, em seu artigo *Protocolos de Roteamento Multicast*, o primeiro protocolo de roteamento multicast desenvolvido foi o*Distance Vector Multicasting Routing Protocol* (DVMRP). Este emprega o algoritmo vetor de distâncias, no qual os roteadores possuem uma tabela que armazena as menores distâncias para os destinos conhecidos e por onde os pacotes devem ser enviados,afim de determinar as rotas a cadaoriginador de tráfego multicast. Destarte, quando um roteador com suporte a DVMRP recebe mensagens de algum remetente, este inicialmente verifica se os dados chegaram pela mesma interface que seria utilizada para propagar pacotes a esta origem.Em caso afirmativo, os pacotes são encaminhados a todas as interfaces de saída, inundando os segmentos diretamente conectados. Outros roteadores ligados a estas redes poderão solicitar o cancelamento do envio dos pacotes multicast, se não possuírem usuários participando do grupo.

Devido a estas características de operação, o protocolo DVMRP é denominado*dense-mode*, uma filosofia que pressupõe a existência de muitos transmissores e receptores na rede, transmitindo os fluxos em todos os enlaces da comunicação. Portanto, é necessário que os roteadores que não possuam interesse nos pacotes de algum grupo notifiquem explicitamente os dispositivos que estão propagando tais mensagens.

Outra opção é o *Multicast Open Shortest Path First* (MOSPF), expansão do *Open Shortest Path First* (OSPF), protocolo de roteamento de pacotes unicastextensivamente utilizado. O MOSPF encaminha as mensagens IP multicast de um emissor para as aplicações solicitantes por meio de uma árvore, que apresenta como raiz o roteador que as recebeu, e galhos que terminam em clientes participantes do grupo. Este protocolo emprega o IGMP para determinar a localização dos usuários interessados nas mensagens multicast.

Comparado ao DVMRP, o MOSPF é mais estável, porquanto utiliza o algoritmo global estado de enlaces (onde a topologia completa da rede é conhecida por todos os roteadores), que converge rapidamente e não apresenta problemas mesmo quando ocorrem mudanças em redes complexas e redundantes. Por outro lado, sua principal desvantagem é a dependência da utilização do OSPF como protocolo de roteamento unicast.

O *Protocol Independent Multicast* (PIM) se mostra como uma alternativa aos protocolos DVMRP e MOSPF, que pode ser implementada segundo duas variantes: o PIM-DM (*Dense-Mode*) e o PIM-SM (*Sparse-Mode*).A primeira, com operação similar ao DVMRP, ou seja, realiza a inundação periódica, propagando os pacotes multicast para todos os dispositivos conectados à rede.

Já o PIM-SM é um dos protocolos de roteamento multicast mais usados em grandes e complexas redes, pois assume que a distribuição dos receptores é esparsa. A denominação PIM decorre do fato da propagação dos pacotes multicast não depender de nenhum protocolo de roteamento unicast específico, sendo sua implantação simplificada em redes que estão em produção, pois suportaas configurações prévias existentes.

O PIM-SM foi proposto para cenários em que o número de clientes multicast é pequeno ou quando estes estão espalhados na rede.Esse protocolo somente é suportado pelos roteadores da infraestrutura, ou seja, os emissores e receptores de conteúdo multicast não devem implementá-lo. Periodicamente, os roteadores configurados como PIM-SM enviam mensagens *PIM-SM Hello* para identificar e manter as sessões ativas com seus vizinhos (**Figura 15**). Caso um roteador deseje receber os pacotes de certo grupo (*G*), este deve enviar mensagens *PIM-SM Join* (similar ao *IGMP Join*, porém entre os roteadores), conforme ilustrado na **Figura 16**.

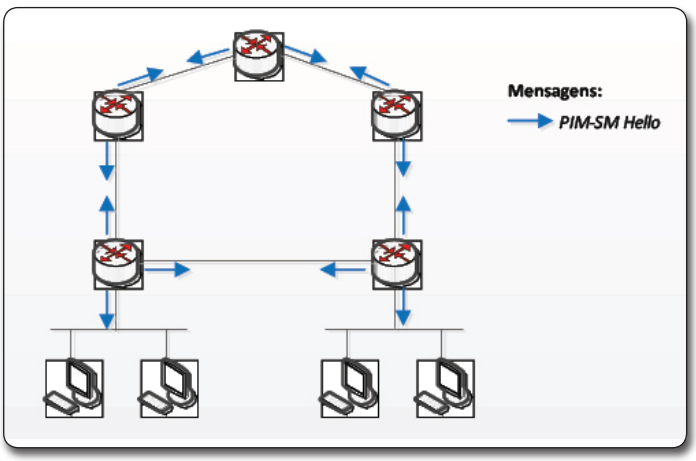


Figura 15. Identificação e manutenção de sessões ativas com roteadores vizinhos

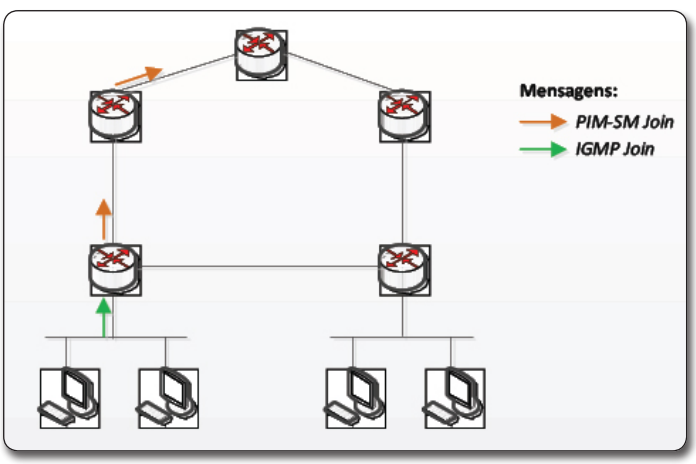


Figura 16. Envio de mensagem para participação em certo grupo

O PIM-SM utiliza árvores de encaminhamento paracada grupo. Com isso, um dos roteadores passa a ser denominado *Rendezvous Point* – RP (ponto de encontro), possuindo a função de reunir os servidores de conteúdo e os clientes consumidores destas mensagens. Neste cenário, todos os pacotes multicast recebidos pelos roteadores da infraestrutura, que sejam originados pelos servidores, deverão ser encaminhados ao RP. Analogamente, os pedidos de participação em grupos gerados pelos clientes também são enviados ao mesmo roteador (**Figura 17**). Desta forma, são estabelecidas as *Rendezvous Point Trees* (RPT), as quais podem ser reconfiguradas como*Shortest Path Trees* (SPT) após a propagação do fluxo inicial de pacotes. Estas últimas são caminhos multicast otimizadoscom base nas informaçõesdo protocolo de roteamento unicast suportado, viabilizando a comunicação direta entre os emissores e os receptores de conteúdo (**Figura 18**).

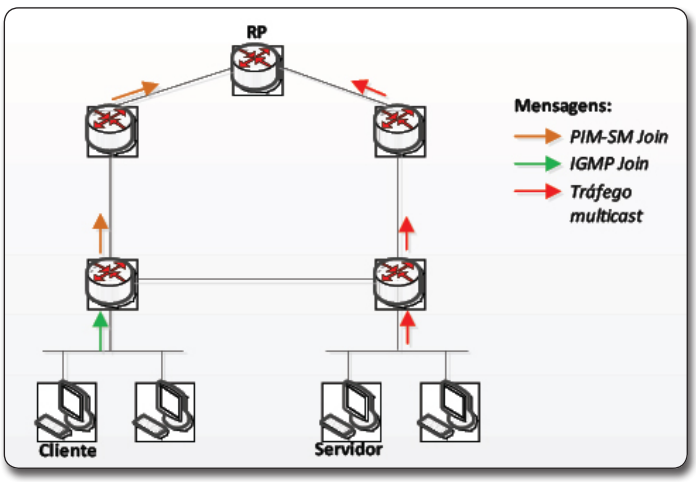


Figura 17. Encontro de servidores e consumidores de conteúdo multicast no RP

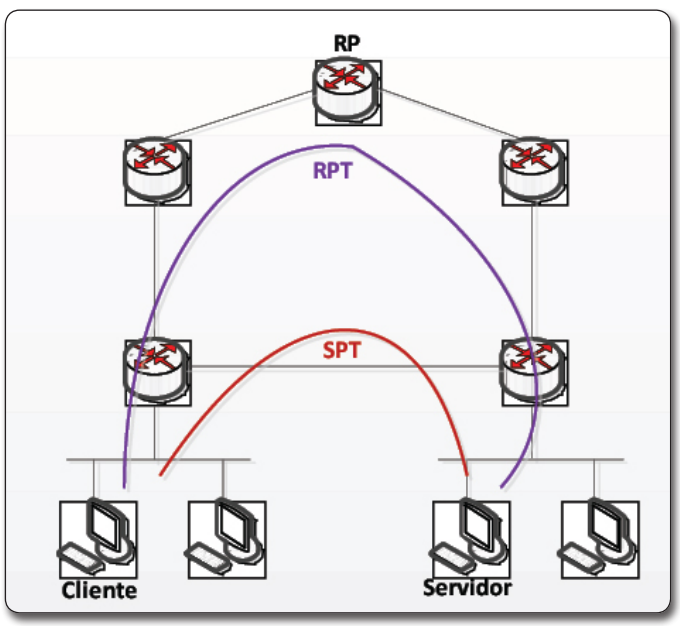


Figura 18. Otimização do caminho multicast por meio da SPT

Os protocolos apresentados anteriormente (DVMRP, MOSPF e PIM) são empregados com o intuito de permitir a comunicação

entre dispositivos de uma mesma organização (sistema autônomo). A implantação dafuncionalidade IP multicast entre empresas, por intermédio da Internet é muito complexa, pois transcendeas questões técnicas, envolvendopolíticas e estratégias que não são objeto de análise neste artigo.

Conclusões

A demanda pelo suporte ao serviço IP multicast está crescendo, principalmente pelo célere desenvolvimento das aplicações multimídia, como IPTV, videoconferência, ensino a distância, computação distribuída, entre outras. Dentre suas principais vantagens, está a redução no uso dos recursos da rede, bem como o menor consumo de largura de banda nos enlaces que conectam os originadores e os usuários consumidores deste conteúdo. Além disso, geralmente não são necessários investimentos na infraestrutura da rede de dados e no software de servidores e clientes, pois esta é uma tecnologia suportada pelos equipamentos e sistemas operacionais atuais. Por outro lado, existem sérias limitações relacionadas aos aspectos de segurança da informação e à capacitação técnica dos profissionais da área, pois esta envolve conceitos e protocolos diferenciados daqueles frequentemente empregados nas transmissões unicast.

A arquitetura das redes IP multicast comumente é descrita em duas partes com funções específicas.A primeiraestá relacionada ao gerenciamento (inclusão e exclusão) dos participantes nos grupos multicast, e é mantida pelo protocolo *Internet Group Management Protocol*, que possui três versões distintas. Já a segunda parte refere-se à infraestrutura da rede necessária à propagação dos pacotes IP multicast. Neste contexto, os protocolos *Distance Vector Multicasting Routing* e *Protocol Independent Multicast – Dense-Mode* não são aplicáveis às grandes redes, pois suas filosofias pressupõem a transmissão inicial dos fluxos de pacotes multicast em todos os enlaces de comunicação, gerando tráfegos de dados muitas vezes desnecessários. O *Multicast Open Shortest Path First*, embora se destaque pela estabilidade, possui dependência do *Open Shortest Path First*, inviabilizando sua configuração em redes que empregam outros protocolos. Por fim, o *Protocol Independent Multicast – Sparse-Mode* se apresenta como uma alternativa extensivamente utilizada, especialmente em grandes e complexas redes, pois pode ser habilitado conjuntamente com qualquer protocolo unicast. Além disso, possibilita a otimização dos fluxos de pacotes multicast, enviando-os somente aos clientes que explicitamente notificaram o interesse em recebê-los.



André Koide da Silva
andre@aksilva.com

Mestre em Engenharia pela Escola Politécnica da Universidade de São Paulo, especialista em Redes de Computadores pela Universidade Estadual de Campinas e bacharel em Sistemas de Informação pela Universidade Presbiteriana Mackenzie. Atualmente é especialista em redes de computadores pelo UOL Diveo, com ampla experiência em projetos e implementação de soluções Cisco Systems, Brocade Communications Systems e Juniper Networks. Atua também como professor na Faculdade Impacta Tecnologia. Trabalhou em empresas como Goldnet TI, EDS (Electronic Data Systems do Brasil) – atual HP Brasil (Hewlett-Packard), Alog Data Centers e Gennari & Peartree Projetos e Sistemas. Experiência de doze anos na área de redes de computadores e tecnologia da informação, além de seis anos como docente do ensino superior nestas áreas. Certificado Cisco IP Communications Express Specialist, Cisco Certified Network Associate (CCNA), Extreme Network Associate (ENA), 3Com Certified Wireless Expert, Juniper Networks Certified Internet Specialist (JNCIS-M), Project Management Professional (PMP), Information Technology Infrastructure Library (ITILv3) e ISO/IEC 20000 - IT Service Management.

Artigo "Introduction to IP Multicast Routing", escrito por Chuck Semeria e Tom Maufer.
http://www.stanford.edu/class/ee384a/files/Introduction_to_IP_Multicast_Routing.pdf.

Artigo "Protocolos de Roteamento Multicast", escrito por Daniel Barroso Monteiro.
http://www.midiacom.uff.br/~debora/fsmm/trab-2007-1/multicast.pdf.

Artigo "Roteamento multicast na Internet", escrito por Luís Henrique M. K. Costa e Otto Carlos M. Bandeira Duarte.
http://gta.ufrj.br/ftp/gta/TechReports/CoDu03.pdf.

Monitorando servidores com collectd

Thiago Nache

O monitoramento em um ambiente de infraestrutura de TI é um dos componentes básicos que o administrador de sistemas precisa para oferecer um serviço de qualidade. Imagine ter que entrar em servidor por servidor para saber se está tudo funcionando bem em seu ambiente. Em um ambiente pequeno, isso é possível, mas desnecessário, pois esse tempo pode ser gasto em outras tarefas.

Atualmente, muitas vezes, só se sabe que algo está com problema quando o usuário final liga para informar. Isso é algo que pode ser evitado. Quando o cliente ligar para reclamar, o administrador do sistema deve conhecer quais itens estão com problema e qual a previsão para normalizar. Isso demonstra que o administrador tem controle sobre sua infraestrutura e traz confiança para seu cliente, seja ele interno ou externo. Trabalhar de forma proativa é muito melhor do que de forma reativa e para isto é necessário um processo de monitoramento bem estabelecido.

O monitoramento deve contemplar todos os itens de infraestrutura que envolvam o funcionamento normal do seu ambiente, ou seja, ativos de rede (roteadores e *switches*), servidores e o que mais for possível monitorar.

Um sistema de monitoramento bem definido faz com que o administrador saiba o que está acontecendo no ambiente sem sequer se autenticar em um servidor. Em outras palavras, o administrador deve conter uma tela única que aponte se existe problema no ambiente computacional ou não. Para atingir este nível de maturidade, leva-se um tempo. Portanto não é preciso se preocupar se, no início, não for possível chegar a essa situação. Um processo contínuo de revisão e melhoria deve ser instaurado até que se alcance a qualidade esperada de monitoramento.

Resumo DevMan

De que se trata o artigo:

Nesse artigo abordam-se aspectos de monitoramento de servidores Linux utilizando as principais ferramentas do mercado, ampliando a visão do administrador e possibilitando ações preventivas no ambiente, como alertar seu cliente que o consumo de recursos está aumentando e que em breve ele poderá ter problemas.

Em que situação o tema é útil:

Esse artigo pode ser aplicado em qualquer empresa que possua servidores Linux que queira monitorar. O artigo é igualmente útil para empresas que estão montando sua infraestrutura de TI e desejam evitar problemas no futuro, ou para empresas que desejam aprofundar o nível de monitoramento dos sistemas em produção.

Monitorando servidores com collectd:

Neste artigo abordam-se aspectos de monitoramento de servidores Linux utilizando o collectd como ferramenta de coleta de dados e o rrdcached para armazenamento dos dados (utilizados para a geração de gráficos). Durante esta parte da configuração, demonstra-se como compilar e instalar os pacotes collectd e rrdcached no Linux. Para isso utilizam-se alguns comandos do dia-a-dia do administrador de sistemas, entre eles: yum, wget, tar, scp e chkconfig.

Para visualização dos gráficos se utiliza o collection3 como front-end. Durante esta configuração se demonstra como instalar bibliotecas Perl através do CPAN, como criar scripts de inicialização baseado nas funções padrões da Red Hat e como se faz a instalação básica do apache httpd.

Monitoramento de servidores

Existem dois tipos de monitoramento em servidores: monitoramento ativo e monitoramento passivo. Basicamente, o monitoramento ativo é aquele onde o servidor busca as informações no item monitorado (máquina em que se executa um processo cliente). Por sua vez, o monitoramento passivo é aquele onde o processo cliente envia os dados para o servidor de monitoramento. A arquitetura e as ferramentas para isso devem ser avaliadas de acordo com o tipo de negócio e as necessidades.

Atualmente, no ambiente computacional aplicam-se ambos os tipos de monitoramento, pois além de ter a visão do servidor, é necessário ter a visão do usuário. Explica-se: imagine monitorar de forma passiva o processo do ntpd (*network time protocol daemon*). O processo está rodando, mas por algum motivo, o sincronismo de horário não está sendo feito. Então, de forma ativa, monitoram-se quantos minutos o servidor está diferente do servidor *ntp* (*Network Time Protocol*). Assim, tem-se a visão do sistema operacional (processo rodando) e a visão do usuário (quantos minutos de diferença de horário). Este tipo de estratégia deve ser aplicado em todo monitoramento.

Outro item importante é chegar ao valor do limite ideal para o monitoramento. Esse valor, chamado *threshold*, é o valor mínimo ou máximo que o item monitorado deve trabalhar. Por experiência, definem-se valores comumente utilizados, conforme citado nas explicações a seguir. Porém é conceitualmente errado predefinir o *threshold* para monitoramento, pois este deve ser adequado ao ambiente que se quer monitorar. Quando estiver montando o ambiente computacional, o administrador deve gastar um tempo

analisando os gráficos de utilização dos recursos para chegar aos valores ideais. Se o administrador implementar o ambiente computacional sem esta tarefa, problemas com falsos-positivos podem ocorrer. Chamam-se falso-positivos os alarmes que aparecem no monitoramento, mas não correspondem a um problema real no ambiente. Isso é um erro de configuração do monitoramento e o processo de monitoramento deve ser reavaliado.

Monitoramento passivo

O monitoramento passivo é feito por um processo cliente instalado no item monitorado que coleta as informações de tempos em tempos e envia para o servidor central. O tempo de coleta no processo cliente pode ser diferente do tempo configurado na monitoração. Por exemplo, a coleta é realizada em intervalos de um minuto e o monitoramento é realizado a cada cinco minutos. Isso pode ser útil, pois ao gerar gráficos com o intervalo menor, o administrador do sistema terá maior visibilidade do comportamento do item monitorado. Porém, quanto menor o intervalo do monitoramento, mais carga haverá no cliente e no servidor. Por isso é importante avaliar os recursos disponíveis e sua necessidade. Se o ambiente possuir muitos servidores e não houver muitos recursos para o monitoramento, é possível melhorar o ambiente com o intervalo de coleta de 5 minutos.

CPU

Para o monitoramento de CPU, geralmente utiliza-se o valor de CPU *idle* (ociosa) com *threshold* mínimo de 10% do tempo de ociosidade para *critical* e 20% do tempo de ociosidade para *warning*, ou seja, quando a utilização for maior que 80% da capacidade total da CPU, está na hora de preocupar-se em aumentar a capacidade de processamento ou adicionar mais um servidor no grupo de servidores. Porém este *threshold* deve ser ajustado de acordo com a característica do serviço. Por exemplo, um servidor que faz processamento de *logs* tem seu *threshold* de *warning* em 95% e *critical* em 100%, pois a característica do serviço é de alto consumo de CPU. Então, o fato da CPU estar em 90% é aceitável. Porém, para um servidor de *memcached* pode-se diminuir bastante o *threshold* da CPU. Quando a CPU está acima de 80% de carga de processamento o administrador deve começar a se preocupar para evitar futuros problemas.

Memória

Quando se fala de monitoramento de memória, o ideal é monitorar sempre a memória utilizada e a memória de *buffers*, pois em sistemas de alto desempenho, o papel do *cache* é extremamente significativo para o sistema operacional, posto que operações de escrita e leitura em memória são muitas vezes mais rápidas do que as mesmas em disco. Portanto uma parte da memória total deve estar sendo para realizar *cache*.

Swap

Quando a área de *swap* começa a ser utilizada é porque a memória do sistema já foi alocada e o sistema operacional precisa disponibilizar mais memória para um processo. Conforme mencionado anteriormente, operações de escrita e leitura são muito mais lentas em disco do que em memória. O total da memória *swap* deve ser pequeno, senão o servidor perderá desempenho significativamente até ocasionar seu próprio travamento. Alguns megabytes ou no máximo um gigabyte já é o suficiente para um momento de maior consumo. Se o servidor em questão fizer *swapping* frequentemente, deve-se analisar o aumento da memória ou alguma aplicação com *memory leak*. A falha *memory leak* é causada quando o sistema não desaloca memória. Sendo assim, o processo irá consumir cada vez mais memória até ocupar toda a área de *swap* ou travar. Em casos onde não é necessário alto desempenho por todo o tempo, o uso de *swap* pode se tornar aceitável.

Sistema de arquivos

O monitoramento do sistema de arquivos é realizado por porcentagem utilizada ou quantidade de espaço livre. O que vai determinar a melhor forma de monitorar é o tamanho do sistema de arquivos. Se o tamanho total do sistema de arquivos for pequeno (menor que 100 gigabytes), utiliza-se porcentagem de espaço livre. Porém, se for grande (maior que 100 gigabytes) é melhor utilizar o total de espaço livre. O */usr* normalmente tem entre 3 e 8 gigabytes. Para esse tamanho estabelece-se o *threshold* de 80% para *warning* e 90% para *critical*, pois este tamanho é considerado pequeno. Porém, para um servidor de arquivos de um terabyte, é melhor monitorar por espaço livre.

Network File System

Pelo lado do servidor, deve-se utilizar as estatísticas do servidor *Network File System* (NFS), ou seja, a quantidade das chamadas de cada tipo, por exemplo: *read*, *write*, *create*, *commit* etc. Pelo lado do cliente, deve-se certificar que o sistema de arquivos esteja em modo de leitura e escrita. A forma mais comum de realizar esta monitoração é escrever um arquivo no sistema de arquivos, medir o tempo da escrita, realizar a leitura do arquivo e medir o tempo da leitura.

Discos

Um item importante para monitorar em disco é o tempo de resposta, ou seja, quanto tempo leva cada operação de escrita e leitura no disco. Quanto menor for esse tempo melhor desempenho terá seu ambiente. O tempo varia muito entre fabricantes. Se o disco é local ou *storage*, qual modelo de RAID adotado, se a tecnologia é SATA, SSD, Storage FC, NAS etc. Outra alternativa é a quantidade de operações por segundo (IOPS). Quanto maior esse valor, mais carga haverá no disco. Um valor muito alto aumentará o tempo de resposta.

Processos

É importante observar todos os processos que precisam estar funcionais no servidor. Os processos do sistema operacional são mais comuns, por exemplo, *syslog*, *ntp*, *sshd*, *crond* e *sendmail*. Os processos de aplicações variam bastante, sendo que os mais

comuns são o *Hypertext Transfer Protocol Daemon* (*httpd*) ou simplesmente servidor *web* e os processos *Java*. Pode-se monitorar apenas a quantidade de processos ou *threads* ou então entrar em um detalhamento melhor, ou seja, monitorar a quantidade de memória, a quantidade de escrita e leitura, e o tempo de uso da CPU do processo específico. Com as ferramentas aqui expostas, o administrador do sistema conseguirá chegar ao nível alto de detalhamento.

Monitoramento ativo

O monitoramento ativo pode ser feito pelo próprio servidor de monitoramento ou por outro servidor. Isso vai depender da quantidade de itens monitorados e da quantidade de recursos do servidor alocado para essa tarefa.

Quando o processo de monitoramento estiver atrapalhando o próprio monitoramento, ou seja, quando a utilização dos recursos feita pelos processos que correspondem ao monitoramento dos clientes for maior que a utilização dos recursos feita pelo processo do sistema de monitoramento, o administrador deve separar as tarefas em servidores diferentes.

Para definir o monitoramento ativo, deve-se cumprir basicamente duas tarefas:

1. Monitoramento de portas (TCP e UDP): O monitoramento de portas TCP/UDP consiste em um teste de conectividade na porta e protocolo determinado. Por exemplo: telnet para TCP e netcat para UDP.
2. *Scripts* que simulam a situação atual do ambiente: Esses *scripts* devem reproduzir as ações do usuário final.

Alguns exemplos de como fazer o monitoramento ativo são apresentados a seguir. A **Tabela 1** mostra que para monitorar o serviço Syslog configura-se o monitoramento da porta 1514 TCP e 514 UDP. Porém, habitualmente, não se cria nenhum script para monitorar o serviço.

Serviço	Porta	Script
Syslog	1514 TCP e 514 UDP	
NTP	123 TCP e 123 UDP	Diferença de horário
SMTP	TCP 25 e/ou 465 TCP	Envio de e-mail
SSH	TCP 22	
Web Server	TCP 80	Página de health check
Application Server	TCP 8080	Página de health check
Database	TCP 1521/ TCP 3306	Query

Tabela 1. Serviços, portas e scripts

Para monitorar o serviço de NTP configura-se o monitoramento da porta 123 TCP e 123 UDP e cria-se um script para monitorar a diferença de horário entre o servidor de monitoramento e o item monitorado. Nesse caso, é preciso se certificar do horário do servidor de monitoramento.

No caso de um servidor de correio eletrônico, é preciso que o protocolo *Simple Mail Transfer Protocol* (SMTP) esteja funcionando no servidor. Para monitorá-lo cria-se um script que envia uma mensagem eletrônica.

É importante destacar que, sempre que for necessária a autenticação para monitorar o serviço – por exemplo: uma *query* no banco de dados – é preciso ter um usuário específico para monitoramento.

Hands on

Agora se propõe um laboratório para ver as coisas funcionando! Neste artigo, demonstram-se algumas ferramentas, mas nada que impeça o usuário de montar sua própria arquitetura e escolher suas ferramentas. O usuário pode fazer seus próprios monitores. Porém, se já existe algo bom que funciona, não é preciso gastar tempo desenvolvendo os próprios monitores. Deve-se criar os próprios monitores em casos muitos específicos, ou seja, quando não existir um *plugin* já pronto.

O sistema operacional em questão é o Mac OS X 10.6.8 e o Parallels Desktop para criar as máquinas virtuais. Deve-se criar no mínimo três servidores: um para compilar os pacotes (não é recomendado que se compile os pacotes no servidor que roda o serviço), outro para representar o papel de servidor central e, por último, outro para representar o papel de cliente. Os nomes dos servidores serão: *builder01*, *server01* e *client01*. O sistema operacional de todas as máquinas virtuais é o CentOS 5.7 x86_64.

Na seção de *downloads* da Revista Infra Magazine, disponibiliza-se dois arquivos para instalação do Sistema Operacional. Se o usuário possuir o software *kickstart*, deve utilizar o arquivo *anaconda-ks.cfg*, senão deve usar o *rpm-qa.txt*. Se o usuário seguir esses passos, o sistema operacional deverá ter os mesmos pacotes apresentados no arquivo *rpm-qa.txt*. Caso ocorram problemas, o usuário deve verificar se todos os pacotes foram instalados corretamente.

Após a instalação do sistema operacional, é preciso configurar a rede. A máscara de rede será 255.255.255.240. Assim a sub-rede pode ter até 14 máquinas virtuais (VM), mais que suficiente para esse caso. Os endereços IP serão 10.211.55.9, 10.211.55.10 e 10.211.55.11 para os servidores *builder01*, *server01* e *client01*, respectivamente. Além disso, cada máquina virtual tem 1 vCPU e 512 megabytes de memória RAM.

Compilando pacotes

O servidor para compilar os pacotes necessários para nosso laboratório será o *builder01*. Deve-se executar a sequência de comandos a seguir para instalar o compilador:

```
# ssh 10.211.55.10
# yum -y install gcc
```

O *gcc* é um compilador de programas na linguagem C. Em servidores de produção em que sua função não é atuar como um compilador, não é recomendado que este pacote seja instalado, pois com um compilador C disponível é muito mais complexo garantir a segurança no servidor.

RRDtool

O RRDtool é uma ferramenta para gerenciar dados e gráficos coletados de tempos em tempos. Para o ambiente proposto, o binário rrdcached, que é provido pelo pacote do RRDtool, e a biblioteca *librrd.h*, serão necessários para compilar o plugin RRDtool e o rrdcached. Veja mais sobre isso mais adiante neste texto.

O rrdcached armazena uma quantidade pré-configurada de dados antes de atualizar o RRD, ou seja, diminui significativamente a quantidade de escrita e leitura em disco feitas para gerar os gráficos. Detalhes sobre o plugin rrdcached podem ser consultados no *wiki* do *collectd*. Execute a sequência de comandos mostrada na **Listagem 1** para instalar o RRDtool.

Listagem 1. Instalando o RRDtool.

```
# yum -y install cairo-devel pango-devel libxml2-devel
# cd /usr/src
# wget http://oss.oetiker.ch/rrdtool/pub/rrdtool.tar.gz
# tar xzvf rrdtool.tar.gz
# cd rrdtool-1.4.7/
# ./configure --prefix=/opt/rrdtool-1.4.7
# make && make install
```

O comando *yum* é utilizado para gerenciar os pacotes do sistema operacional.

O comando *wget* é utilizado para baixar arquivos da internet. Provavelmente, de dentro da rede, o usuário não terá acesso para baixar arquivos da internet. Assim, o usuário deve solicitar o acesso ou baixar os códigos fontes e copiá-los para o servidor.

O *tar* é um comando para compactar/descompactar arquivos. A **Tabela 2** apresenta alguns parâmetros para utiliza-lo. Para consultar todos os parâmetros, deve-se executar o comando *man tar*.

Parâmetro	Funcionalidade
x	Descompactar o arquivo
c	Compactar o arquivo
z	Utilizar gzip na descompactação/compactação
v	Imprimir no STDOUT os arquivos que estão sendo descompactados/compactados
f	Especifica o nome do arquivo

Tabela 2. Parâmetros do comando tar

O próximo comando é o *configure*, que é um *script* padrão contido em todos os arquivos fontes para o usuário preparar o sistema. Se quiser conhecer mais sobre, deve-se executar o comando *./configure --help*. O comando *make* compila os códigos fontes para gerar os binários, bibliotecas, arquivos de configuração, documentos etc. A inclusão do parâmetro && significa que se o comando *make* for executado com sucesso o próximo comando será executado em seguida. Caso contrário, o comando seguinte não será executado.

O comando *make install* instala, isto é, copia todos os arquivos gerados pelo comando *make* para o caminho informado através do parâmetro *--prefix* do *script* de *configure*.

Collectd

O collectd é um agente de monitoramento bastante utilizado atualmente. Foi escrito visando consumir o mínimo de recursos possíveis. Para monitorar os recursos é preciso utilizar outros recursos, por isso o coletor de dados deve ser o mais leve possível. O collectd e a maioria dos *plugins* foram escritos na linguagem de programação C, portanto utilizam pouco recurso do servidor monitorado. O usuário pode ter um servidor para gerar os gráficos ou então o próprio servidor monitorado pode gerar os gráficos. Deve-se avaliar bem a segunda alternativa, pois gerar gráficos usa muitas operações de escrita em disco.

Seguem algumas características do collectd:

- Possui um escalonador próprio. Deste modo, não tem aquele velho conhecido problema do *cron* de não rodar os *scripts* ou de precisar de um sistema de automação pago;
- Possui muitos *plugins* para monitorar diversos serviços. Exemplos: httpd, nginx, mysql, oracle, smtp etc.

O collectd é uma ferramenta muito bem documentada. No *wiki* (*http://collectd.org/wiki/index.php*) encontra-se uma explicação detalhada sobre cada funcionalidade, ou seja, cada item de configuração e *plugin* disponível.

Preparar a instalação

Este é um ponto crucial. Aqui o usuário deve preparar seu sistema, ou seja, habilitar todos os *plugins* que utilizará. Por padrão, o *script ./configure* do collectd tenta compilar todos os *plugins*, porém ele só habilitará os *plugins* cujo as bibliotecas necessárias estiverem disponíveis.

Com os pacotes instalados anteriormente, nem todos os *plugins* estarão habilitados, pois nem todas as bibliotecas necessárias para a compilação dos *plugins* estão instaladas. Instale o pacote de acordo com o plugin que quer habilitar conforme a **Tabela 3**.

Plugin	Pacote
Generic	libgcrypt-devel e libxml2-devel
apache, ascent, bind, curl, curl_xml, nginx e write_http	curl-devel
Dbi	libdbi-devel
MySQL	MySQL-devel
DNS	libpcap-devel
Libvirt	libvirt-devel
Sensors	lm_sensors-devel
SNMP	net-snmp-devel
notify_desktop	libnotify-devel e gtk2-devel
PostgreSQL	postgresql84-devel
Python	python-devel

Tabela 3. Plugins e pacotes

Após instalar todas as bibliotecas necessárias, execute a sequência de comandos da **Listagem 2**. Se nunca usou o *CPAN* e não sabe

configurá-lo, quando for executá-lo pela primeira vez, ele solicitará as informações necessárias para funcionar. Assim, basta escolher sempre a resposta padrão que já vem informada no *prompt*. CPAN (*www.cpan.org*) é onde se encontram todos os códigos e módulos Perl.

Listagem 2. Instalando o collectd.

```
# cd /usr/src
# wget http://collectd.org/files/collectd-5.0.1.tar.gz
# tar xzvf collectd-5.0.1.tar.gz
# cd collectd-5.0.1
# ./configure --prefix=/opt/collectd-5.0.1 --enable-debug --with-librrd=/
    opt/rrdtool-1.4.7
# make && make install
# mkdir /opt/collectd-5.0.1/contrib
# cp /usr/src/collectd-5.0.1/contrib/redhat/init.d-collectd /opt/collectd-5.0.1/contrib/
# sed -i 's/\/etc\/collectd.conf/\/opt\/collectd\/etc\/collectd.conf/g' /opt/
  collectd-5.0.1/contrib/init.d-collectd
# sed -i 's/\/usr\/sbin\/collectd/\/opt\/collectd\/sbin\/collectd/g' /opt/
  collectd-5.0.1/contrib/init.d-collectd
# # sed -i 's/\"collectdmon\"/\/opt\/collectd\/sbin\/collectdmon/g' /opt/
  collectd-5.0.1/contrib/init.d-collectd
# perl -MCPAN -e'install HTML::Entities, Config::General, URI::Escape, Regexp::Common'
# tar czvf perl-HTML-Entities.tar.gz /usr/lib64/perl5/site_perl/5.8.8/x86_64-linux-
  thread-multi/HTML/Entities.pm
# tar czvf perl-Config-General.tar.gz /usr/lib/perl5/site_perl/5.8.8/Config/General /
  usr/lib64/perl5/site_perl/5.8.8/x86_64-linux-thread-multi/auto/Config/General /
  usr/lib/perl5/site_perl/5.8.8/Config/General.pm
# tar czvf perl-URI-Escape.tar.gz /usr/lib/perl5/site_perl/5.8.8/URI/Escape.pm
# tar czvf perl-Regexp-Common.tar.gz /usr/lib/perl5/site_perl/5.8.8/Regexp/
  Common /usr/lib64/perl5/site_perl/5.8.8/x86_64-linux-thread-multi/auto/
  Regexp/Common /usr/lib/perl5/site_perl/5.8.8/Regexp/Common.pm
# tar czvf perl-HTML-Parser.tar.gz /usr/lib64/perl5/site_perl/5.8.8/x86_64-linux-
  thread-multi/HTML/Parser.pm /usr/lib64/perl5/site_perl/5.8.8/x86_64-linux-
  thread-multi/auto/HTML/Parser
# cd /usr/src/collectd-5.0.1/contrib/
# tar czvf /opt/collection3.tar.gz collection3
```

Os gráficos que serão gerados pelo collectd serão armazenados em um RRD. Devido à forma de armazenamento do RRD para visualizar os gráficos, precisa-se de um sistema *front-end*, ou seja, um sistema para nos mostrar os dados que o collectd está coletando. Existem vários atualmente, como *collection3*, *collectgraph*, *heymon*, entre outros. Neste artigo aborda-se o collection3.

Enviando os arquivos para outros servidores

Após compilar e instalar o collectd, deve-se copiar os arquivos para o servidor que executará a tarefa. Para isso, crie um arquivo compactado no formato *tar* de cada sistema instalado, ou seja, RRDtool, collectd e collection3. Execute a lista de comandos da **Listagem 3**.

Listagem 3. Copiando arquivos para servidor e cliente.

```
# cd /opt
# tar czvf rrdtool-1.4.7.tar.gz rrdtool-1.4.7/
# scp rrdtool-1.4.7.tar.gz 10.211.55.10:/opt/
# tar czvf collectd-5.0.1.tar.gz collectd-5.0.1
# scp collectd-5.0.1.tar.gz 10.211.55.10:/opt/
# scp collection3.tar.gz perl-* 10.211.55.10:/opt/
# scp collectd-5.0.1.tar.gz 10.211.55.11:/opt/
```

O leitor realizou as seguintes atividades: entrou no diretório onde os arquivos foram instalados, compactou os arquivos do RRDtool e copiou o *tar* para o servidor de monitoramento, *server01*. Depois, fez a mesma coisa com o collectd e enviou para ambos os servidores, *client01* e *server01*. O *builder01* é o servidor onde gera-se os pacotes, portanto não se deve copiar nada para ele.

Configurando client01

O *client01* será o servidor monitorado. Portanto instale o collectd e configure o envio dos dados para o *server01*. Para isso, execute a sequência de comandos da **Listagem 4**.

Listagem 4. Configurando collectd no cliente.

```
# cd /opt
# tar xzvf collectd-5.0.1.tar.gz
# ln -s /opt/collectd-5.0.1 /opt/collectd
# ln -s /opt/collectd/contrib/init.d-collectd /etc/init.d/collectd
# vi /opt/collectd/etc/collectd.conf
```

Crie um *link* simbólico para organização dos seus pacotes, utilizando o comando *ln*, de acordo com a **Listagem 4**. Muitas vezes é preciso manter duas ou mais versões do sistema no servidor, geralmente em caso de atualização. Assim, deve-se apontar o *script* de inicialização do collectd para o caminho especificado no *link* simbólico.

Dessa forma, não será preciso fazer atualizações do *script* de inicialização somente por causa de uma atualização de versão do collectd, pois o nome do *link* simbólico permanecerá o mesmo, apesar da alteração da versão. Outra vantagem de criar o *link* simbólico é que o usuário saberá mais facilmente qual versão está em funcionamento.

É importante destacar que neste texto, apenas os principais parâmetros do arquivo de configuração do collectd são abordados. Porém existem muitas outras funcionalidades que podem ser conhecidas no arquivo de configuração e também no *wiki* (*http://collectd.org/wiki/index.php*).

Neste momento o arquivo do collectd deve ser editado com os seguintes parâmetros:

- **#Interval 10:** indica o intervalo de coleta. Vem comentado, pois o intervalo padrão é de 10 segundos. Neste caso altere para 60 segundos, ou seja, um minuto e remova o comentário;
- **#ReadThreads 5:** Indica a quantidade de *threads* que o collectd utilizará para fazer as coletas. Nesse caso não se deve alterar;
- **LoadPlugin syslog:** Vem habilitado por padrão. Comente a linha, pois o *log* será específico, ou seja, ao invés de enviar os logs para o syslog, vamos criar um arquivo separado. Desta forma fica mais fácil verificar os logs;
- **#LoadPlugin logfile:** Vem desabilitado por padrão, remova o comentário para habilitá-lo. A configuração do plugin ficará conforme apresentado na **Listagem 5** e a explicação dos parâmetros aparece a seguir:

– **LogLevel:** *debug*, *info* ou *error*. *Debug* para imprimir todos os logs; *info* para imprimir *logs* informativos e de erros; e *error* para apenas imprimir *logs* de erros;

– **File:** Arquivo onde será gerado o log. As aspas duplas não devem ser esquecidas;
– **Timestamp:** *true* ou *false*. Imprimir ou não a data no log. Para conseguir investigar problemas ou erros são necessárias as informações da data no *log*;
– **PrintSeverity:** *true* ou *false*. Imprimir ou não loglevel no arquivo de log.

Em seguida retire os comentários de alguns plugins, removendo o caractere **#**:
• **#LoadPlugin *contextswitch*:** Vem desabilitado por padrão, mas deve ser habilitado. Esse *plugin* monitora a troca de contexto da CPU. Não é necessária nenhuma configuração;
• **#LoadPlugin df:** Vem desabilitado por padrão, mas deve ser habilitado. Este *plugin* monitora todos os sistemas de arquivos. Não é necessária nenhuma configuração;
• **#LoadPlugin disk:** Vem desabilitado por padrão, mas deve ser habilitado e configurado conforme a **Listagem 6**. Este *plugin* monitora os discos, quantidade de *IOPS*, *response time* etc.;
• **#LoadPlugin network:** Vem desabilitado por padrão, mas deve ser habilitado e configurado conforme a **Listagem 7**. Esse é o plugin que envia os dados para o servidor;
• **#LoadPlugin swap:** Vem desabilitado por padrão, mas deve ser habilitado. Esse *plugin* monitora o swap;
• **# LoadPlugin protocols:** Vem desabilitado por padrão, mas deve ser habilitado. Esse *plugin* monitora os protocolos de rede (*TCP, UDP, ICMP* etc.);
• **#LoadPlugin tcpconns:** Vem desabilitado por padrão, mas deve ser habilitado. Esse *plugin* monitora a quantidade de conexões por determinado estado (*established, listen, time_wait* etc.);
• **#LoadPlugin uptime:** Vem desabilitado por padrão, mas deve ser habilitado. Esse *plugin* monitora o tempo que o sistema operacional está ligado;
• **#LoadPlugin users:** Vem desabilitado por padrão, mas deve ser habilitado. Esse *plugin* monitora a quantidade de usuários com sessão aberta no servidor.

Listagem 5. Configuração do plugin logfile.

```
<Plugin logfile>
 LogLevel info
 File "/opt/collectd/var/log/collectd.log"
 Timestamp true
 PrintSeverity true
</Plugin>
```

Listagem 6. Configuração do Plugin disk.

```
<Plugin disk>
 Disk "/^[h|s]d[a-f][0-9]?$/"
 # IgnoreSelected false
</Plugin>
```

Listagem 7. Configuração do plugin network cliente.

```
<Plugin network>
 # cliente setup:
 Server "10.211.55.10" "25566"
</Plugin>
```

O arquivo que está sendo editado deve ser salvo como *collectd.conf*.

Demonstra-se a seguir algumas configurações adicionais que podem ser aplicadas no arquivo *collectd.conf*, se desejar monitorar o serviço.

O Postfix, por exemplo, é um sistema de e-mail bastante completo e utilizado. Observe a **Listagem 8** para verificar como monitorar uma fila de e-mails. Além disso, adicione o texto *LoadPlugin filecount* no arquivo *collectd.conf*.

O banco de dados MySQL é atualmente utilizado por empresas de grande porte e diversas soluções de código aberto. Observe a **Listagem 9** para configurar o monitoramento da instância MySQL. Além disso, adicione o texto *LoadPlugin mysql* no arquivo *collectd.conf*.

Listagem 8. Monitorando a fila do postfix.

```
<Plugin filecount>
 <Directory "/var/spool/postfix/active/">
  Instance "active"
 </Directory>
 <Directory "/var/spool/postfix/bounce/">
  Instance "bounce"
 </Directory>
 <Directory "/var/spool/postfix/corrupt/">
  Instance "corrupt"
 </Directory>
 <Directory "/var/spool/postfix/deferred/">
  Instance "deferred"
 </Directory>
 <Directory "/var/spool/postfix/incoming/">
  Instance "incoming"
 </Directory>
 <Directory "/var/spool/postfix/hold/">
  Instance "hold"
 </Directory>
</Plugin>
```

Listagem 9. Monitorando o MySQL.

```
<Plugin mysql>
 <Database mysql>
  Database "mysql"
 </Database>
</Plugin>
```

Conforme mencionado anteriormente, o serviço de NTPD é responsável pelo sincronismo do horário. Para habilitar sua monitoração, adicione a linha abaixo no arquivo de configuração do collectd:

```
LoadPlugin ntpd
```

Para concluir, é importante monitorar os processos do sistema operacional. Observe na **Listagem 10** um exemplo de configuração do plugin para isso. Em seguida, insira o texto *LoadPlugin processes* no arquivo *collectd.conf*.

Até este momento, apenas algumas configurações prévias necessárias foram feitas para que o serviço do collectd funcione adequadamente. Agora é preciso definir como o collectd será

instanciado quando a máquina monitorada for inicializada. Isso é feito ao se executar a sequência de comandos da **Listagem 11**.

Listagem 10. Monitorando processos do SO.

```
<Plugin processes>
 Process "klogd"
 Process "syslogd"
 Process "portmap"
 Process "crond"
 Process "sshd"
 Process "httpd"
 Process "mysqld"
 Process "mysqld_safe"
 Process "ntpd"
 Process "collectdmon"
 Process "collectd"
</Plugin>
```

Listagem 11. Inicialização do collectd cliente.

```
# chmod +x /etc/init.d/collectd
# /etc/init.d/collectd start
# tail -f /opt/collectd/var/log/collectd.log
# chkconfig --add collectd
# chkconfig --list collectd
```

Segue a explicação dos comandos executados:

1. Adição da permissão de execução para o *script* de inicialização do collectd;
2. Inicialização do *daemon*;
3. Leitura das últimas linhas do arquivo e apresentação das próximas linhas escritas. Com isso verifica-se a ocorrência de algum erro durante o processo de inicialização do collectd;
4. Adição do script de inicialização do collectd para ser executado no *boot* do servidor;
5. Listagem dos *run level* e verificação se o script é executado ou não.

Configurando server01

O servidor *server01* será o servidor de monitoramento. Ele receberá os dados do collectd cliente para gerar os gráficos e fazer o monitoramento. Execute a sequência de comandos da **Listagem 12** para configurar o RRDtool. O conteúdo do arquivo */etc/init.d/rrdcached* é apresentado na **Listagem 13**. Este arquivo é o script de inicialização do rrdcached. Não vem disponível no código fonte, por isso disponibiliza-se um caso necessite.

Conforme o parâmetro *–w* (em segundos) contido no *script* de inicialização, os gráficos serão atualizados a cada vinte minutos. Deve-se adequá-lo conforme o ambiente a se monitorar. Se o intervalo for pequeno, a quantidade de entrada e saída (I/O) gerada pelo collectd não diminuirá muito. Se for muito alto demorará muito para ver os gráficos.

A configuração inicial do collectd será exatamente igual aos passos da configuração do cliente. Portanto, deve-se executar a sequência de comandos da **Listagem 4** até a parte de editar o arquivo *collectd.conf*. Vamos então conhecer o que difere a partir deste ponto.

Listagem 12. Configuração do RRDtool no servidor.

```
# cd /opt
# tar xzvf rrdtool-1.4.7.tar.gz
# ln -s /opt/rrdtool-1.4.7 /opt/rrdtool
# vi /etc/init.d/rrdcached
# chmod +x /etc/init.d/rrdcached
# /etc/init.d/rrdcached start
# /etc/init.d/rrdcached status
# chkconfig --add rrdcached
# chkconfig --list rrdcached
```

Listagem 13. Arquivo de inicialização do rrdcached.

```
#!/bin/bash
#
# by Thiago Nache > thiago.borges@tivit.com.br || thiagonbcarvalho@gmail.com
# 20111229
#
# chkconfig: 2345 15 85
# description: script to management rrdcached
# processname: rrdcached
# enviroment
RRDCACHEDBIN="/opt/rrdtool/bin/rrdcached"
RRDCACHEDPARAMS=" -l /var/run/rrdcached.sock -w 1200 -z 480 -t 36 -F > /dev/
null 2>&1"
# source function library
. /etc/init.d/functions
RETVAL=0
start() {
 echo -n $"Starting rrdcached service: "
 if [ ! -x ${RRDCACHEDBIN} ];
 then
  echo -n $"Cannot execute rrdcached bin: ${RRDCACHEDBIN}!"
 fi

 daemon "${RRDCACHEDBIN} ${RRDCACHEDPARAMS}"
 RETVAL=$?
 echo
}

stop() {
 echo -n $"Shutting down rrdcached service: "
 killproc ${RRDCACHEDBIN}
 RETVAL=$?

 echo
}

case "$1" in
 start)
  start
  ;;
 stop)
  stop
  ;;
 restart|reload)
  stop
  sleep 2
  start
  ;;
 status)
  status ${RRDCACHEDBIN}
  RETVAL=$?
  ;;
 *)
  echo $"Usage: $0 {start|stop|restart|status}"
  exit 1
esac

exit $RETVAL
```

Resumindo, a diferença da configuração do collectd é que os *plugins* UnixSock e rrdcached são carregados (eles não são utilizados na configuração do cliente) e o *plugin* network terá configuração diferente. Ao invés de informar o servidor, cria-se uma porta em estado de receber conexão (*listening*).

O plugin UnixSock é necessário para conseguir ler os dados do collectd *server*. Observe a configuração do mesmo na **Listagem 14**. Para concluir esta etapa, adicione *LoadPlugin unixsock* no arquivo *collectd.conf*.

Listagem 14. Configuração do plugin unixsock.

```
<Plugin unixsock>
 SocketFile "/var/run/collectd-unixsock"
 SocketGroup "root"
 SocketPerms "0666"
 # DeleteSocket false
</Plugin>
```

Analisando os parâmetros:

- **SocketFile:** Indica o caminho onde o socket será criado;
- **SocketGroup:** Indica o grupo que é o dono do arquivo;
- **SocketPerms:** Indica a permissão do socket.

O plugin rrdcached, por sua vez, armazenará os dados do RRD em memória cache. Observe a **Listagem 15** para saber como configurá-lo. Para findar esta etapa, adicione *LoadPlugin rrdcached* no arquivo *collectd.conf*.

Listagem 15. Configuração do plugin rrdcached.

```
<Plugin rrdcached>
 DaemonAddress "unix:/var/run/rrdcached.sock"
 DataDir "/opt/collectd-5.0.1/var/lib/collectd/rrd"
 CreateFiles true
 CollectStatistics true
</Plugin>
```

Analisando os parâmetros:

- **DaemonAddress:** Indica o caminho para o *socket*. Esse caminho deve ser o mesmo que o do *script* de inicialização do rrdcached;
- **DataDir:** Indica o diretório onde os rrds serão criados;
- **CreateFiles:** *true* ou *false*. Sempre configure como *true*, pois do contrário os arquivos nunca serão criados;
- **CollectStatistics:** *true* ou *false*. Opção para gerar ou não os gráficos de estatísticas do rrdcached.

Já no plugin network, configura-se o endereço IP e a porta que o collectd irá receber as conexões. A configuração do mesmo é apresentada na **Listagem 16**. Assim como realizado nos passos anteriores, adicione *LoadPlugin network* no arquivo *collectd.conf*.

Como mencionado anteriormente, será necessário um *front-end* para exibir os gráficos. Dessa forma, para configurar o collection3, execute a sequência de comandos da **Listagem 17**. O conteúdo do arquivo */etc/httpd/conf.d/colletion3* é exibido na **Listagem 18**.

Listagem 16. Configuração do plugin network servidor.

```
<Plugin network>
 # server setup:
 Listen "10.211.55.10" "25566"
</Plugin>
```

Listagem 17. Configurando o collection3 no servidor.

```
# yum -y install httpd
# vi /etc/httpd/conf.d/collection3
# cp -r /opt/collectd-5.0.1/lib/perl5/site_perl/5.8.8/Collectd /usr/lib/perl5/
  site_perl/5.8.8/
# cp -r /opt/rrdtool-1.4.7/lib/perl/5.8.8/x86_64-linux-thread-multi/* /usr/lib/perl5/
site_perl/5.8.8/
# cd /opt
# tar xzvf perl-HTML-Entities.tar.gz -C /
# tar xzvf perl-HTML-Parser.tar.gz -C /
# tar xzvf perl-Config-General.tar.gz -C /
# tar xzvf perl-URI-Escape.tar.gz -C /
# tar xzvf perl-Regexp-Common.tar.gz -C /
# tar xzvf collection3.tar.gz -C /var/www/html/
# chown -R apache: /var/www/cgi-bin/collection3/
# echo "DataDir \"/opt/collectd-5.0.1/var/lib/collectd/rrd\"" >> /var/www/cgi-bin/
  collection3/etc/collection.conf
# echo "UnixSockAddr \"/var/run/collectd-unixsock\"" >> /var/www/cgi-bin/
  collection3/etc/collection.conf
```

Listagem 18. Configuração do collection3 para o httpd.

```
<Directory "/var/www/html/collection3/bin/">
 AllowOverride None
 Options +ExecCGI
 Order allow,deny
 Allow from all
</Directory>
```

Nestas listagens instala-se o Apache httpd através do *yum*, configura-se um virtual host para o collection3 e descompacta-se as bibliotecas Perl.

Conclusão

Por fim, se todas as configurações e comandos sugeridos foram realizados com sucesso, o browser apresentará os gráficos quando apontado para o endereço *http://10.211.55.10/cgi-bin/collection3/bin/index.cgi*. Lembre-se de considerar o tempo de atualização do rrdcached, pois configuramos para atualizar a cada 20 minutos.

Pronto, o monitoramento passivo está finalizado. Os dados já estão sendo monitorados e disponibilizados. Para completar sua infraestrutura de monitoramento, os próximos passos são analisar o ambiente para definir os *thresholds* e configurar um software para gerar os alertas.



Thiago Nache
thiagonbcarvalho@gmail.com
Atua na área de infraestrutura há mais de 8 anos, tem grande experiência em sistema de alta disponiblidade e alta performance. Cursou ensino médio técnico em processamento de dados, graduação em Tecnologia em Redes de Computadores na FIAP e possui certificação Red Hat e ITIL. Tem experiência em empresas de grande porte.

Monitoramento de infraestrutura com Zabbix

Mário de Mello Bittencourt Neto

Resumo DevMan

De que se trata o artigo:

Este apresenta como implantar uma ferramenta de monitoramento de infraestrutura usando a solução Zabbix.

Em que situação o tema é útil:

Em um ambiente de TI com vários sistemas operacionais, servidores e serviços, saber como eles estão se comportando e ser avisado preventivamente ajuda a intervir antes que problemas maiores se apresentem.

Monitoramento de infraestrutura com Zabbix:

A infraestrutura de TI (Tecnologia da Informação) corresponde às plataformas de hardware, telecomunicações, redes, instalações físicas e pessoas necessárias para exercerem os papéis e responsabilidades relativos à TI. Neste contexto, este artigo apresenta uma ferramenta que oferece um serviço distribuído de monitoramento, possibilitando o acompanhamento e a geração de alertas e relatórios para auxiliá-lo na gestão e a fazer intervenções em sua infraestrutura de TI.

"Você não pode gerenciar o que não pode medir". Esta frase, presente em qualquer livro sobre gerência, joga luz sobre um assunto que muitos responsáveis pela infraestrutura de suas empresas por vezes desconhecem: Como está a minha estrutura/rede/serviço?

Responder a esta pergunta é cada vez mais difícil por que nossas redes e serviços são cada vez mais complexos e não raramente envolvem plataformas (Windows, Mac, Linux), versões (Vista, 7, 2008, Ubuntu, CentOS), serviços (bancos de dados, servidores web) e dispositivos (servidores, roteadores, switches) diferentes.

A infraestrutura de TI corresponde às plataformas de hardware, telecomunicações, redes, instalações físicas e pessoas necessárias para exercerem os papéis e responsabilidades relativos à TI. Uma vez que estabelecemos a arquitetura de TI, que é o desenvolvimento do modelo de dados corporativo e ainda dos serviços necessários para atender os requisitos de negócio e o alcance dos objetivos definidos para o mesmo, podemos então passar para a definição do hardware, dos recursos de TIC e das habilidades e capacidades que são necessárias para que a infraestrutura possa ser operada e produza os resultados esperados.

Após a definição da infraestrutura de TI de uma organização, podemos agora tratar das necessidades de recursos humanos necessários para a gestão, operação e manutenção dos demais itens que compõemtal infraestrutura. Além disto, se ainda não conhecemos os requisitos do negócio, torna-se difícil a definição das habilidades e capacidades que precisamos contratar ou desenvolver, além de planejar o aperfeiçoamento das mesmas ao longo do ciclo de vida da infraestrutura. Além disso, aliado às pessoas, precisamos também definir quais ferramentas de apoio poderão ser utilizadas no apoio às atividades de manutenção da infraestrutura de TI.

Neste contexto, neste artigo apresentaremos uma ferramenta que se propõe a oferecer um serviço distribuído de monitoramento, sendo capaz de acompanhar e gerar alertas e relatórios para auxiliá-lo na gestão e a fazer intervenções na sua infraestrutura de TI.

O cenário

A realidade das empresas hoje já envolve a necessidade de gerir diferentes itens de TI, como:

- Acesso à Internet (talvez mais de um provedor por questão de redundância);
- Servidor de arquivos (um Linux com Samba ou Windows com Active Directory/Servidor de domínio);
- Servidor de hospedagem do site/e-mail/banco de dados (hospedado na própria rede ou na nuvem – ler **Nota DevMan 1**);
- VPN ligando a empresa com filiais ou clientes (ler **Nota DevMan 2**).

Como gestor você precisa saber como cada um dos componentes acima está se comportando e deseja ser informado de eventuais problemas que aconteçam.

Os problemas de gerenciar esta infraestrutura começam a surgir quando você percebe que cada fornecedor pode ou não disponibilizar um software de monitoramento, e quando faz, você precisa acessar vários programas (específicos de cada componente de sua infraestrutura) para obter as informações desejadas.Como resolver isso?

A solução

A solução para suprir essa falta de integração é usar uma ferramenta que permita coordenar a obtenção dos dados e unificá-los sob a forma de um controle único.

Existem várias alternativas no mercado que prometem fornecer essa integração, como o HP Operations Manager (ler **Nota DevMan 3**) ou o IBM Tivoli (ler **Nota DevMan 4**). Entretanto, estas ferramentas possuem um custo de implantação e manutenção elevados, o que os torna proibitivos para muitas empresas.



Nota do DevMan 1

Computação em Nuvem

O conceito de computação em nuvem (em inglês, cloudcomputing) refere-se à utilização da memória e das capacidades de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet, seguindo o princípio da computação em grade.

O armazenamento de dados é feito em serviços que poderão ser acessados de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da Internet – daí a alusão à nuvem.



Nota do DevMan 2

VPN: Rede Privada Virtual é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros.

VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.



Nota do DevMan 3

HP Operations Manager: O HP Operations Manager monitora a infraestrutura de TI e consolida e correlaciona eventos de falhas e desempenho para ajudar a identificar as causas dos incidentes de TI. Para isso, o HP Operations Manager fornece um console de monitoramento único para infraestruturas virtuais e em nuvem.



Nota do DevMan 4

IBM Tivoli: O Gerenciamento de Serviços IBM oferece soluções interessantes para você planejar, construir e gerenciar uma infraestrutura dinâmica que viabiliza a melhoria dos serviços, a redução de custos e o gerenciamento de riscos. Para exemplificar temos o IBM MaximoAsset Management, que é um sistema de software que fornece suporte abrangente para suas necessidades de gerenciamento de cadeia de suprimentos de ativos, manutenção, recursos e peças.

O Tivoli permite que você gerencie seus serviços, aplicativos e processos operacionais de TI críticos com base nas prioridades dos negócios, fornecendo visibilidade, controle e automação para uma infraestrutura de serviço continuamente otimizada.

Entram então em cena soluções *open-source*, das quais o Zabbix (ver link de acesso na seção **Links**) se destaca por ser uma solução completa e escalávelconsiderando milhares de recursos monitorados.

Dentre as funcionalidades oferecidas pelo Zabbix destacamos:

- Descoberta automática de servidores e dispositivos de rede;
- Monitoramento distribuído e administração via web centralizada;
- Servidor com suporte de software para vários sistemas operacionais, tais como Linux, Solaris, HP-UX, AIX, FreeBSD, Open BSD, OS X;
- Agentes de monitoramento para Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OSX, Tru64/OSF1, Windows NT4.0, Windows 2000, Windows 2003, Windows XP e Windows Vista;
- Autenticação de usuários;
- Sistema de permissões de acesso flexíveis;
- Controle de notificação por e-mail na ocorrência de eventos;
- Logs para auditoria.

Uma característica adicional interessante é a relativa baixa exigência que o Zabbix tem quanto ao hardware necessário para seu uso. O desenvolvedor da solução sugere como referência os valores abaixo:

- Pequenas instalações (até 20 elementos monitorados) –Ubuntu Linux, PII 350Mhz, 256 MB RAM e MySQL (MyISAM);
- Médias instalações (até 500 elementos monitorados) –Ubuntu Linux 64Bits, AMD Athlon 3200+, 2 GB RAM e MySQL (InnoDB);
- Grandes instalações (acima de 1000 elementos monitorados) –Ubuntu Linux 64Bits, Intel dual core 6400, 4 GB RAM e RAID10 MySQL (InnoDB) ou PostgreSQL;
- Instalações muito grandes (acima de 10000 elementos monitorados) –RedHat Enterprise, 2x Intel Xeon, 8 GB RAM e RAID10 MySQL (InnoDB) ou PostgreSQL.

O ambiente de testes

Seria impossível cobrir todas as funcionalidades ou possibilidades de uso do Zabbix em um artigo. Sendo assim, para exemplificar o uso do Zabbix nosso ambiente irá monitorar:

- Um serviço Web Apache;
- Um serviço de banco de dados MySQL;
- A carga da CPU do servidor;
- Um *gateway* para acesso a Internet no endereço 10.0.0.1.

Com isso, iremos acompanhar como monitorar a disponibilidade de serviços (MySQL, WWW), a conexão à Internet e a performance do servidor.

Para tornar o monitoramento possível, seguiremos aqui um conjunto de etapas que serão discutidas nas próximas seções. De forma resumida, nosso trabalho será desenvolvido considerando os seguintes passos:

- **Passo 1 – Instalação do Servidor Zabbix:** aqui efetuaremos a instalação do servidor Zabbix de forma que possamos dar início à sua configuração;
- **Passo 2 – Configuração do Servidor:** uma vez que os programas do Zabbix tenham sido compilados e instalados no passo anterior, trabalharemos nesta etapa com a configuração de alguns parâmetros do servidor;
- **Passo 3 – Configuração da Interface Web de Monitoramento:** nesta etapa veremos como configurar a interface web para facilitar nossas atividades de monitoramento da infraestrutura;
- **Passo 4 – Configurando o monitoramento:** nesta etapa definiremos os itens que serão monitorados em nossa infraestrutura de TI;
- **Passo 5 – Acessando os dados monitorados:** esta é a última etapa, onde veremos como acessar os dados coletados pelo Zabbix.

Passo 1 –Instalação do servidor Zabbix

Em nosso estudo de caso, utilizaremos um servidor Linux, com distribuição CentOS 6 com o Apache, PHP e MySQL instalados

para servir de base para o Zabbix realizar o monitoramento e consulta.

Como pré-requisitos para a instalação você deve se certificar que os pacotes abaixo estão instalados no servidor:

- Apache;
- Mysql-server;
- PHP;
- Php-mbstring;
- Php-mysql;
- GCC;
- Net-snmp-devel;
- Libcurl-devel.

A instalação do sistema operacional e dos serviços mencionados acima está fora do escopo deste artigo.

O primeiro passo da instalação do Zabbix consiste em obter os fontes do Zabbix. A versão atual é a 1.8.6 e pode ser obtida em *http://prdownloads.sourceforge.net/zabbix/zabbix-1.8.6.tar.gz?download*.

Você deve descompactar o pacote obtido executando o comando apresentado abaixo:

```
#tar -zxvf zabbix-1.8.6.tar.gz
```

Este comando irá criar uma pasta *zabbix-1.8.6* na qual você poderá compilar o código-fonte.

O segundo passo consistirá em criar o banco de dados e as estruturas de dados para o Zabbix. Para isso, siga os comandos da **Listagem 1**. Perceba que na **Listagem 1**inicialmente criamos o banco dados *zabbix* e definimos o conjunto de caracteres válidos para utf8. Na sequência, criamos o esquema do banco de dados considerando para isso o script disponibilizado na pasta do Zabbix.

Criada a estrutura de dados, no terceiro passo faremos a compilação do Zabbix. Na **Listagem 2** vemos os comandos que devem ser executados.

Listagem 1. Criando o banco de dados zabbix e estruturas de dados.

```
# cd zabbix-1.8.6
# mysql
mysql> create database zabbix character set utf8;
mysql> quit;
# cd create/schema/
# mysql zabbix < mysql.sql
# cd ../data
# mysql zabbix < data.sql
# mysql zabbix < images_mysql.sql
```

Listagem 2. Compilando o servidor.

```
# cd ../..
# ./configure --enable-server --enable-agent --with-mysql --with-net-snmp --
  with-libcurl
# make
# make install
```

No final deste processo teremos compilado e instalado os programas necessários em */usr/local/bin* e */usr/local/sbin*.

O quarto passo consistirá em criar o usuário zabbix no sistema operacional. Isso é necessário por que o Zabbix não pode ser executado com privilégios de *root*. Para criar o usuário zabbix, observe o código abaixo:

```
#useradd zabbix
```

Por fim, para finalizarmos a instalação do Zabbix, devemos copiar os arquivos da interface web de monitoramento. Isto deve ser feito conforme código apresentado na **Listagem 3**.

Passo 2 –Configuração inicial do servidor

Uma vez que os programas do Zabbix foram compilados e instalados, você precisa realizar a configuração do servidor. Como modelo, existe um arquivo de exemplo que vem com o pacote do código-fonte que foi obtido na etapa anterior.

Iremos usar esse arquivo e modificá-lo de acordo com anossa necessidade.Apenas um pequeno número de configurações será feita no arquivo, já que os monitores, alertas e o funcionamento em si do Zabbix serãocriados através de uma interface web própria que veremos em breve. Na **Listagem 4** fazemos a cópia do arquivo de configuração inicial.

Listagem 3. Copiando os arquivos da interface web.

```
# mkdir /var/www/html/zabbix
# cd frontends/php/
# cp -a . /var/www/html/zabbix
```

Listagem 4. Copiando o arquivo de configuração padrão.

```
# mkdir /etc/zabbix
# cp misc/conf/zabbix_server.conf /etc/zabbix
# cp misc/conf/zabbix_agentd.conf /etc/zabbix
```

Como vimos anteriormente, por questões de segurança o Zabbix não aceitará ser executado com privilégios de *root*(por isso você precisou criar o usuário zabbix). Neste sentido, precisamos agora editar o arquivo de configuração e alterar os parâmetros conforme a **Listagem 5**.

Você deverá usar na variável *DBUser* o nome do usuário que terá acesso ao banco de dados, por padrão *root*,e em *DBPassword* qual a senhadeste usuário. Caso você não tenha alterado a senha padrão do MySQL, você deve deixar em branco o campo *DBPassword*. Em seguida você pode iniciar o servidor conforme a **Listagem 6**.

Listagem 5. Configurando o usuário esenha do banco de dados.

```
# vi /etc/zabbix/zabbix_server.conf
DBUser=root
DBPassword=senha
```

Listagem 6. Iniciando o servidor Zabbix.

```
# /usr/local/sbin/zabbix_server
# /usr/local/sbin/zabbix_agentd
```

Neste momento o servidor Zabbix já está operacional, apesar de não estar monitorando nenhum recurso. Você deverá agora configurar a interface de monitoramento web.

Passo 3 –Configurando a interface web de monitoramento do servidor

Durante a instalação do servidor foram copiados os arquivos de interface web. Utilizar a interface web para monitoramento é uma boa prática uma vez que ela irá facilitar e muito nossas atividades como administrador da infraestrutura de TI.

Porém, antes que você possa usar a interface web é preciso verificar se o PHP está configurado com os requisitos mínimos necessários pelo Zabbix. Para configurar a interface web de monitoramento, edite o arquivo */etc/php.ini* de maneira que as variáveis estejam pelo menos com os valores apresentados na **Listagem 7**.

Conforme a**Listagem 7**, definimos que o tamanho máximo será de 32M e os tempos máximos de execução e entrada serão de 600.

Como parte do processo de configuração da interface será necessário ainda dar permissão para que o servidor web possa criar e alterar arquivos de configuração.Para isso, execute os comandos apresentados na **Listagem 8**.

Listagem 7. Parâmetros mínimos do PHP.

```
#vi /etc/php.ini
post_max_size = 32M
max_execution_time = 600
max_input_time = 600
```

Listagem 8. Alterando permissão para os arquivos de configuração.

```
# chown apache /var/www/html/zabbix/conf/
# chmod g+rwx /var/www/html/zabbix/conf/
```

Feito isso, agora você pode abrir o seu navegador e digitar o endereço *http://localhost/zabbix*. Ele irá mostrar a tela de início de instalação da ferramenta visual de monitoramento. Nesta tela, clique na opção *Next*.

A tela seguinte basicamente exibe a licença de uso. Você deverá marcar a opção *I agree*e mais uma vez selecionar a opção *Next*.

O Zabbix irá fazer então uma verificação de pré-requisitos do sistema (**Figura 1**). Se todas as variáveis analisadas possuírem ao menos os valores mínimos necessários, o assistente de instalação irá indicar com OK ao lado de cada pré-requisito e habilitar a opção *Next*.

Caso algum pré-requisito não esteja satisfeito ele não irá habilitar a opção de avançar. Se este for o caso, você deve verificar os valores indicados e recarregar a página.

Você deverá agora configurar a conexão com o banco de dados. Informe o *User* e *Password* de acordo com os utilizados em */etc/zabbix/zabbix_server.conf* – veja a **Figura 2**. Clique em *Test Connection* e se ele apresentar o OK, clique em *Next*. Caso não seja possível efetuar a conexão com o banco, verifique se os parâmetros informados estão corretos.

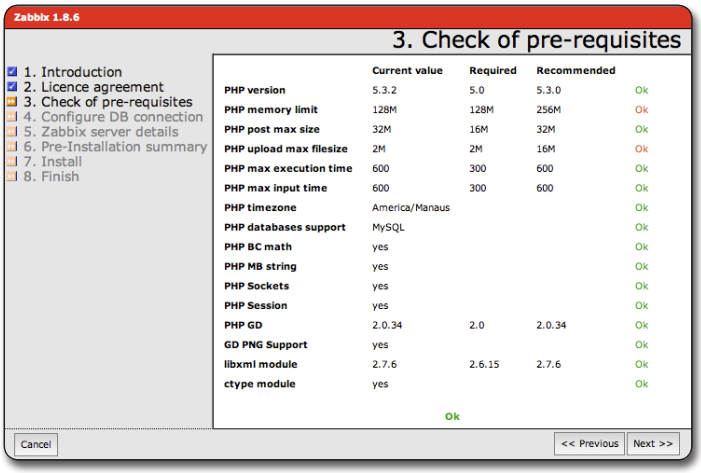


Figura 1. Verificação de pré-requisitos

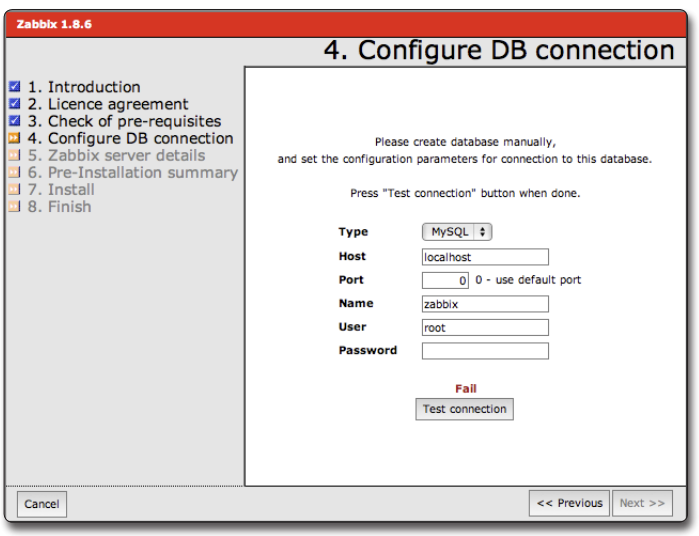


Figura 2. Configurando a conexão com banco de dados

O próximo passo é informar um nome para a instalação no campo *Name* e manter os demais parâmetros conforme o padrão (host = localhost; port = 10051). Clique então na opção*Next*.

Agora você irá conferir os parâmetros informados (**Figura 3**)e clicar em *Next* para realizar a criação do arquivo de configuração para a interface de monitoramento. Se você desejar alterar algum parâmetro, basta escolher a opção *Previous* e fazer as mudanças que achar necessário.

Pronto! Os parâmetros informados foram gravados e você pode clicar em *Next* para finalizar a instalação.Feito isso, a instalação estará finalizada e você poderá realizar o primeiro acesso e iniciar as configurações da interface de monitoramento.O primeiro login é feito com o usuário *admin* e senha *zabbix*(ver **Figura 4**).

Passo 4 –Configurando o monitoramento

O Zabbix traz uma série de definições que são necessárias para a sua operação. Dentre elas, quatro são fundamentais:

1. Hosts: para o Zabbix, um *host* é uma entidade lógica que agrupa itens de interesse para o monitoramento. Um *host* pode ser um servidor, um roteador, um switch etc.;
2.Item:itens representam quaisquer indicadores que desejamos monitorar, quer seja o uso de CPU, o espaço em disco ou ainda tempo de resposta de um serviço;
3.Triggers: um *trigger* é um limite a partir do qual alguma ação, normalmente de notificação, será executada automaticamente. Criaremos *triggers* quando quisermos ser avisados sobre eventos específicos, tais como espaço em disco de um servidor ou consumo de banda de um link;
4.Actions: uma *action* corresponde a uma ação que será executada quando um trigger for acionado. Podemos definir ações como envio de e-mail, sms ou ainda execução de scripts.

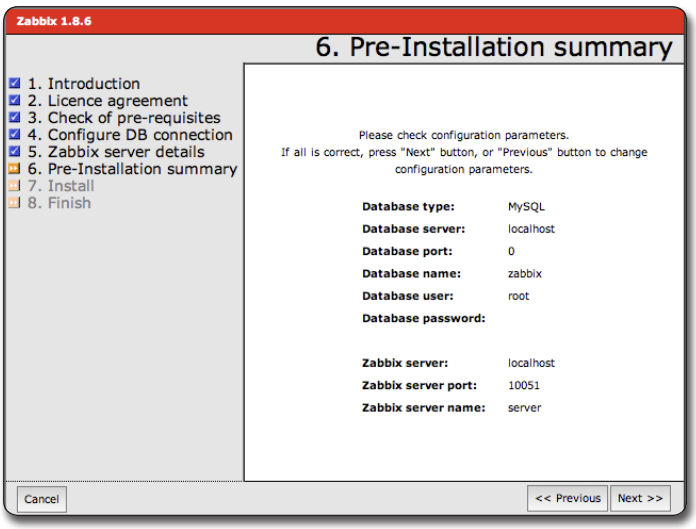


Figura 3. Confirmando os parâmetros do servidor

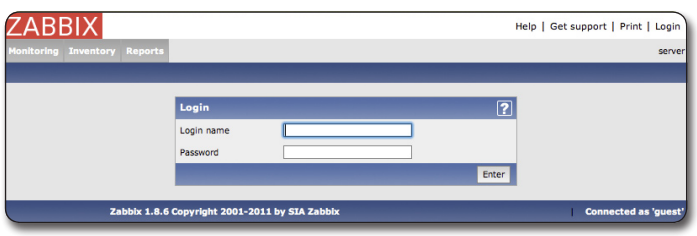
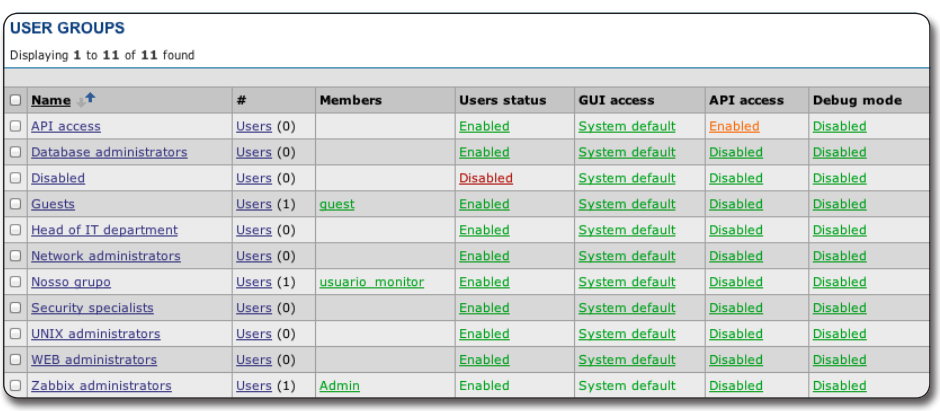


Figura 4. Primeiro acesso


USER GROUPS

Displaying 1 to 11 of 11 found

Name	#	Members	Users status	GUI access	API access	Debug mode
API access	Users (0)		Enabled	System default	Enabled	Disabled
Database administrators	Users (0)		Enabled	System default	Disabled	Disabled
Disabled	Users (0)		Disabled	System default	Disabled	Disabled
Guests	Users (1)	guest	Enabled	System default	Disabled	Disabled
Head of IT department	Users (0)		Enabled	System default	Disabled	Disabled
Network administrators	Users (0)		Enabled	System default	Disabled	Disabled
Nosso grupo	Users (1)	usuario_monitor	Enabled	System default	Disabled	Disabled
Security specialists	Users (0)		Enabled	System default	Disabled	Disabled
UNIX administrators	Users (0)		Enabled	System default	Disabled	Disabled
WEB administrators	Users (0)		Enabled	System default	Disabled	Disabled
Zabbix administrators	Users (1)	Admin	Enabled	System default	Disabled	Disabled

Figura 5. Lista de usuários do sistema Zabbix

Além disso, é importante sabermos que o Zabbix pode monitorar vários aspectos de nossa infraestrutura, agrupados abaixo em categorias:
• **Disponibilidade:** Se serviços (ou dispositivos) estão acessíveis;
• **Performance:** Quais os tempos de resposta de serviços, o consumo de banda de links, de I/O de discos;
• **Segurança:** Quais portas estão abertas, que versões de software estão instaladas;
• **Eficiência:** Quais as medidas de acerto (hit/miss ratio) de proxy, cache de bancos de dados.

De maneira a obter as informações que serão usadas no monitoramento, o Zabbix tem suporte a vários tipos de itens, dentre eles:
• **Agente Zabbix (Zabbixagent):** É o tipo default e corresponde ao software que podemos instalar em computadores. Atua de duas maneiras, passiva, no qual o servidor consulta o agente periodicamente, ou ativa, no qual o agente é que se conecta ao servidor Zabbix;
• **Teste simples (Simplecheck):** Operações simples com portas TCP/UDP e ICMP;
• **Agente SNMP (Snmpagent):** Utiliza o protocolo SNMP para acessar os recursos monitorados;
• **Testes externos (Externalcheck):** Permite ao Zabbix executar programas externos e armazenar o resultado destes. Muito útil quando o que se deseja monitorar é específico e não permite o uso de outros recursos vistos anteriormente;
• **Monitor de banco de dados (Database monitor):** Conectores para testes a servidores de bancos de dados de diversos tipos;
• **Agente SSH:** Permite executar comandos remotos através de SSH e armazenar o resultado.

Conhecidas estas definições, a partir de agora definiremos um conjunto de configurações para nosso estudo de caso de monitoramento envolvendo e-mails de notificação, *triggers*, servidores e *actions*, dentre outras coisas.

Configurando e-mail para notificação

A forma mais comum de notificação é o e-mail. Para que o administrador do Zabbix seja informado de eventos que aconteçam você precisa configurar qual o endereço de e-mail que ele deverá receber.

Para isso, acesse *Administration>Users*. Você verá a lista já existente de usuários do Zabbix, conforme a **Figura 5**.

Escolha o usuário *Admin*. Você verá que no campo *Media* (**Figura 6**) não há meio de notificação definido (*No media defined*). Clique no botão *Add*.

Informe o e-mail que você deseja que receba as notificações no campo *Sendto* e clique em *Add*.

Na **Figura 7** vemos que por padrão serão enviadas para o e-mail indicado todas as

mensagens geradas pelo Zabbix em qualquer dia/horário. O campo *Whenactive* indica os dias (1-7) e as horas de notificação. Você pode criar vários e-mails de notificação de acordo com a severidade e até mesmo horários específicos. No momento criaremos apenas um e-mail.Clique em *Add* novamente e em seguida em *Save*.

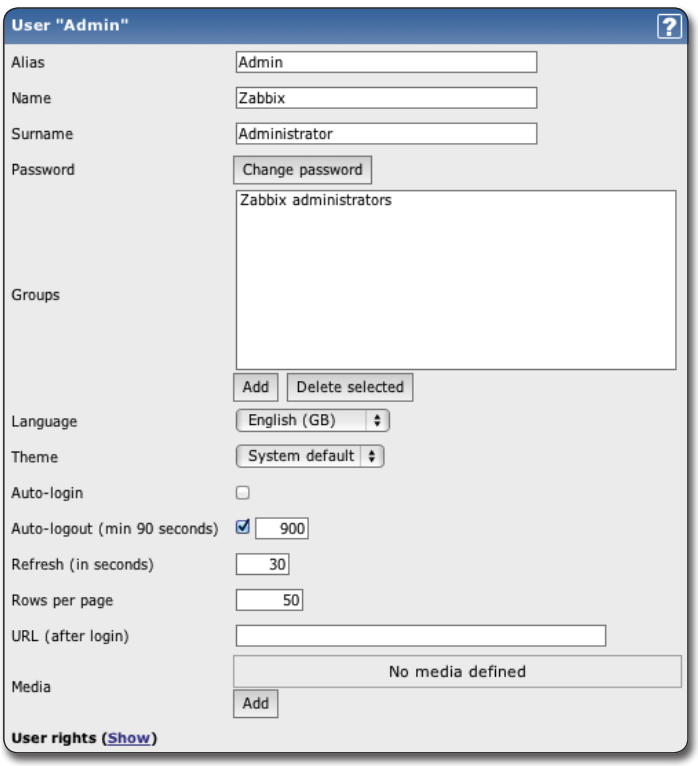


Figura 6. Propriedades do usuário Admin

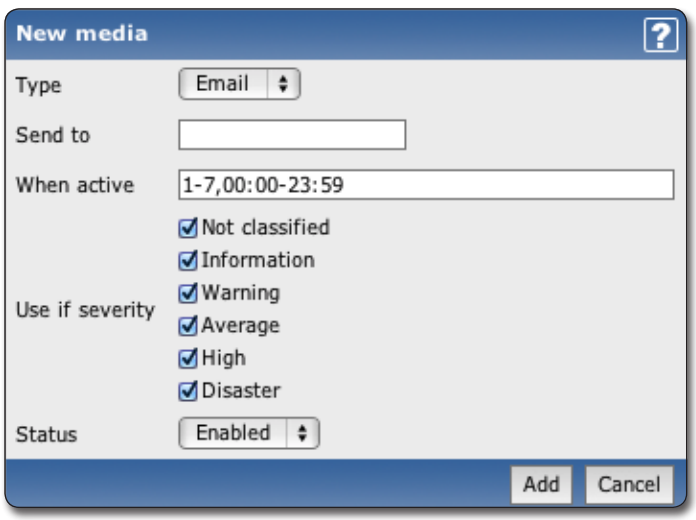


Figura 7. Definindo o e-mail de notificação do Admin

Adicionando um host para monitoramento

Iremos agora adicionar em nosso Zabbix um servidor para monitorarmos. Para tanto, escolha no servidor a opção *Configuration*> *Hosts*. No campo *Group* escolha *Linux Servers* e clique no botão *Create Host*.Feito isso, preencha os dados abaixo (**Figura 8**):

- **Name:** Nome que identificará nosso servidor;
- **DNS Name ou IP address:** Se o servidor que você irá monitorar possuir um nome registrado no DNS, use-o, caso contrário, use o IP do servidor;
- **Connect to:** De acordo com a opção escolhida anteriormente, indique se você deseja usar o nome ou o IP.

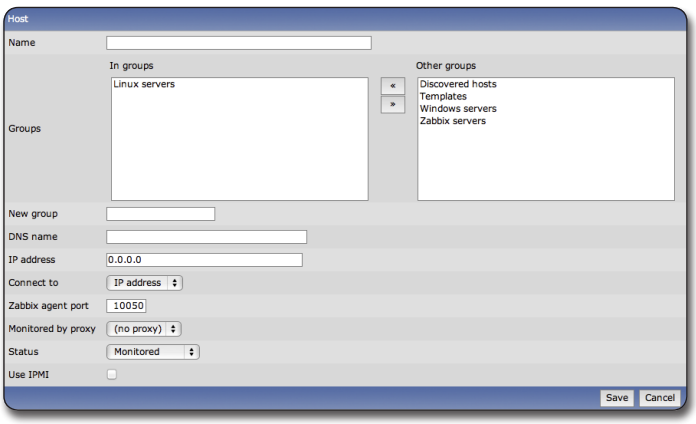


Figura 8. Definindo o host

Para fins deste artigo iremos monitorar os serviços localizados na própria máquina onde o Zabbix está instalado. Nesse caso, use no campo *IP Address* 127.0.0.1 e no *Name*digite"Servidor aplicativos". Em seguida clique em *Save*. A **Figura 9** ilustra como ele irá aparecer.

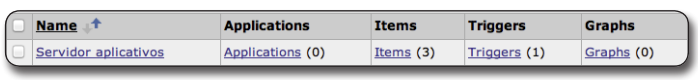


Figura 9. Host criado

Adicionando um serviço para monitoramento

Neste momento, nosso servidor já está na lista de servidores conhecidos pelo Zabbix. Precisamos agora adicionar um item para monitoramento que, em nosso exemplo, será o serviço web (WWW).

Selecione novamente *Configuration*> *Hosts* e clique em *Items* ao lado do servidor que você criou.Escolha a opção *Create Item*. Existem vários campos para configuração do item. Deixaremos a maioria com os valorespadrão (**Figura 10**), definindo apenas:

- **Description:** Servidor WWW (é o nome com o qual o item será identificado);
- **Key:**net.tcp.service[http,,80]. Esta chave indica que desejamos monitorar um serviço que usa a porta TCP. O campo http é o nome do serviço que desejamos monitorar e o último é a porta na qual o serviço deve ser encontrado.

Em seguida clique em *Save*. Você terá acrescentado o serviço WWW que passa a ser monitorado pelo servidor.

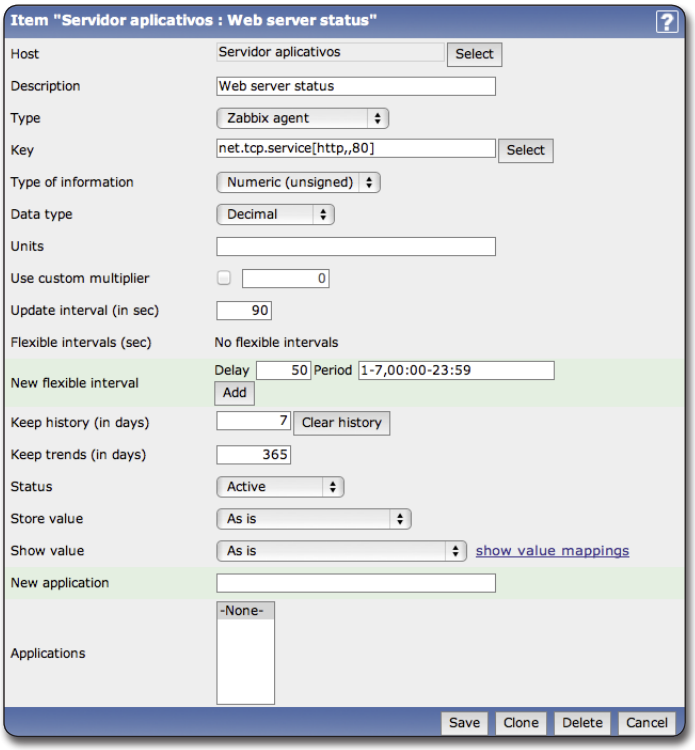


Figura 10. Criando um item

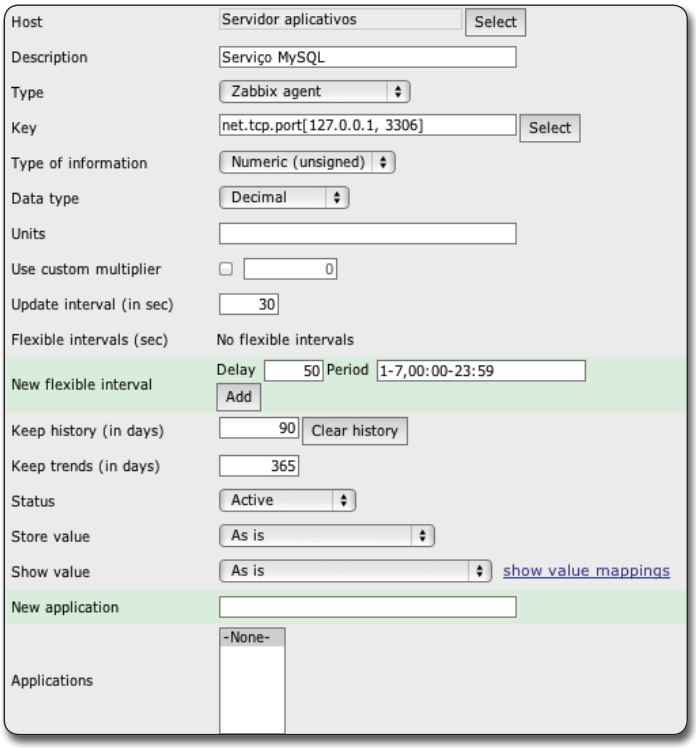


Figura 11. Monitorando o servidor MySQL

Iremos agora repetir o mesmo procedimento, só que desta vez para monitorar o serviço do servidor MySQL (**Figura 11**) e a carga do processador (**Figura 12**).

Os dados para uso serão:

a) MySQL
- *Description*: Serviço MySQL
- *Key*: net.tcp.port[127.0.0.1,3306]

b) CPU
- *Description*: CPU Load
- *Key*: system.cpu.load

- *Type of information*: numeric (float)

A principal diferença para o item **a)** é que como a carga da CPU é indicada como um número com casas decimais, usará o tipo *float*. Até então estávamos usando o tipo inteiro, já que o monitoramento de serviços só assume dois valores: 0 para problemas e 1 para OK.

Observe agora na **Figura 13** o conjunto de itens que iremos monitorar e configurados até o momento.

Passo 5 –Acessando os dados monitorados

Até o momento, o que fizemos foi adicionar *hosts* e itens para o Zabbix. Ele já está monitorando e armazenando o resultado para consultas. Veremos a partir de agora algumas alternativas para manipularmos estas informações.

Para acessar os dados você pode escolher a opção*Monitoring>Latest data*.Você pode filtrar quais elementos deseja ver baseado no grupo ou nome do *Host*. No exemplo da **Figura 14**, vemos os itens sendo monitorados para o servidor aplicativos e quais os valores obtidos

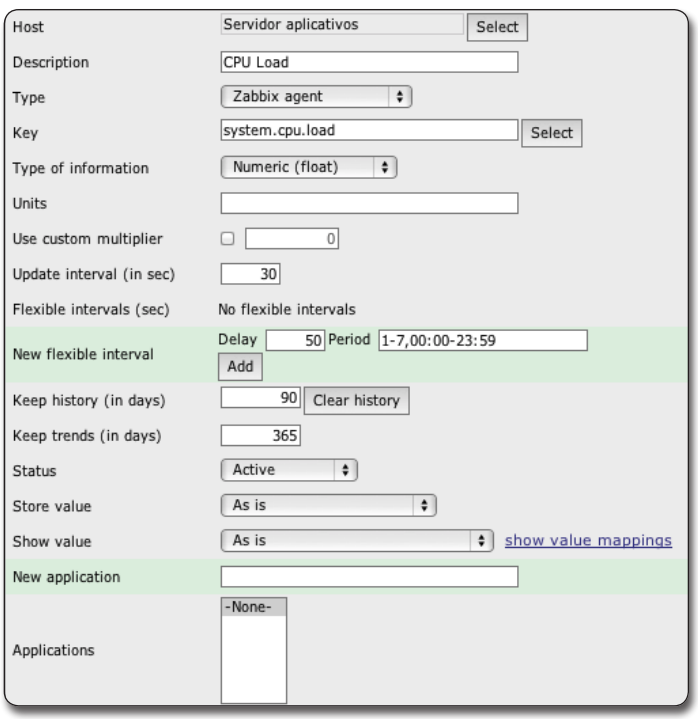


Figura 12. Monitorando o consumo da CPU

na última checagem. Ainda nesta tela, é possível acessar os gráficos gerados pela ferramenta clicando no link *Graph*.

Criando triggers

O processo que utilizamos adiciona itens para monitoramento pelo Zabbix. Você pode acompanhar seus desempenhos ou

Wizard	Description	Triggers	Key	Interval	History	Trends	Type	Status	Applications	Error
	CPU Load	Triggers (1)	system.cpu.load	30	90	365	Zabbix agent	Active	-	✓
	Serviço MySQL		net.tcp.port[127.0.0.1, 3306]	30	90	365	Zabbix agent	Active	-	✓
	Serviço WWW		net.tcp.service[http,,80]	90	7	365	Zabbix agent	Active	-	✓

Figura 13. Itens sendo monitorados

ITEMS — Group: Linux servers — Host: Servidor aplicativos

Filter

Show items with description like [ ] Filter Reset

Description	Last check	Last value	Change	History
- other - (3 Items)				
CPU Load	31 Oct 2011 16:06:52	0.43	-0.27	Graph
Serviço MySQL	31 Oct 2011 16:07:02	1	-	Graph
Serviço WWW	31 Oct 2011 16:06:24	1	-	Graph

Figura 14.Itens monitorados

mesmo ter acesso a relatórios de uso. Entretanto, você às vezes precisa ser informado (ou executar outras tarefas) quando certos eventos acontecerem. Por exemplo, você deseja receber um e-mail (ou um SMS) quando o servidor WWW estiver inoperante ou a carga de CPU ultrapassar 50%.

Para atingir este objetivo você precisa inicialmente criar um *trigger*.Este define condições que você deseja monitorar em um item.

Vamos agora criar um *trigger* que será ativado toda vez que a carga da CPU ultrapassar 100%. Para isso,acesse*Configuration*> *Hosts* e clique em *Items* para o servidor aplicativos.

Feito isso, clique sobre a opção *CreateTrigger*e preencha os dados abaixo (ver **Figura 15**):

- **Name:**"CPU Alta";
- **Expression:**"{Servidor aplicativos:system.cpu.load.last(180)}>1".

O campo *Name* indica apenas o nome que você deseja utilizar para identificar seu *trigger*. O campo *Expression* define qual condição você deseja avaliar. Em nosso exemplo ele indica que se a carga da CPU nos últimos 180s ultrapassar 100%, o trigger será acionado.

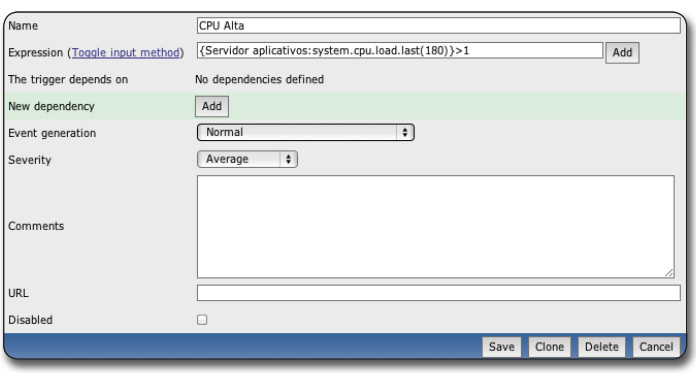


Figura 15. Criando um trigger

É importante lembrar que o *trigger*, por si só,não executa nenhuma ação, apenas definimos condições para monitorar.Na seção seguinte iremos criar ações (*actions*) que farão uso dos *triggers* para saber quando deverão ser executadas.

Criando actions

Para o Zabbix,*actions* correspondem a operações que serão executadas toda vez que um trigger alterar seu status. A ação mais comum que existe é a notificação. Dessa maneira, o administrador (ou quem ele indicar) pode ser informado quando condições de interesse se manifestarem.

Imagine, por exemplo, que estejamos monitorando o servidor web responsável por atender a intranet de nossa empresa ou ainda o nosso site. Ou ainda que a CPU do servidor está com uma carga acima do esperado. É desejável saber,o quanto antes,que eventuais problemas ou funcionamento fora do esperado ocorreram.

Iremos fazer exatamente isso.Portanto, devemos selecionar *Configuration*>*Actions* e escolher a opção *CreateAction*.Para criar a ação você irá realizar as três operações a seguir:

1. Informar um nome para a ação;
2. Selecionar a(s) condição(ões) para indicar que a ação deve ser realizada;
3. Selecionar a ação a ser executada (em nosso caso enviar uma notificação).

A tela inicial deste processo pode ser vista na **Figura 16**. Informe o nome (*Name*) CPU Alta Action.

Em seguida clique em *New* na parte chamada *Actionconditions* (**Figura 17**). Escolha a opção *Trigger* e clique em *Select*. Você irá escolher dentro da lista de *triggers* existentes qual você deseja utilizar (**Figura 18**).

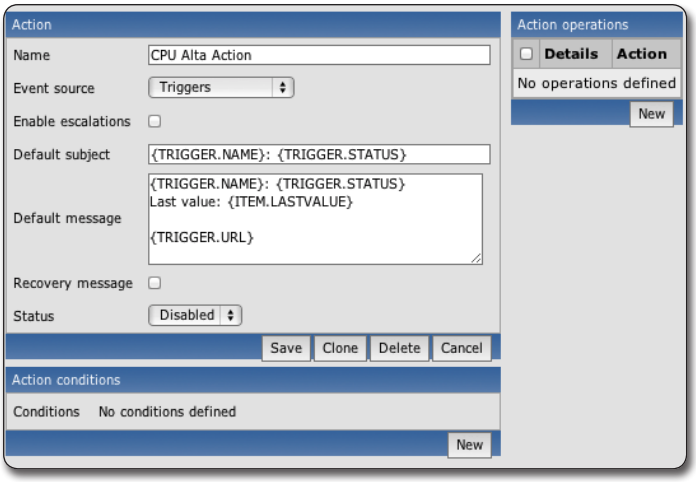


Figura 16. Informando o nome da action



Figura 17. Escolhendo a condição – Parte 1

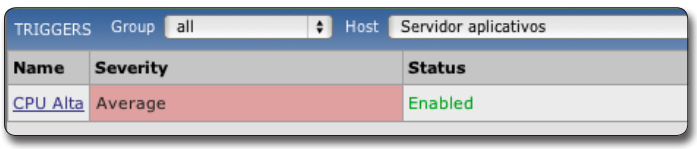


Figura 18. Escolhendo a condição – Parte 2

Feito isso, escolha o trigger recém-criado e clique em *Add* (**Figura 19**).

A última operação consiste em indicar que ação desejamos executar. Para isso, clique em *New* no *Actionoperations* (ver **Figura 16**). Ao selecionar esta opção, a tela da **Figura 20** será apresentada. Troque a opção *SendMessageto* para *Single User*.

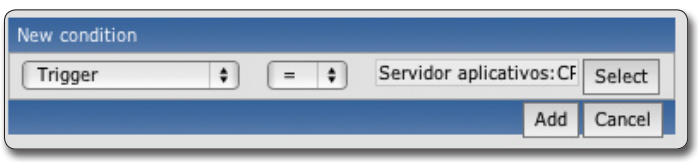


Figura 19. Adicionando condição ao trigger selecionado

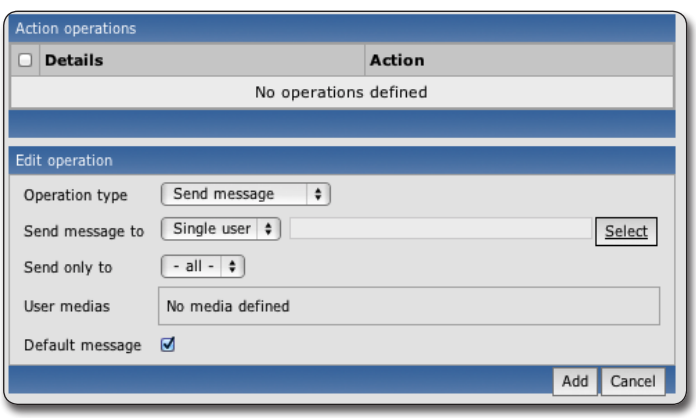


Figura 20. Indicando a notificação

Ainda na tela da **Figura 20**, clique em *Select* para exibir a lista de usuários existentes. Selecione o usuário *Admin*, clique em *Add* (**Figura 21**) e em seguida em *Save* para finalizar o processo de criação da ação (**Figura 22**).

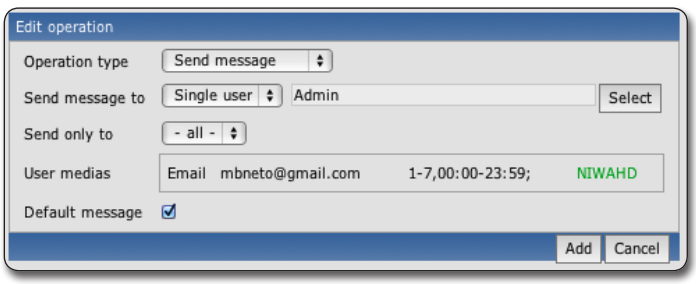


Figura 21. Selecionando o usuário



Figura 22. Ação criada

Pronto! Neste momento você terá criado uma ação de notificação que será enviada toda vez que as condições (*triggers*) selecionadas mudarem de status. Isso significa em nosso exemplo que toda vez que a CPU ultrapassar a carga indicada o administrador será notificado e quando a CPU reduzir a carga (abaixo desse limite) também.

Conclusão

Ao longo deste artigo vimos uma solução que permite o monitoramento de recursos de forma centralizada e com um sistema de notificação para auxiliar na gestão de seus recursos de infraestrutura, sobretudo de rede.

O exemplo aqui apresentado, apesar de funcional, representa apenas uma pequena parte da real capacidade que o software disponibiliza.

O Zabbix possui muitas outras funções e por ser de código aberto permite expandir seu funcionamento, além de contar com uma comunidade que está realizando constantes melhorias e correções no mesmo.



Mário de Mello Bittencourt Neto
mbneto@gmail.com
Diretor técnico da Argo Internet desde 1996, atuando na área de redes e desenvolvimento de aplicativos Web, eCommerce e segurança. Engenheiro eletrônico e Mestre em informática.ZendCertifiedEngineer.

Antivírus Corporativo

A escolha correta para sua organização

Roberto Henrique de Sousa

Resumo DevMan

De que se trata o artigo:

Este artigo aborda as principais razões para a adoção de um sistema de antivírus corporativo e quais as implicações que uma organização pode sofrer por não seguir as melhores práticas de segurança contra ameaças virtuais.

Em que situação o tema é útil:

Espera-se que, com este artigo, as equipes responsáveis pelos departamentos de Tecnologia da Informação e de Segurança possam argumentar junto aos departamentos responsáveis pela aprovação dos orçamentos que a aquisição incorreta deste tipo de solução pode comprometer seriamente a continuidade das atividades da organização, seja devido a ataques na rede como o pagamento de multas pelo uso indevido da licença dos aplicativos.

Antivírus Corporativo:

A batalha dos antivírus contra as mais perigosas pragas virtuais (malwares) não é recente, vem do início da década de 70. Ainda assim, têm-se inúmeros casos de mau uso dos sistemas de proteção dentro das organizações.Seja por dificuldades técnicas ou por questões financeiras, o fato é que muitas destas empresas ou instituições ainda não adotaram um sistema de antivírus corporativo, preparado para proteger grandes quantidades de equipamentos, de forma centralizada e segura.

Há aproximadamente 40 anos o mundo teve seu primeiro contato com o vírus de computador. Essa praga ficou conhecida como *Creeper*, devido à mensagem que ele apresentava na tela dos computadores: *"Eu sou o Creeper, pegue-me se você puder"*. Esse fato ocorreu em 1971, dentro da *AdvancedResearch Project Agency Network* ou se preferir, a famosa ARPANet do Departamento de Defesa dos Estados Unidos da América. Esta rede foi criada com o objetivo de interligar diversos pontos estratégicos do governo, de forma a garantir a continuidade das comunicações em caso de uma guerra. Esta rede foi a precursora do que hoje chamamos Internet.

Através desta estrutura de comunicação o vírus se replicava, fazendo surgir a tal mensagem nos diversos computadores conectados na ARPANet, rodando o sistema TENEX. Para combater a disseminação dessa praga, foi criado outro programa, chamado de *Reaper*. Este também possuía o comportamento de se replicar, similar ao *Creeper*, porém seu objetivo era o de entrar em sistemas que já estivessem infectados com o vírus para eliminá-lo. Estava então inaugurada na prática a batalha dos antivírus no mundo virtual.

Hoje, com a democratização da Internet permitindo o acesso nos locais mais remotos do planeta, por pessoas de todos os tipos e empresas de todos os tamanhos, o que se vê é uma explosão de *malwares*, um novo "Big Bang" de ameaças virtuais que se transformaram em ameaças reais.

Já passou o tempo em que ter um antivírus instalado e atualizado no computador era garantia de segurança para o usuário. Nos últimos anos, os *malwares* têm explorado vulnerabilidades em diversos programas, como por exemplo, falhas em sistemas operacionais desatualizados, *bugs* em aplicativos como pacotes Office ou Adobe, e *browsers* como Internet Explorer ou Firefox.

Quer um exemplo recente? Lembram-se do Conficker, aquele *malware* que em poucos dias infectou cerca de nove milhões de computadores explorando falhas de segurança dos sistemas operacionais desatualizados da Microsoft. Em Novembro de 2008, *hackers* disseminaram na rede este novo vírus que buscava explorar basicamente três tipos de vulnerabilidades:

- Explorar uma falha do serviço de RPC, acrônimo de *Remote Procedure Call*, ou Chamada Remota de Procedimento, em todos os computadores com sistema Windows desatualizados. O *patch* que corrigia essa vulnerabilidade havia sido lançado em outubro de 2008;
- Quebrar senhas fracas do usuário Administrador dos alvos, permitindo o acesso aos compartilhamentos na rede, aumentando o seu poder de disseminação;
- Explorar o recurso de *Autorun* dos dispositivos de armazenamento móvel, assim que conectado ao computador, infectando os sistemas que não possuíam as atualizações com as devidas correções.

O diagrama da **Figura 1** exemplifica um ataque.

E não adiantava ter o antivírus atualizado, pois como se tratava de uma nova ameaça, as vacinas precisavam ser criadas nos laboratórios dos diferentes fabricantes e, mesmo assim, ainda era necessário corrigir as atualizações do Windows, pois o que esse *malware* fazia era utilizar recursos habilitados no sistema operacional para se propagar. Essa batalha durou até o primeiro semestre de 2009, quando descobriram que, além do próprio Conficker, esse *malware* abria portas para injetar novas pragas virtuais, inclusive requisitando os computadores para fazerem parte de uma rede de computadores zumbis.

Devemos sempre nos lembrar de que nenhum antivírus consegue proteção 100% efetiva, só que no passado, o mercado de forma geral vendeu muito esta ideia, quando na verdade o que

se tinha eram antivírus de excelente qualidade, mas que não precisavam atuar em diferentes formas de ataque, pois os *malwares* de antigamente eram limitados, assim como sua disseminação. A Internet da década de 90 ainda não estava acessível a todos, portanto a multiplicação do conhecimento também não. Hoje, porém, vemos um processo de massificação na aquisição de computadores, dispositivos móveis, serviços de banda larga e tudo mais que possa auxiliar tanto na disseminação das pragas atuais quanto na colaboração dos criadores para desenvolverem novas ameaças.

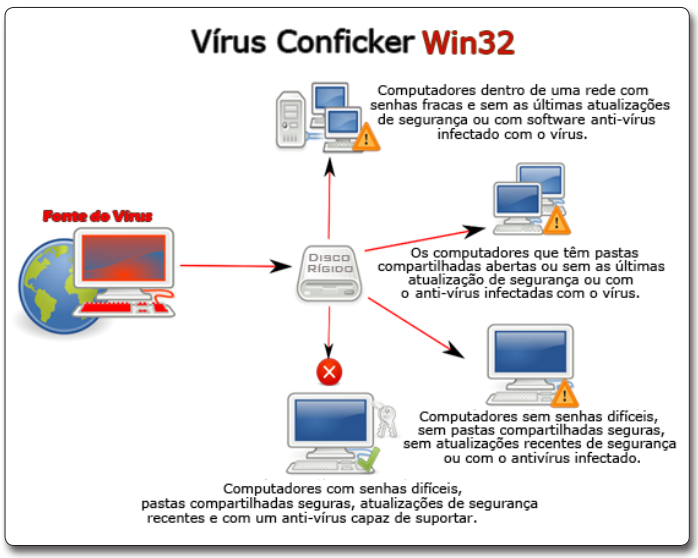


Figura 1. Diagrama Conficker

Frente a estas novas ameaças, aumenta a demanda por soluções que possam garantir um nível adequado de proteção, onde a atualização das vacinas quase que em tempo real, recursos extras como *anti-spyware*, filtro contra *phishing*, *anti-rootkit*, *firewall* integrado e bloqueio de dispositivos deixaram de ser um diferencial para tornarem-se uma espécie de *commodity*, ou seja, todos esses recursos devem fazer parte dos sistemas de antivírus por *default*.

Hoje não faltam opções entre os diversos fabricantes de antivírus com excelentes produtos no mercado e baixo custo de licenciamento por equipamento ao ano. Entre os fabricantes mais conhecidos aqui no Brasil, tem-se a Symantec, McAfee, Kaspersky, F-Secure, Sophos, ESET, Microsoft, Panda, Trend Micro, Avira, Avast e AVG. Cada fabricante oferece um leque de opções, desde antivírus de celulares para o usuário doméstico até soluções completas para grandes corporações, incluindo proteções específicas para *servers*, *desktops*, *smartphones* e *tablets*.

No caso dos usuários domésticos, esses ainda possuem a vantagem de poderem usar aplicativos de antivírus gratuitos. Entre os mais populares temos o *AVG Anti-VirusFree*, *Avast! FreeAntivirus*, *AviraAntiVirPersonalEdition Classic* e *Microsoft Security Essentials*. Esses antivírus possuem alguns requisitos básicos de segurança, mas em testes recentes realizados por uma empresa especializada no Brasil, ficou evidente a baixa taxa de detecção dessas versões. Isso chega a ser óbvio, pois estes produtos citados são disponibilizados principalmente para divulgação da marca, de forma a permitir um primeiro contato da solução pelo usuário.

A AVG e Microsoft possuem versões gratuitas de seus antivírus para empresas de pequeno porte, como é o caso da versão *AVG Anti-VirusFreeSmall Business*, disponível para até cinco computadores por 12 meses, e o *Microsoft Security Essentials* para até 10 computadores, sem limite de tempo, desde que instalado em sistema operacional Windows original. Além da baixa taxa de detecção das versões gratuitas, estes antivírus trabalham de forma isolada, não permitindo sua administração de forma centralizada.

Mas em ambos os casos, os fabricantes oferecem suas outras ferramentas de segurança, com muitos recursos adicionais e maior garantia de proteção efetiva, como o *AVG Anti-Virus Business Editione* o *Microsoft ForefrontClient Security*.

Mas o que vemos nas empresas aqui no Brasil? Antivírus gratuitos instalados indiscriminadamente em empresas de pequeno, médio e, em alguns casos, até em empresas de grande porte. Quando questionados, muitos acham que estão corretos, pelo fato do antivírus instalado ser um produto *freeware*. Mas todos os fabricantes que disponibilizam uma versão *free* de seus softwares de segurança deixam explicitamente registradas as permissões do uso de seus produtos gratuitos apenas para fins não comerciais (usuários domésticos e estudantes). Alguns fabricantes ainda abrem uma exceção para pequenas empresas com 5 ou até 10 computadores, conforme dito anteriormente.

Em uma recente pesquisa do Núcleo de Tecnologia do CIESP de São Bernardo do Campo/SP com empresas industriais da região, foi constatado que 52% das empresas utilizavam o software AVG ou AVAST em seu parque. Isso não é uma característica apenas do setor industrial, mas de todo o tipo de organização. Os motivos para tal prática são os mais variados, mas as consequências do uso irregular destes softwares são bem conhecidas:

- Multa por uso de software sem licenciamento;
- Ausência de suporte técnico do fabricante;
- Limitação de funcionalidades para proteção completa;
- Impossibilidade de gestão do parque de antivírus instalado;
- Consumo do link devido atualização descentralizada das vacinas;
- Ausência de informações consolidadas sobre quais computadores foram mais atacados, quais as principais ameaças ou qual o período de maior ataque;
- Ação reativa a qualquer ataque, pois não há como ser notificado no exato momento de uma tentativa de disseminação de *malwares* na rede, o que permitiria o isolamento de um computador ou um grupo.

Vamos expor em detalhes alguns destes itens para mostrar as justificativas em adotar um antivírus corporativo. Estas justificativas devem ser levadas ao corpo diretivo da organização de forma clara e objetiva, pois o que se vê, muitas vezes, são situações em que os responsáveis técnicos que sabem da importância em se trabalhar com antivírus corporativos, possuem uma imensa dificuldade em mostrar os benefícios de tal adoção aos diretores

e gerentes que assinam a aprovação de novos investimentos para o departamento de TI. E quando se fala em benefícios a serem mostrados, não é apenas sobre detalhes técnicos, mas financeiros. Lembrem-se sempre disso: Quem aprova tais investimentos (pelo menos em sua maioria) não está preocupado se antivírus A, B ou C é melhor tecnicamente mas, sim, se ele é financeiramente vantajoso. Hoje, a maior parte dos fabricantes de antivírus corporativos está oferecendo soluções adequadas para garantir um nível aceitável de proteção para sua rede. O que difere de um para o outro é o preço e o tipo de suporte técnico que o cliente poderá obter, e isso é fundamental para garantir a segurança dos seus ativos. Não adianta comparar qualidade técnica da ferramenta e preços, quando se compara uma empresa que apenas vende a licença de uso (ou como se diz, vendem apenas a caixinha) com outras empresas que vendem um serviço agregado, como instalação em 100% do parque, higienização da rede em busca de *malwares*, elaboração de políticas de segurança para uma administração correta da solução, monitoramento proativo ou mesmo emissão de relatórios periódicos com análises e recomendações para evitar a ocorrência de novos ataques.

Multa por uso de software sem licenciamento

O combate ao uso de softwares piratas tem ganhado força nos últimos anos, pela ação conjunta da Polícia com os fabricantes de softwares e as associações como a ABES (Associação Brasileira de Empresas de Softwares). Somente no mês de Julho de 2011 houve um aumento de 468% na apreensão desses softwares. Estes números comprovam o aumento das ações para reduzir os índices desta prática criminosa, principalmente no comércio e nas empresas.

Quanto aos antivírus considerados gratuitos (*freewares*), eles não se enquadram no critério de softwares piratas, mas seu uso por empresas não é autorizado pelos fabricantes. Com exceção das versões para pequenas empresas citadas anteriormente, todas as demais são consideradas cópias ilegais. Isso poderá resultar em multas de até 3000 vezes o valor de cada cópia, além de detenção por até 4 anos.

Se você acha que isso não acontece com frequência, é bom começar a se preocupar. De acordo com a ABES, a grande maioria das denúncias parte internamente, através de funcionários insatisfeitos ou demitidos da organização. Com a denúncia registrada, a ABES inicia um processo de investigação e com a obtenção de um mandato de busca e apreensão a associação pode encaminhar um representante com o acompanhamento da Polícia para coletar as provas de tal prática. Chegando nesse ponto, o prejuízo financeiro será consideravelmente alto, além do prejuízo imensurável contra a imagem da organização, que muitas vezes pode não ser recuperado.

Essa preocupação vem crescendo tanto que algumas empresas começam a exigir de seus prestadores de serviços a comprovação do uso de softwares licenciados para preservar o contrato entre as partes, o que não é nenhum absurdo, pois dependendo do valor da multa, e as consequências das demais penalidades previstas, uma empresa prestadora de serviço pode simplesmente fechar suas portas, deixando os seus clientes na mão.

Ausência de suporte técnico do fabricante

Parece um problema simples, mas não se engane. A ausência do apoio de um suporte técnico especializado pode acarretar em grandes transtornos para a equipe de TI da organização. Hoje, com as inúmeras atribuições do departamento de Tecnologia, cada vez mais o uso de serviços gerenciados por terceiros vem trazendo benefícios às organizações. Que empresa hoje, por exemplo, se preocupa em manter um técnico especializado em impressoras para realização de manutenção do parque? Quem mantém um estoque de peças de reposição para consertar estes equipamentos? Praticamente não se encontra mais este profissional nos departamentos de TI, pois há um consenso de que terceirizar o parque é muito mais vantajoso, tanto na questão financeira quanto na rapidez para resolver os problemas de impressão. Assim a equipe interna de TI mantém o seu foco apenas nas questões diretamente relacionadas ao negócio.

Hoje, com a grande quantidade de *malwares* ameaçando todos os tipos de equipamentos e sistemas, de computadores a celulares, da plataforma Windows ao Mac, demandando grande atenção por parte da equipe técnica responsável pela segurança dos ativos da organização, é fundamental que haja um tempo de resposta rápido e eficaz, que possa eliminar, ou ao menos reduzir, o impacto de um incidente causado por pragas virtuais. Frente a isso, ainda há a necessidade de constante aprendizado para operar corretamente as variadas funcionalidades das soluções de proteção. Não é simplesmente detectar e apagar arquivos suspeitos e pronto, estamos protegidos. Saber aplicar as configurações de acordo com as necessidades de cada grupo de usuários e aplicar as devidas políticas de segurança é fundamental para o correto funcionamento das ferramentas de proteção. Muitas vezes, sem o apoio de um especialista, essa proteção poderá não ser tão eficiente como deveria. Lembrem-se, independente da marca do antivírus, o que faz realmente a diferença é o apoio técnico que não vem dentro de uma caixinha. O relacionamento entre prestadores de serviços e clientes é o grande diferencial competitivo para os fornecedores, pois há muitas empresas de segurança que vendem um excelente produto, mas não possui uma política de capacitação de seus canais de revenda, para que elas possam dar o devido suporte lá na ponta do negócio.

Limitação de funcionalidades para proteção completa

Os antivírus gratuitos são limitados se comparados com as suas versões pagas, o que acaba expondo as organizações, pois como se sabe, o número de novas ameaças cresce a cada dia e cada vez mais aperfeiçoadas. Até mesmo as soluções completas correm o risco de não possuírem a vacina no momento da descoberta de um novo vírus na Internet. Para isso os principais fabricantes desenvolveram funções em seus produtos que protegem o sistema contra algumas ameaças, mesmo que ainda não tenham a vacina criada em seus laboratórios para distribuir aos seus clientes. Algumas funcionalidades principais:

• ***Análise Heurística:*** Consiste em analisar um arquivo não para procurar uma assinatura conhecida do vírus, mas para encontrar dentro de sua estrutura de código padrões que possam indicar um comportamento suspeito como, por exemplo, a inscrição de *loops* sem uma necessidade específica. Há também outro tipo de análise heurística baseada na emulação do código em um ambiente isolado do sistema, justamente para identificar alguma atividade suspeita durante o processo. Quando detectado algum código malicioso, o antivírus registra com uma nomenclatura genérica, até ser identificada a sua assinatura;

• ***Análise Comportamental:*** Esta função permite com que o antivírus possa interpretar o comportamento de determinados programas no sistema, identificando possíveis *malwares* em execução sem a percepção do usuário. Por exemplo, podem existir programas que, sem avisar, tentam enviar pacotes para endereços na Internet ou tentam realizar gravações em diretórios específicos do sistema operacional. Neste caso o antivírus bloqueia a ação e alerta o usuário;

• ***Protetor Integrado ao Browser:*** Mais conhecido em seu termo em inglês como *Browsing Protection*, tem como objetivo impedir que o usuário acesse páginas infectadas, com base em um banco de dados. Este recurso é muito útil, ainda mais com o grande número de páginas invadidas, para inserção de códigos maliciosos. A **Figura 2** apresenta alguns exemplos deste recurso de fabricantes como F-Secure, Kaspersky e McAfee;

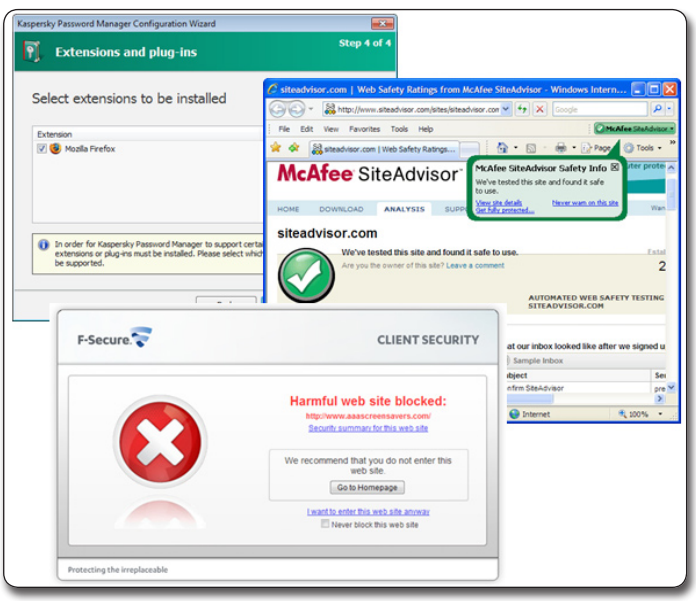


Figura 2. Exemplos de diferentes Protetores de Browser

• ***Anti-rootkit:*** Função essencial para detectar códigos maliciosos ocultos ao sistema e aos antivírus comuns, por possuírem características específicas em sua programação. Acabam sendo confundidos com programas comuns por algumas soluções, mas podem permitir o acesso não autorizado de *hackers*, ou mesmo permitir a execução de um *malware*. Um caso muito conhecido de *rootkits* foi registrado em 2005, quando a gravadora Sony/BMG utilizou uma tecnologia para restringir a cópia de seus CDs chamada XCP. Esse sistema impedia o usuário de criar mais do que três cópias do álbum, inserindo um programa de forma oculta no sistema operacional (na época, o Windows XP), só que este programa criava uma vulnerabilidade que permitia a ação de invasores remotamente e, o que era pior, na tentativa de removê-lo, o XCP acaba por danificar o sistema. Álbuns de artistas consagrados estavam entre os 2 milhões de CDs vendidos com tal tecnologia embutida de forma oculta. Por este fato, a Sony/BMG teve sua reputação atingida ao ponto de ter que recolher os CDs com os *rootkits*;

• ***Bloqueio de Dispositivos:*** Esse novo recurso que vem sendo incorporado nos principais antivírus do mercado é de extrema importância, ao ponto de ser exigido em processos de licitação do Governo brasileiro. A proteção aqui tem duas finalidades, impedir que arquivos contaminados possam ser transferidos de um dispositivo de armazenamento removível para o computador, e vice-versa, como também cria uma proteção contra vazamento de informações. Hoje pesquisas apontam que 6 em cada 10 funcionários levam informações da empresa sem autorização para casa, sendo que, na maior parte dos casos, o funcionário não toma qualquer prevenção para reduzir o risco de vazamento. Outro uso muito utilizado do Bloqueio de Dispositivos atualmente é a restrição do uso de dispositivos como modens 3G, que em muitas empresas acabam sendo uma brecha de segurança, permitindo com que funcionários não autorizados possam acessar conteúdos que, pela rede convencional, são bloqueados;

• ***Controle de Aplicativos:*** Funcionalidade muito interessante, que complementa a segurança da rede, evitando com que certos aplicativos não autorizados possam ser usados para burlar regras do *firewall* e outras políticas de segurança da empresa. Um exemplo muito comum é o Ultrasurf. Esse aplicativo consegue burlar servidores *proxy*, e seu bloqueio pelo *firewall* da rede é complexo e, na maioria dos casos, não é funcional. É neste ponto que uma solução de antivírus com Controle de Aplicativos consegue impedir a execução deste tipo de software, assim como tantos outros que realizem comunicação com a rede, como comunicadores instantâneos, programas P2P e aplicativos multimídia;

• ***Firewall:*** Ferramenta fundamental que tem como principal característica filtrar todo o tráfego da rede e Internet, impedindo ataques de *malwares*, como também acessos não autorizados ao computador.

Além destes itens, todo antivírus devem também possuir as funções já conhecidas como *anti-spyware* e *anti-spam*.

Impossibilidade de gestão do parque de antivírus instalado

Este é considerado como o maior diferencial entre uma solução gratuita e uma solução corporativa. Mesmo as soluções pagas que não são preparadas para o ambiente corporativo ficam devendo neste critério também.

Saber o que acontece em tempo real com os computadores conectados em uma rede é o requisito fundamental para qualquer

departamento de TI bem administrado. Não é possível garantir um nível básico de segurança da rede se o administrador não possuir as informações do estado de saúde de suas estações e servidores. Vide um modelo de administração na **Figura 3**.

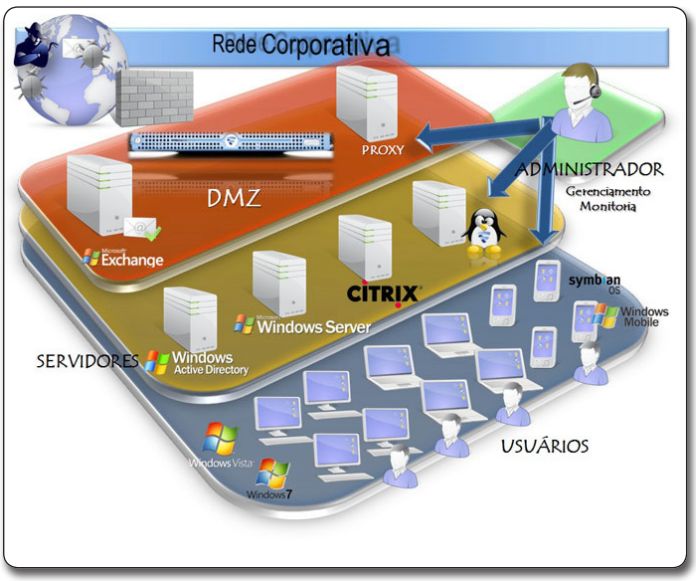


Figura 3. Modelo de administração da solução F-Secure em uma rede corporativa

Em hipótese alguma a rede de uma organização pode ficar inoperante e, para isso, o administrador deve garantir que nada de anormal esteja trafegando em seu ambiente. Isso inclui principalmente os *malwares*. Um simples *pen drive* infectado conectado em um computador pode disseminar o código malicioso por toda a rede. Como já dito antes, uma nova ameaça pode explorar uma vulnerabilidade do sistema até então desconhecida e, em situações em que o antivírus esteja desatualizado, o risco é eminente.

Para evitar tais surpresas, é necessário ter todas as informações sobre os softwares de proteção de rede centralizadas, de forma a permitir a identificação de qualquer comportamento suspeito na rede ou mesmo identificar possíveis brechas de segurança, como vacinas desatualizadas ou mesmo sistemas operacionais sem as suas últimas correções. Estas informações são adquiridas em painéis como os da **Figura 4**.

Através de um console de operação da solução de antivírus, o administrador pode criar diferentes políticas para cada grupo de computadores na rede. Um exemplo muito comum é a criação de uma política específica para *notebooks*, pois estes equipamentos podem ficar sem comunicação com a rede por dias e, em alguns casos, podem ficar sem as devidas vacinas atualizadas. Para evitar possíveis focos de ataque, pode-se criar uma política que mantenha o *notebook* isolado da rede até que todas as suas atualizações estejam em dia.

Além disso, uma gestão centralizada permite ao departamento de TI uma visão geral do que acontece na rede, e mesmo em redes de outras unidades da empresa.



Figura 4. Painel de administração de alguns fabricantes de antivírus corporativos

Consumo do *link* para atualização descentralizada das vacinas

Outra característica importante é a redução do consumo do *link*, pois quando se tem um servidor de antivírus gerenciando as estações da rede, apenas ele se conecta com a Internet em busca de atualizações, distribuindo-as na rede de forma controlada. Imagine um parque com 1000 estações saindo para buscar suas vacinas ao mesmo tempo, diversas vezes por dia! Degradaria totalmente o *link* de comunicação, ainda mais em nosso país com estes *links* totalmente limitados. Evitar este tipo de consumo é evitar dor de cabeça para o departamento de TI.

Conclusão

Concluindo, ainda daria para listar uma série de novos motivos, mas estes são mais do que suficientes para convencer primeiramente a equipe de TI sobre as vantagens e razões técnicas que comprovam a importância de um pacote de antivírus corporativo para a empresa. Também é importante justificar financeiramente, para que o corpo diretivo de uma organização possa aprovar a compra de uma solução corporativa, desde que os responsáveis técnicos saibam usar esses argumentos a seu favor. Não adianta explicar os motivos partindo apenas do ponto de vista técnico, mas também mostrando o valor agregado para a escolha correta. Isso significa traduzir as vantagens técnicas em números palpáveis para a direção. Quando se consegue convencê-los que a escolha "mais barata" pode sair na verdade "mais caro", com certeza o investimento necessário será obtido.



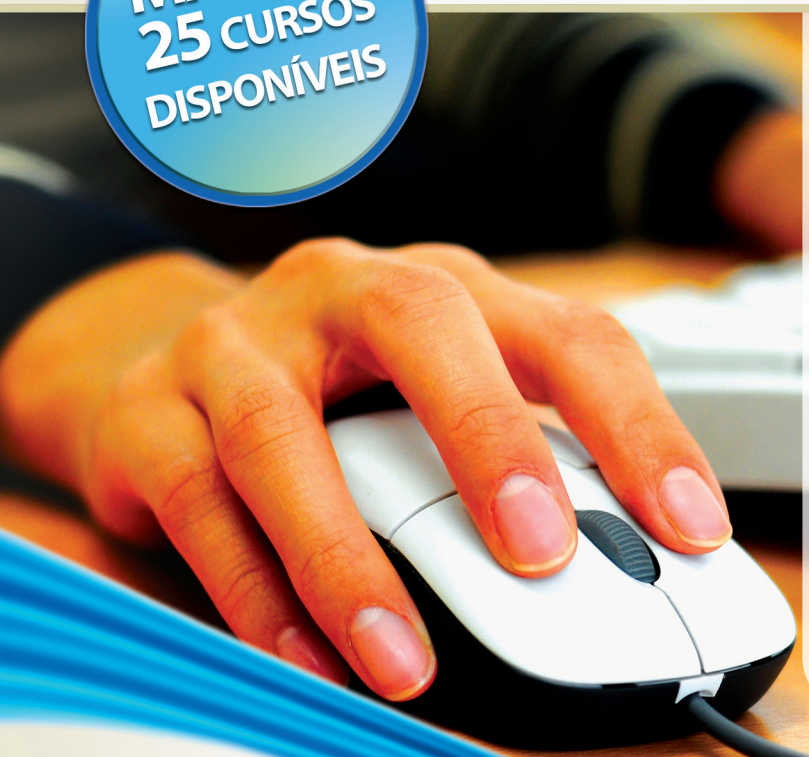
Roberto Henrique de Sousa
roberto@abctec.com.br, www.abctec.com.br
É Analista de Segurança da Informação na ABCTec, com 14 anos de experiência na área de TI (Suporte, Gestão, Consultoria), especializado em análise de vulnerabilidades e no tratamento de incidentes de segurança da informação.

CURSOS ONLINE

.net magazine

A Revista .net Magazine oferece aos seus assinantes uma série de Cursos Online de alto padrão de qualidade.

MAIS de 25 CURSOS DISPONÍVEIS



CONHEÇA OS CURSOS MAIS RECENTES:

- Curso .net Entity Framework - Loja Virtual
- Novidades do Visual Studio 2010
- Componentes DevExpress
- Crie um chat utilizando Asp.Net 3.5 e Linq
- Novidades do C# (csharp) 3.0
- POO com C#
- Microsoft Visual Studio Tools for Office (VSTO)
- Computação na Nuvem com a Plataforma Microsoft Windows Azure

Para mais informações :

www.devmedia.com.br/curso/netmagazine

(21) 3382-5038

http://www.devmedia.com.br

DevMedia