

ESPECIAL: Data Deduplication no Windows Server
Elimine os dados duplicados de seus servidores



Edição 17



Introdução ao Amazon Web Services

Conheça os serviços e
saiba quando utilizá-los

Gerenciando privilégios e permissões

Como planejar o acesso de
usuários a arquivos e sistemas

SEGURANÇA EM AMBIENTES VIRTUALIZADOS

Confrontando vulnerabilidades e
mecanismos de defesa



SEU CARRO TEM SEGURO, SUA SAÚDE TEM SEGURO, MAS E O SEU EMPREGO... TÁ SEGURO??

Ministério do Trabalho e Emprego

NÃO DEIXE JUSTAMENTE A SUA CARREIRA FICAR EM RISCO!

Manter-se atualizado com todas as novidades do mercado de desenvolvimento é obrigação de todo bom programador. Faça agora mesmo um seguro para a sua carreira. Seja um assinante MVP!

Saia do risco!

TENHA ACESSO A:



+DE **290** CURSOS ONLINE



09 REVISTAS MENSAIS



9.074 VÍDEO-AULAS

POR
APENAS **69,90**
MENSAIS

QUEM TEM ESTÁ TRANQUILO.



DEV MEDIA

Acesse: www.devmedia.com.br/mvp



Edição 17 • 2014



Assine agora e tenha acesso a todo o conteúdo da DevMedia: www.devmedia.com.br/mvp

EXPEDIENTE

Editor

Eduardo Spínola (eduspinola@gmail.com)

Sub Editores

Marco Antônio Pereira Araújo (maraujo@devmedia.com.br)

Rodrigo Oliveira Spínola (rodrigo.devmedia@gmail.com)

Consultor Técnico

Daniella Costa

Jornalista Responsável Kaline Dolabella - JP24185

Capa e Diagramação Romulo Araujo

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 Infra Magazine, entre em contato com o editor, informando o título e mini-resumo do tema que você gostaria de publicar:



EDUARDO OLIVEIRA SPÍNOLA

eduspinola.wordpress.com

[@eduspinola](https://twitter.com/eduspinola) / [@Java_Magazine](https://twitter.com/Java_Magazine)

Artigo no estilo Solução Completa

04 – Data Deduplication: Removendo dados duplicados no Windows Server

[Luiz Cláudio Tebexreni Bezerra]

12 – Hypervisor: Segurança em ambientes virtualizados

[Arthur dos Santos Macedo e Christian Conceição Guerreiro Santos]

Conteúdo sobre Boas Práticas

22 – Controle de Acesso: Gerenciando privilégios e permissões

[Juliana Márcia Rezende Calado]

28 – Introdução ao Amazon Web Services

[Mateus Espadoto]

Sumário

Data Deduplication: Removendo dados duplicados no Windows Server

Saiba como eliminar os dados duplicados de seus servidores

Um dos grandes desafios da administração de TI nos dias atuais é atender as crescentes demandas de armazenamento de dados dentro de uma organização. Hoje os usuários necessitam armazenar milhares de arquivos texto, planilhas, imagens, vídeos, músicas, e-mails, entre outros tipos de dados. Há anos essa situação também já existia, em uma proporção menor, porém, com o avanço tecnológico, os arquivos e processos ficaram maiores. Assim, para que a TI possa atender as novas demandas de negócio, é necessário investimento em várias frentes, e no armazenamento é uma delas.

Contudo, não bastasse o grande desafio de fornecer armazenamento para os usuários, lidando com altos volumes de dados e alto investimento em hardware, é necessário entender também como os usuários armazenam estes dados nos servidores. Não é incomum verificar diversos tipos de arquivos duplicados em um servidor de arquivos. Por exemplo, um grupo de usuários do departamento de Contabilidade recebe por e-mail a ata de reunião realizada por eles. Supondo que este grupo tenha 30 pessoas, este mesmo arquivo poderá ser armazenado até 30 vezes em locais diferentes em um compartilhamento de rede, já que, além de pastas departamentais, os usuários possuem também pastas pessoais.

Neste exemplo, uma ata de reunião pode significar pouco espaço. Porém, dependendo do tipo de arquivo (apresentações de slides, vídeos, músicas, etc.) esse volume desperdiçado pode ser muito maior. Assim, seria de grande ajuda se estes dados duplicados pudessem ser eliminados, sem atrapalhar as atividades dos usuários.

Pensando nisso, neste artigo será abordado o conceito de Data Deduplication no Windows Server 2012, ferramenta poderosa que auxilia os administradores de TI a eliminar os dados duplicados no seu ambiente.

O que é o Data Deduplication?

Data Deduplication é um recurso disponível no Windows Server 2012 e Windows Server 2012 R2 utilizado

Fique por dentro

O crescente aumento do volume de dados das organizações é um assunto pertinente às equipes de infraestrutura de TI. Devido a esse aumento, torna-se necessário oferecer uma capacidade de storage com um volume cada vez maior.

Para o usuário, é imprescindível dispor de um bom volume de espaço disponível para armazenar os arquivos utilizados no dia-a-dia de suas atividades. Porém, grande parte do armazenamento consumido está relacionado a arquivos duplicados e outros dados redundantes armazenados pelos usuários em um ambiente de rede.

Pensando em solucionar esse problema, este artigo apresentará, na teoria e na prática, o Data Deduplication, sendo útil para os administradores de TI que pretendem implantar tal tecnologia em seu ambiente, tendo como principal objetivo a economia de espaço utilizado e a consequente redução dos custos de armazenamento.

para maximizar o espaço de armazenamento de dados.

O conceito de eliminação de dados duplicados não é novo. Atualmente existem diversas ferramentas (em formato de appliance de hardware ou software) que realizam esta função, porém, por apresentarem um alto custo e uma alta curva de aprendizado, não são adotadas pelas empresas.

Até que tivemos o lançamento do Windows Server 2012, que trouxe como uma de suas principais novidades uma nova função, chamada de Data Deduplication. O Data Deduplication é uma tecnologia baseada em software que permite maximizar o uso da capacidade de armazenamento de dados da organização, e o seu o princípio básico é a não necessidade de armazenamento do mesmo arquivo várias vezes.

Como funciona a eliminação dos dados duplicados?

Quando configurada a ferramenta Data Deduplication, o primeiro passo efetuado é uma varredura no volume em busca dos dados duplicados.

Durante este processo, o Data Deduplication simplesmente identificará os dados que estão em duplicidade. Após identificados, a

ferramenta irá manter apenas uma cópia do mesmo, e as demais serão substituídas por uma referência à cópia principal.

Todos sabem que os arquivos são formados por metadados, que contêm informações sobre o nome do arquivo, atributos, entre outras. Além disso, também sabemos que um arquivo é composto por diversos pedaços. Na **Figura 1** temos o exemplo do arquivo Teste01 no formato NTFS. Note que este arquivo possui diversos “pedaços”, descritos como A, B, C, D e E.

Já a **Figura 2** mostra o arquivo Teste02, que possui também diversos pedaços, assim como o arquivo Teste01, descritos como A, B, C, W e K.

Durante o processo de análise, o Data Deduplication irá analisar os arquivos do volume em que está configurado e irá encontrar os dados que estão em duplicidade.

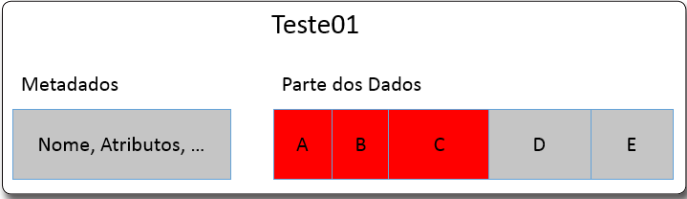


Figura 1. Formato do arquivo Teste01

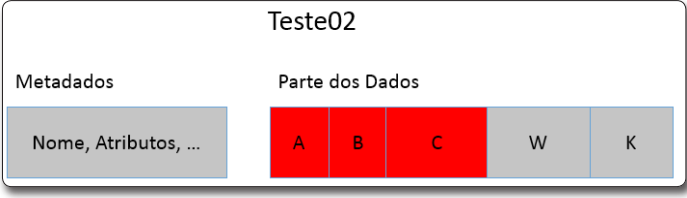


Figura 2. Formato do arquivo Teste02

Nesse momento, o Data Deduplication identificará que os arquivos Teste01 e Teste02 possuem dados em comum (duplicados). Então, serão gerados dados de análise na estrutura dos dois arquivos, como indicado na **Figura 3**. Estes dados de análise armazenarão informações sobre a identificação dos dados do arquivo e também dos links de apontamento para os blocos da cópia principal, eliminando assim o dado duplicado.

Quais resultados esperar com Data Deduplication?

Para que se possa realizar uma avaliação dos resultados a serem alcançados com a utilização do Data Deduplication, devemos primeiro avaliar os dados que estão dentro do volume que será afetado. A eficiência da eliminação dos dados duplicados será diretamente proporcional ao tipo de arquivo que o volume possui. As taxas de economia de espaço podem variar de 30% a 90%, segundo dados da própria Microsoft.

A **Tabela 1** apresenta a relação de economia de volume de acordo com o tipo de conteúdo dos arquivos.

Como a eliminação dos dados também exige tempo de leitura, processamento e gravação de dados, é necessário avaliar os recursos do servidor onde este recurso será aplicado. Um servidor que sempre estiver utilizando sua capacidade máxima

terá falta de recursos para realizar a eliminação dos dados. Podemos exemplificar essa situação com um servidor de arquivos que utiliza todos os seus recursos durante o período comercial (08h00 as 18h00). Em casos como este, onde o consumo de memória, de processamento e de disco são elevados, o Data Deduplication poderá ser configurado para ser executado em um período no qual a demanda é praticamente nula (fora do horário comercial), e desta forma, irá aumentar a eficiência do Data Deduplication.

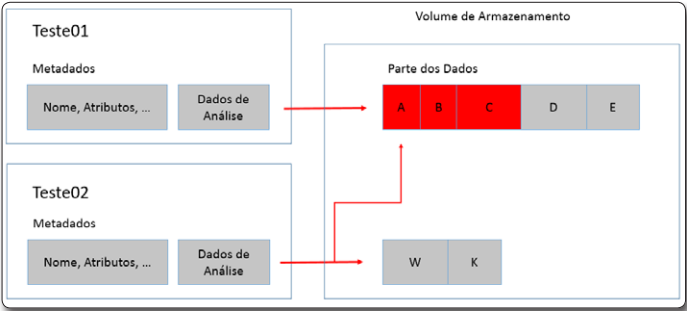


Figura 3. Identificação dos dados duplicados e link para substituição da informação

Cenário do Volume de dados	Conteúdo	Economia de espaço (variação)
Documentos diversos	Texto, imagem, áudio e vídeo	30-50%
Arquivos compartilhados pelo sistemas	Binários de software, arquivos de sistema, arquivos de símbolo	70-80%
Volumes de virtualização	Arquivos de disco rígido virtual	80-95%

Tabela 1. Redução variável de dados em um volume com Data Deduplication

Segundo a Microsoft, os tipos de servidores candidatos à eliminação de dados podem ser classificados a partir da análise da economia de espaço adquirida e dos recursos utilizados (memória, processamento, etc.).

De acordo com exaustivos testes e laboratórios por ela realizados, os candidatos são divididos em três categorias:

- Ótimos candidatos para eliminação de duplicação:
 - Servidores de redirecionamento de pastas;
 - Repositório de virtualização ou biblioteca de provisionamento;
 - Compartilhamentos de implantações de software;
 - Volumes de backup do SQL Server e do Exchange Server.
- Candidatos que devem ser avaliados com base no conteúdo dos dados a serem eliminados:
 - Servidores de linha de negócios (servidores que hospedam aplicações críticas para o negócio);
 - Provedores de conteúdo estático;
 - Servidores Web.
- Candidatos ruins para a eliminação de duplicação:
 - Hosts de Hyper-V;

- WSUS (*Windows Server Updates Services*) – Servidor de atualizações do Windows;
- Servidores que executam SQL Server ou Exchange Server;
- Arquivos com tamanho próximo a 1 TB ou que sejam maiores que isso.

Além das informações citadas anteriormente, outros fatores devem ser levados em consideração antes da implementação do Data Deduplication. São eles:

- O volume a ser configurado não pode ser o de inicialização de sistema. O Data Deduplication não suporta configuração em volumes que contenham a instalação do sistema operacional;
- A partição pode ser MBR (*Master Boot Record*) ou GPT (*GUID Partition Table*), e devem estar formatadas em NTFS;
- Os arquivos com atributos estendidos, arquivos criptografados e arquivos menores que 32 KB não são processados pelo Data Deduplication;
- Arquivos que são abertos ou alterados constantemente não terão economia (como máquinas virtuais, bancos de dados, etc.), já que, como os dados estão em uso, não será possível realizar a eliminação dos dados duplicados;
- Não suporta dispositivos removíveis.

Backup e Restore

Um recurso que é bastante impactado (de forma positiva) pelo uso de Data Deduplication é o backup dos dados da organização, visto que, com o aumento crescente da quantidade de dados sendo armazenados, consequentemente necessita-se de mais espaço para realização do backup.

Dito isso, atualmente, quais são os fatores que influenciam a realização de uma política de backup em uma organização?

- **Investimento:** Compra de hardware para backup. Se a empresa pretende gravar os dados em fitas, é necessário um hardware específico para que a gravação seja realizada;
- **Volume:** Quanto maior o volume de dados, maior será a quantidade de fitas necessárias para realização do backup;
- **Janela de Backup:** A junção do volume de dados ao hardware utilizado irá influenciar diretamente na janela de backup, já que quanto maior o volume de dados, maior será o tempo necessário para gravação. Para diminuir essa janela, é necessário hardware com velocidade maior para acelerar o processo. Consequentemente, a janela de backup também é importante, porque ela deve estar alinhada às necessidades da política de backup da empresa. Por exemplo, caso a empresa tenha necessidade de garantir uma retenção de dados que foram salvos nas fitas por uma semana, esta janela não pode ter um período maior do que sete dias para ocorrer, caso contrário, não atenderá à política adotada;
- **Restore:** Quanto tempo seria necessário para restauração dos dados em caso de um desastre? Se por algum motivo acontecer um problema e a restauração dos dados se torna necessária, o tempo do *restore* será proporcional ao volume de dados persistido no backup, ou seja, quanto maior o volume, mais tempo será gasto para executar a restauração.

Um volume com os dados duplicados eliminados irá proporcionar a realização de um backup mais rápido, consumindo um menor número de fitas e otimizando o tempo de restore.

A função Windows Backup, nativa no Windows Server, possui suporte para realização de backups de volumes que estejam com o recurso de Data Deduplication ativado. E além da Microsoft, existem outros fornecedores que disponibilizam ferramentas de backup com suporte a esta função (HP, CA, etc). Deste modo, antes de adquirir uma destas soluções, é aconselhável consultar a documentação de cada produto.

Com isso, podemos afirmar que além do benefício da economia de espaço em disco gerado pela eliminação dos dados duplicados, o ganho com a performance do backup também é muito válido e deve ser analisado no momento da implantação desse recurso.

Data Deduplication no Windows Server 2012 R2

Neste tópico será demonstrado como implementar a função de Data Deduplication no Windows Server 2012 R2. Para isto, existem duas opções: através do Server Manager e através do Powershell.

O Server Manager é uma ferramenta que tem como função auxiliar os administradores de TI, centralizando diversas opções para instalação, configuração e gerenciamento de funções e recursos de servidores. Quando um usuário faz logon em um servidor, por padrão, a janela do Server Manager é iniciada, conforme demonstra a **Figura 4**.

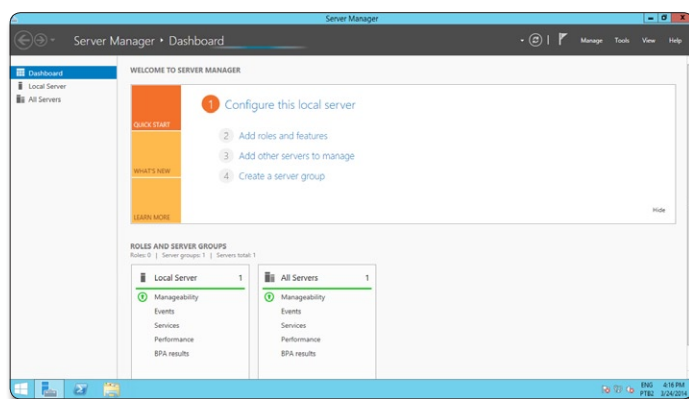


Figura 4. Tela Inicial do Server Manager

Para realizar a instalação do Data Deduplication através do Server Manager, na tela inicial, clique em *Add roles and features*. Feito isso, será carregada a tela inicial para instalação e configuração de Roles (Funções) e Features (Recursos).

A primeira tela mostra uma visão geral do assistente e lista algumas informações antes de prosseguir com a instalação. Esta lista destaca algumas boas práticas ao administrar servidores, a saber: ter uma senha de administrador forte; que as configurações de rede, como os endereços IP estáticos, já estejam definidas; e ter as atualizações do Windows Update instaladas (ver **Figura 5**). Para confirmar estas informações, basta clicar em *Next*. Neste ponto vale ressaltar que esses itens não são pré-requisitos, portanto,

mesmo não sendo atendidos, a instalação poderá continuar sem problemas.

A segunda janela do assistente irá definir o tipo de instalação, fornecendo duas opções: Instalação baseada em Role ou Feature ou Instalação para Serviços de Desktop Remoto. Neste caso, utilizaremos a primeira opção, como indica a **Figura 6**. Feito isso, clique mais uma vez em *Next*.

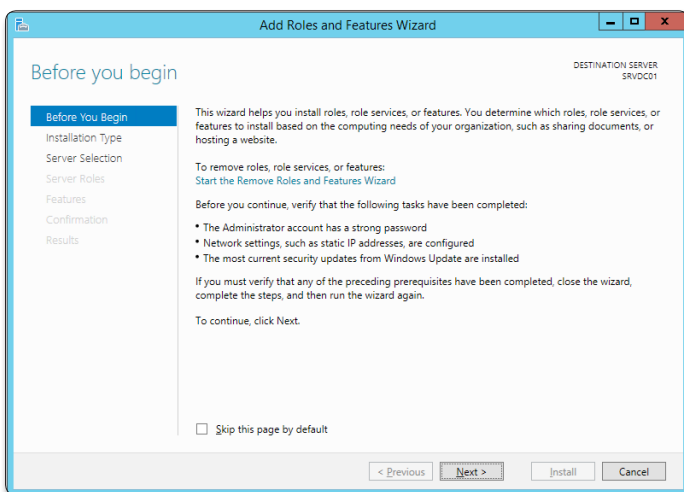


Figura 5. Tela inicial do assistente para adicionar Roles e Features

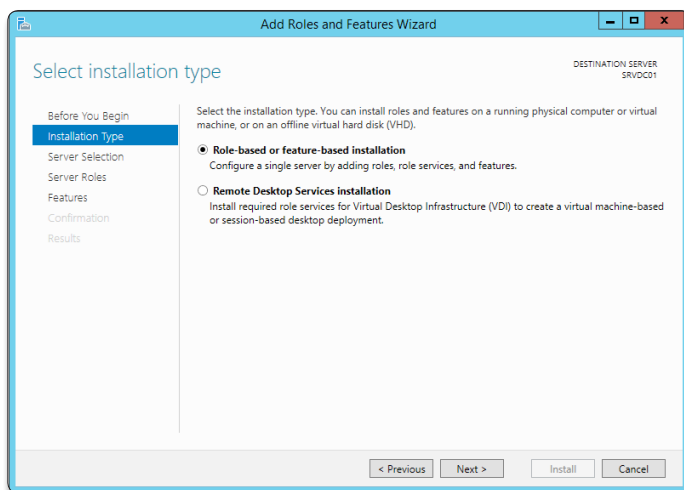


Figura 6. Seleção do tipo de instalação

No terceiro passo deve-se selecionar o servidor ou o disco virtual onde desejamos implantar o Data Deduplication. Neste caso, marque a primeira opção e depois selecione o servidor *SRVDC01*, conforme indica a **Figura 7**. Em seguida, clique em *Next*.

No quarto passo, devemos selecionar quais Roles serão instaladas. O assistente irá listar as Roles disponíveis para instalação no servidor (como DNS Server, Hyper-V, DHCP Server, entre outros). Para tanto, expanda a opção *File and Storage Services*, depois *File and iSCSI Services* e selecione *Data Deduplication*, conforme a **Figura 8**. Logo após, clique novamente em *Next*.

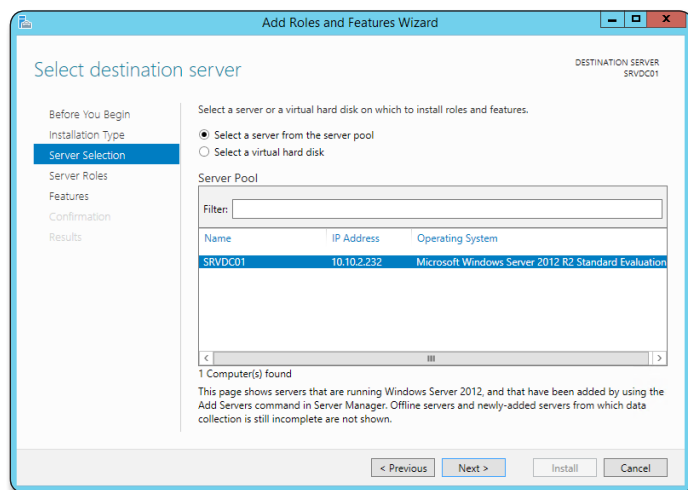


Figura 7. Seleção do servidor de destino

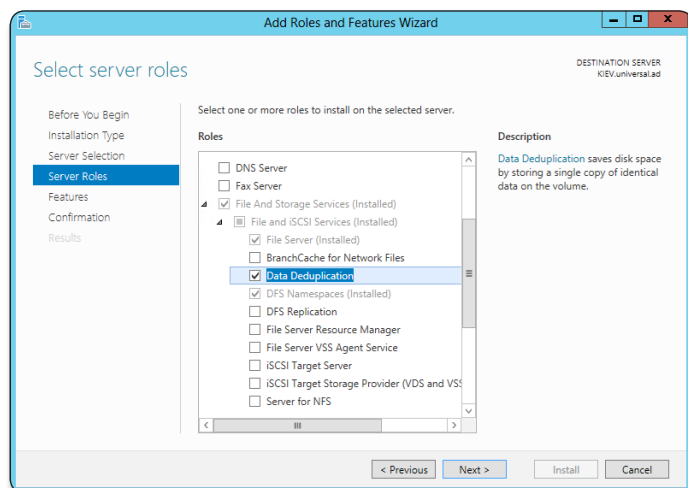


Figura 8. Seleção da Role Data Deduplication

No quinto passo, deve-se selecionar as Features que serão instaladas. Neste laboratório, não iremos instalar nenhuma Feature. Portanto, podemos avançar neste passo. O sexto passo, que é o final, irá mostrar um resumo do que será instalado. Nesta janela também há uma opção que, ao ser marcada, reiniciará o servidor destino assim que a instalação for concluída, caso seja necessário. Observe a **Figura 9**.

A segunda forma para instalação do Data Deduplication é através do PowerShell. Para tanto, abra o Windows Powershell e execute os comandos apresentados a seguir, que também podem ser analisados na **Figura 10**:

```
Import-Module ServerManager
Add-WindowsFeature -name FS-Data-Deduplication
Import-Module Deduplication
```

Após completar a instalação do Data Deduplication, podemos verificar no Server Manager uma nova guia de navegação,

denominada *File and Storage Services* (veja a **Figura 11**). Será esta guia que será utilizada para realizar as configurações deste recurso.

Agora que a função está instalada, o próximo passo é habilitá-la e configurá-la nos volumes de dados desejados. Para esta demonstração, foi criada uma partição de

30 GB, denominada *Teste_Dedup*, conforme a **Figura 12**, que pode ser analisada através do *Computer Management*, localizado junto às ferramentas administrativas do Windows.

Para iniciar a configuração do Data Deduplication, no Server Manager, acesse a guia *File and Storage Services* e depois a guia *Disk*, para exibir os discos e os volumes existentes no servidor (veja a **Figura 13**).

No espaço *Volumes*, visualizado na parte inferior da janela, são exibidos os volumes disponíveis. Conforme comentado anteriormente, foi criado um volume para realização desta demonstração, representado pela unidade E.

Assim, clique com o botão direito do mouse sobre este volume e selecione a opção *Configure Data Deduplication*, de acordo com a **Figura 14**.

Na janela *Deduplication Settings*, é necessário selecionar algumas opções para configurar o Data Deduplication, a saber:

- Em *Data deduplication*, podemos definir o tipo do volume a ser utilizado, que pode ser *General Purpose file server* (Servidor de Arquivos de Uso Geral) ou *Virtual Desktop Infrastructure (VDI) Server* (Servidor para infraestrutura virtual VDI);
- Em *Deduplicate files older than (in days)*, podemos definir a partir de quantos dias o arquivo será eliminado. Caso informe 3, os dados que forem gravados só serão analisados após o terceiro dia;
- Em *Custom file extensions to exclude*, podemos definir extensões de arquivos a serem excluídas do processo de eliminação de dados duplicados;
- Por fim, em *To exclude selected folders from data deduplication*, podemos definir pastas que devem ser excluídas da verificação para eliminação de dados duplicados.

Na **Figura 15** apresentamos as configurações que realizamos para o nosso exemplo.

Nesta janela também é possível clicar no botão *Set Deduplication Schedule...*, que permite configurar a opção *Enable background optimization* (Otimização de Desempenho em Segundo Plano), onde o Data Deduplication irá utilizar o sistema de forma a minimizar o impacto

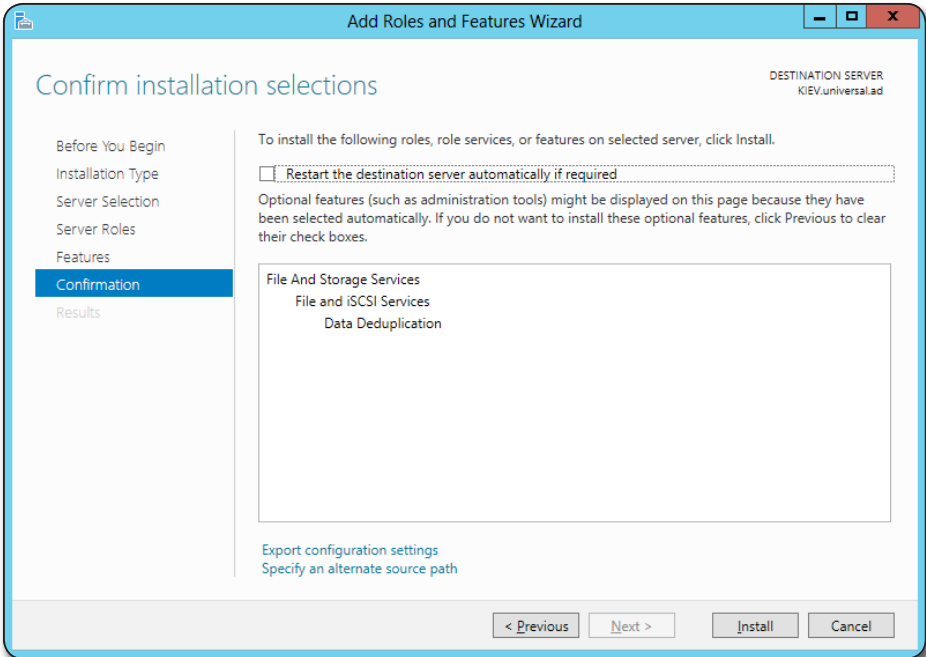


Figura 9. Resumo da instalação

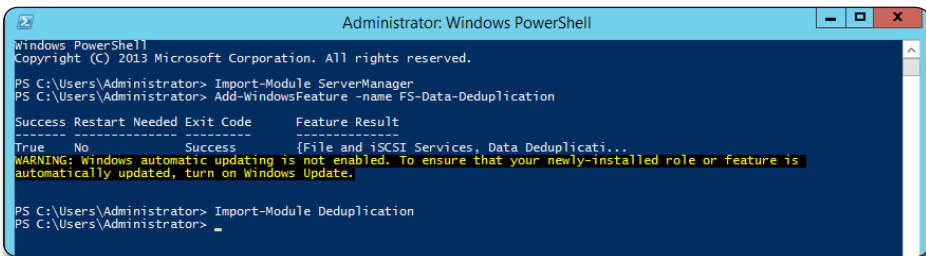


Figura 10. Instalação do Data Deduplication através do PowerShell

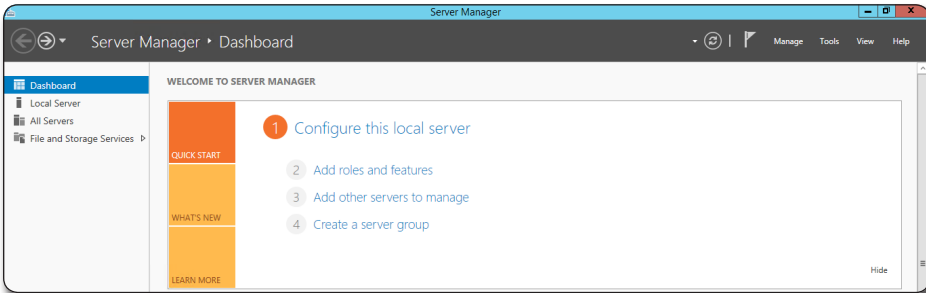


Figura 11. Server Manager com a guia File and Storage Services

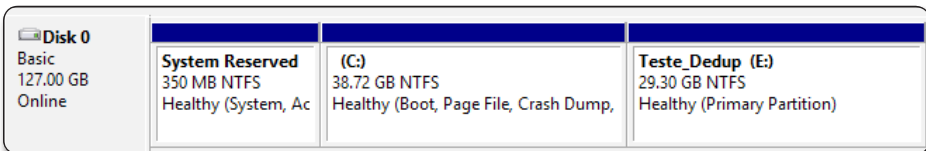


Figura 12. Volume de dados criado para realizar a demonstração do Data Deduplication

no desempenho do servidor, e também a opção *Enable throughput optimization* (Habilitar a otimização do rendimento), que possibilita agendar as datas e horários específicos para rodar o Data Deduplication, podendo assim consumir o máximo de recursos disponíveis no servidor (veja a Figura 16).

Verificando o desempenho do Data Deduplication

Para demonstrar a execução deste recurso, foram gravados neste disco de teste aproximadamente 25 GB de dados variados, contendo documentos de texto, imagens, arquivos de áudio, vídeos, entre outros, como pode ser verificado na Figura 17.

Neste ambiente de teste, após 48 horas, já é possível verificar e analisar os resultados obtidos com a utilização do Data Deduplication. O tempo necessário para realização da eliminação de dados duplicados varia de acordo com o tipo de dado armazenado, o volume total de dados, entre outros fatores, como a utilização da otimização em segundo plano e a otimização de desempenho.

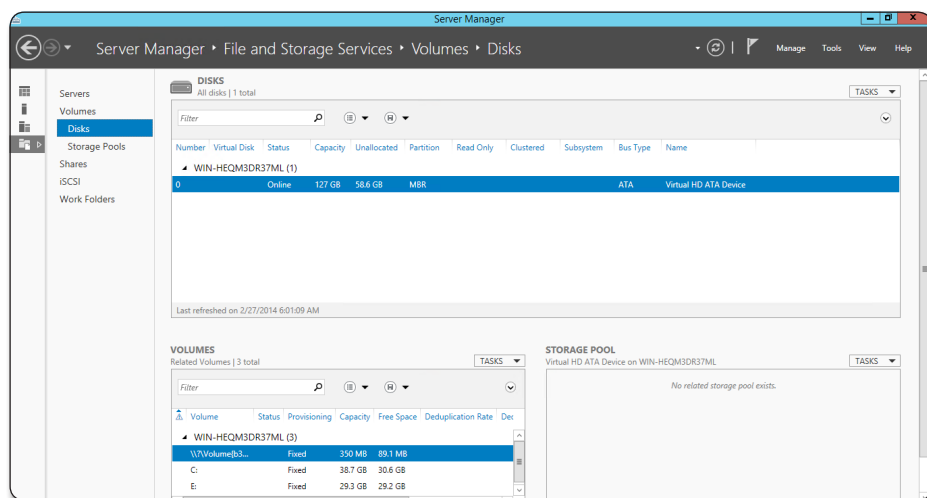


Figura 13. Discos e volumes disponíveis no Server Manager

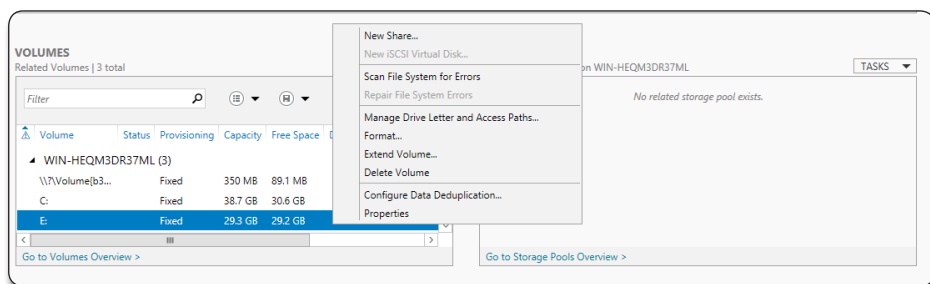


Figura 14. Configurando o Data Deduplication no volume E



RENOVE JÁ!

Sua assinatura pode estar acabando

Renovando a assinatura de sua revista favorita
você ganha brindes e descontos exclusivos.



Analisando as propriedades da pasta *Documentos*, conforme a **Figura 18**, pode-se verificar que o volume possui um total de dados de 23,4 GB, informado no campo *Size*, e após a realização da eliminação dos dados duplicados, passa a apresentar um volume gravado no disco (*Size on Disk*) de 187 MB. Como pode-se notar, neste exemplo a economia de armazenamento de disco gerada pelo Data Deduplication foi de 23 GB.

Também é possível verificar nas propriedades do disco a economia gerada pelo Data Deduplication, como demonstra a **Figura 19**.

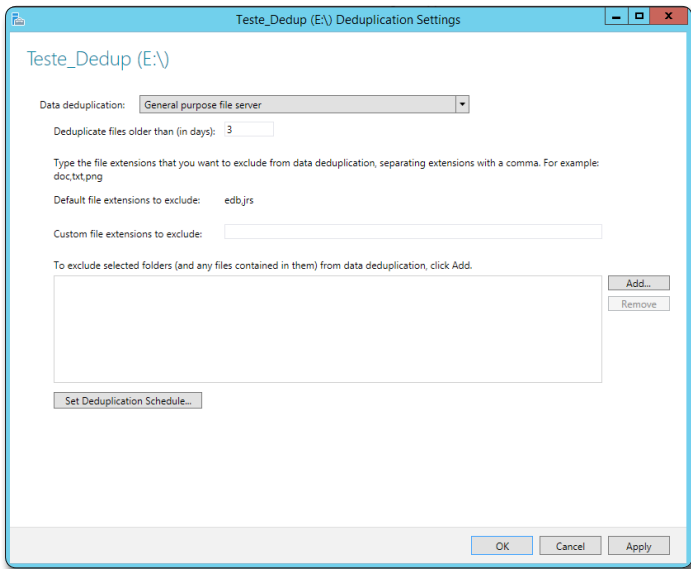


Figura 15. Propriedades de configuração do Data Deduplication

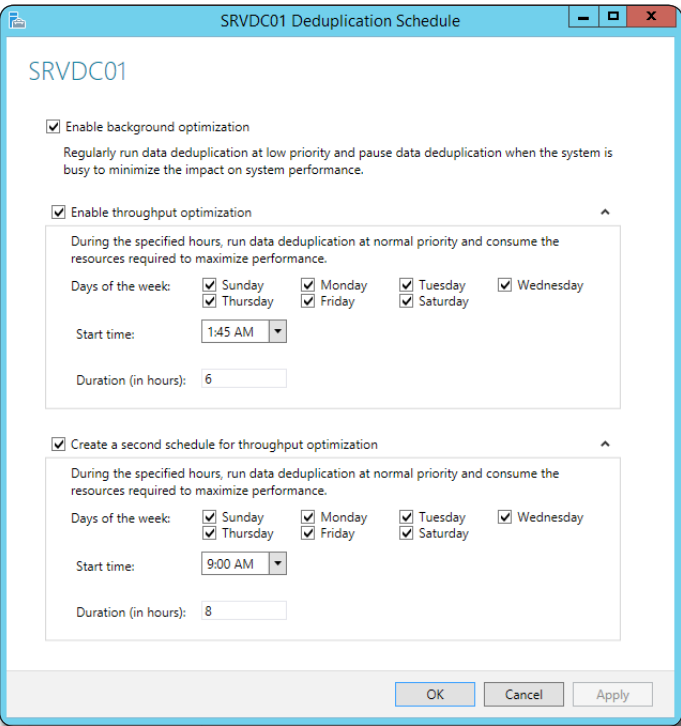


Figura 16. Opções de agendamento para eliminação de dados duplicados

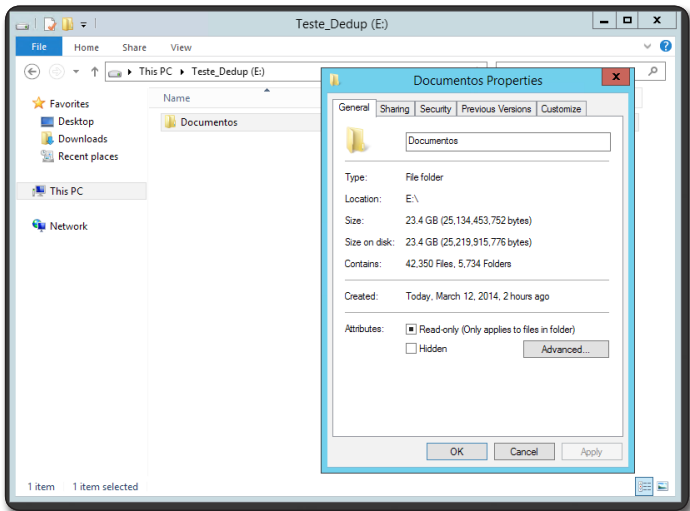


Figura 17. Volume de dados gravado no volume

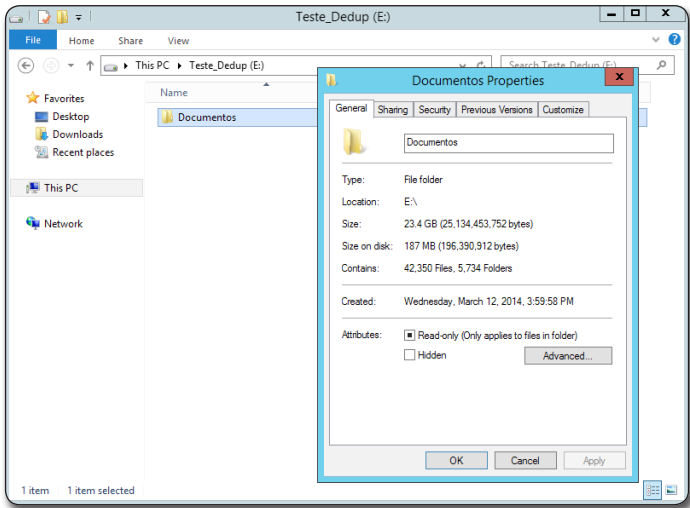


Figura 18. Volume de dados após a eliminação dos dados duplicados

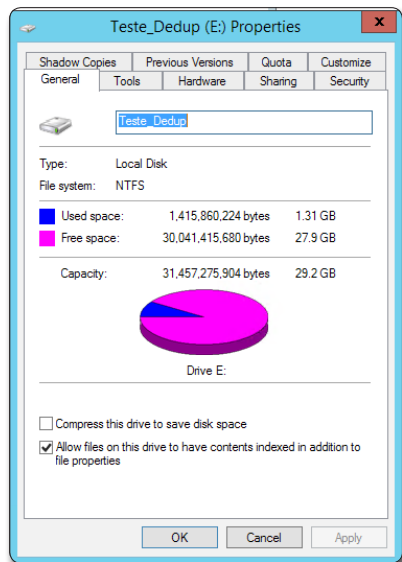


Figura 19. Propriedades do volume de dados

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-DedupVolume

Enabled      UsageType      SavedSpace      SavingsRate      Volume
-----      -
True         Default        22.57 GB        94 %             E:
```

Figura 20. Resultado do comando Get-DedupVolume

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-DedupVolume |fl

Volume           : E:
VolumeId          : \\?\Volume{75d920cc-9018-11e3-80b2-00155d01d000}\
Enabled           : True
UsageType         : Default
DataAccessEnabled : True
Capacity          : 29.3 GB
FreeSpace         : 27.98 GB
UsedSpace         : 1.32 GB
UnoptimizedSize   : 23.89 GB
SavedSpace        : 22.57 GB
SavingsRate       : 94 %
MinimumFileAgeDays : 3
MinimumFileSize   : 32768
NoCompress        : False
ExcludeFolder     : 
ExcludeFileType   : 
ExcludeFileTypeDefault : {edb, jrs}
NoCompressionFileType : {asf, mov, wma, wmv...}
ChunkRedundancyThreshold : 100
Verify           : False
OptimizeInUseFiles : False
OptimizePartialFiles : False

PS C:\Users\Administrator>
```

Figura 21. Resultado do comando Get-DedupVolume |fl

Outra forma de validar os ganhos com Data Deduplication é através do PowerShell. Com dois comandos podemos analisar o status da eliminação dos dados e diversas outras informações.

O primeiro comando mostra um resumo do volume que teve os dados duplicados eliminados (ver Figura 20). Para verificar esses dados, abra o PowerShell e digite o seguinte comando: *Get-DedupVolume*.

O segundo comando também mostra um resumo, porém mais detalhado (ver Figura 21). Para verificar esses dados, com o PowerShell aberto, execute o seguinte comando:

Get-DedupVolume |fl.

Em ambos os casos é possível constatar que, no laboratório realizado, o Data Deduplication economizou 94% do espaço no volume (informação indicada no campo *SavingsRate*).

A utilização da ferramenta Data Deduplication pode trazer muitos resultados positivos para as organizações. Dentre eles, podemos destacar a redução do espaço utilizado para armazenamento de dados, maior agilidade na realização e restauração de backups, e redução do custo de investimento em TI.

Assim, com a realização de um planejamento para implantação deste recurso, a administração de TI terá uma poderosa ferramenta que proporcionará tanto benefícios de economia de espaço em disco, como benefícios financeiros, já que, com a redução de consumo, não será necessário o investimento recorrente em hardware para armazenamento de dados.

Autor



Luiz Cláudio Tebexreni Bezerra

luizctbezerra@gmail.com

Administrador de Redes Windows Senior pela All Net Group, com ampla experiência no planejamento, implementação e administração de servidores na plataforma Microsoft e seus produtos. Formado em Administração de Empresas com Ênfase em TI pela Faculdade Impacta de Tecnologia, possui as certificações Microsoft (MCP, MCSA, MCSA, MCSE, MCSA+M, MCSE+M, MCTS, MCITP, MCT), ITIL e ISO 20.000.



Links:

Visão Geral de Eliminação de Duplicação de Dados

<http://technet.microsoft.com/pt-br/library/hh831602.aspx>

Microsoft Press blog - Windows Server 2012's Data Deduplication feature

http://blogs.msdn.com/b/microsoft_press/archive/2012/10/22/from-the-mvps-windows-server-2012-s-data-deduplication-feature.aspx

Step-by-Step: Reduce Storage Costs with Data Deduplication in Windows Server 2012

http://blogs.technet.com/b/keithmayer/archive/2012/12/12/step-by-step-reduce-storage-costs-with-data-deduplication-in-windows-server-2012.aspx#.UyGiZ_IdWBG

Hypervisor: Segurança em ambientes virtualizados

Confrontando vulnerabilidades e mecanismos de defesa

Virtualização é a simulação de um *hardware/software* que roda sobre outro *software*. Este conceito de ambiente simulado é chamando de máquina virtual (VM – *Virtual Machine*).

Basicamente, a virtualização permite que as organizações possam trabalhar com diversas plataformas de *software* (sistemas operacionais), não havendo necessidade de aumento no número de máquinas físicas. Ou seja, a virtualização permite um alto nível de flexibilidade e portabilidade. Com isso desmitificou-se a ideia de que para um novo serviço de TI a ser implantado em um ambiente era necessário uma máquina física nova.

Outra característica deste tipo de tecnologia é o compartilhamento dos recursos de *hardware* (processador, memória, interface de rede, disco, etc.) do *host* físico com todas as máquinas virtuais ali presentes. Por exemplo, caso um *host* possua quatro processadores, ele pode compartilhar um processador com cada uma das quatro máquinas virtuais.

Todo o gerenciamento e alocação de recursos de *hardware* de uma máquina virtual é feito pelo *Hypervisor* ou Monitor de Máquina Virtual (VMM – *Virtual Machine Monitor*). O *Hypervisor* é uma camada de *software* localizada entre a camada de *hardware* e o sistema operacional. É, também, responsável por controlar o acesso do sistema operacional visitante (máquina virtual) aos dispositivos de *hardware*. Ele também deve prover recursos que garantam a segurança das máquinas virtuais através de mecanismos como isolamento, particionamento e encapsulamento.

A virtualização é dividida basicamente em paravirtualização e virtualização completa. Na completa, o *hypervisor* simula todo o *hardware* da máquina física, fazendo com que as máquinas virtuais executem de forma isolada. Em outras palavras, o *hypervisor* emula todo o *hardware* para as VMs, fazendo com que o sistema operacional execute como se não estivesse em um ambiente virtual. Sua vantagem é a larga aceitação por parte de diversos tipos de sistemas operacionais.

Fique por dentro

O avanço da tecnologia de virtualização permitiu seu uso em grandes proporções nos ambientes de TI. A razão principal do uso de máquinas virtuais tem sido a consolidação de servidores e, consequentemente, a redução de custos em *hardware*, *software* e gerenciamento do ambiente. No entanto, há muitas dúvidas sobre a segurança desse tipo de tecnologia. Este artigo apresenta fundamentos e características da virtualização, e expõe o quanto ambientes virtualizados podem sofrer ataques à segurança. Explora também medidas de combate para as ameaças e formas de como planejar um ambiente virtual seguro.

Já a paravirtualização entrega para as VMs um *hardware* igual ao real, com isso o sistema a ser virtualizado pode sofrer alterações no decorrer do tempo. Funcionalidade esta que a virtualização completa não permite, já que nela o *hardware* é entregue de forma virtual. A principal característica da paravirtualização é o desempenho, ou seja, sua facilidade em se adaptar às modificações do sistema operacional devido a sua similaridade com o *hardware* real.

A virtualização contribuiu para o desenvolvimento e aprimoramento de outras tecnologias já existentes, fazendo com que elas se aperfeiçoassem, tais como: sistemas operacionais, componentes de *hardware*, *storage* e rede.

Com os avanços desta tecnologia, as técnicas e melhorias em segurança em ambientes deste tipo também tiveram que ser aperfeiçoadas e recriadas para garantir a integridade e segurança de dados e *hardware*.

O objetivo deste trabalho é analisar ambientes virtualizados quanto à segurança, trazendo à tona assuntos às vezes incomuns quando se fala de virtualização. Este trabalho pretende verificar o quanto o *hypervisor* é seguro. Para isso, identificará possíveis brechas para ataques, descreverá quais são estes ataques e as contramedidas oferecidas pelas soluções disponíveis no mercado.

Em complemento, vamos estabelecer um contraponto entre as tecnologias existentes, mostrando como algumas tratam a temá-

tica da segurança e como as organizações podem se precaver de incidentes e ameaças.

Visão Geral do Hypervisor

O *Hypervisor* é uma camada de *software* localizada entre o *hardware* e as máquinas virtuais, sendo responsável por fornecer recursos (*storage*, CPU, memória, rede, etc.) da máquina física para a máquina virtual. Ele permite que vários sistemas operacionais possam ser executados em um mesmo *host*.

A virtualização do tipo completa fornece dois tipos de *hypervisor*. O tipo 1, chamado de *bare-metal* e o tipo 2, chamado de *hosted*. O *hypervisor* do tipo *bare-metal* interage diretamente com o *hardware* da máquina física. Ele é completamente independente do sistema operacional do *host*. Já no tipo *hosted*, o *hypervisor* roda sobre o sistema operacional do *host*, sendo isto possível em qualquer tipo de SO.

Como mostra a **Figura 1** o tipo *hosted* possui uma camada a mais de aplicação junto com a camada do *hypervisor*, e ambas sobre o sistema operacional do *host*. Esta camada de aplicação permite, por exemplo, a troca de arquivos entre o SO do *host* com o ambiente virtual e também permite que os usuários possam executar aplicações tais como *web browsers* e clientes de e-mail paralelamente ao ambiente virtualizado. Isto não é possível no tipo *bare-metal*.

Os servidores são frequentemente virtualizados no modo *bare-metal*. Já o *hosted* é comumente utilizado em soluções voltadas para uso em desktops, como o VirtualBox. A maioria dos *hypervisors* oferecem recursos adicionais de *hardware*, que vão desde controladores USB até *direct memory access* (DMA), visando com o DMA melhorar o desempenho de controladores de *storage* (no que diz respeito a acesso a disco) e placas de rede.

Visto isso, a decisão de usar *hypervisor bare-metal* ou *hosted* vai além de “ter ou não ter sistema operacional no *host*”. A primeira opção, por exemplo, por estar situada diretamente sobre o *hardware*, consegue prover um número maior de opções de acesso de entrada e saída (I/O *access*), disponibilizando mais desempenho para aqueles que optam por essa arquitetura.

Já a segunda opção consegue prover maior compatibilidade de *hardware*, o que permite executar o *software* de virtualização em uma gama mais ampla de configurações de *hardware*, diferentemente do modo *bare-metal*.

Como já informado, o *hypervisor* utiliza os recursos oferecidos pelo sistema operacional nativo para oferecer recursos virtuais ao sistema operacional convidado que executa sobre ele.

É importante frisar que medidas operacionais e de segurança também devem ser levadas em consideração na escolha da arquitetura utilizada, como será apresentado nas próximas seções.

Segurança em Ambientes Virtualizados

Uma pesquisa da Associação Brasileira de e-business (e-business Brasil) realizada em 2012 constatou que os investimentos em virtualização nos ambientes de TI aumentaram cerca de 80% em relação aos últimos três anos. A pesquisa, que durou cerca de um ano e entrevistou mais de 500 investidores, constatou um aumento gradativo a partir de 2009, principalmente com o surgimento e aprimoramento da técnica de computação em nuvem.

Outra pesquisa, também em 2012, constatou que 85% das organizações de todo o mundo planeja ou já possui virtualização em seus ambientes de TI. E 52% de todos os ambientes, com servidores x86, são virtualizados, sendo esperado um aumento para 75% em dois anos.

Tais pesquisas indicam a importância que a virtualização vem conquistando nos ambientes de tecnologia da informação. Ainda assim, existe certa resistência em seu uso. De um lado existem benefícios como: redução de custos com energia elétrica (com a redução de equipamentos de *hardware*), redução de investimento em *hardware* (tanto em compra de equipamento, como em manutenção), flexibilidade, disponibilidade, etc.

Do outro, a segurança neste tipo de ambiente ainda provoca dúvidas nos profissionais de TI. Fazendo uma análise hipotética, supondo que um ambiente totalmente virtualizado sofra qualquer tipo de ataque à integridade física (*hardware*) ou lógica (*software*) do *host* e o mesmo venha a parar, as máquinas virtuais ali presentes também irão parar, causando sérios danos à empresa/organização.

Por mais que existam técnicas de replicação, *backup* e *cluster*, ainda há o risco de um ataque que, a depender da intensidade, acabe afetando a disponibilidade das máquinas virtuais. Até porque, se algum invasor conseguir penetrar em uma VM, ele provavelmente vai conseguir acesso a alguma outra. E acessando qualquer máquina virtual ele pode apagar dados de *backup*, dados do *storage*, apagar as máquinas virtuais do *host*, etc.

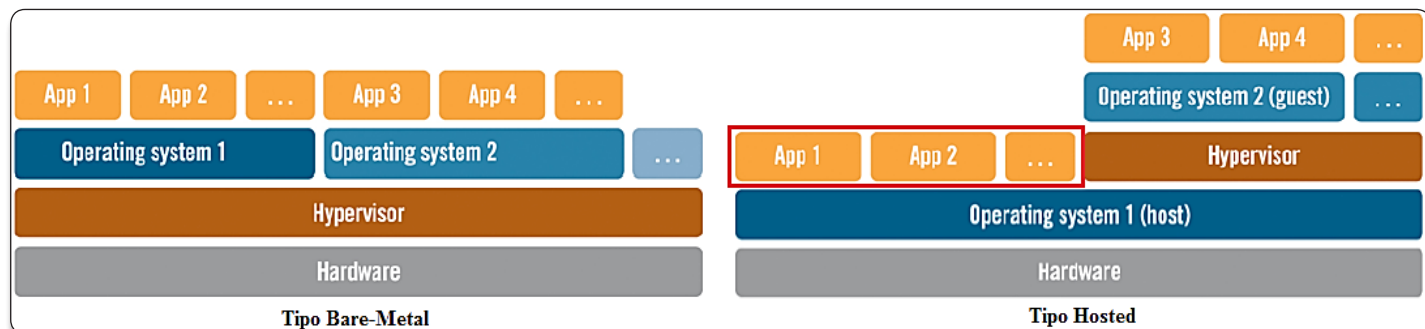


Figura 1. Ilustração do hypervisor tipo hosted e bare-metal

Em fevereiro de 2011, uma companhia farmacêutica japonesa chamada Shionogi foi invadida por um administrador de TI, chamado de Jason Cornish. Jason utilizou uma conta de serviço para acessar a rede da companhia. Estando dentro do ambiente da empresa, Jason, através de uma instalação do VMware vSphere deletou 88 máquinas virtuais. Sendo que dentro dessa contagem de VMs excluídas há servidores de e-mail, BlackBerry Server, servidores de aplicações financeiras, etc.

A Shionogi passou alguns dias para conseguir se reestabelecer, perdendo vendas, comunicação por e-mail, entre outros prejuízos. A partir deste exemplo, é notório os prejuízos que qualquer tipo de indisponibilidade em um ambiente de TI pode causar, principalmente quando se trata de ambiente virtualizado, já que o host físico acomoda diversas VMs com funcionalidades distintas.

Vale ressaltar que este exemplo não é caracterizado como um ataque, mas sim como uma falha humana, já que a credencial de acesso do funcionário deveria ter sido desativada uma vez que ele havia sido demitido. Contudo, falhas humanas também podem acarretar em brechas que possam facilitar a vida de um invasor.

Técnicas de Segurança em Ambientes Virtualizados

O simples fato de migrar um ambiente de TI para um ambiente virtual não traz praticamente nenhuma ameaça à segurança ou um aumento ou diminuição das ameaças e vulnerabilidades. Independente se um ambiente é virtual ou não, quando ocorre a migração, as mesmas ameaças, vírus e vulnerabilidades continuam presentes. O que pode ocorrer é uma forma diferente de ataque e defesa devido ao acréscimo de uma funcionalidade ou uma camada de *software*.

Este tópico foca justamente nesta discussão, mostrando alguns recursos da virtualização e como eles se relacionam com a segurança.

Anéis de Proteção (Protection Rings)

A família de CPUs x86 fornece quatro modos de operação para o processador em sua arquitetura, que são comumente chamados de anéis de proteção (*protection rings*) que são identificados de 0 a 3. Esses anéis funcionam como mecanismos de proteção de dados e funcionalidades contra falhas e ações maliciosas. Esses níveis de proteção são níveis de hierarquia de privilégio dentro de uma arquitetura de computação.

Como mostra a **Figura 2**, eles são organizados na hierarquia do mais privilegiado (0 é considerado o de maior nível hierárquico) ao menos privilegiado (os de maior número). O anel 0 interage mais especificamente com o *hardware* físico (CPU e memória) e é utilizado pelo sistema operacional. Ele pode executar qualquer tipo de instrução de CPU ou endereçamento de memória. Falhas neste nível do anel são catastróficas, tendo como consequência uma possível parada da máquina.

Já o anel 3 é empregado para os processos do usuário. Caso um processo do usuário tente acessar alguma instrução privilegiada do anel 0, uma exceção (*trap*) é gerada. Este nível não permite o acesso aos níveis mais baixos e privilegiados. Por conta deste

isolamento, falhas no modo usuário são, na maioria dos casos, passíveis de recuperação.

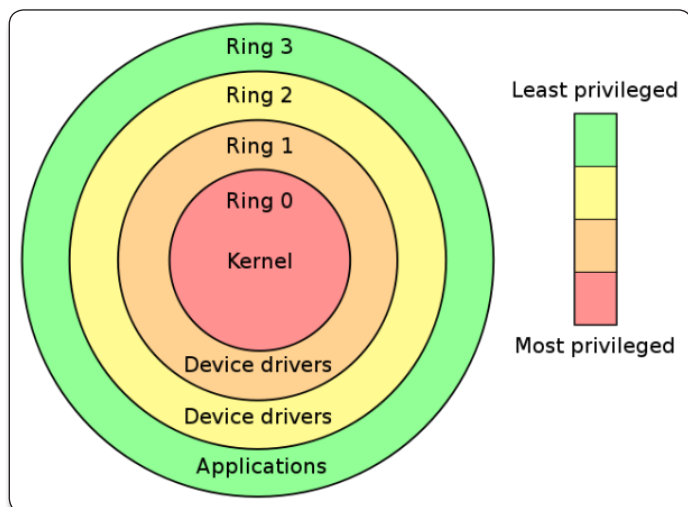


Figura 2. Anéis de Proteção

Isolamento da Máquina Virtual (Guest OS Isolation)

O *hypervisor* é responsável por gerenciar o acesso ao *hardware* pelos sistemas operacionais das VMs. Ele faz com que a máquina virtual enxergue o hardware como sendo apenas para seu uso, porém o hardware pode ser compartilhado com diversas outras, como geralmente ocorre. No entanto, esse compartilhamento não é visto pela máquina virtual. Assim, a VM assume que aquele hardware é dedicado unicamente para ela. Isso possibilita que uma VM funcione de forma separada uma da outra, não havendo possibilidade de uma acessar o recurso da outra. Por esta razão o recurso foi batizado de “isolamento da máquina virtual” e, por exemplo, está presente em ferramentas como Hyper-V e VMware ESXi.

Os recursos são divididos em duas categorias: lógica e física. A divisão lógica significa que o *hypervisor* entrega recursos para uma máquina virtual ou para várias máquinas virtuais. Isso quer dizer que os recursos (memória e processador, por exemplo) podem ou não ser compartilhados com várias VMs, como se fosse um *pool* de recursos com o *hypervisor* intermediando o acesso a eles. A divisão física propõe limitações à alocação de recursos para uma determinada VM, pois não compartilha com as outras máquinas virtuais. O *hypervisor* aloca um recurso fixo para uma determinada VM, o que significa que se determinada máquina virtual utilizar apenas uma parte do seu recurso disponível, o que não é utilizado por ela acaba ficando ocioso.

Essas características impostas pelo *hypervisor* possibilitam que caso uma VM seja infectada por algum *malware*, por exemplo, ele potencialmente não atinja a outra máquina virtual ou algum arquivo infectado de uma acabe passando para outra. Porém, foi emitido um alerta sobre este risco em meados de 2010 pela IBM, através de um de seus relatórios de segurança que medem a ocorrência de vulnerabilidades em ambientes virtualizados.

Este relatório apontava a ocorrência de um novo tipo de vulnerabilidade, chamado de “*escape-to-hypervisor*”, onde um invasor, a partir de uma máquina virtual, podia acessar qualquer outro recurso de uma VM qualquer.

A vulnerabilidade foi confirmada dois anos depois pela U.S. Computer Emergency Readiness Team (US-CERT), que afirmava que alguns sistemas operacionais x64 rodando em *hardware* Intel eram vulneráveis a ataques do tipo “*escape-to-hypervisor*”. A partir daí diversos outros fabricantes de *hypervisor* passaram a buscar correções para o “*bug*”.

A partir do exemplo de vulnerabilidade supracitado, percebe-se que o *hypervisor* ainda não pode ser classificado como um componente intransponível, como muitos o classificam. Ainda existem falhas e a cada dia são descobertas novas, fazendo com que seja necessário um cuidado especial na hora de levar algum serviço específico e de pouca possibilidade de paradas para um ambiente virtual.

Monitoramento da Máquina Virtual (Guest OS Monitoring)

O *hypervisor* possui recurso de auditoria em tudo o que é feito sob seu domínio, tendo plena capacidade de monitorar cada sistema operacional que executa sobre ele, sendo esta técnica conhecida como introspecção. A introspecção pode prover um monitoramento completo, que pode incluir tráfego de rede, memória, processos e diversas outras funcionalidades de um S.O., mesmo quando a segurança deste já foi comprometida.

Muitos produtos de virtualização incorporam a isso algumas outras funcionalidades, muitas vezes adicionando outras ferramentas para auxiliar, como por exemplo, a VMware, através do vSphere. Isto, em conjunto com a auditoria de introspecção, pode fornecer uma variedade extensa de parâmetros que controlam e monitoram os acessos à VM.

Imagem e Gerenciamento de Snapshot

Diversas ferramentas de virtualização disponibilizam para seus usuários a funcionalidade de *snapshot*, que permite que o sistema grave o estado atual da VM para que a mesma possa ser restaurada para algum ponto anteriormente capturado a qualquer momento. Pode-se citar o Hyper-V da Microsoft como um dos exemplos de ferramentas que possuem a funcionalidade de *snapshot*.

Oferecem também outra funcionalidade que é a imagem ou clone, que permite ao usuário criar uma cópia de VM e utilizá-la como sendo outra VM. Em outras palavras, supondo a necessidade de se criar uma VM nova no ambiente, o usuário pode recorrer a uma imagem/clone de uma VM, uma máquina virtual base, e a partir dela criar uma nova acrescentando apenas as funcionalidades necessárias.

Nota-se que o maior problema no uso dessas técnicas é o fato delas possuírem dados sensíveis (senhas, dados pessoais de usuários e etc.), similarmente como um disco rígido (HD) de um computador, podendo assim implicar em um vazamento de informações sigilosas. Tal comparação fica evidenciada na facilidade de manuseio das imagens e snapshots, por isso o contraste com o

HD e por isso, também, a necessidade de cuidados especiais.

Um *snapshot* pode prover mais riscos de segurança do que as imagens, pois o mesmo, além dos dados sensíveis, traz também conteúdo da memória e isso pode incluir informações confidenciais que nem sequer foram armazenadas na unidade.

Uma aplicação e sistemas operacionais podem ser configurados, testados e instalados em uma imagem e ser distribuída para diversos *hosts*. Tal prática proporciona ganho de tempo considerável, especialmente ao se imaginar a criação de muitas máquinas virtuais novas, operação que normalmente levaria um tempo considerável. Com isso, o controle de acesso a essas imagens é importante, visto que uma imagem em poder de alguém não autorizado se torna vulnerável a modificações indevidas e/ou maliciosas.

Movimentação de Máquinas Virtuais

Outra funcionalidade bastante presente nas ferramentas de virtualização (por exemplo, o vMotion no VMware ESXi) é a movimentação das máquinas virtuais presentes em um *host* para outro, provendo alta disponibilidade ao ambiente virtual. Por exemplo, caso seja necessário o desligamento ou reinicialização do *host* físico, é possível mover as máquinas virtuais ali presentes para outro *host*, sem que as mesmas desliguem, mantendo assim a disponibilidade do ambiente. Esse recurso também pode ser



Não perca tempo reinventando a roda!

COBREBEMX

Componente completo para sua Cobrança por Boleto Bancário e Débito em Conta Corrente

Mais de 40 exemplos em diversas linguagens de programação

Geração e leitura de arquivos (remessa e retorno) nos padrões FEBRABAN e CNAB

Testes e Downloads gratuitos em nosso site

ACESSE E CONHEÇA O COMPONENTE EM:
WWW.COBBREBEM.COM

utilizado em casos de ameaças de ataques ao *host* físico, tentando eliminar a chance da VM também ser infectada.

O *hypervisor* é capaz de realizar esta movimentação de forma automática a depender das configurações realizadas. Por exemplo, quando a carga de processamento em um dado *host* estiver muito alta, o *hypervisor* identifica isso e automaticamente move algumas VMs para outro *host*. Muitas vezes este *host* secundário fica em *standby* justamente para ocasiões desta natureza.

Contudo, não há garantia de sucesso nesse tipo de procedimento, até porque outros fatores estão envolvidos em uma movimentação como aspectos de rede, por exemplo. Se houver falha na rede durante a movimentação, o risco de a movimentação falhar e a VM desligar é grande.

Uma desvantagem em nível de segurança que merece ser destacada é que caso uma máquina virtual esteja infectada ou comprometida, e ela seja movida para outro *host* físico, isso pode acabar infectando, também, o próximo hospedeiro. O mesmo pode ocorrer em caso de migração de uma máquina física para virtual.

Criptografia de Máquina Virtual

Uma máquina virtual é essencialmente composta por arquivos, por conta disso um possível roubo de uma VM se torna ainda mais fácil. Sair de uma empresa com um *pendrive* é muito mais discreto do que sair com um servidor nas mãos.

Existem diversas formas de se criptografar os arquivos de uma máquina virtual, independentemente de onde ela esteja, se em um datacenter ou na nuvem, por exemplo. Cada forma de criptografia possui prós e contras, principalmente quando se trata de gerenciamento de chaves de decifração.

A seguir, alguns exemplos de locais onde as máquinas virtuais e seus dados podem ser criptografados:

- Dentro da própria máquina virtual. Exceto quando estão armazenadas em arquivos VMDK (Formato de arquivo desenvolvido pela VMware);
- Dentro do *hypervisor*. Porém, ainda não há indícios de criptografia no *hypervisor* em virtualização de servidores;
- Em um dispositivo de armazenamento NAS – Network-Attached Storage (qualquer dispositivo com quantidade grande de disco e que funcione como armazenador de dados). Com a vantagem de poder escolher qual parte da VM será criptografada caso o protocolo entre o dispositivo e o *hypervisor* seja o NFS;
- Dentro de *storage* (dispositivo com grande quantidade de discos para armazenamento, que oferece redundância de fontes de energia, alta disponibilidade, etc.). Geralmente utilizado através da tecnologia FDE (*Full Disk Encryption*), que criptografa todo o disco em nível de *hardware*.

Todas as opções citadas podem garantir alguma proteção para uma máquina virtual, porém elas não garantem flexibilidade para acompanhar o fluxo de trabalho de um ambiente de TI, por conta da rapidez do avanço da tecnologia.

Por exemplo, em alguns momentos os administradores de TI podem identificar a necessidade de migrar algum serviço para a

nuvem, o que no caso da adoção de alguns desses locais a migração seria mais difícil, já que não é viável levar toda sua massa de dados para a nuvem, por exemplo.

Uma forma de solucionar esta questão seria adotar algum modelo de armazenamento flexível, que englobaria tanto a criptografia como uma gerência melhor das chaves de descifração.

Ameaças e ataques mais comuns em ambientes virtuais

Embora a virtualização forneça inúmeras funcionalidades, ainda não é possível afirmar sua contribuição com relação à segurança. Além dos problemas de segurança enfrentados pelos profissionais de TI em ambientes físicos, a virtualização traz um novo risco, associado ao *hypervisor*.

O principal ponto de falhas e ataques em ambientes virtualizados é o *hypervisor*, por ser o elemento central de todo o sistema de virtualização e por gerenciar todo o ambiente virtual em um *host* físico, reunindo as principais funcionalidades e portas de acesso às VMs.

Em alguns sistemas de virtualização existe uma funcionalidade que permite que as máquinas virtuais sejam movidas de um *host* para o outro. Esta funcionalidade é acionada quando é necessário fazer alguma manutenção no *host*, quando há falhas e ameaças contra o *hypervisor* ou sistema operacional. A movimentação pode ocorrer mesmo quando a VM está em execução.

As empresas fornecedoras de *hypervisor* buscam a todo o momento formas de aumentar a segurança do seu produto e, consequentemente, passar mais credibilidade aos seus usuários. De acordo com Schwartz (2010), um estudo realizado pela IBM em 2010 contabilizou que cerca de 35% dos ataques em ambientes virtualizados são direcionados ao *hypervisor*. Como consequência, há uma preocupação dos fabricantes em consertar suas vulnerabilidades.

A todo o momento um ambiente de TI está sujeito a sofrer com os diversos tipos de ameaças à segurança, desde erros de algum funcionário até programas maliciosos que roubam dados. Em ambientes virtuais existem outros parâmetros que merecem ser analisados com cautela ao se manter ou projetar um ambiente virtualizado. Dentre os parâmetros existentes, destacam-se o controle de expansão do ambiente virtual, falta ou pouco monitoramento do ambiente, gerenciamento das responsabilidades perante o gerenciamento do ambiente virtual, detalhes de configuração (*firewall* e *networking*), entre outros.

As ameaças e ataques que serão expostos a seguir se tratam de visões abrangentes e em muitos casos não houve comprovação de em qual tecnologia de virtualização (VMware, Hyper-V, Xen, etc.) específica pode ocorrer tal ataque/ameaça. Portanto, na sequência serão analisados alguns tipos de ataques/ameaças, assim como técnicas para mitigá-los.

VM Escape

O assunto mais discutido quando se fala em segurança em virtualização e o mais temido entre os profissionais de TI é o *VM Escape* (*escape to hypervisor*, fuga do *hypervisor*), que se trata de uma

brecha de segurança em *hypervisors* VMware ESXi. Através dessa brecha um invasor consegue executar códigos maliciosos dentro de uma máquina virtual, podendo também executar comandos em outra VM ou até mesmo no *hypervisor*.

Alguns fabricantes possuem ferramentas que se assemelham ao comportamento do VM Escape, porém não foram classificadas como tal e não têm o mesmo objetivo. As ferramentas se caracterizam por permitir a livre transferência de dados entre uma VM e outra, necessitando que ambos os lados estejam com a ferramenta ativa. O que difere totalmente das características do *VM escape*, onde não há necessidade de se ter o mesmo código executando na outra VM. O invasor consegue acessar a outra VM se beneficiando de vulnerabilidades do sistema.

Existem outros tipos de ataques dentro dos conceitos de *VM Escape* que surgiram nos últimos anos. A seguir são apresentados alguns deles:

- **Directory Traversal Attack (Ataque de Passagem de Diretório):** A maior parte dos ataques *VM escape* partiram de ataques de passagem de diretório, que consistem em um atacante obter acesso a pastas/diretórios considerados seguros e com controle de acesso. Este tipo de vulnerabilidade esteve presente no VMware Workstation, permitindo a um atacante salvar, alterar, excluir ou mover arquivos entre diretórios até então restritos.

Em uma das conferências realizadas na SANSFIRE 2007, em Washington, DC, Tom Liston e Ed Skoudis apresentaram uma noção muito real de *VM escape*. Eles apresentaram ferramentas que exemplificavam como era possível ataques de *VM escape*. Dentre elas, destacam-se duas: VMchat e VM Drag-n-Sploit. A VMchat utilizava o canal de comunicação do *hypervisor* da VMware para passar mensagens entre máquinas virtuais e/ou entre máquina virtual e *host*. Não requerendo nenhum tipo de código especial e nenhum recurso adicional de redes, ou seja, a aplicação consistia em apenas um mensageiro comum. A VM Drag-n-Sploit utilizava os benefícios fornecidos pelo VMchat e com isso conseguia interceptar os dados que transitavam pelo canal de comunicação, podendo ele alterar os dados que estavam trafegando por ali. Isso era possível através da funcionalidade “*drag-n-drop*” (função de arrastar e soltar, geralmente utilizada para transferir um dado de uma VM para outra) fornecida pela própria VMware;

- **Blue Pill:** Criado pela pesquisadora Polonesa Joanna Rutkowska, a Blue Pill causou uma grande comoção na época. O ataque foi caracterizado como do tipo *rootkit*. Ataques deste tipo têm como princípio passar despercebido por métodos de detecção de intrusão. No caso da Blue Pill, o objetivo era passar despercebido também pela auditoria do *hypervisor*, o que gerou bastante contestação de diversos outros pesquisadores, já que para eles passar despercebido pelo *hypervisor* seria muito difícil.

A Blue Pill é um código malicioso que ao ser executado age como um gerenciador de máquinas virtuais (*hypervisor*), tentando virtualizar todo o sistema operacional, sem que este perceba. Dessa forma, ele consegue controlar e monitorar todo o sistema.

A contestação da comunidade de virtualização veio justamente sobre o encapsulamento invisível citado por Joanna, pois é extre-

mente difícil fazer com que um sistema virtualizado tenha o mesmo tempo de execução de uma instrução que um sistema não virtualizado, tornando assim improvável a invisibilidade da Blue Pill;

- **TXT Hack:** Também criado pela pesquisadora Joanna Rutkowska e outros pesquisadores, o ataque visava invadir a ferramenta *Trusted Execution Technology (TXT)*, presente em chips Intel vPro. O TXT foi desenvolvido como uma extensão de *hardware* para processadores Intel, tendo como objetivo permitir mais segurança aos usuários e organizações. Segurança no sentido de fornecer mais controle no acesso aos dados, armazenamento de chave secreta e acesso autenticado a dados criptografados, além de proteção ao acesso direto à memória (DMA – *Direct Access Memory*). Um exemplo de *hypervisor* que pode ser afetado é o Xen da IBM.

Os pesquisadores tiveram que explorar um *bug* no *software* do sistema Intel seguido de um ataque contra uma falha do *software* TXT. Isso acabou permitindo que eles obtivessem acesso a áreas de memória até então tidas como altamente protegidas. Tal proteção no acesso a memória é considerado ainda mais privilegiado que o anel 0 de proteção (mencionado no tópico “Anéis de Proteção”). O sucesso do ataque se deu também em virtude de alguns erros de implementação de alguns módulos de código de autenticação que estão presentes nos chips TXT, os chamados SINIT (*Authenticated Code Module Privilege Escalation*).

Em 30 de setembro de 2009, foi enviado à Intel um relatório contendo todo o processo e comprovando a vulnerabilidade. A Intel confirmou a existência da mesma e anunciou posteriormente um novo pacote de atualização para o SINIT, corrigindo assim a falha.

Em meados de 2010, um grupo de pesquisa da North Carolina State University divulgou um documento relatando a criação de um mecanismo baseado em segurança e monitoramento do *hypervisor*, chamado de HyperSafe. Essa tecnologia garantia que qualquer *malware* ou outros ataques do tipo VM Escape não pudessem modificar a plataforma de execução do *hypervisor*. O HyperSafe foi criado com três propostas básicas: a primeira, de não afetar em nada o *hypervisor* original, mantendo assim sua estrutura padrão de funcionalidades e recursos, não causando impacto algum ao usuário; a segunda, é promover autoproteção do *hypervisor*, agindo de forma proativa e confiável, até mesmo ao se reportar um *bug* em endereçamentos de memória, o que poderia causar catástrofes ao sistema; e por fim, a terceira proposta é a compatibilidade com os diversos tipos de *hardware* existentes, fornecendo assim uma gama de possibilidades de proteção aos mais diversos ambientes virtualizados.

VM-Aware Malware

Uma das preocupações mais recorrentes desde 2006 são os ataques de *malwares* a ambientes virtualizados, o que compreende uma leva considerável de *bots*, *worms*, *rootkits*, e diversos outros tipos de códigos maliciosos, que são capazes de identificar em que ambientes estão sendo executados (virtuais ou físicos) tendo como base informações de memória, *hardware*, processos, etc.

A maior preocupação ocorre devido à presença crescente de vírus “inteligentes”, que identificam se estão executando em uma máquina virtual ou não. A partir desta informação ele irá dificultar a análise de seu comportamento. Por exemplo, caso alguém necessite analisar o comportamento de algum vírus, é necessário executá-lo em uma VM e isso dificulta e muito o combate a este tipo de ameaça, pois o mesmo tende a mascarar seu real funcionamento ao identificar que está sendo analisado.

Roubo de Máquina Virtual

Uma preocupação recorrente com a segurança das máquinas virtuais é o roubo delas. Tendo em vista que as máquinas virtuais são apenas arquivos, um usuário/funcionário com acesso físico ao local de armazenamento (em geral *storages*) onde os dados das VMs estão guardados, ou até mesmo acesso a um local do *hypervisor*, pode copiar todos os arquivos das VMs em uma mídia local, por exemplo, e removê-los posteriormente.

Injeção de Código/Arquivo Malicioso

Pelo fato das máquinas virtuais serem, a grosso modo, apenas arquivos armazenados, qualquer alteração realizada nesses arquivos pode trazer grandes riscos. Sejam alterações de adição ou alteração de algum dado específico da VM, os ataques de injeção de código malicioso visam fazer com que o código injetado seja executado. Com isso, abre-se precedentes para diversas possibilidades de ataques, dentre elas ataques de negação de serviço (DoS – Denial of Service). Em ataques de injeção de código, uma máquina virtual com um vírus ou qualquer outro código malicioso pode ser inserida dentro de um ambiente virtual através dos seguintes métodos:

- Um invasor pode comprometer uma máquina virtual utilizando o *hypervisor* para transferir uma VM infectada para outro *host* via FTP e iniciando-a do outro lado;
- O invasor pode se passar por um “*man-in-the-middle*” (homem no meio, em tradução livre), que significa que o invasor fica “escutando” a comunicação entre o *host* físico e a máquina virtual, conseguindo assim modificar a troca de informações ali e fazer com que uma VM infectada se passe como uma VM segura;
- Outra forma de ataque ocorre quando o invasor faz uma busca na rede pelo local onde a máquina virtual está armazenada, e caso não haja controle de acesso lá é possível fazer uma cópia da mesma para outro local. A partir daí o atacante fica em condições de tentar qualquer modificação que lhe convenha.

Ataque de Negação de Serviço (DoS – Denial of Service)

Ataques de negação de serviço são inerentes a qualquer tipo de sistema ou aplicação. O DoS envia um grande número de pacotes (maliciosos ou não) endereçados a algum sistema ou aplicação, acarretando um alto processamento no alvo que está sendo atacado, causando falhas no sistema.

É comum encontrar ataques DoS em ambientes virtuais devido à funcionalidade de compartilhamento de recursos entre as VMs e o *host* físico. Se várias VMs começarem a consumir muito

processamento, memória, disco, banda de rede no *host* físico, a tendência é esse *host* não conseguir mais operar de forma correta ou até mesmo seus recursos ficarem inacessíveis, podendo gerar danos às outras máquinas virtuais.

Um exemplo de ocorrência de ataque DoS foi em um ambiente com VMware ESXi, onde uma vulnerabilidade no protocolo NFC (Network File Copy) permitia a modificação do tráfego NFC entre o cliente e o servidor ESXi.

Footprinting

Footprinting é uma técnica de invasão baseada em conseguir informações de um possível alvo sem parecer que aquilo é um ataque. Geralmente a obtenção dessas informações se dá a partir de comandos remotos direcionados a quem se quer atacar. As respostas obtidas vão desde qual sistema operacional que está sendo executado na máquina alvo, quais portas estão abertas, até qual a ferramenta de proteção utilizada na máquina virtual.

O objetivo de quem está tentando invadir é traçar um perfil daquele alvo, identificando padrões anômalos de tráfego pela rede. Por exemplo, para identificar se o sistema alvo é uma VM ou não, os invasores analisam o tempo de sincronização entre um *host* e seu S.O. e o tempo de sincronização de uma VM com seu S.O. Geralmente o tempo de sincronização e alocação de um processo, por exemplo, em uma VM, é alto, já no *host* é baixo.

Existem ferramentas *open source* que auxiliam o invasor na identificação se o alvo é virtual ou não, utilizando diversos outros métodos de detecção. Sendo assim, o simples fato do atacante identificar que ali se trata de uma VM ou não o ajuda bastante no direcionamento das ações de invasão.

Recomendações de Segurança para Ambientes Virtualizados

Mediante os ataques e ameaças destacadas na seção anterior, identifica-se que o *hypervisor* tem um papel primordial no combate ou prevenção desses ataques. Tendo em vista que é o principal componente do sistema, acaba sendo muito visado e por conta disso precisa de uma atenção especial para torná-lo seguro. Para isso, é necessário adotar medidas não apenas específicas ao *hypervisor*, mas sim a todo o ambiente em que ele está inserido, como *storage*, máquina física, infraestrutura de rede e *desktops*.

O foco das próximas seções é destacar algumas formas de tentar fornecer mais segurança tanto ao *hypervisor* como em boa parte dos componentes que fazem parte de um ambiente de virtualização.

Hypervisor

Quando se fala em segurança do *hypervisor* é necessário pensar no *software* de gerenciamento que o controla. É a partir desse *software* que é estabelecida a comunicação entre o usuário e o *hypervisor*. Com ele se torna possível usufruir das funcionalidades que o *hypervisor* proporciona, desde o gerenciamento de imagens até configurações de processador e memória.

Por conta disso, o primeiro parâmetro quando se pensa em formas de manter o *hypervisor* seguro é garantir ao máximo a segurança do *software* de gerenciamento.

A maioria das ferramentas de gerenciamento utiliza o tradicional controle de acesso por *login*/senha, o que a depender das normas de segurança da empresa pode ser insuficiente, fazendo com que muitas empresas adotem outras medidas de segurança. Muitos sistemas de gerenciamento fornecem o controle de acesso baseado em permissões, onde apenas um grupo tem acesso irrestrito e outros apenas leitura, por exemplo.

Existem várias maneiras de tentar manter o *hypervisor* mais seguro, e para isso é imprescindível assegurar um bom gerenciamento da segurança dos diversos componentes (storage, switch, firewall, etc.) que suportam, de alguma forma, a comunicação com o *hypervisor*. Deste modo, toda e qualquer comunicação com redes externas deve ser criptografada utilizando métodos da própria ferramenta de virtualização ou de terceiros, como uma rede privada com VPN (*Virtual Private Network*).

A seguir é apresentada uma listagem de mais algumas recomendações de segurança para o *hypervisor*:

- Instalar todas as atualizações disponíveis sempre que disponibilizadas pelo fabricante;
- Restringir o acesso não autorizado à central de gerenciamento do *hypervisor*;
- Desconectar componentes de *hardware* que não estejam em uso. Por exemplo, discos removíveis utilizados para armazenar backups das máquinas virtuais;
- Manter desativado os recursos de compartilhamento e transferência de arquivos entre máquinas virtuais e/ou *host* físico. Como foi discutido anteriormente, pode haver potenciais ataques a partir dessas funcionalidades através do “*escape-to-hypervisor*”;
- Analisar continuamente o *hypervisor* e seu *log* com o objetivo de identificar ocasionais anormalidades;
- Prover controle ao acesso físico ao *host* em que o *hypervisor* se encontra, prevenindo contra reinicialização inesperada ou a inserção de algum componente USB, por exemplo.

É importante que as empresas e os profissionais de TI, ao implantarem um ambiente de virtualização, saibam que não se deve levar em consideração apenas o *hypervisor*. Muitas vezes um ataque surge em componentes ou recursos que estão fora dele, mas que possuem contato e caminho facilitado para chegar até ele.

Máquina Virtual

O sistema operacional de uma máquina virtual que executa em um ambiente virtual se comporta de forma semelhante a um sistema operacional de uma máquina física. Portanto, todas as considerações de segurança recomendados para sistemas operacionais em máquinas físicas também se aplicam aos virtuais.

A maior preocupação é o fato de uma VM infectada poder contaminar outras no mesmo ambiente. Por conta disso, é necessária uma preocupação que vai além de proteger o *host* físico. Para isso, medidas preventivas podem ser tomadas para prever alguma eventualidade. A seguir são listadas algumas delas:

- Seguir melhores práticas recomendadas pelos fabricantes de *hardware*, boas práticas em gerenciamento de *log*, autenticação e acesso remoto;
- Manter o sistema sempre atualizado de acordo com os *updates* recomendados pelos fabricantes;
- Manter rotinas de *backup* das máquinas virtuais;
- Desconectar componentes de *hardware* não utilizados, evitando assim alguma manobra maliciosa, como o uso de dispositivos USB que podem conter códigos maliciosos para infectar o *host*;
- Utilizar soluções de autenticação de usuários separadas para cada *host*, dificultando assim que caso uma senha seja descoberta o invasor consiga acesso a outras máquinas.

Infraestrutura de Virtualização

Prevenir e manter uma infraestrutura de virtualização seguindo as recomendações de segurança significa não apenas olhar para o *hypervisor*, *host* físico ou sistema operacional. A virtualização compreende também interfaces de armazenamento e rede. Por conta disso, o acesso a este tipo de dispositivo deve ser bem controlado, limitado apenas aos sistemas operacionais que o utilizam. Por exemplo, caso um disco rígido de um dispositivo de armazenamento seja compartilhado com duas máquinas virtuais, é preciso que haja um controle de acesso para que apenas essas duas venham a acessá-los.

Com relação aos componentes de rede, alguns *switches* não fornecem formas de monitoramento de tráfego para atividades suspeitas e também não oferecem um gerenciamento qualificado. Por conta disso, é comum adotar tecnologias de segurança adicionais para garantir o monitoramento, controle e inspeção da rede.

Como planejar e manter ambientes virtualizados seguros

A parte mais crítica na implantação de um projeto de virtualização seguro é o planejamento cuidadoso antes da implantação, configuração e instalação. Isso tornará mais fácil seguir as políticas organizacionais e pode garantir maior segurança ao ambiente. Muito dos problemas de segurança e desempenho ocorrem devido a problemas de planejamento de implementação.

Aspectos de segurança devem ser os primeiros a serem levados em consideração no planejamento para melhorar ambientes virtuais e diminuir os custos, até porque é muito mais caro tratar a segurança após a implantação e implementação. Os aspectos tratados no tópico “Visão Geral do Hypervisor” e “Segurança em Ambientes Virtualizados” deste artigo devem ser levados em consideração para uma melhor estruturação das medidas a serem adotadas no projeto, visando auxiliar a organização no melhor caminho a seguir na implantação de soluções de virtualização.

As próximas seções serão dedicadas à exploração de um ciclo de vida de cinco fases que ajudam as organizações a definir em qual momento na implantação de um ambiente de virtualização uma recomendação de segurança pode ser relevante. O modelo foi adaptado de um ciclo de vida para sistemas pelo NIST (*National Institute of Standards and Technology*) para ambientes virtualizados. As fases do ciclo são definidas em Iniciação, Planejamento, Implementação, Operação e Manutenção, e Eliminação.

Fase 1: Iniciação

Esta fase compreende as tarefas necessárias que uma organização deve considerar ao projetar uma solução de virtualização para seu ambiente de TI, levando em conta os preceitos de confiabilidade, integridade e disponibilidade. Ou seja, a fase de iniciação envolve muitas ações preparatórias, como a identificação das necessidades atuais e futuras, e especificação de requisitos de desempenho, funcionamento e segurança.

Deve-se pensar como essas soluções serão administradas analisando também a possibilidade de atualização das políticas, tendo em vista a probabilidade de mudanças tecnológicas ou nas políticas de segurança da empresa.

Todos esses aspectos são necessários por se tratarem de pontos chave, já que a depender da escolha de uma política de segurança, isso pode impactar no tipo de virtualização a ser adotada no ambiente.

Fase 2: Planejamento

Passada a fase de iniciação, escolha da política de segurança e definições do que será necessário para a realização do projeto, o próximo passo é planejar a solução a ser implantada. Esta fase de planejamento engloba o detalhamento das características da solução escolhida, como qual método de autenticação será utilizado e mecanismos de criptografia, por exemplo. Tudo isso baseado em três parâmetros: arquitetura, criptografia e autenticação.

A arquitetura constitui na escolha do tipo de virtualização, do *software* de virtualização, assim como o armazenamento, topologia de rede, entre outros. Já a autenticação fica responsável por definir quais camadas de virtualização vão precisar de políticas de autenticação, tais como: S.O. da máquina virtual, *hypervisor*, S.O. do *host* físico, etc. E, por último, a criptografia, que inclui as escolhas do algoritmo de criptografia e proteção da integridade das comunicações de virtualização.

Nessa fase também é definido e documentado o plano de segurança a ser adotado para aquele projeto.

Fase 3: Implementação

A implementação compreende a instalação e validação de todo o ambiente que foi previamente discutido e definido na fase de planejamento da solução. Além disso, trata da validação e teste dos aspectos de segurança especificados. Ou seja, é a fase em que tudo é instalado, configurado e testado, porém ainda não é colocado em produção.

Nessa fase alguns aspectos precisam ser validados, a saber:

- **Introspecção:** determinar se a solução de virtualização escolhida no planejamento fornece informações necessárias para monitorar eventos de segurança que ocorrem no S.O. das máquinas virtuais;
- **Autenticação:** garantir que haja autenticação nas diversas camadas de virtualização;
- **Conectividade:** verificar se os usuários estão acessando o que a eles foi permitido e se acessam o que foi negado. Havendo divergência nesses pontos, é preciso rever a política de acesso;

- **Segurança da implementação:** mesmo na fase de implementação pode haver riscos do ambiente sofrer algum ataque. Por conta disso, é aconselhável manter atualizado e configurado corretamente todos os componentes que estão envolvidos na implementação do projeto de virtualização.

Fase 4: Operação e Manutenção

Nesta etapa os sistemas estão instalados, em operação, além de melhorias e modificações estarem sendo desenvolvidas e testadas. O sistema como um todo é monitorado para verificar se os requisitos de segurança estão sendo alcançados e como as modificações que estão sendo desenvolvidas e testadas estão agindo dentro do ambiente de virtualização.

Apesar de o sistema estar operacionalizado, caso seja necessário reimplementar ou modificar algo, pode ocorrer do ciclo voltar a alguma fase anterior. Devido à importância da manutenção do sistema/ambiente para a segurança, é importante ficar atento para os seguintes tópicos :

- **Administração:** ter certeza de que apenas administradores possuem acesso ao ambiente tanto de software como hardware;
- **Atualização:** verificar constantemente se há atualizações para *hypervisor*, sistemas operacionais (tanto das VMs como dos *hosts*), além também da atualização dos componentes que englobam o ambiente virtual;
- **Sincronização:** garantir que o relógio de sincronização de cada componente de virtualização esteja sincronizado com o relógio dos outros sistemas. Geralmente é utilizado o relógio do sistema operacional como guia;
- **Controle:** sempre manter as configurações de controle de acesso de acordo com as políticas de segurança, mudanças tecnológicas e constatações da auditoria;
- **Logging:** documentar anomalias que indicam atividade maliciosa ou suspeita dentro do ambiente virtual.

As organizações devem revisar periodicamente esses tópicos a fim de confirmar se as políticas da organização sobre segurança, procedimentos e processos estão sendo seguidas corretamente.

Fase 5: Eliminação

Após o uso de um dispositivo de virtualização, sendo este destinado à devolução (em caso de aluguel de equipamento) ou descarte, é preciso cuidado especial com a limpeza das informações que permanecem nele. Esta tarefa se torna bastante complicada devido à disposição dos arquivos no dispositivo. Cabe ressaltar que não há um local central onde os dados ficam armazenados e organizados. Por conta disso, essa fase do ciclo precisa ser bem definida por cada organização.

Este artigo foi elaborado seguindo três vertentes. Primeiramente foi feita uma descrição das técnicas de segurança e implantação mais comumente utilizadas em ambientes virtuais, as quais tentam minimizar os prejuízos causados por um ataque ou até mesmo evitar a ocorrência do mesmo.

Posteriormente foi realizada uma análise destacando vulnerabilidades e ataques mais comuns em ambientes virtuais, enfatizando o que pode ocasioná-los e, em alguns casos, como tentar combatê-los. Por fim, foi analisada e adaptada uma metodologia para segurança de sistemas, destacando a aplicação dessa metodologia em ambientes virtualizados.

Diante do que foi exposto neste artigo, pode-se concluir que a maior parte das vulnerabilidades e ataques em ambientes virtuais se dá a partir de falhas de controle de acesso, falha humana e falhas em outros *hardwares*/componentes que se comunicam com a máquina virtual/*host* físico. Sendo assim, é possível considerar que algumas das técnicas de segurança abortadas no tópico “Técnicas de Segurança em Ambientes Virtualizados” podem ajudar a melhorar a segurança em ambientes virtualizados. Além disso, é sempre bom destacar a importância de manter o ambiente atualizado.

Entre as técnicas tratadas neste artigo, destacam-se três como possíveis soluções às ameaças e vulnerabilidades. São elas: Anéis de proteção, monitoramento e criptografia de máquina virtual. Os anéis de proteção, por fornecerem um controle de acesso bastante rígido, o que dificulta o acesso não autorizado às camadas tanto de aplicação como do *hypervisor*, combatendo assim o roubo de máquina virtual e ataques do tipo VM escape, por exemplo.

O monitoramento, por prover a auditoria do ambiente, o que acaba auxiliando na detecção de intrusão no sistema, ajudando a combater ataques, prevenindo ameaças do tipo *VM-Aware Malware*, negação de serviço (DoS), etc. Por fim, a criptografia da máquina virtual, que camufla as informações ali existentes, permitindo que os dados, caso sejam acessados, não consigam ser interpretados pelo invasor, auxiliando no combate de ataques do tipo *Footprinting* e inserção de código malicioso. A **Tabela 1** confronta as ameaças e suas respectivas defesas com base nas análises realizadas.

Ameaças	Defesas
VM Escape	Anéis de Proteção
N. Serviço (DoS), VM Escape	Monitoramento de VM
Footprinting, Inserção de Código Malicioso	Criptografia de VM

Tabela 1. Confronto entre ameaças e ataques

Contudo, a adoção das técnicas de segurança não pode ser considerada como a principal e única forma de prevenção e proteção do ambiente. Por conta disso, no tópico “Como planejar e manter ambientes virtualizados seguros” foi mostrada uma adaptação de uma metodologia de segurança para sistemas, a ser aplicada em ambientes virtuais. Esta metodologia consistiu em um ciclo de vida de cinco etapas, que tratam desde o planejamento do projeto de virtualização até sua entrega final, sempre levando em consideração os aspectos de segurança em cada etapa. Ou seja, é uma forma de organização e planejamento da implementação de um ambiente, levando em consideração diversos parâmetros que são importantes e que se não forem bem discutidos podem acarretar em uma vulnerabilidade futura.

Por exemplo, ataques provenientes de inserção de código malicioso e roubo de máquina virtual podem ser evitados com um planejamento de como será o acesso às máquinas virtuais e/ou ao *host* físico, controlando assim o risco de alguém inserir um *pendrive* no *host* ou até mesmo ter permissão de acesso, que foi atribuída por engano, e a partir daí conseguir extrair informações que até então não lhe eram permitidas.

Com isso, conclui-se também que a segurança em virtualização não depende única e exclusivamente do combate a falhas em seu *software* de gerenciamento, *hypervisor* ou *hardware*, mas sim de um planejamento, manutenção e gerenciamento rigoroso durante todo seu tempo de vida útil. Qualquer deslize, por menor que seja, pode acabar comprometendo a segurança de todo um ambiente.

Autor



Arthur dos Santos Macedo

arthurmacedoti@gmail.com

Graduando em Ciência da Computação pela Universidade Salvador (UNIFACS). Atualmente é Analista de Suporte Jr na Provide IT – Suporte e Treinamento.



Autor



Christian Conceição Guerreiro Santos

christian.guerreiro@pro.unifacs.br

Graduado em Ciência da Computação e Pós-graduado em Sistemas Distribuídos pela UFBA, atualmente é Gerente de Auditoria em TI do CEDASC, autarquia vinculada ao Tribunal de Contas do Estado, e professor da Graduação Tecnológica em Redes de Computadores na UNIFACS. Certificado COBIT 4.1 e ITIL v3 Foundations, além de MCSA e instrutor Linux, possui mais de 15 anos de experiência, atuando em projetos de virtualização com VMWare, Governança, Business Intelligence com IBM Cognos e SQL Server, implementação e migração de Windows e Linux, serviços de infra-estrutura como DNS ISC Bind, Apache e aplicações de gerenciamento como CACIC e What's Up, e ainda soluções de colaboração Mediawiki, Joomla e Egroupware.



Links:

Fawzi, M., (2009). Virtualization and Protection Rings Part 1.

<http://fawzi.wordpress.com/2009/05/24/virtualization-and-protection-rings-welcome-to-ring-1-part-i/>

Schwartz, M. (2012). Nova vulnerabilidade de virtualização permite ataque a hypervisor. InformationWeek EUA

<http://informationweek.itweb.com.br/8913/nova-vulnerabilidade-de-virtualizacao-permite-ataque-a-hypervisor/>

Shackleford, D (2013). Virtualization Security: Protecting Virtualized Environments, Indianapolis, Indiana: John Wiley & Sons, Inc. 2013. 253 páginas. ISBN 978-1-118-28812-2.

Caicedo, C., Brooks, T. e Park, J. (2012). Security Vulnerability Analysis in Virtualized Computing Environments. International Journal of Intelligent Computing Research (IJICR), Volume 3, 2012, pp. 280-281.

VMware (2010). vSphere 5.1 Monitoring and Performance. VMware, Inc, 2009-2011.

Controle de Acesso: Gerenciando privilégios e permissões

Como planejar o acesso de usuários a arquivos e sistemas

Bilhões de dólares foram gastos na última década para aumentar a segurança da informação nas empresas, com o objetivo de manter afastada a rede dos hackers e invasores. Ainda hoje, num relatório liberado pela Vanson Bourne, que avaliou 3,2 mil tomadores de decisões de TI em 16 países, metade deles revelaram não estarem confiantes de que suas organizações têm capacidade adequada para as diretrizes de segurança necessárias. Somente nos últimos 12 meses, 27% deles responderam ter sofrido falhas e 19% relataram terem sido vítimas de ataques e fraudes.

De forma geral, ainda relacionado a este relatório, as empresas com maior maturidade na área de segurança têm perda financeira proporcionalmente 1,5 vezes maior que as empresas de menor maturidade. No Brasil, o custo destes incidentes foi de US\$ 421.538 para falhas de segurança, US\$ 298.824 para perda de dados e US\$ 594.000 para inatividade nas operações. Além destes custos, os indicadores de perda de produtividade dos funcionários (46%), atraso no desenvolvimento de produtos (40%), perda de novas oportunidades de negócio (40%), são importantes indicadores gerenciais para visualizarmos o impacto da segurança da informação no ambiente corporativo.

Por isto, as empresas têm investido cada vez mais em tecnologias de proteção de informações, como sistemas de bloqueio de invasões, antivírus, firewalls, entre outros. No entanto, a segurança que envolve os próprios funcionários, parceiros e terceiros que possuem acesso às informações institucionais, podem custar muito mais que qualquer ataque de hacker. Ainda assim, percebemos que este tipo de proteção de informações nas organizações é precário, básico e, comumente, possui falhas que possibilitam que as quebras de segurança ocorram facilmente.

O relatório da EY (Ernest Young) de 2012, realizado entre os países das Américas, apontou que as empresas irão investir mais em aspectos de segurança nos próximos

Fique por dentro

Este artigo levanta as principais questões que envolvem o planejamento de permissões num ambiente de usuários corporativo. De forma objetiva, são salientadas melhores práticas em relação à segurança, auxiliando na análise do ambiente, na elaboração de diretrizes e na prevenção de acessos internos não autorizados, visando à redução do nível de permissão com base em teorias já existentes.

A segurança de informação não envolve apenas os ataques externos. Às vezes, o risco encontra-se dentro da própria organização. Deste modo, planejar as permissões internas de sistemas, aplicações e arquivos é o primeiro passo para a mitigação deste risco.

três anos do que em qualquer outro aspecto. A **Figura 1** expõe o gráfico desta pesquisa.

Por esta razão a segurança da informação é um assunto tão discutido dentro das organizações. As várias mudanças que ocorreram nas últimas décadas nos levaram a uma explosão de informações. Aplicações, cloud computing, redes sociais, serviços integrados, todos estes são responsáveis por um crescimento exponencial no volume de dados.

Estima-se que uma empresa hoje, com mil funcionários, gere anualmente cerca de 1.000 Terabytes de informação e que 71% de todas as brechas de segurança estão dentro da organização, com algum funcionário/parceiro agindo maliciosamente. Portanto, é importante considerar o quão grande e pervasivo para os profissionais de TI é a manutenção e gerenciamento deste sistema de informações, e como fazer para que estes dados estejam acessíveis, mas, ao mesmo tempo, seguros.

Definições importantes

Antes de iniciarmos o processo de planejamento do ambiente de permissões, é necessário definirmos alguns conceitos que servirão como base teórica para o processo. As definições listadas a seguir são os princípios utilizados para qualquer modelo de segurança existente. Caso seja necessário um maior aprofundamento do

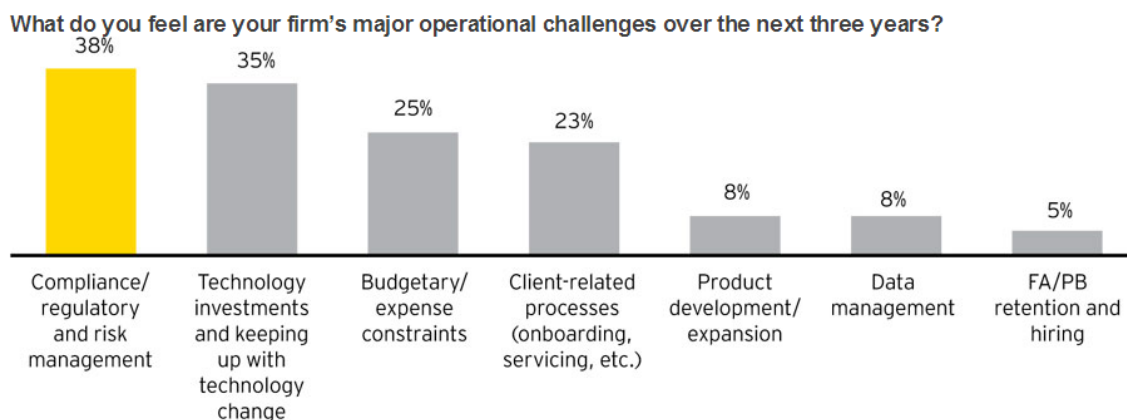


Figura 1. Relatório da EY de 2012 sobre investimentos na área de segurança da informação

assunto, a ISO/IEC 29146, na sua parte I, contém informações mais detalhadas sobre cada uma delas.

- **Contas** – são objetos criados no seu ambiente de rede ou em sistemas que definem uma identidade, que pode ser um usuário, computador, sala de reunião, servidor ou qualquer outro que necessite ter uma determinada ação em algum sistema;
- **Usuários** – sujeito da ação de executar, acessar, monitorar e/ou intervir em um sistema. Pode ser indivíduos ou agentes autônomos, como agentes de softwares;
- **Permissões** – são os direitos de executar uma ou mais ações em objetos de um sistema. Isto é, um objeto pode ser um arquivo, registro de um banco de dados, tela de um sistema, impressão de um determinado arquivo, entre outros. Neste caso, o objeto pode ser definido como a área/registo de informação a ser analisada;
- **Acessos** – é a resultante dos direitos de execução/permissão relacionado a um objeto de sistema;
- **Papéis** – são as diferentes funções dentro de um sistema ou ambiente analisado. Neste caso, ao invés de atribuir as permissões ao usuário, define-se as permissões por papéis e enquadram-se os usuários a cada tipo de papel existente, como por exemplo, Administrador, Auditor, Gerente de sistema;
- **Controle de acesso** – para o usuário executar determinadas tarefas na sua estrutura de TI, acessar recursos de sistemas e realizar algumas alterações em seus dispositivos pessoais, faz-se necessário o uso de algum mecanismo de controle de acesso;
- **Autenticação** – processo pelo qual a conta ou usuário é validado pelo sistema e autorizado de acordo com as permissões atribuídas;
- **Sessão** – quando o usuário é autenticado e acessa um determinado sistema ele inicia uma sessão. É possível um usuário ter várias sessões ativas paralelamente e, durante uma sessão, é possível ter mais de um papel.

Levantamento do ambiente

Realizar o levantamento do ambiente a ser analisado é importante até mesmo para quem já tenha um ambiente de usuários

e permissões em funcionamento. Sendo assim, é recomendável que faça este exercício de análise da rede, buscando observar com cautela as configurações atuais.

O objetivo desta fase é definir como desenhar, de acordo com o ambiente em análise, a melhor estrutura de atribuição de permissões. A Figura 2 representa um modelo segmentado por departamentos x papéis x sistemas. Com base no seu ambiente, é possível construir a solução que melhor se adeque ao seu caso.

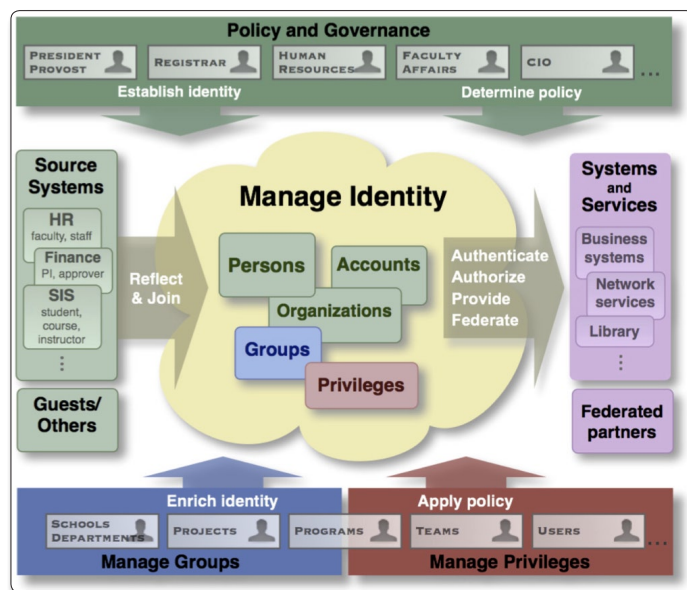


Figura 2. Visão geral de estrutura de atribuição de permissões

Para realizar o planejamento, provavelmente será necessário que se recorra aos usuários e/ou chefias para entender quais as atividades desempenhadas por cada um. Porém, caso o ambiente em questão seja amplo demais ou exista alguma questão que impeça este contato, é sugerido que se analise a função descrita pelo RH e restrinja as permissões ao máximo possível, adicionando posteriormente somente as que lhe forem solicitadas.

No entanto, este tipo de ação pode trazer transtornos aos usuários que precisarão solicitar e aguardar o suporte da TI para obter permissão para uma tarefa a qual já realizavam anteriormente.

Para esta fase de levantamento de informação, foram definidos seis passos a serem seguidos, estruturados e colocados nesta ordem para facilitar a organização dos dados nas tabelas. Vamos a eles:

1. Lista dos sistemas / aplicações: Neste item o foco é levantar todas as aplicações e/ou sistemas que movimentam informações importantes como o ERP da empresa, banco de dados, sistemas de engenharia, análise, processos, acesso físico, entre outros. Inclua também os sistemas de arquivos compartilhados e, se o seu ambiente possui recursos que são acessados externamente, separe-os também por tipo de acesso, interno ou externo. Na **Tabela 1** é apresentado um exemplo de como se criar uma lista de softwares, considerando o tipo de acesso;

Software	Acesso	Departamentos
ERP	Interno	Financeiro, Logística
Project Web	Interno/Externo	Engenharia, TI
Make Process	Interno	Todos

Tabela 1. Lista de aplicações

2. Definição de atributos: Com base no item anterior, para cada um dos sistemas levantados (ou para um grupo deles, se for possível agrupar) levante os atributos que podem ser trabalhados. Neste momento não se preocupe em avaliar qual o nível de detalhamento. Para facilitar, a seguir é apresentada uma lista dos atributos mais utilizados:

- Leitura;
- Listar;
- Modificar;
- Escrita / Gravar;
- Excluir;
- Listar atributos;
- Execução;
- Alterar permissões;
- Completo.

3. Lista de usuários: Neste item o foco é entender a sua estrutura de usuários, não sendo necessário que se realize uma lista com todos os nomes, mas que sejam considerados todos os tipos. Para isto é importante que seja analisada cada pessoa dentro da empresa e suas funções. De qualquer forma, você terá uma lista ao final que delineará os vários tipos de perfis com os quais poderá trabalhar numa política de controle de acesso. Portanto, quanto mais informação conseguir reunir, melhor será o resultado. A **Tabela 2** traz um exemplo que poderá ser usado nesta etapa;

4. Lista de papéis: Considerando a lista anterior, é possível repensar os usuários em determinados papéis. Isto é, normalmente o time de um departamento da sua empresa possui uma função determinada, mas mesmo assim possuem atividades diferentes

entre seus componentes. É importante entender que um usuário não precisa ter as mesmas permissões que o seu chefe, somente porque pertence ao mesmo departamento. Para construir sua lista de papéis, analise a lista de usuários e veja se é possível agrupá-los de acordo com as funções que executam. No exemplo da **Tabela 3**, os papéis de Financeiro-NotasFiscais e Financeiro-Coordenação podem ser agrupados, pois possuem a mesma permissão no sistema de Notas Fiscais;

Departamento	Usuário	Perfil
Financeiro	Jane Silva	Financeiro-atendimento
Financeiro	Claudia Costa	Financeiro-NotasFiscais
Financeiro	Meire Maura	Financeiro-coordenação

Tabela 2. Lista de usuários

Ação Sistema	Finan-atend	Finan-NF	Finan-Coord
Visualização informações financeiras	X	X	X
Entrada de Notas fiscais	X	X	X
Alteração de Info em Notas Fiscais	-	X	X
Remoção de Notas fiscais	-	X	X

Tabela 3. Lista de papéis

5. Tempo de permissão: Este item refere-se a casos em que o sistema não permite atribuir permissões especiais e/ou o acesso do usuário será em momentos pontuais e/ou esporádicos. Isto é, suponha que um usuário precise alterar um arquivo no diretório do Windows. Este acesso, no entanto, é restrito a administradores do computador e não tem como atribuir permissão específica e/ou não se deve manter o usuário com permissões completas. Deve-se considerar, então, a duração da permissão atribuída. Outro exemplo, um funcionário do financeiro pode solicitar a permissão temporária de exclusão de registros no sistema, pois isto faz parte de um projeto corporativo de otimização dos processos;

6. Análise de normatização / regulações / requisitos governamentais: Existem algumas regulações governamentais que requerem maior controle e auditoria de acesso, como SOX, HIPAA, GLBA. Estes tipos de normatizações são geralmente aplicáveis em empresas de maior porte e que possuem o capital aberto na bolsa de valores, por exemplo. Caso esta situação se aplique ao seu ambiente, faça uma análise criteriosa dos requisitos necessários a cada uma delas e elabore uma lista de prioridades para elaboração e análise dos dados. É sugerido ainda que, após finalizar o trabalho, seja realizada uma auditoria com base nestas exigências para verificação e validação do ambiente.

Com esses dados levantados é possível iniciar a fase de análise e estruturação das informações. Neste momento será necessário

um esforço adicional de observação, com o intuito de organizar o ambiente e definir a partir deste ponto os processos para a requisição de acesso, onde é possível:

- Criar tabelas específicas de acesso por sistema utilizando-se o exemplo da tabela RACI (veja o **BOX 1**), conforme exemplo mostrado no item 4;
- Criar tabelas por papéis, reunindo os usuários por grupos e funções específicas na empresa;
- Criar tabelas por tipo de acesso e sistema, levando em consideração se o acesso for realizado interna ou externamente, em um desktop ou servidor;
- Criar tabelas por escopo x tempo, quando o ambiente requer uma segmentação de permissões temporárias, delineando o privilégio x escopo x tempo.

BOX 1. Tabela RACI

A tabela ou matriz RACI é uma ferramenta da gestão de projetos que estrutura a relação entre papéis e responsabilidades de cada atividade ou processo. O nome RACI é um acrônimo de Responsible, Accountable, Consult and Inform (Responsável, Autoridade, Consultoria e Informação).

A partir deste ponto você terá condições de estruturar o seu ambiente com base nas variáveis que mais se aplicarem ao seu caso: sistemas, papéis, tipo de acesso ou tempo. Neste momento, busque reduzir ao máximo o volume de informações geradas, como por exemplo, criando estruturas de matrizes utilizando-se de duas variáveis.

Após a criação das tabelas, realize um levantamento de quem são os usuários que devem ter privilégio elevado. Segundo Carpenter, no Gartner Information Security Summit 2010, a recomendação é que estes tipos de usuários, que se enquadram em três tipos de contas listadas a seguir, devem ser monitorados e auditados:

- Pessoas com permissão completa de super usuário permanente – para algumas contas e administradores da TI;
- Pessoas com permissão completa, mas de super usuário temporária – para gestores, desenvolvedores de produtos, entre outros;
- Pessoas com permissão restrita, mas de super usuário temporária – para desenvolvedores de aplicações e administradores de banco de dados. Isto é, com privilégio de super usuário somente para as aplicações e sistemas que precisam acessar.

Portanto, identifique nas tabelas quem são e crie processos separados de aprovação, criação e exclusão para estes casos. Por exemplo, no caso de um administrador de banco de dados, é imprescindível que ele possua um usuário com privilégio elevado na aplicação. Para que ele consiga esta permissão, será necessário que ele abra uma requisição no sistema de atendimento, especifique o ambiente ao qual ele precisa de acesso e obtenha a aprovação de um responsável pela área ou serviço – gerente de TI ou de projeto. Somente após este procedimento, será autorizada a criação de um usuário com sua identificação,

que será monitorado e auditado durante todas as sessões de login que fizer.

Análise e detalhamento

Uma vez realizado o levantamento inicial, é possível ter uma visão melhorada de como está estruturada sua organização em relação a cargos, perfis, pessoas e funções. Neste momento, o importante é ter como foco a simplificação ao máximo da sua estrutura, com o objetivo de facilitar a criação do ambiente e dos procedimentos necessários para a sua equipe de TI.

Primeiramente tente agrupar ao máximo os usuários por sistemas e privilégios, de forma que possua um número fixo de perfis dentro de cada aplicação. Por exemplo, dentro de uma determinada aplicação financeira você pode tentar reunir os usuários que realizam adição de registros e consultas (Financeiro-Atendimento), outros que realizam alterações (Financeiro-Completo) e os administradores do banco (TI-Completo). Veja a **Tabela 2** para acompanhar o exemplo.

Caso já possua um ambiente em funcionamento, realize uma auditoria de autorizações dentro de cada aplicação. Verifique quais usuários já possuem contas privilegiadas e compare-os com sua análise feita anteriormente. Procure analisar e conversar com os mesmos para entender se realmente existe a necessidade de se manter permissões deste tipo. Negocie no sentido de reduzir ao máximo o acesso, pois a quantidade dessas contas deve ser minimizada.

Lembre-se que toda política de segurança prevê proteção para a organização e para o usuário, evitando riscos operacionais. Todos estão sujeitos a erros, acidentes, invasões, que independem do seu nível de conhecimento. Sendo assim, não tenha receio em colocar limites ao seu time de TI, à chefia do departamento ou ao gerente geral, pois quando não há limites claros e estabelecidos, o legal e o ilegal são imprecisos e as consequências podem ser desastrosas tanto para o TI quanto para o negócio.

Este é o momento de desenhar/redesenhar suas políticas internas e ter as permissões de usuários gerenciadas de forma mais padronizada e granular. Portanto, defina qual o nível de detalhamento necessário para cada aplicação e perfil e estabeleça padrões. Caso opte por uma estrutura com um nível maior de detalhamento, terá um custo maior de administração dos recursos posteriormente. Assim, avalie de forma criteriosa se realmente é necessário este tipo de esforço.

Por exemplo, considere um sistema de gestão integrada, onde dois módulos estão em operação: financeiro e logística. Suponha que um usuário do financeiro precise ter acesso a uma determinada tela da logística e que no perfil criado no sistema para este departamento, esta permissão não é aplicada. Ao invés de criar um novo perfil para este tipo de exceção, opte por atribuir mais de um perfil a um mesmo usuário, possibilitando o acesso dele a vários ambientes e simplificando a administração dos perfis.

Uma vez finalizada a etapa de levantamento e análise dos perfis de segurança da rede, inicia-se o processo de planejamento das ações necessárias para implantação.

ID	Ação	Requisitos	Testes	Responsável	Início	Entrega	Status
1.1	Comunicar ao departamento financeiro			Coord. TI	6/1/2014	6/1/2014	Concluído
1.2	Alterar permissões no sistema - tela finanças	a. Após ação ID 1.1 b. Elaborar cronograma considerando as atividades do setor c. Realizar avaliação e teste de impacto	Realizar teste de acesso de pelo menos três usuários após implementação	Coord. Sistema	8/1/2014	15/01/2014	Em progresso

Tabela 4. Plano de ação

Plano de ação

Após definir os perfis e níveis de detalhamento, é interessante considerar alguns pontos de análise antes de iniciar o planejamento da execução da nova estrutura de permissões. São eles:

- Quais as falhas de segurança de maior risco para a operação?
- Qual/quais os departamentos que realizam movimentações mais críticas?
- Qual/quais os processos mais críticos para a organização?
- Qual o calendário de atividades da organização?

O plano de ação é uma tabela que conterá todas as atividades que serão desenvolvidas para que se atinja uma meta num tempo determinado. Portanto, ele deve conter informações como: a descrição da ação, o cronograma, passos e requisitos para realização, testes/avaliação, status, os responsáveis e/ou envolvidos. A **Tabela 4** apresenta um exemplo de plano de ação para servir como base na construção. No entanto, lembre-se de adequar as colunas às suas necessidades locais.

Ao elaborar o plano de ação, alguns pontos importantes devem ser considerados, para que não haja imprevistos durante o processo de implantação das políticas:

- Considere atividades importantes do setor que será afetado, como entregas de relatórios gerenciais, datas de fechamento fiscais, data de entrada de mercadorias, entre outros. Estas datas podem impactar na execução do planejamento, uma vez que realizar mudanças em períodos críticos não é recomendável;
- Procure minimizar o impacto da segurança na produtividade dos usuários, para obter o apoio da empresa e dos funcionários nas iniciativas da TI;
- Implemente logs detalhados (principalmente no início da implantação) para que possa buscar padrões que indiquem problemas de configuração.

Preparar um plano de ação é uma tarefa relativamente simples. O princípio básico é ser o mais específico e estabelecer metas e objetivos claros. Além disso, o acesso às informações contidas no plano pela equipe é fundamental para que todos compreendam o papel que terão e o quanto suas ações poderão impactar no cronograma e resultado estabelecido. A seguir elaboramos um passo-a-passo para criação do plano:

1. Defina o seu objetivo em várias metas e objetivos secundários;
2. Gere uma lista de ações para cada meta ou objetivo definido;
3. Adicione cada uma das ações no plano, organizando-as e estabelecendo o requisito, responsável e cronograma de cada uma delas;

4. Aloque os recursos necessários a cada uma das tarefas, o que inclui pessoas, materiais e equipamentos;
5. Elabore um plano paralelo de acompanhamento da execução, pois a reelaboração, reorganização e reagendamento de atividades é necessário;
6. Levante os fatores de riscos, identificando possíveis problemas e reconsidere as datas previstas, já que o prazo deve ser estendido de forma a abranger contratempos.

As informações têm sido consideradas o principal ativo de uma organização. Hoje, a vantagem competitiva de uma empresa está na sua estratégia, que por sua vez está diretamente relacionada ao bom uso da informação disponível. Por esta razão, as organizações têm investido tanto na área de segurança, criando e discutindo políticas e procedimentos claros, adquirindo softwares e equipamentos onerosos para aumentar a proteção contra invasões.

No entanto, pesquisas recentes têm questionado a segurança destas organizações, principalmente quando a proteção está no controle de um funcionário. Uma das maiores dificuldades das organizações atuais é assegurar que todos os seus funcionários conheçam e sigam as políticas internas e entendam a sua importância. Atitudes que incluem riscos operacionais como o simples ato de dar uma espiada, fazem com que a área de segurança não descanse nunca. A natureza humana tem sido o elo mais fraco na interface entre pessoas, processos e tecnologia.

Trabalhar com proteção é estabelecer regras que sejam implementadas e que impactem o menos possível na produtividade da empresa. Por isso, o privilégio mínimo é uma forma de reduzir estes riscos e tentar criar um ambiente seguro ao funcionário, dando somente autorização (permissão) aos recursos de TI compatíveis com sua função e responsabilidade e não super ou sub autorizá-lo.

Empresas hoje são dinâmicas e podem ser consideradas sistemas fluidos de troca de informações. A ilusão de ser possível bloquear todos os acessos e impedir toda tentativa de roubo de informações não é possível. Por todas estas razões, é fundamental incluir outros departamentos neste projeto, como por exemplo, o RH ou a comunicação, já que toda a ação de TI deve alcançar a todos da organização. Regras que não estejam claras, política ou procedimentos não conhecidos, fazem com que grande parte deste esforço seja em vão. Por isto, preveja um código de conduta, avisos, contratos de confidencialidade, entre outros, para apoiar suas ações com base nestes documentos.

A implantação efetiva da segurança da informação demanda um conjunto de fatores que incluem a política, diretrizes, processos, ferramentas, controle e planejamento. Se conseguir que os limites sejam respeitados, a TI permanece no controle da segurança e tem a autoridade de tomar ações proativas para continuar a proteger a empresa.

Autor



Juliana Márcia Rezende Calado

jmrcalado@hotmail.com

Especialista em Gestão de Infraestrutura de TI pela Pontifícia Universidade Católica de Minas Gerais. Atua como professora de pós-graduação no curso de Gestão de TI pelo SENAC e pelo Centro Universitário UNA. Trabalha como Analista de TI na área de administração de serviços e gerência de redes. Experiência de 13 anos na área de redes de computadores e administração de servidores, além de três anos como docente de ensino superior na graduação e pós-graduação.



Links:

Balancing growth- and regulatory-related technology spending

<http://www.ey.com/US/en/Industries/Financial-Services/Banking---Capital-Markets/2012-Americas-wealth-management-study---Balancing-growth---and-regulatory-related-technology-spending#.UqZc3NJDtyw>

Identity and Access Management Services

<http://www.usc.edu/org/iamsc/>

ISO/IEC 24760-1:2011. Information Technology – Security techniques –

A framework for identity management – Part 1: Terminology and concepts

http://standards.iso.org/ittf/PubliclyAvailableStandards/c057914_ISO_IEC_24760-1_2011.zip

Preventing good people from doing bad things

http://books.google.com.br/books/about/Preventing_Good_People_From_Doing_Bad_Th.html?id=9kWrjE_E9MC&redir_esc=y

Segurança da informação desafia executivos de TI

<http://computerworld.uol.com.br/seguranca/2013/12/03/seguranca-da-informacao-desafia-executivos-de-ti/>

FÓRUM DEV MEDIA

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



No fórum da DevMedia você irá encontrar uma equipe disponível e altamente qualificada com consultores e colaboradores prontos para te ajudar a qualquer hora e sobre qualquer assunto. Temos as salas de Java, .NET, Delphi, Banco de Dados, Engenharia de Software, PHP, Java Script, Web Design, Automação comercial, Ruby on Rails e muito mais!

ACESSE AGORA
www.devmedia.com.br/forum



Introdução ao Amazon Web Services

Conheça os serviços de cloud computing da Amazon e saiba quando utilizá-los

A maioria dos leitores provavelmente já ouviu falar na Amazon. O negócio que começou com a venda de livros em 1994, hoje é considerado a maior loja online do mundo, com mais de 100 mil funcionários e faturamento de mais de 60 bilhões de dólares em 2012.

Para um negócio desse porte funcionar, foi preciso a criação de uma infraestrutura de TI colossal, com literalmente milhares de servidores distribuídos em vários datacenters pelo mundo. Com essa quantidade de servidores, só existem duas alternativas para uma administração eficiente: contratar um exército de técnicos, ou automatizar o quanto for possível. A Amazon escolheu o segundo caminho, e após muito trabalho de pesquisa e desenvolvimento, onde foram criadas soluções para diversos problemas comuns de infraestrutura, eles perceberam que poderia ser um negócio interessante a venda de recursos computacionais utilizando a própria infraestrutura. Até aí, não parece diferente do que os provedores tradicionais faziam com serviços de hospedagem, por exemplo. A grande diferença é que na Amazon, só se paga pelo uso do serviço, ou seja, se você possui um site que tem picos de acesso em determinadas épocas, você pode provisionar recursos adicionais por um período, e simplesmente deixar de usá-los quando não forem mais necessários. Isso é uma grande mudança de paradigma: hoje, quando falamos do modelo tradicional, onde a empresa é dona de um parque de servidores dentro do datacenter, quando houver a necessidade de aumento de capacidade, provavelmente será necessário investir em equipamentos, seja servidor, storage ou rede. Aí começam os problemas: a empresa pode ter determinados equipamentos que foram descontinuados e que agora possuem um custo de expansão maior do que o custo de equipamentos novos. Ao comprar novos equipamentos, é preciso decidir se vale a pena manter os antigos em uso, ao lado dos novos, ou se é melhor

Fique por dentro

Este artigo tem como objetivo apresentar os principais serviços de cloud computing oferecidos pela Amazon, e ilustrar casos onde seu uso pode ser útil em um projeto de infraestrutura. A Amazon é o principal player de cloud computing do mercado e, portanto é fundamental para todos os interessados no assunto conhecer sua oferta de serviços.

migrar tudo para os novos equipamentos, o que envolve projetos de migração complexos.

A virtualização ajuda a minimizar muitos desses problemas, mas ainda está sujeita a alguns, como por exemplo, o caso do pico sazonal. Quando há a necessidade de se suportar uma demanda alta e inesperada com uma infraestrutura interna, provavelmente será necessário ter uma infraestrutura dimensionada “por cima”, ou seja, com uma grande capacidade de processamento, que será utilizada poucas vezes por ano.

O Amazon Web Services (daqui para frente, chamado apenas de AWS), fornece uma alternativa interessante para esses problemas. É como se tivéssemos à nossa disposição uma infraestrutura “infinita”, em que podemos alocar recursos quando necessário, de forma rápida e relativamente barata.

Para alguns tipos de empresa, como bancos, existem questões quanto à segurança e interoperabilidade dos serviços em nuvem que com o tempo precisam ser esclarecidas. Por exemplo, no Brasil existem leis que proíbem o armazenamento de dados fora do país. No entanto, com o modelo de operação atual oferecido pelos provedores de cloud computing, não é possível garantir que dados de empresas brasileiras não serão replicados para servidores em outros países. Para empresas cujo negócio está baseado na web, a aderência é muito mais óbvia. O maior exemplo disso foi a migração da Netflix, um dos maiores provedores de conteúdo *ondemand* do mundo, para o AWS em 2011.

O AWS oferece diversos serviços, desde a infraestrutura até bancos de dados e enfileiramento de mensagens. Veremos neste artigo os principais serviços relacionados à infraestrutura (IaaS –

Infrastructure as a Service), e em alguns casos procuraremos mostrar casos de uso de cada tecnologia.

Regiões e zonas de disponibilidade

O AWS está distribuído em datacenters presentes em várias localidades no mundo. Esses datacenters são chamados pela Amazon de regiões. Para aprimorar a disponibilidade, dentro de cada região existem ao menos duas zonas de disponibilidade, que são infraestruturas completamente independentes com links de baixa latência entre elas para garantir uma comunicação eficiente.

Atualmente as regiões da Amazon são as seguintes, com as respectivas quantidades de zonas de disponibilidade:

- US East: Virginia (três zonas de disponibilidade);
- US West: Oregon (três zonas de disponibilidade);
- US West: Califórnia (duas zonas de disponibilidade);
- São Paulo (duas zonas de disponibilidade);
- Europa: Irlanda (três zonas de disponibilidade);
- Ásia e Pacífico: Tóquio (três zonas de disponibilidade);
- Ásia e Pacífico: Cingapura (duas zonas de disponibilidade);
- Ásia e Pacífico: Sydney (duas zonas de disponibilidade).

Como um diferencial, muitos serviços possuem replicação de dados transparente entre zonas de disponibilidade, para garantir a contingência em caso de falhas. Além deste recurso, a replicação de dados entre regiões também é possível, mas deve ser implementada caso a caso. Assim, ao desenharmos uma arquitetura para funcionar sobre o AWS, devemos levar em conta as regiões e zonas de disponibilidade para garantir a contingência da aplicação, evitando que falhas no AWS causem impacto para a aplicação.

Diante desse cenário, já ocorreram grandes falhas em regiões isoladas do AWS que causaram indisponibilidade para grandes clientes como Sony e Netflix. Estatisticamente, ao considerarmos a infraestrutura apresentada, a probabilidade de todas as zonas de disponibilidade de uma região falharem ao mesmo tempo é muito pequena, e a probabilidade de todas as regiões falharem é menor ainda. Se desenharmos nossa arquitetura com isso em mente, o que teremos é uma infraestrutura com um nível de resiliência altíssimo, ao custo de alguns milhares de dólares, e que custaria muito mais se implementada de forma tradicional, com servidores instalados *on-premises*. Sendo assim, é preciso analisar cada caso de forma independente, mas de modo geral, o custo das soluções no AWS é bastante atrativo.

Simple Storage Service – S3

O S3 foi o primeiro serviço do AWS, tendo sido lançado em 2006. Ele fornece um sistema de armazenamento online bastante simples, onde os arquivos são acessados via HTTP, web services (REST ou SOAP) ou protocolo BitTorrent. No S3, o armazenamento é feito em buckets (containers de arquivos), e cada bucket possui uma série de funcionalidades, que listamos a seguir:

- **Permissions:** Cada bucket possui um controle individual de permissões (leitura, upload e remoção de arquivos, visualização e edição de permissões) que podem ser concedidas a todos ou

apenas a usuários autenticados no AWS;

- **Static Web Hosting:** É possível publicar um web site estático utilizando o S3. Basta habilitar a opção e indicar qual o documento “index” do web site, que o S3 passa a servir este conteúdo;
- **Logging:** Pode ser habilitado o log de acesso aos seus objetos no S3, para efeito de estatísticas e auditoria;
- **Lifecycle:** Define regras de expiração e arquivamento de objetos dentro do bucket. É possível configurar políticas baseadas em data para remover os objetos do S3, ou ainda movê-los para o Glacier, que é o serviço de arquivamento, que veremos mais adiante;
- **Requester Pays:** É um modelo onde o custo de transferência de dados é cobrado do usuário que está solicitando o objeto. Nesse modelo, o acesso público e anônimo ao bucket é desabilitado;
- **Versioning:** Este recurso permite o versionamento de objetos dentro de um bucket. É útil para arquivos cujo histórico de alterações precisa ser guardado.

O S3 tipicamente é utilizado para hospedagem de arquivos que serão acessados diretamente pela web, como imagens e páginas web estáticas, mas pode ser utilizado também como repositório de arquivos de backup de instâncias e imagens do EC2.

Elastic Compute Cloud – EC2

O EC2 é o serviço de virtualização de servidores do AWS, onde é possível criar servidores virtuais (chamados de instâncias, na terminologia da Amazon) com diversas opções de tamanho e sistema operacional.

A Amazon classifica o tamanho das instâncias oferecidas através da métrica chamada de ECU – *Elastic Compute Unit*. Uma ECU equivale à capacidade de um processador Xeon ou Opteron de 1.0 GHz de 2007. Conforme os servidores físicos da Amazon são atualizados e passam a utilizar processadores de maior capacidade, a oferta das instâncias muda e o número de ECUs de um determinado tipo de instância muda também. Nesse ponto vale destacar que a informação de tamanho de um tipo de instância é descrita pelo número total de ECUs.

A seguir podemos ver os principais tipos de instância disponíveis no AWS equal a indicação de uso para cada um deles:

- **M1 e M3 - Instâncias de uso geral:** Tipo de instância genérica, que possui uma distribuição dos recursos equilibrada entre CPU, memória e I/O;
- **C1, CC2 e C3 – Otimizadas para CPU:** Tipo de instância indicada para aplicações que possuem grande demanda de CPU, como servidores de encoding de vídeo;
- **G2 e CG1 – Instâncias com GPU:** Tipo de instância que permite o acesso a recursos da placa gráfica para processamento, o que é muito utilizado em aplicações científicas que necessitam de alto desempenho;
- **M2 e CR1 – Otimizadas para Memória:** Tipo de instância que possui grandes quantidades de memória, o que é ideal para servidores de banco de dados e de cache;
- **HI1 e HS1 – Otimizadas para Storage:** Tipo de instância que é otimizada para aplicações que possuem demanda por grandes

volumes de I/O. Também possui grande capacidade de processamento e memória, o que a torna indicada para uso em servidores de banco de dados de alto volume;

- **T1 –Instâncias Micro:** Tipo de instância mínima, ideal para testes e sites com pouco acesso.

Na **Tabela 1** podemos ver a relação entre os tipos de instância e os tamanhos oferecidos.

Tipo de Instância	Tamanho	vCPU	ECU	Memória (GB)
Uso Geral	m3.xlarge	4	13	15
Uso Geral	m3.2xlarge	8	26	30
Uso Geral	m1.small	11	1	1.7
Uso Geral	m1.medium	1	2	3.75
Uso Geral	m1.large	2	4	7.5
Uso Geral	m1.xlarge	4	8	15
Otimizadas para CPU	c3.large	2	7	3.75
Otimizadas para CPU	c3.xlarge	4	14	7
Otimizadas para CPU	c3.2xlarge	8	28	15
Otimizadas para CPU	c3.4xlarge	16	55	30
Otimizadas para CPU	c3.8xlarge	32	108	60
Otimizadas para CPU	c1.medium	2	5	1.7
Otimizadas para CPU	c1.xlarge	8	20	7
Otimizadas para CPU	cc2.8xlarge	32	88	60.5
Instâncias com GPU	g2.2xlarge	8	26	15
Instâncias com GPU	cg1.4xlarge	16	33.5	22.5
Otimizadas para Memória	m2.xlarge	2	6.5	17.1
Otimizadas para Memória	m2.2xlarge	4	13	34.2
Otimizadas para Memória	m2.4xlarge	8	26	68.4
Otimizadas para Memória	cr1.8xlarge	32	88	244
Otimizadas para Storage	hi1.4xlarge	16	35	60.5
Otimizadas para Storage	hs1.8xlarge	16	35	117
Instâncias Micro	t1.micro	1	Até 2	0.615

Tabela 1. Tamanhos das instâncias disponíveis no EC2

Vejamos os principais recursos oferecidos pelo EC2:

- **Instances:** É onde criamos as máquinas virtuais, chamadas de instâncias na terminologia do EC2. Na seção **Links**, mais precisamente no endereço relacionado a “Amazon EC2 Instance Details”, podemos ver todos os tipos de instância disponíveis e as suas diferentes configurações;
- **AMIs:** AMI significa *Amazon Machine Image*. São imagens de sistema operacional prontas para serem executadas, com software pré-instalado. É possível escolher dentre centenas de imagens existentes (por exemplo, com Linux, Apache e MySQL instalados), ou começar com uma imagem de sistema operacional básica, instalar o software desejado e criar a sua própria AMI para uso futuro;
- **Security Groups:** São as “regras de firewall” que controlam o acesso às suas instâncias do EC2. Através do security group é

possível controlar de forma granular o acesso a endereços IP e portas, externos ou internos;

- **Elastic IPs:** São endereços IP públicos que podem ser atribuídos a qualquer instância EC2;

- **Load Balancers:** É possível criar balanceadores de carga para distribuir os acessos entre os seus servidores web, por exemplo. Os balanceadores de carga ainda possuem a funcionalidade de detectar servidores que não estão respondendo, e colocá-los fora de serviço, de modo a não causarem problemas na sua aplicação;

- **Auto Scaling Groups:** Para compreender esse recurso, imaginemos o seguinte cenário: nosso site de e-commerce possui enormes picos de tráfego em datas comemorativas, como dia das mães, dos pais, Natal, etc., mas durante o resto do ano o tráfego é razoavelmente estável. Em uma infraestrutura tradicional, o ambiente seria dimensionado pelo pico, ou seja, para suportar a maior quantidade possível de acessos prevista. Isso faz com que paguemos o ano inteiro por uma infraestrutura que só é utilizada algumas vezes por ano. O auto scaling serve para racionalizar o uso da infraestrutura. Ele monitora o consumo de recursos dos seus servidores, e baseado em políticas, pode adicionar ou remover servidores do grupo para atender a demanda. Ou seja, no caso de um pico de tráfego, o auto scaling pode aumentar a capacidade de 2 para 10 servidores, e quando o pico passar, eliminar os servidores adicionais e deixar somente os dois que existiam antes. Dessa forma, somente pagamos pelo utilizado;

- **Volumes e Snapshots:** Dentro do EC2 existe um produto chamado EBS – *Elastic Block Storage*, que implementa funcionalidades de storage para instâncias EC2. Nele podemos criar discos, chamados de volumes, e snapshots desses volumes, com o objetivo de extrair uma cópia dos dados. Os volumes podem ter até 1 TB de tamanho, e podem ser do tipo Standard, ou do tipo Provisioned IOPS, onde se paga um pouco mais caro para garantir um throughput previsível. Um volume EBS é replicado dentro de uma mesma Zona de Disponibilidade para garantir a contingência quanto a falhas de hardware.

Com todos os recursos citados, é possível implementar soluções completas de infraestrutura de servidor na nuvem, tanto para uso em aplicações públicas, como sites de e-commerce, como para aplicações internas e privadas. Com os vários tamanhos de instância disponíveis, é possível hospedar serviços diversos como e-mail, banco de dados, servidores web, entre outros. Além disso, existem casos de empresas que utilizam o AWS para a criação de supercomputadores, empregando tecnologias de clustering sobre centenas de instâncias EC2. Essa é uma estratégia que proporcionou grande economia para estas empresas, que tradicionalmente investiam milhões de dólares na construção de supercomputadores.

Virtual Private Cloud – VPC

VPC é o serviço que possibilita a configuração de uma rede privada no AWS. Dentro de uma rede privada é possível ter todos os recursos do EC2, como instâncias e balanceadores, bem como

montar sub-redes separadas, com endereços IP privados, e rotear entre elas. É um serviço bastante útil para manter organizado o ambiente em nuvem quando a solução começa a depender de vários componentes, como servidores de aplicação, banco de dados, balanceadores de carga, etc. Além disso, a rede privada é interessante do ponto de vista da segurança, porque com uma VPC as nossas instâncias EC2 não precisam de endereço IP público para serem acessadas. É possível ainda criar uma VPN entre sua empresa e uma VPC no AWS para ter o seu ambiente na nuvem pública, mas com acesso totalmente isolado. A seguir podemos ver as principais configurações oferecidas pelo serviço de VPC:

- **VPCs:** Uma VPC simplesmente define o bloco de endereçamento IP contíguo que será utilizado no seu ambiente, como 10.0.0.0/16. Para ser utilizado por instâncias EC2, por exemplo, esse bloco deve ser dividido em subnets, que devem possuir um endereçamento que faça parte do bloco definido na VPC. Além disso, quando desejamos ter ambientes totalmente isolados e com uma política de acesso diferenciada, podemos criar mais de uma VPC;
- **Subnets:** Uma subnet é uma partição do bloco de endereçamento IP configurado na VPC. Dentro de uma VPC deve existir ao menos uma subnet, para que componentes do AWS, como instâncias EC2, possam se conectar. No entanto, podem ser criadas quantas subnets forem suportadas pelo bloco de endereçamento IP;
- **Route Tables:** É possível configurar rotas estáticas entre as subnets, para habilitar a comunicação entre instâncias que estão em subnets diferentes;
- **VPN Connections:** É possível configurar conexões VPN do seu escritório ou datacenter para uma VPC no AWS. Para isso é utilizado um *Customer Gateway*, que representa o gateway VPN do lado do datacenter, e um *Virtual Private Gateway*, que representa o gateway VPN do lado do AWS.

Glacier

O Glacier é o serviço de storage off-line do AWS. É um serviço de baixíssimo custo (1 centavo de dólar por GB) direcionado para o armazenamento de grandes volumes de dados e que são muito pouco acessados, como soluções de backup histórico e backup off-site. Os dados copiados para o Glacier são automaticamente replicados dentro da infraestrutura do AWS, com o objetivo de garantir máxima durabilidade. O baixo custo de armazenamento tem uma contrapartida de custo no acesso aos dados. Deste modo, se o cliente acessar em um mês mais do que 5% da média histórica do volume armazenado mensalmente, essa transferência é cobrada. É a forma utilizada pela Amazon para garantir que o acesso seja infrequente. Se precisamos de acesso frequente, o S3 e o EBS são produtos mais apropriados.

Relational Database Services – RDS

O RDS é o serviço de banco de dados relacional do AWS. Através dele podemos criar instâncias de banco de dados MySQL, Microsoft SQL Server, Oracle ou PostgreSQL. O RDS cria servidores virtuais com o DBMS desejado de acordo com os parâmetros especificados pelo usuário. Para bancos de dados que necessitam

de alto desempenho de I/O, é possível utilizar a opção de Provisioned IOPS, que garante uma quantidade de IOPS (operações de I/O por segundo) mínima e previsível.

Uma opção que o RDS oferece é a possibilidade de criarmos instâncias de contingência, utilizando a feature Multi-AZ, que indica que a instância será replicada automaticamente para outra instância que está em uma zona de disponibilidade diferente, e o AWS fará o failover para esta instância caso uma falha seja detectada. Essa funcionalidade está disponível para todos os DBMSs, exceto para o MS SQL Server. No caso do MySQL, podem ser criadas réplicas somente para leitura, que são úteis no caso de aplicações web de alto tráfego.

A seguir são apresentadas as principais funcionalidades do RDS:

- **Instances:** Uma instância RDS representa um único banco de dados de um DBMS particular. Um banco de dados no RDS funciona da mesma forma que um banco de dados instalado em um servidor local, com a diferença que não temos acesso ao console do servidor onde o banco de dados está hospedado;
- **Snapshots:** Snapshots são como “fotografias” do seu banco de dados em um determinado momento no tempo. São úteis como estratégia de backup e para congelar uma versão do banco de dados antes de uma mudança em produção, por exemplo;
- **Parameter Groups:** Com Parameter Groups é possível definir valores customizados para os parâmetros de cada DBMS, que podem ser aplicados a todas as instâncias que forem criadas. É um excelente recurso para garantir a padronização na configuração de instâncias;
- **Option Groups:** Option Groups fornecem um mecanismo de controle de funcionalidades adicionais e particulares de cada DBMS. Por exemplo, para o MySQL é possível habilitar a funcionalidade de memcache, para o Oracle é possível habilitar a funcionalidade do Statspack, entre outras.

Custos

Todos os produtos do AWS possuem políticas de preço bastante detalhadas e com farta documentação no site. É importante estudar a forma de cobrança de cada produto antes da contratação para evitar sustos na hora da conta. É muito comum provisionarmos mais recursos do que precisamos porque todos os serviços estão a um clique de distância, de forma muito simples. Outro ponto importante é que existem duas formas de contratação para a maioria dos recursos: on-demand e reservado.

No caso do EC2, por exemplo, instâncias on-demand são aquelas que nós criamos e removemos a qualquer momento. Nesse caso pagamos um valor por hora, pelo total de horas em que a instância esteve ligada. No caso de demandas de prazo mais longo, a Amazon oferece descontos bastante atrativos para clientes que querem se comprometer a manter um contrato por períodos de 1 ou 3 anos. Deste modo, ao pagarmos um valor por instância no momento do contrato, o valor pago por hora cai para menos da metade do valor de instâncias on-demand, em alguns casos. A recomendação geral é que, da mesma forma que não se deve investir em hardware ou datacenter sem planejamento, não se deve

fazê-lo com recursos na nuvem. O planejamento antecipado pode maximizar enormemente a economia que pode ser conseguida ao se optar por contratar infraestrutura na nuvem.

Neste artigo foram apresentados os principais serviços de cloud computing fornecidos pela Amazon e foram mostrados alguns casos de uso. Além desses, existem vários outros serviços, mais focados em aplicação, que omitimos aqui por questões de brevidade.

Sendo assim, sugerimos que o leitor visite o site do AWS e explore os produtos, para entender em profundidade do que a plataforma é capaz. Além do site, vale mencionar que todos os manuais dos produtos do AWS estão disponíveis na loja do Kindle (leitor de livros digitais da Amazon) sem custo. A documentação é bastante completa e certamente ajudará a esclarecer os detalhes de cada produto.

Para os que gostam de programar, vale mencionar que existem bibliotecas para as linguagens de programação mais populares, como Java, C# e Python, por exemplo, que permitem a automação de todos os aspectos de todos os produtos do AWS. Esse é um recurso extremamente interessante, que possibilita a construção de ferramentas de gerenciamento e automação bastante poderosas, e que facilitam a vida no dia-a-dia.

Apesar de o artigo ser totalmente baseado no AWS, que por ter sido o pioneiro, ainda é a referência no mercado quando se fala de nuvem pública, vale mencionar que existem outras ofertas no mercado, sendo o Windows Azure, da Microsoft, e o Compute Engine, da Google, as mais conhecidas. Com base no que falamos, é importante conhecê-los para poder avaliar qual é o serviço mais adequado para cada situação, e o mais importante, para que comparemos os valores e vejamos qual oferece o melhor custo benefício. Com a tendência da popularização do uso da nuvem pública, espera-se que a concorrência se torne cada vez mais acirrada, e com isso podemos esperar uma oferta de serviços de qualidade cada vez melhor e com menor custo.

Autor



Mateus Espadoto

mespadoto@yahoo.com

Há 14 anos trabalhando com TI, já trabalhou em áreas tão diversas como desenvolvimento de software, infraestrutura e arquitetura corporativa. Atualmente trabalha como Arquiteto de Software.



Links:

Site do Amazon Web Services.

<http://aws.amazon.com>

Site de preços do EC2.

<http://aws.amazon.com/ec2/pricing/>

Site com os detalhes dos tipos de instância do EC2.

<http://aws.amazon.com/ec2/instance-types/instance-details/>

Site de preços do S3.

<http://aws.amazon.com/s3/pricing/>

Site de preços do RDS.

<http://aws.amazon.com/rds/pricing/>

Site de preços do Glacier.

<http://aws.amazon.com/glacier/pricing/>

Site com exemplos de uso do AWS em substituição a supercomputadores.

<http://aws.amazon.com/hpc-applications/>

Case de migração para AWS da Netflix.

<http://www.slideshare.net/adrianco/migrating-netflix-from-oracle-to-global-cassandra>

Site do Windows Azure.

<http://www.windowsazure.com/pt-br/>

Site do Google Compute Engine.

<https://cloud.google.com/products/compute-engine/>

Somos tão apaixonados por tecnologia que o nome da empresa diz tudo.

Porta 80 é o melhor que a Internet
pode oferecer para sua empresa.

Já completamos 8 anos e
estamos a caminho dos 80, junto
com nossos clientes.

Adoramos tecnologia.
Somos uma equipe composta
de gente que entende e
gosta do que faz,
assim como você.



Estrutura

100% NACIONAL.
Servidores de primeira
linha, links de alta
capacidade.



Suporte diferenciado

Treinamos nossa equipe
para fazer mais e melhor.
Muito além do esperado.



Serviços

Oferecemos a tecnologia
mais moderna, serviços
diferenciados e
antenados com as suas
necessidades.



1-to-1

Conhecemos nossos
clientes. Atendemos
cada necessidade de
forma única.
Conheça!



Porta 80
WEB HOSTING

Hospedagem | Cloud Computing | Dedicados | VoIP | Ecommerce |
Aplicações | Streaming | Email corporativo

porta80.com.br | comercial@porta80.com.br | twitter.com/porta80

SP 4063-8616 | RJ 4063-5092 | MG 4063-8120 | DF 4063-7486

Ele está trabalhando em seu saque e não na sua nova aplicação.



Mais de 95%* dos times de desenvolvimento e testes de aplicativos relatam tempos de espera e atrasos para acessar os sistemas que necessitam para realizar suas atividades. A Virtualização de Serviços elimina estas dependências gerando ambientes simulados similares à realidade, permitindo o desenvolvimento em paralelo. Isto significa que suas aplicações serão lançadas mais rapidamente, com maior qualidade e menor custo. Game over!

Conheça mais em ca.com/br/GoDevOps

*De acordo com o estudo 2012 North America/Europe Service Virtualization Study, Coleman-Parkes.

