

Windows Server 2012 R2

Estudo dirigido para MCSA prova 70-410



© Casa do Código

Todos os direitos reservados e protegidos pela Lei nº9.610, de 10/02/1998.

Nenhuma parte deste livro poderá ser reproduzida, nem transmitida, sem autorização prévia por escrito da editora, seja quais forem os meios: fotográficos, eletrônicos, mecânicos, gravação ou quaisquer outros.

Edição

Adriano Almeida

Vivian Matsui

Revisão e diagramação

Bianca Hubert

Vivian Matsui

[2015]

Casa do Código

Livro para o programador

Rua Vergueiro, 3185 – 8º andar

04101-300 – Vila Mariana – São Paulo – SP – Brasil

www.casadocodigo.com.br

SOBRE O AUTOR



Eduardo R. S. Popovici é aficcionado por tecnologia. É geek, escritor, professor, empresário e profissional certificado pela Microsoft, tendo sido aprovado em diversos exames, com os quais obteve certificações como MCSE, MCSA, MCTS, MTA, MS e MCPS. Tornou-se instrutor certificado pela Microsoft obtendo o título de MCT.

É formado pelo curso de Tecnologia em Redes de Computadores pela Faculdade Módulo Paulista, sendo pós-graduado pelo curso de MBA, Planejamento estratégico de negócios com suporte da TI pela Faculdade Htbraz; MBA em Projetos de Data Center também pela Faculdade Htbraz e MBA Arquitetura de Redes e Cloud Computing pela Faculdade de Administração Paulista (FIAP). Atualmente, cursa pós-graduação de Cyber Security pela instituição Daryus.

Atua como consultor em Infraestrutura e TI, além de ministrar treinamentos para diversas instituições de ensino Brasil afora. Já

trabalhou em projetos dentro de empresas como Varig, HP, TV Globo, TV Record, Editora Abril, Copel Colchões, Brasoftware, entre outras.

É autor de mais de 800 postagens técnicas e diversos livros na área de TI, incluindo o livro de 2.100 páginas com o título Windows Server 2012 R2 e Active Directory - Curso Completo - Passo a Passo, em parceria com o mestre Julio Battisti. É mantenedor do site <http://www.htbraz.com.br> e da comunidade HTBRAZ no Facebook.

O primeiro livro escrito por Eduardo Popovici tratava-se de Excel em sua versão 2013.

AGRADECIMENTOS

Foi um longo caminho até aqui, mas finalmente esta grande obra tomou forma, volume e uma personalidade marcante. Quando recebi a proposta de desenvolver um conteúdo como este, fiquei, além de lisonjeado, muito empolgado.

Foram horas de trabalho árduo conciliado com minhas consultorias e treinamentos Brasil afora, além do desenvolvimento de apostilas para diversas escolas especializadas em tecnologia. Devo confessar aos amigos que houve dias em que achei que não seria possível continuar devido à alta carga de trabalho e estresse do cotidiano (pensei em desistir). Neste momento de extrema luta, recebi o apoio de bons amigos e da família de uma forma que jamais imaginei. Então percebi de uma forma tão única que nosso apoio está mais próximo do que realmente imaginamos. Este livro ganhou forma enquanto ainda desenvolvia o livro sobre Windows Server 2012 R2, direcionado ao público como curso completo, em parceria com o mestre Julio Battisti.

Deixo aqui registrado com todo o carinho meus agradecimentos mais que humildes e especiais à minha mãe Regina Celia, professora de matemática e ex-progamadora em Cobol dos tempos da Proceda, ao meu pai Antonio Abbondanza, especialista em Unix e excelente profissional técnico em infraestrutura de redes, ao meu irmão Rene Abbondanza e à minha irmã Talita Abbondanza, que sempre estão próximos quando preciso de apoio. Sou extremamente grato a toda a minha família pelo carinho e companheirismo nos momentos mais sombrios e nas vitórias mais ilustres; muito obrigado.

Deixo também um obrigado mais que especial agora para pessoas que aguentaram firme e forte cada um de meus momentos mais complexos. Obrigado à minha esposa Priscilla Lopes,

especialista em comércio exterior, por tantas palavras de carinho em momentos de dificuldade e cansaço. Obrigado também à minha filha Carolina, que faz de meus dias extremamente iluminados, ao meu filho Pietro, que chegou há pouco para trazer alegria adicional, e meu filho Miguel, que tem um sorriso único. São estes momentos de extrema carga emocional que vemos quão importante são nossa família e amigos.

Seria injusto agradecer alguns amigos quando tantos tiveram seu mérito em minha vida, afinal aprendi e aprendo a cada dia com cada um deles, sem exceção. Porém, gostaria de citar aqui alguns nomes que fizeram realmente a diferença neste momento tão arrebatador. Obrigado ao amigo de longa data, Maximiliano Abdao Amui, especialista em projetos com PMP, pela paciência e companheirismo além de longas conversas. Obrigado ao mestre Rogerio Molina, que me acompanhou com muito conhecimento e desafios ao longo do percurso. Obrigado aos amigos de todos os cursos de MBA que fiz, pois é incontável a quantidade de conhecimento que adquiri com vocês. Obrigado ao amigo Claudio Yamashita que atua como Pre-Sales Systems Engineer na Fujitsu do Brasil, pela ajuda com materiais e conteúdo técnico, difíceis de serem encontrados e muito específico. Também obrigado ao meu amigo Maycon Henrique dos Santos, especialista em redes e Linux do Hospital da Pedreira em São Paulo, que desenvolve o conteúdo do curso de Zimbra, pelo apoio nos trabalhos e na vida pessoal.

E meu muito obrigado a todos os amigos leitores. Afinal, sem vocês, esta obra não teria fundamento. É por vocês que dedicamos tantas horas de estudo e dedicação. Lembro-me dos tempos em que era complicado encontrar materiais em nosso idioma e a melhor forma de estudo na época era o *help* do sistema operacional (tempos difíceis).

Hoje, com os meios digitais e grande aderência à qualidade dos

produtos Microsoft, podemos escrever estas obras não só baseados em documentos e conteúdo teórico, mas em nossa experiência de mercado de trabalho. O meu muito obrigado a você, amigo leitor, é de grande forma especial, pois tudo o que vivi nas empresas em relação a ambientes Microsoft e sua interoperabilidade está aqui resumido.

Para finalizar, deixo aqui meu muito obrigado ao Papai do Céu (como dizia minha avó), e a todos os desafios colocados em minha vida. Sem os desafios, seríamos apenas seres mimados e descrentes de nós mesmos. É incrível o que podemos fazer quando uma dura realidade ou grande desafio se apresenta em nossa frente.

É importante deixar aqui registrado que sou imensamente grato a tudo o que aconteceu em minha vida, seja pelas conquistas que me deixaram com o sorriso no rosto, quanto pelas derrotas que me fizeram conhecer o chão duro, baixando meu ego e me lembrando de que sempre podemos vencer com a humildade e perseverança. A dedicação, a disciplina e a humildade são ferramentas poderosas para quem pretende alavancar como referência dentro da área em que ama atuar.

Aos amigos, deixo meu muito obrigado e desejo que todos realizem seus sonhos pessoais, financeiros e familiares.

Muito obrigado, muito obrigado, muito obrigado.

O MCSA E O WINDOWS SERVER 2012 R2

Entendendo o objetivo do MCSA

A nova certificação MCSA (Microsoft Certified Solutions Associate) é um título atribuído a profissionais da área de TI que se proponham a entender muito de um determinado assunto, como o Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SQL Server e Office 365. Caso você tenha curiosidade e até mesmo interesse em se aprofundar no Windows Server 2012 R2, procure pelo livro Windows Server 2012 R2 e Active Directory - Curso Completo - Passo a Passo, também de minha autoria com 2.100 páginas em dois volumes.



Figura 1: MCSA Geral

Este conteúdo recebe foco para a certificação MCSA do Windows Server 2012 R2, em especial para a prova 70-410. Para que um profissional da área de TI obtenha o título MCSA, é necessária a aprovação em três provas sobre o Windows Server 2012 R2. O profissional deve se sair bem nas provas 70-410, 70-411 e 70-412, obtendo um mínimo de 700 pontos em cada uma delas.

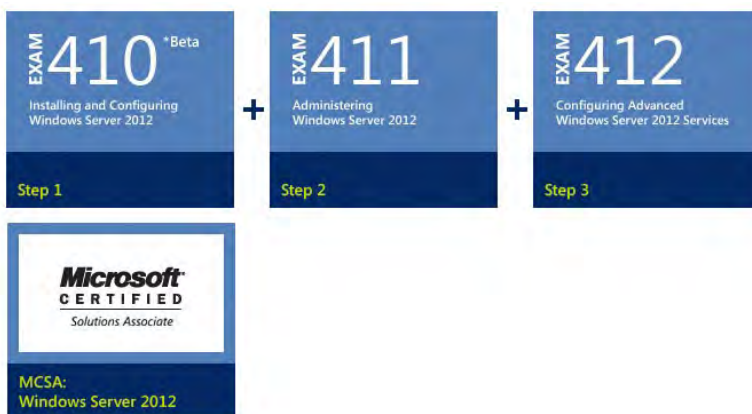


Figura 2: MCSA WS2012R2

A prova 70-410 não é exatamente uma prova difícil, mas isso não significa que será uma tarefa fácil. As questões encontradas na prova podem variar em quantidade e pesos diferentes. A certificação MCSA (Microsoft Certified Solutions Associate), do Windows Server 2012 R2, é a atual base para a carreira Microsoft e também as demais certificações relacionadas ao MCSE (Microsoft Certified Solutions Expert). Veja que é necessário entender que a prova foi dividida em seis partes com pesos que variam entre 15% a 20% do conteúdo. Aqui é importante lembrar de que é necessário um bom conhecimento sobre todo o conteúdo para não precisar depender da sorte para obter uma boa nota.

- (+) Instalar e configurar servidores (15–20%)
- (+) Configurar funções e recursos de servidor (15–20%)
- (+) Configurar o Hyper-V (15–20%)
- (+) Implantar e configurar serviços básicos de rede (15 – 20%)
- (+) Instalar e administrar o Active Directory (15–20%)
- (+) Criar e gerenciar Política de Grupo (15–20%)

Figura 3: Requisitos da prova 70-410

É importante entender que o Windows Server 2012 nasceu com uma concepção diferente das versões anteriores do Windows. Sua nova arquitetura foi desenhada para atender também a uma nova proposta chamada *Cloud Computing*, ou computação em nuvem. Cito como nova, porém a Cloud Computing não é tão nova assim. Todo o MCSA do Windows Server 2012 R2 trabalha não só com a administração de servidores, mas também a interoperabilidade com servidores em nuvem, além da integração com a Microsoft Azure, System Center e Office 365.

Realizando a prova

Até o ano de 2014, as provas eram realizadas pela Prometric e, desde 2015, passaram a ser realizadas pela Pearson VUE. Mas exatamente o que isso muda em relação à forma com que as provas são aplicadas? Bom, essa mudança traz uma série de benefícios, como por exemplo, a integração dos portais Microsoft e Pearson VUE, disponibilizando um acesso muito mais rápido e efetivo ao status de cada prova realizada. O tempo de assimilação da nota da prova pelo portal do MCP ficou bem mais baixo. Agora, também é possível efetuar sua prova fora de um centro de exames, ou seja, em sua própria casa.

A partir de 2015, a Microsoft liberou para o Brasil e outros países (já antes disponível nos EUA) a opção de realizar o exame online, chamado de Online Proctored e oferecido pela Pearson VUE.

Exames online supervisionados são os mesmos oferecidos em centros de testes, administrados por um inspetor remoto que vai supervisionar você via webcam e microfone, enquanto você realiza seu teste.

O candidato pode realizar os exames online supervisionados em casa, no trabalho, ou em qualquer outro local que atenda às nossas

necessidades de segurança e meio ambiente. É importante lembrar de que existe uma série de regras para esta modalidade, além de ser exigido um hardware específico para tal feito com direito a webcam e microfone.

Caso o candidato possa garantir que os requisitos de hardware sejam atendidos antes do check-in para o exame, o processo de check-in só deve demorar cerca de dez minutos. Exames online supervisionados oferecem uma grande quantidade de conveniência, se você mora longe de um centro de testes, mas existem alguns compromissos importantes dos quais você precisa estar ciente, incluindo:

1. Serão gravados vídeo e áudio durante o exame.
2. Você não pode tomar notas durante o exame.
3. Você não pode comer, beber ou mascar chiclete enquanto você faz o exame.
4. Você não pode fazer uma pausa por qualquer motivo.
5. Se alguma das situações acima representar um problema, você deve fazer o exame em um centro de testes.

Durante este período de testes, exames online supervisionados estão disponíveis pelo mesmo preço que os exames presenciais equivalentes. Neste momento, o beta está aberto apenas para residentes dos Estados Unidos, mas pretendem expandir a disponibilidade no futuro. O candidato pode agendar o seu exame com tão pouco quanto 15 minutos de antecedência, e os resultados estarão imediatamente acessível a partir de seu painel MCP quando terminá-lo.

Aí vem a pergunta: usar o recurso de exames em casa ou ir a um centro de exames? Bom, se você pode garantir que não haverá interrupções, ruídos, barulhos, quedas de internet, telefone tocando e chefe chamando, é uma boa ideia realizar o exame de casa. Eu

ainda prefiro me dirigir a um centro de exames, mas fazer as coisas de forma remota é uma excelente opção.

CRIANDO UM PLANO DE ESTUDOS

Plano de estudos

Primeiramente, é interessante avaliar os objetivos do seu treinamento, ou seja, por que você está praticando e estudando o Windows Server 2012 R2. Parece algo óbvio demais, porém, cada aluno dentro da sala busca um objetivo diferente dentro do treinamento. Então por meio deste plano de estudos, podemos direcionar aqueles que pretendem aprender sobre esta solução direcionada a servidores, ou aqueles que pretendem fazer as provas relacionadas ao Windows Server 2012 R2 obtendo o título de Microsoft Certified Solutions Associate (MCSA).

Como dito anteriormente, para obter o título de Microsoft Certified Solutions Associate, é necessária aprovação de pelo menos três provas relacionadas ao Windows Server 2012 R2, que seria a 70-410 (Installing and Configuring Windows Server 2012), 70-411 (Administering Windows Server 2012) e 70-412 (Configuring Advanced Windows Server 2012 Services). O MCSA permite que você tenha a base de conhecimento para ocupar um cargo de administrador de sistemas computacionais ou de administrador de rede, ou ainda especialista em redes de computadores, e é a etapa mais próxima para a obtenção da certificação Microsoft Certified Solutions Expert (MCSE). Para conseguir a certificação MCSE Server Infrastructure, são necessárias mais duas provas, além das provas do MCSA, que são a 70-413 (Designing and Implementing a Server Infrastructure) e a 70-414 (Implementing an Advanced Server Infrastructure).

- Requisitos do MCSA —
<https://www.microsoft.com/learning/pt-br/mcsa-windows-server-certification.aspx>
- Requisitos do MCSE —
<https://www.microsoft.com/learning/pt-br/mcse-server-infrastructure-certification.aspx>

Após prestar sua primeira prova (sendo aprovado ou não), você terá acesso ao portal do MCP com seu *score*, certificados válidos e histórico de provas. Aqui encontramos seu *transcript* e demais comprovações. Quando você inicia uma sequência de provas, é apresentada uma área dentro do portal que indica quantas provas faltam para a obtenção de um determinado título.

[Início](#)
[Treinamento](#)
[Certificações e exames](#)
[Carreiras](#)
[Seus benefícios e exames](#)
[Mais](#)

Seus benefícios e exames

Com base em seu exame mais recente, aparentemente você está buscando a seguinte certificação. Se você é um MCP, encontre mais opções com o [Planejador de Certificação](#).

	410	411	412	Destino da certificação
Caminho recomendado	✓	✓	↻	MCSA: Windows Server 2012

Faça gratuitamente treinamentos ministrados pelos principais especialistas

Participe do [Microsoft Virtual Academy](#) e faça gratuitamente treinamentos técnicos ilimitados sobre dezenas de tópicos e tecnologias.

[Promova-se](#)

[Recursos](#)


Compromissos

Apenas Pearson VUE. A exibição de algumas atualizações pode demorar.

Nenhuma informação de compromisso disponível.

[Visualizar meu relatório de notas](#)


Histórico



[Exibir e baixar](#)

[Compartilhar](#)

Certificados



[Baixar ou comprar](#)

Figura 1: Portal do MCP - <https://mcp.microsoft.com/>

Para iniciar seus estudos, você primeiramente deve responder a algumas perguntas básicas:

1. Qual é o seu objetivo? (Conhecer / certificar)
2. Quanto tempo pode dedicar ao estudo diário para teoria? (Tempo efetivo em horas)
3. Quanto tempo pode dedicar ao estudo diário para laboratórios? (Tempo efetivo em horas)
4. Quando pretende fazer a prova após o término do curso? (Se é que pretende fazer)

Após responder tais questões, é possível definir um plano de ação para realizar as provas de forma rápida e organizada. Minhas dicas sobre as provas:

- Marque a prova. Quando o ser humano em geral trabalha com prazos bem estabelecidos, temos a tendência de trabalhar melhor. Trabalhar com data estipulada faz você atribuir uma meta e correr atrás do conteúdo e dos laboratórios. Faça da pressão por resultados sua aliada nos estudos.
- Disciplina de estudo é ponto fundamental, sem isso você apenas conhecerá o conteúdo, mas ficará perdido dentro das perguntas das provas. Será necessário não apenas conhecer sobre uma solução, mas como aplicá-la dentro de uma determinada situação. Não existe segredo para isso, serão necessárias a prática e a leitura constante.
- Estude com calma, mas de forma contínua. Guarde um espaço do dia para estudar pelo menos 3 horas por dia, e defina metas com prazos a serem alcançados. Se houver um prazo, a chance de se preparar e alcançar o objetivo é maior. É importante lembrar: faça seu estudo direcionado de 3 em 3 horas com pausas de 15 a 20 minutos. Quando o conteúdo é muito denso, não adianta estudar mais de 3 horas sem uma pausa, isso somente desgasta seu emocional e psicológico.
- Comece pela prova 70-410 e concentre-se nesse objetivo. Além do conteúdo deste livro, recomendo que você faça todas as atividades do MVA (Microsoft Virtual Academy). Esta academia virtual fará uma rápida passagem por cada prova relacionada ao MCSA do Windows Server 2012 e Windows Server 2012 R2.
- Leia os fóruns oficiais da Microsoft. Ali temos situações reais de administradores de redes reais. Isso ajuda muito com a solução de problemas e até mesmo em

situações relacionadas a prova. A certificação MCSA está direcionada ao mercado de trabalho, ou seja, não é algo acadêmico. Portanto, possuir o conhecimento prático do dia a dia ainda é a melhor forma de estudar.

- PowerShell e ferramentas de linha de comando despençam em todas as provas do MCSA e MCSE, logo, pratique a linha de comando. Se possível, crie uma máquina virtual com o Windows Server 2012 R2 em modo de Instalação Server Core. Isso ajuda a aplicar os comandos com maior flexibilidade.

A prova 70-410 é considerada fácil se comparada às demais (eu disse se comparada às demais), e envolve prática direcionada à instalação do Windows Server 2012 R2 em sua enorme gama de opções, como por exemplo, pendrives, DVDs e arquivos de extensão .ISO ou .WIN. Muito do conteúdo cobrado é também visto para as provas do Windows 7, Windows 8 e demais sistemas operacionais Microsoft. Busque material complementar para blindar o conhecimento. Fazer a blindagem do conhecimento é conhecer além do que será cobrado na prova, fazendo com que seu dia a dia seja mais tranquilo e a aplicação prática mais simples.

A prova 70-411 é mais complexa e exigirá de você um bom conhecimento com a administração geral de sistema, incluindo a atualização de estações de trabalho e servidores, uso de replicação de imagens e customização de ambientes. É uma prova que considero simples, mas que pode demandar mais atenção do que a 70-410.

A prova 70-412 é bem interessante e cheia de detalhes. Acredito que seja a prova que mais tome tempo de estudo e revisão de laboratórios. Ela é cheia de detalhes e respostas que possuem mais de uma alternativa correta, muitas vezes confundindo e gerando certo desconforto durante sua execução.

Estude no seu tempo, porém com prazo definido (prova marcada), permitindo que o conhecimento se mantenha fresco e latente em sua cabeça. Isso dará a você uma grande vantagem, pois as provas são sequenciais e utilizam o mesmo conceito em situações mais complexas. O conceito de DNS, por exemplo, cai em todas as provas, assim como o conceito do Hyper-V, porém com sistemáticas e dificuldades diferentes.

Sumário

1 Instalando o Windows Server 2012 R2	1
1.1 Requisitos de Hardware do WS2012R2	1
1.2 Roles (funções) e features (recursos)	7
1.3 Instalação Server Core (sem área gráfica)	10
1.4 Diferenças entre migração e upgrade do Windows	17
1.5 RSAT — Kit de ferramentas para o dia a dia	21
1.6 Modo de instalação Server Core	23
1.7 Acionando o sconfig	32
1.8 Minimal Server Interface	33
2 Introdução ao Active Directory (ADDS)	36
2.1 Subindo o ambiente	36
2.2 Gerenciador do servidor	39
2.3 Configurar o servidor local	42
2.4 Introdução ao Active Directory Domain Services (ADDS)	50
2.5 Implementando controladores de domínio no Windows Server 2012 R2	53
2.6 Implementando controladores de domínio pelo IFM	66
2.7 Pesquisar objetos no Active Directory	69
2.8 FSMO	69
2.9 Usando a interface do Windows	71

3 Objetos do AD	77
3.1 As contas de usuário	78
3.2 Propriedades do usuário	83
3.3 Unidades organizacionais (OU)	87
3.4 Grupos de trabalho	88
3.5 Escopos de grupos de trabalho	89
3.6 Alterando o escopo dos grupos	93
3.7 Delegando acessos no Active Directory Domain Services	95
4 Administração por linha de comando	99
4.1 PowerShell	109
4.2 PowerShell ISE	117
4.3 CSVDE	118
4.4 Ldifde	121
4.5 DISM	122
4.6 NETSH	125
4.7 SLMGR	126
4.8 NETDOM	127
4.9 Winrm	129
4.10 Commandlets do PowerShell	130
5 Active Directory Administrative Center (ADAC)	133
5.1 Lixeira do Active Directory	136
5.2 Gerenciamento de contas de usuário	138
5.3 Canais de segurança	143
5.4 Administração centralizada	146
6 DHCP	149
6.1 Tipos de opção	159
6.2 Estatísticas do DHCP	163
6.3 Opções de escopo	165

7 DNS	167
7.1 DNS reverso	170
7.2 Round-Robin DNS	171
8 TCP/IP	175
8.1 IPV4	175
8.2 IPV6	178
8.3 NAT	182
8.4 ISATAP	185
9 Volumes de disco	187
9.1 Gerenciador de Disco — Disk Management	191
9.2 Diskpart	198
9.3 Disco GPT	201
9.4 Storage Pool	203
10 Computer Management — Gerenciador do Computador	205
10.1 Permissões NTFS e compartilhamento	207
10.2 Herança de permissões	210
10.3 Shadown Copy (cópia de sombra)	212
10.4 Servidor de impressão	217
11 GPO — Group Policys	220
11.1 Hierarquia das GPOs	221
11.2 Heranças de GPOs	225
11.3 Gpupdate	227
11.4 Gpresult	230
12 Hyper-V	232
12.1 Virtualização Microsoft	232
12.2 Client Hyper-V	233
12.3 Requisitos de hardware para o Hyper-V	236

12.4 Memória dinâmica	237
12.5 Paginação inteligente	238
12.6 Medição de recursos	238
12.7 Arquivos de armazenamento (VHD / VHDX)	239
12.8 Instantâneos — Snapshots	242
12.9 Comutador virtual — Switch virtual	243
13 Descrição sobre os servidores	246
13.1 Tipos de servidores	247
14 Montando seu laboratório prático no Hyper-V	265
14.1 Instalando o Hyper-V no Windows 8	266
14.2 Dicas de utilização do Hyper-V	273
15 Simulado	280
15.1 Instalação e configuração	280
15.2 Acesso a dados	292
15.3 Configuração do Hyper-V	298
16 Respostas do simulado	300
16.1 Instalação e configuração	300
16.2 Acesso a dados	313
16.3 Configuração do Hyper-V	317

INSTALANDO O WINDOWS SERVER 2012 R2

1.1 REQUISITOS DE HARDWARE DO WS2012R2

Diferentemente dos sistemas direcionados a estações de trabalho, a Microsoft opera em requisitos mais baixos de hardware para sistemas operacionais direcionados a servidores. É possível encontrar servidores com apenas 512 MB de memória RAM com o Windows Server 2012 e 2012 R2 instalados e com recursos básicos ativos. Devo lembrar de que, na prática, uma coisa é instalar, e outra é funcionar bem e de forma performática.

Lembre-se de que seu papel é se preparar para a prova 70-410 que cobrará requisitos técnicos aplicados à instalação, portanto, todo este conteúdo direciona as explicações para esse objetivo. No dia a dia, você não subirá um servidor com o Windows Server 2012 R2 com 512 MB RAM para atender uma rede com vários usuários sendo controlador de domínio. Seria insano e extremamente lento.

No mundo real, fazendo consultoria com diversas empresas, vi servidores com apenas 512 MB atuando em produção como DHCP e DNS. Em momentos de crise, trabalha-se com o que se tem na mão e utiliza-se pouco do bom senso, mas muitas vezes é o que dá para fazer no momento. Não temos como criticar quem monta esse tipo de estrutura, mas se pudermos evitar, seria bem interessante.

Vamos falar dos requisitos oficiais disponibilizados pela Microsoft sobre o Windows Server 2012 R2. Separei uma lista de requisitos mínimos de hardware iniciais utilizada como base para uma instalação limpa do Windows Server 2012 e 2012 R2. Estes dados são referentes à instalação de uma máquina completa, seja ela em uma VM ou servidor Host. Caso você precise instalar novos papéis ou novas funções, será necessário rever o hardware disponível e efetuar um upgrade.

- Processador de 1,4 GHz e 64 bits;
- Memória 512 MB;
- Hard Disk 32 GB
- Adaptador Gigabit (10/100/1000baseT) Ethernet;
- Unidade de DVD (caso pretenda instalar o sistema operacional usando mídia de DVD);
- Monitor Super VGA (1024 x 768) ou com resolução superior;
- Teclado e mouse Microsoft (ou outro dispositivo apontador compatível);
- Acesso à internet.

A Microsoft aboliu os sistemas de servidores com plataforma de 32 bits. Desde o Windows Server 2008 R2, não se trabalha com sistemas operacionais para servidor com 32 Bits. O Windows Server 2012 e 2012 R2 segue a mesma linha de pensamento, e não disponibiliza sua instalação em 32 bits, ou seja, não funciona em servidores com hardware mais antigo. O processador e a placa mãe devem suportar 64 bits de forma nativa.

Avaliação do produto (180 dias)

É possível baixar gratuitamente o Windows Server 2012 R2 diretamente do site da Microsoft para um período de degustação. Isso significa que você pode baixar e instalar o Windows Server sem o medo de ser pego com softwares piratas. Para baixar o Windows Server 2012 R2 (a partir de agora usarei a sigla WS2012R2), basta acessar o link disposto nesta página, ou digitar o texto chave “Download Windows Server 2012 R2” em buscadores como Bing e Google. Meu último acesso neste link foi no dia 14 de janeiro de 2016, e estava tranquilo para efetuar o download:

<https://technet.microsoft.com/pt-br/evalcenter/>

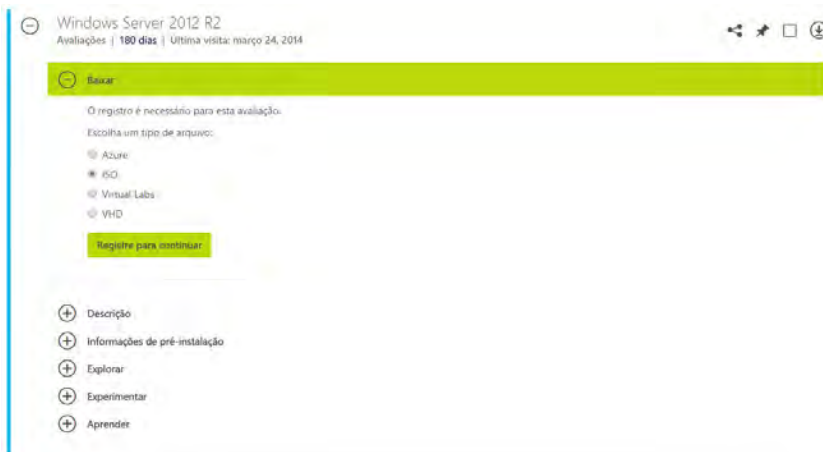


Figura 1.1: Baixando o WS2012R2



Figura 1.2: Detalhes do download

A degustação funciona assim: você recebe um prazo de 10 dias para a conclusão da ativação online após a instalação com período efetivo de avaliação de 180 dias. Durante todo o período de avaliação do WS202R2, será apresentada uma notificação no canto direito inferior da área de trabalho (ali próximo à área de notificação), que exibe os dias remanescentes do período de avaliação.

É possível também validar o tempo restante da degustação (caso

não apareça como deveria na área de trabalho) pelo comando `slmgr.vbs /dlv` em um prompt de comando, ou pelo Power Shell em modo elevado. Para estender o período de ativação por mais 60 dias, utilize o comando `slmgr.vbs -rearm`. Lembre-se de que você possui uma quantidade limitada de `rearms` disponíveis, portanto nunca use uma versão de avaliação em um ambiente de produção.

Recomendo que utilize o arquivo `.ISO` disponível pela instalação, porém prepare o link, pois o download é superior a 4 GB. Quando efetuei o download, o arquivo era o `WINBLUE_REFRESH.X64FRE_SERVER_EVAL_EN-US-IR3_SSS_X64FREE_EN-US_DV9.ISO` de 4.2 GB. Esse arquivo vai sendo trocado e atualizado com o passar do tempo.

Já é possível baixar o Windows Server 2016 Technical Preview 4 (com arquivo `.ISO` de 4.8 GB), mas como este lançamento é apenas para mais tarde, vamos concentrar nossos esforços para o Windows Server 2012 R2.



Figura 1.3: Detalhes do download do WS2016 RP4

Edições do Windows Server 2012 R2

Poucas pessoas realmente se preocupam em conhecer as edições e versões do Windows corretamente, tanto porque a prova 70-410 cobra efetivamente o conhecimento apenas da edição Standard e Datacenter, já que são as mais completas quando pensamos em funções e recursos de um servidor. São nestas edições que está toda gama de melhorias e funcionalidades que nos interessam, como o Active Directory, o Failover Cluster (que cai na prova 70-412) e o Load Balance (que também cai na 70-412).

A prova 70-410 manterá o foco nas edições Standard e Datacenter, mas é importante saber que é possível encontrar diversas edições espalhadas por empresas Brasil afora, como por exemplo, a edição Windows MultiPoint Server 2012 Standard ou o Windows Storage Server 2012 Workgroup. Nosso foco não é o de adentrar nestas distribuições; apenas menciono neste livro sua existência, pois caso exista alguma questão que cobre esse fator pela prova 70-410, não haverá dúvidas.

O livro Windows Server 2012 R2 e Active Directory - Curso Completo - Passo a Passo, que escrevi em parceria com o mestre Julio Battisti, contempla muito conteúdo adicional e servirá como referência para todo o MCSA. Acesse: <http://www.juliobattisti.com.br/loja/detalheproduto.asp?CodigoLivro=LIV0001438>.

Caso você queira assistir o treinamento com vídeos e certificado, fique à vontade para nos visitar em nossa escola virtual pelo link <http://htbraz.edools.com/>.

A seguir, trataremos as edições do Windows Server 2012 R2 de forma simplificada através de uma lista de opções. Lembre-se de que a prova pode questioná-lo sobre quando aplicar cada uma destas edições em um cenário de aquisição de licenças.

As edições Essentials e Foundations não possuem adição de Call (Call é uma licença que deve ser comprada separadamente para cada usuário da rede), ou seja, cada uma possui licenciamento reduzido e travado. Isso significa que possuem um custo monetário mais interessante, e podem ser facilmente assimiladas para o que a Microsoft chama de Small Business (pequena empresa).

Contudo, vale lembrar de que as edições Foundation e Essentials não possuem diversas funções e recursos disponíveis pela edição Standard. Recomendo muita cautela ao aplicar estas licenças em clientes diversos, mas podem ser incrivelmente estratégicas para negócios situações específicas em que é exigido um servidor com Windows Server 2012 ou 2012 R2.

- Windows Server 2012 R2 Datacenter
- Windows Server 2012 R2 Standard
- Windows Server 2012 R2 Essentials
- Windows Server 2012 R2 Foundation
- Windows Storage Server 2012 Workgroup
- Windows Storage Server 2012 Standard
- Windows MultiPoint Server 2012 Standard
- Windows MultiPoint Server 2012 Premium
- Hyper-V Server 2012 R2

1.2 ROLES (FUNÇÕES) E FEATURES (RECURSOS)

Uma curiosidade interessante do WS2012R2 está nas funções e serviços disponíveis para instalação. Houve a junção das instalações

em um único assistente (Wizard), disponível pelo Gerenciador do Servidor (Server Manager). A

ntes de iniciar a instalação efetiva das funções e recursos, atrevo-me a perguntar: você sabe a diferença básica entre funções (roles) e recursos (features)? Se a resposta é não, fique tranquilo que esta resposta é mais comum do que se possa imaginar. Vamos desmistificar estes pontos nas próximas páginas.

A próxima figura trata exatamente da tela de instalação de funções e recursos pelo Gerenciador do Servidor, especificamente pelo item Gerenciamento no canto direito superior da janela.

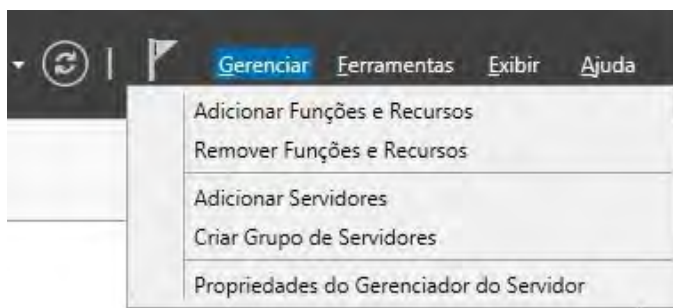


Figura 1.4: Gerenciar pelo Server Manager (Gerenciador do Servidor)

Pode-se também adicionar funções e recursos através do Gerenciador do Servidor (*Server Manager*), logo à primeira vista do painel chamado *Dashboard*. Este modelo de instalação está mais fácil de ser encontrado e de forma mais efetiva que o anterior apresentado pelo Windows Server 2008 e 2008 R2. As provas cobram sempre as novidades de um sistema operacional, portanto fique atento aos detalhes.

A função também é conhecida pelo termo em língua inglesa *role*. A role é utilizada para definir uma ou mais funções primárias executadas por um servidor com Windows Server dentro de uma infraestrutura de rede. Lembre-se de que um servidor com

Windows Server pode possuir mais de uma função ao mesmo tempo. Existem, porém, algumas recomendações técnicas relacionadas à segurança e performance que devem ser levadas em consideração. Fique tranquilo que trataremos destas características mais adiante, apenas lembre-se de que o servidor não precisa ser dedicado a uma determinada atividade.

Já os recursos são funções auxiliares empregadas a um servidor com o Windows Server. Todo recurso é instalado visando à complementação das funcionalidades de uma determinada função primária. Geralmente, ela acompanha algum pré-requisito de uma determinada função, como o IIS, que acompanha grande parte das funções primárias de um servidor com WS2012R2.

O IIS não recebeu exatamente um foco administrativo no WS2012R2, porém é uma ferramenta de extrema importância para os administradores de redes. Recomendo que você considere um estudo futuro mais aprimorado. Não teremos um capítulo do IIS neste livro, pois trataremos aqui apenas do conteúdo para a prova 70-410.

Neste capítulo, separei exatamente as funções e recursos disponíveis no Windows Server 2012 R2. Tais funções e recursos serão devidamente cobrados como conhecimento obrigatório pelas provas do MCSA e até mesmo MCSE.

A diferença entre a cobrança do conteúdo do MCSA para o MCSE está no grau de dificuldade da configuração das funções e recursos. No MCSA, tratamos a configuração básica e, no MCSE, tratamos os estudos de caso e lições aprendidas de forma real. Para que fique mais claro o conteúdo proposto aqui, separei as funções em uma tabela e os recursos em outra.

1.3 INSTALAÇÃO SERVER CORE (SEM ÁREA GRÁFICA)

Trabalhar com o Windows sempre foi confortável devido à sua interface gráfica, mas em diversos momentos os administradores de redes sentiram falta da antiga tela escura. Vamos dar o braço a torcer, trabalhar com interface gráfica consome mais recursos de hardware do que deveria e oferece menos segurança. Pois bem, a Microsoft levou isso muito a sério e a partir do WS2008 é possível efetuar uma instalação inteira sem a interface gráfica.

Palavras-chaves da instalação Server Core são: segurança e performance. Isso torna a instalação extremamente performática. Durante o treinamento EAD da HTBRAZ, é visto como efetuar a mudança de formato de instalação da interface gráfica para server core, e vice-versa. Nas próximas páginas, também abordaremos este processo.

Essa inovação foi tão bem aceita que recebeu aprimoramentos consideráveis para a nova versão do Windows e se manteve até o WS2012R2. O que você deve lembrar para as provas do MCSA é que o Windows Server 2008 permite que você faça o processo de ida para o modo Server Core, mas não permite o processo de volta. Ou seja, uma vez removida a interface gráfica, não é possível retornar. Porém, o Windows Server 2012 e 2012 R2 permite ida e volta, ou seja, é possível remover a interface gráfica e depois recolocá-la, seja pelo PowerShell quanto pela ferramenta de linha de comando `dism.exe` (comentaremos mais à frente sobre esta ferramenta).

Se um dia desses houver a necessidade de instalar a interface gráfica em um servidor com o Windows Server 2008 R2 para a

interface gráfica, basta apenas efetuar o upgrade do Windows para a versão 2012 ou 2012 R2, e então reinstalar a interface gráfica. Este é um dos itens mais interessantes que podem ser cobrados em sua prova através de um pequeno cenário, portanto fique atento e lembre-se de que existem técnicas que permitem driblar características do Windows Server 2008 R2 (64 bits).

Deve-se também entender que existem diferenças importantes entre uma instalação limpa e um upgrade de versões. Em uma instalação limpa, todo o conteúdo do servidor é eliminado; já em um upgrade o conteúdo do servidor é mantido operacional. Em muitos casos, recomendo que você dê prioridade para a instalação limpa, mas o upgrade pode ser usado em casos específicos, como no da interface gráfica do WS2008R2 dos parágrafos anteriores.

O fato é que o update é mais demorado e pode apresentar erros dependendo do tipo de aplicação legada que está instalada em um servidor, devendo então ser utilizada apenas em último caso ou em casos específicos.

Existem situações específicas em que será permitido um upgrade de versões (lembre-se de que versões são diferentes de edições), significando que muitas vezes as versões do sistema operacional podem não ser compatíveis entre si, ou seja, não é possível migrar de uma versão 2003 de 32 bits para 2012 R2 de 64 bits. Por via de regra, um servidor de 64 bits com o sistema nativo Windows Server 2008 ,ou Windows Server 2008 R2, poderá ser atualizado para o Windows Server 2012, desde que seja utilizada a mesma edição do sistema operacional (Windows Server 2012 ou 2012 R2). Não serão suportadas atualizações que obtenham as seguintes características:

- Atualizações a partir de versões do Windows Server anteriores ao Windows Server 2008;
- Atualizações a partir de edições de pré-RTM do Windows Server 2012;

- Upgrades de sistemas operacionais de estação de trabalho do Windows, como XP, Vista, 7 ou 8;
- Atualizações de mudança de plataforma, de 32 bits do Windows Server 2008 para o Windows de 64 bits server 2012;
- Atualizações a partir de qualquer edição Itanium;
- Atualizações entre idiomas, tais como a partir do Windows Server 2008, US Inglês para o Windows Server 2012 em francês.

A Instalação Server Core permite utilização das seguintes ferramentas listadas pela tabela a seguir:

Ferramenta	Função
<i>Cmd.exe</i>	Permite executar ferramentas de linha de comando tradicionais, como <i>ping.exe</i> , <i>ipconfig.exe</i> e <i>netsh.exe</i> .
<i>PowerShell.exe</i>	Inicia uma sessão do Windows PowerShell pela implantação Server Core.
<i>Sconfig.cmd</i>	Uma ferramenta administrativa de linha de comando baseada em menu que permite realizar configurações comuns de servidor, como por exemplo, a troca de seu hostname, IP, Gateway etc.
<i>Notepad.exe</i>	Permite usar o editor de texto <i>Notepad.exe</i> no ambiente Server Core.
<i>Regedt32.exe</i>	Fornecer acesso ao Registro no ambiente Server Core.
<i>Msiinfo32.exe</i>	Permite visualizar informações do sistema sobre a implantação Server Core.
<i>Taskmgr.exe</i>	Inicia o Gerenciador de Tarefas.
<i>SCregEdit.wsf</i>	Usado para habilitar a Área de Trabalho Remota na implantação do Server Core.

É possível alternar da instalação Server Core para a versão gráfica do Windows Server 2012 e 2012 R2 executando o seguinte cmdlet do Windows PowerShell, onde `c:\mount` é o diretório raiz de uma imagem montada que hospeda a versão completa dos arquivos de instalação do Windows Server 2012 ou 2012 R2:

```
Install-WindowsFeature -IncludeAllSubFeature User-Interfaces-Infra  
-Source c:\mount
```

É também possível usar o Windows Update, servidor WDS ou o DVD de instalação como origem do arquivo de instalação. Instalar os componentes gráficos oferece a você a opção de realizar tarefas administrativas usando as ferramentas gráficas, porém a instalação Server Core oferece desempenho e segurança elevados. A instalação Server Core foi aprimorada e permite mudança para o modo GUI e o retorno para Server Core, que não era permitido no Windows Server 2008.

É uma prática muito comum realizar as tarefas administrativas necessárias em ambiente gráfico e depois retornar o servidor à sua configuração Server Core original. É possível alternar um computador ou servidor que possui a versão gráfica do Windows Server 2012 e 2012 R2 para a instalação Server Core removendo os componentes gráficos de Interfaces do Usuário e Infraestrutura. Falaremos mais sobre o assunto no decorrer do livro.

Detalhes da instalação do Windows Server 2012 R2

Para muitos, a instalação do Windows torna-se algo simples e básico quando efetuada através de uma mídia como um DVD ou sequência de CDs, mas administrar um ambiente é mais do que apenas acionar uma unidade de leitura de mídia externa e seguir os passos apresentados na tela.

A instalação do Windows pode ser executada de diversas formas, que serão amplamente exploradas pela prova 70-410 do MCSA e, possivelmente, também para as próximas versões do Windows Server. Você pode obter uma mídia de instalação através de um canal de vendas Microsoft, ou ainda baixá-lo para o período de degustação, também chamado de período de testes (<https://technet.microsoft.com/library/hh801901>). As

questões teóricas são de extrema importância para o entendimento dos laboratórios, porém recomendo que você pratique muito os laboratórios oferecidos por este material.

Após obter o Windows Server 2012 R2, será necessário administrar o formato de sua instalação, que pode ser feita pela mídia do sistema operacional, ou pela distribuição de seu arquivo .ISO . Os arquivos dessa extensão estão se tornando mais comuns à medida que as organizações adquirem softwares via internet em vez de obterem a mídia removível física.

Além de facilidade de organização das licenças e contratos de utilização, a aquisição de softwares através de portal de serviços de fornecedores permite aos clientes da Microsoft baixar suas aquisições no idioma desejado diretamente do portal E-open. Será cobrado de você o conhecimento sobre a instalação do sistema operacional não só do modo convencional, mas também com a utilização de mídias USB, boot pela rede utilizando uma placa PXE e demais afinidades.

Hoje é possível instalar o Windows Server 2012 e 2012 R2 das seguintes maneiras:

- Mídia Óptica;
- Mídia USB;
- Imagem ISO montada;
- Compartilhamento de rede;
- Pelo Windows DS;
- Pelo System Center Configuration Manager;
- Pelos Modelos do Virtual Machine Manager.

Imagine que você possua um servidor antigo com o Windows Server 2003, ou ainda o Windows Server 2008 R2. Esse servidor é usado como servidor de arquivos ou, como gostamos de chamar, `file server` . Você então verifica que ali há programas

compatíveis com o Windows Server 2012 R2. Você precisa decidir se fará uma atualização, migração do sistema ou uma instalação limpa removendo qualquer vestígio do sistema operacional mais antigo. Será cobrado de você na prova o conhecimento de quando utilizar cada tipo de instalação em um determinado momento ou ambiente.

Tipos de instalação do Windows Server 2012 R2

Nova instalação: permite que você faça uma nova instalação em um novo disco ou volume (disco limpo que não contenha dados). Instalações novas são as mais frequentes e comuns desde os tempos do Windows 2000 até hoje, sendo consideradas as menos demoradas. Você também pode usar essa opção com o objetivo de configurar o Windows Server 2012 R2 para realizar uma inicialização dupla (*dual boot*), caso queira manter o sistema operacional anterior ainda existente. Apesar de pouco utilizado, o dual boot ainda pode ser encontrado em instituições de ensino que possuem alta rotatividade em seu portfólio de treinamentos.

Atualização: a atualização preserva os arquivos, as configurações e os aplicativos que já são instalados no servidor original, sem levar em conta sua compatibilidade. Você realiza uma atualização quando deseja manter todos esses itens e prefere continuar a usar o mesmo hardware de servidor. Só é possível atualizar para uma edição equivalente ou mais recente do Windows Server 2012 a partir de versões x64 do Windows Server 2008 e do Windows Server 2008 R2. Você inicia uma atualização executando o arquivo `setup.exe` a partir do sistema operacional Windows Server original. É sempre interessante verificar a compatibilidade de todas as aplicações antes de efetuar a atualização do sistema, lembrando também de efetuar um backup do ambiente. Nunca efetue uma atualização sem o devido backup e fora da janela de manutenção.

Migração: utilize o recurso de migração em versões x86 e x64 do Windows Server 2003, do Windows Server 2003 R2 ou do Windows Server 2008 para o Windows Server 2012 ou 2012 R2. É possível usar o recurso Ferramentas de Migração do Windows Server no Windows Server 2012 e 2012 R2 para transferir arquivos e configurações (USMT ou migwiz.exe). Esta ferramenta não está disponível em estações de trabalho com o Windows 10.



Você pode ser cobrado na prova 70-410 em um cenário que envolva um servidor de versão anterior, como o Windows Server 2000, que precise receber uma nova versão de sistema operacional. Você deverá optar por uma nova instalação, atualização ou migração para resolver a proposta. Esta questão é tranquila, desde que você se lembre das limitações e diferenças entre os upgrades e migrações.

1.4 DIFERENÇAS ENTRE MIGRAÇÃO E UPGRADE DO WINDOWS

Existem diversas formas de atualizar ou migrar seu ambiente atual de servidores com Windows Server 2008 ou 2008 R2 para um ambiente com Windows Server 2012 ou 2012 R2. A atualização e a migração são duas abordagens diferentes que devem ser tratadas com cuidado. A atualização refere-se à atualização do seu servidor atual para um novo sistema operacional ou estado sem reinstalar ou reconfigurar os componentes de software ou de hardware. Deixo claro aqui que o risco em problemas e incompatibilidades é alto. A abordagem relacionada à migração introduz um novo sistema operacional do servidor ou em uma nova plataforma de hardware, e todos os recursos existentes para o novo servidor se movem através da ferramenta USMT.

Ambas as opções têm prós e contras. Se você estiver executando uma atualização *in-loco* (*in-place*), precisa se certificar de que todo o hardware, software e aplicações suportam o novo sistema operacional.

O Microsoft Windows Server 2012 R2 está disponível apenas em 64 bits, então cuidado com questões de prova relacionada a 32 bits. Desde que a atualização do servidor local não lhe forneça uma opção para selecionar os componentes ou os dados que precisa migrar, este processo é muitas vezes chamado de *garbage-in* e método de *garbage-out*.

O cenário de migração envolve mais processos do que apenas atualizar o sistema operacional. Ela exige um processo de migração real para todos os recursos existentes no ambiente. Também requer hardware adicional que pode levar a custos mais operacionais e de manutenção durante o período de migração ou coexistência. Se uma empresa pode arcar com o custo do novo hardware, a abordagem de

migração é um método mais seguro e mais limpo do que executar uma atualização *in-loco* (*in-place*).

Imagine que você acabou de receber as mídias de instalação do Windows Server 2012 R2 e, com a empolgação, começa o processo de upgrade ou migração de seu ambiente. Durante o processo, percebe algo interessante e entende que não possui os drivers necessários para deixar tudo funcionando como estava. Ou então, após a atualização, percebe que algumas de suas aplicações não são compatíveis com o Windows Server 2012 R2 e você perderá o dobro do tempo para retornar o ambiente ao devido funcionamento.

Antes de sair atualizando ou migrando seu ambiente plenamente funcional para uma nova versão de sistema operacional, seja em Windows ou qualquer outro sistema operacional, é necessário um pequeno planejamento. Separei seis passos simples para auxiliar com o processo de migração ou atualização de seus servidores.

1. Salve os drivers de armazenamento em massa na mídia removível. Se um fabricante forneceu um driver específico para um dispositivo em seu servidor, salve o driver em um CD, um DVD ou uma unidade flash USB em qualquer diretório raiz da mídia ou a pasta / amd64 . Para fornecer o driver durante a instalação, clique em Carregar Driver ou pressione F6 na página de seleção de disco. Você pode navegar para localizar o driver ou permitir que o programa de configuração procure os meios de comunicação. Isso acontece muito em servidores que usam controladoras HBA para comunicação com storages SAN ou em controladoras de disco que trabalham com RAID direcionado (geralmente, 0/1/5/10).
2. Verifique a compatibilidade de aplicativos e programas. O programa de instalação exibe uma página de relatório de compatibilidade que pode apontar possíveis problemas de

compatibilidade de aplicativos. Em determinado momento, é possível resolver esta questão de atualização com a renovação de versão de suas aplicações, uma versão mais nova de seu sistema de notas fiscais pode resolver o problema de compatibilidade. Crie um inventário de produtos de software instalado no servidor, e verifique nos sites ou suporte dos fabricantes para as respectivas atualizações, disponibilidade de atualizações e anúncios sobre suporte para o Windows Server 2012. Em um ambiente corporativo, você deve testar todos os pedidos de compatibilidade com o Windows Server 2012 antes de executar qualquer atualização do sistema operacional, não importa o que o fabricante diz. Muitas vezes acontece de um determinado fabricante não homologar um sistema operacional em seus produtos, porém isso não significa que ele efetivamente não funcione.

3. Garanta a funcionalidade do servidor. Certifique-se de que o Windows Server 2008 ou Windows Server 2008 R2 está funcionando corretamente no computador antes de iniciar o processo de atualização para o Windows Server 2012 ou 2012 R2. Efetue uma varredura completa de problemas e erros de evento antes de iniciar a transição.
4. Faça um backup completo (incluindo restore em ambiente controlado). Antes de executar qualquer procedimento de atualização, você deve fazer backup de todo o sistema, ou no mínimo os arquivos de dados essenciais. O backup deve incluir todos os dados e informações de configuração que são necessários para o seu servidor de destino funcionar. Quando você executar o backup, certifique-se de incluir as partições de inicialização e de sistema e os dados do estado do sistema. Discos rígidos removíveis podem tornar isso um processo simples, mesmo se não houver um dispositivo de backup adequado no computador. Seu ambiente deve ser totalmente

restaurado caso o processo não funcione.

5. Desative seu software antivírus. Softwares de proteção contra vírus podem tornar a instalação bem mais lenta verificando cada arquivo que for copiado localmente em seu servidor. Se instalado, você deve desabilitar o software antes de executar a atualização.
6. Desligue o dispositivo UPS. Se você tem uma fonte de alimentação ininterrupta (UPS) conectado ao computador de destino, desconecte o cabo de dados antes de realizar a atualização. A instalação tenta detectar automaticamente dispositivos conectados e equipamento UPS podem causar problemas com este processo.

Os requisitos de hardware estão aprimorados

A introdução abordou os requisitos de hardware mínimos para a instalação do Windows Server 2012 R2, porém ao considerar tais requisitos de hardware, lembre-se de que o Windows Server 2012 pode ser implantado virtualmente, exigindo uma nova carga e ou capacidade de seu ambiente dependendo das aplicações que serão implantadas.

O Windows Server 2012 R2 tem suporte nativo ao Hyper-V e em outras plataformas de virtualização que não são da Microsoft, como o VMWare ou o XenServer. As instalações e implantações virtualizadas do Windows Server 2012 R2 precisam corresponder às mesmas especificações de hardware das implantações físicas com as devidas considerações relacionadas a atualizações, serviços em atividade e conexões simultâneas. Por exemplo, ao criar uma máquina virtual para hospedar o Windows Server 2012 R2, você precisa garantir que a máquina virtual seja configurada com uma quantidade suficiente de memória e espaço em disco mínimos para seu funcionamento.

IMPORTANTE

No mundo das máquinas virtuais, a regra de quantidade de memória correspondente ao espaço em disco também deve ser levada em consideração. Se você adicionar a uma VM 16 GB de memória RAM, esse espaço deverá também entrar como excedente no HD em forma de arquivo de paginação, chamado de `pagefile.sys`. Caso você adicione mais memória, aumente também o disco e, se não houver disco disponível, diminua manualmente o tamanho do arquivo de paginação.

1.5 RSAT — KIT DE FERRAMENTAS PARA O DIA A DIA

O RSAT são ferramentas de administração de servidor remoto para Windows 7 com SP1, Windows 8, Windows 8.1 e agora também para Windows 10. Este conjunto de ferramentas permite que administradores de TI gerenciem funções e recursos instalados em computadores remotos que executem Windows Server 2003, Windows Server 2008 R2, Windows Server 2008, Windows Server 2012 ou Windows Server 2012 R2 de um computador. O RSAT foi o sucessor de um conjunto de ferramentas conhecida como Admin Pack, do tempo do Windows XP.

É possível efetuar o download do RSAT pelo Download Center da Microsoft. Deixo aqui disponível o link direto de acesso a esse conteúdo: <http://www.microsoft.com/en-us/download/details.aspx?id=45520>.

Após a instalação do RSAT, será possível abrir o Server Manager do Windows Server 2012 R2 em estações de trabalho. É bom

lembrar de que isso não transforma seu Windows 8.1 em um servidor; o RSAT apenas disponibiliza as ferramentas para que você administre servidores de forma remota sem o consumo de uma sessão TS. A principal desvantagem do uso do RSAT está na velocidade de resposta dos servidores, porém a grande vantagem está relacionada ao não consumo de uma sessão de TS, já que não precisamos usar o `mstsc` para conexão remota.

Antes de iniciar os estudos, recomendo que você instale em sua estação de trabalho o RSAT e já comece a se familiarizar com esta ferramenta. É possível montar os laboratórios e realizar toda a administração de forma centralizada, diretamente pela máquina host de seus laboratórios.

Em um ambiente de produção, o RSAT é utilizado em equipamentos que estejam sendo usados pelos administradores de redes, ou até mesmo pelas equipes de suporte. Uma das grandes vantagens do uso do RSAT pela equipe de *help desk* ou *servisse desk* está no acesso do Active Directory Administrative Center, que permite a localização e renovação de senhas de acesso a usuários sem a necessidade da interação direta com os controladores de domínio. Não é necessário que alguém do suporte acesse remotamente um servidor que controla o domínio para resetar a senha de um usuário da rede.

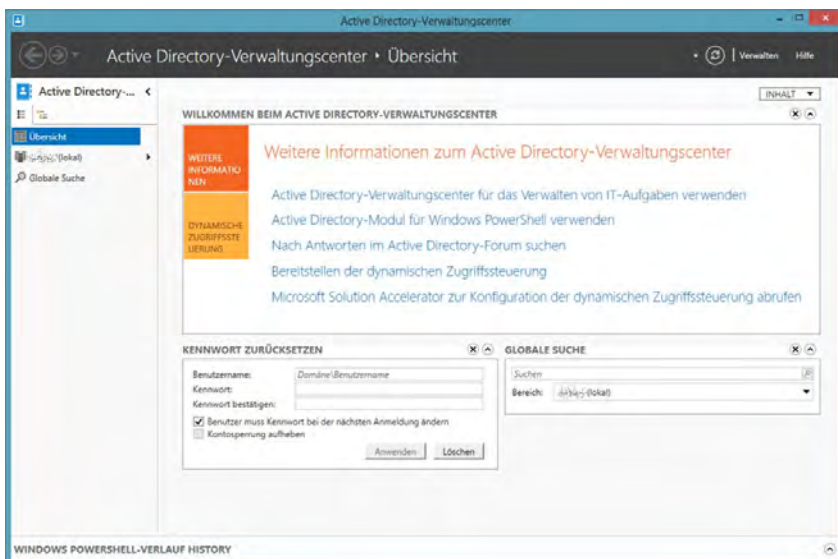


Figura 1.6: Gerenciador do Servidor via RSAT

1.6 MODO DE INSTALAÇÃO SERVER CORE

Muitos servidores em redes corporativas ou Datacenters em uso nos dias de hoje que são dedicados a uma função específica, como servidor web com IIS instalado ou ainda controlador de domínio com o ADDS, não precisam exatamente de seus ambientes gráficos em 100% do tempo. Quando um servidor executa uma única função, não faz sentido manter tantos outros processos em execução.

Eliminar esses processos “extras” permitem o uso mais consciente de processamento e uso da memória RAM, resultando em um melhor desempenho e performance. Muitos administradores de TI, focados em ambiente Microsoft, hoje estão tão acostumados a GUIs que não sabem que já houve outra maneira de operar e administrar o ambiente.

Quando a primeira versão do Windows NT Server apareceu em

1993, muitos reclamaram sobre o desperdício de recursos de servidor em telas gráficas e outros elementos que subentendiam-se desnecessários. Na verdade, muitos servidores não tinham hardware de exibição, contando apenas com ferramentas de administração remota baseadas em texto, como o Telnet. Entretanto, nos dias de hoje, com exigência maior de recursos e operações de processamento, faz-se necessário pensar seriamente na questão da área gráfica.

A próxima figura demonstra a utilização do modo Server Core em uma instalação do Windows Server 2012 R2 Standard:



Windows Server 2012 R2 inclui uma opção de instalação que aborda as queixas mais antigas da época do saudoso Windows NT. Durante a instalação, é possível selecionar a opção Windows Server Core, permitindo uma versão reduzida do sistema operacional ao administrador de redes.

Não há menu Iniciar, nem desktop Explorer, nem o Microsoft Management Console, e praticamente nenhuma aplicação gráfica. Tudo o que você vê quando inicia o computador é uma única janela com um prompt de comando, exigindo habilidade de configuração baseada em linha de comando. Você deverá desenvolver habilidade

para remover e adicionar a área gráfica do Windows Server 2012 R2, pois em muitos casos é comum tal transição em servidores de produção. Muitos administradores convertem a instalação para ambiente gráfico, efetuam as mudanças e novas instalações, e depois retornam para o modo Server Core.

Isso ocorre quando o administrador não tem habilidade com linha de comando e PowerShell. A instalação em modo Server Core remove a interface gráfica comumente chamada de GUI, e sua característica foi pensada com foco em segurança e desempenho dos servidores sendo uma opção de instalação mínima do servidor para computadores que executam o sistema operacional Windows Server 2008, Windows Server 2012 e Windows Server 2012 R2. O modo de instalação Server Core fornece um ambiente de servidor com baixa manutenção e funcionalidade limitada.

A grande vantagem notada pela instalação Server Core é a diminuição da quantidade de reinicializações após atualizações, conforme demonstrado aqui pela tabela a seguir. A tabela mostra quantos meses um computador com Windows Server Core ficou online sem a necessidade de reinicialização.

	Windows Server 2012 Server Core		Windows Server 2008 R2 Server Core	
	Redução	Critical Apenas	Redução	Critical Apenas
Todas as atualizações				
Server com todas as Roles	42%	56%	37%	49%
Meses sem reiniciar	13	19	10	13
Sem o AD, DNS,Print and Media Services, Telnet, .Net, Clustering, Hyper-V, IIS, ou WINS	53%	63%	51%	62%
Meses sem reiniciar	15	21	10	13
Somente atualizações necessárias				
Server com todas as Roles	48%	67%	40%	49%
Meses sem reiniciar	16	26	10	13
Sem o AD, DNS,Print and Media Services, Telnet, .Net, Clustering, Hyper-V, IIS, ou WINS	60%	71%	54%	65%
Meses sem reiniciar	19	28	10	13

Quando a Microsoft introduziu a opção de instalação em modo Server Core no Windows Server 2008, era uma ideia intrigante e, de certa forma, inovadora que quebrava o paradigma do analista Windows não fazer uso de linhas de comando. Poucos

administradores aproveitaram-se desse “novo” recurso na época. Porém, com a crescente preocupação em segurança e redução de custo direcionada ao uso do hardware, as instalações em modo Server Core ganham força.

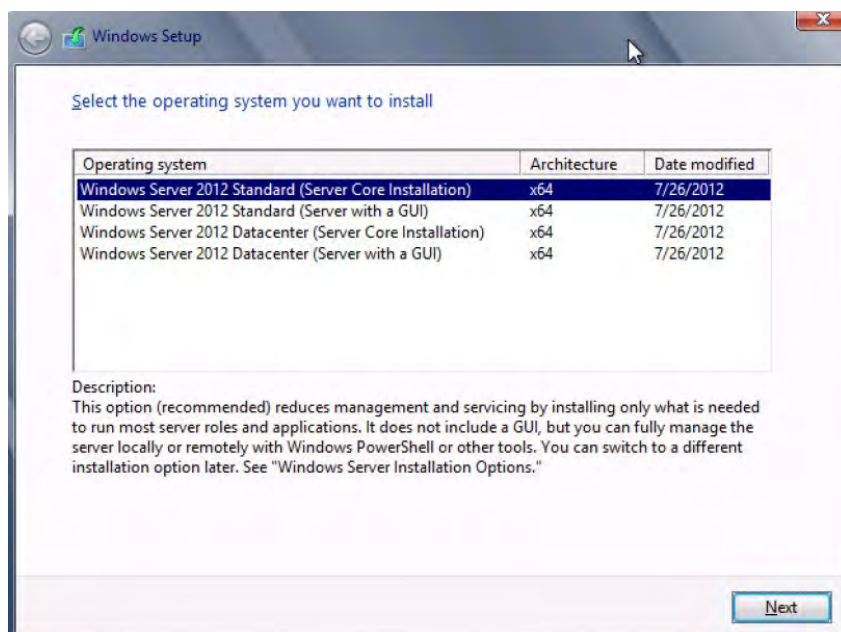
A principal razão para a não adesão do Server Core inicialmente no Windows Server 2008 foi de que a maioria dos administradores de servidores não estava suficientemente familiarizada com a interface de linha de comando para gerenciar um servidor Windows sem uma GUI, além de que, uma vez feito, não poderia ser desfeito. No Windows Server 2008 e Windows Server 2008 R2, a decisão de instalar o sistema operacional usando a opção Server Core era irrevogável.

Uma vez que você instalava o sistema operacional usando o Server Core, não havia nenhuma maneira de obter o GUI de volta, exceto para realizar uma reinstalação completa. Tudo isso mudou no Windows Server 2012. Agora você pode alternar de um servidor a partir da opção Server Core para o servidor com a opção de GUI e de volta à vontade, usando os comandos `WindowsPowerShell` .

Durante a instalação do Windows Server 2012 e Windows Server 2012 R2, o programa copia os arquivos de configuração para todos os componentes do sistema operacional a partir da mídia de instalação para um diretório chamado `winSxS` . Isso permite que os administradores ativem qualquer um dos recursos incluídos no Windows Server 2012 sem ter de fornecer um meio de instalação como mídias, arquivos ISOs etc. Na verdade, este processo é exatamente o que fazíamos de modo manual com o Windows Server 2003 e sua pasta `I386`, só que agora automatizado durante a instalação do Windows Server 2012 R2.

Em uma instalação em modo Server Core, a pasta `winSxS` não recebe todos os componentes, portanto, precisa do uso da ferramenta `Dism` para montar imagens de extensão `.WIM` para

fornecimento de ferramentas e itens de configuração. A prova 70-410 cobrará de você o conhecimento desta ferramenta de linha de comando, assim, pratique os laboratórios relacionados a ela.



A desvantagem desta disposição é que o diretório `WinSxS` ocupa uma quantidade significativa de espaço de disco, que em muitos casos está dedicado a dados que nunca serão usados. Contudo, recomendo sua prática como forma de facilidade para instalações futuras.

Com o uso crescente de máquinas virtuais para distribuir as funções de servidor, redes corporativas muitas vezes têm mais cópias do sistema operacional do servidor do que nunca, logo, mais espaço em disco desperdiçado. Além disso, as tecnologias avançadas de armazenamento, muitas vezes usadas por infraestruturas de servidores de hoje, tais como redes de área de armazenamento (SANs) e drivers de estado sólido (SSDs), estão fazendo com que o

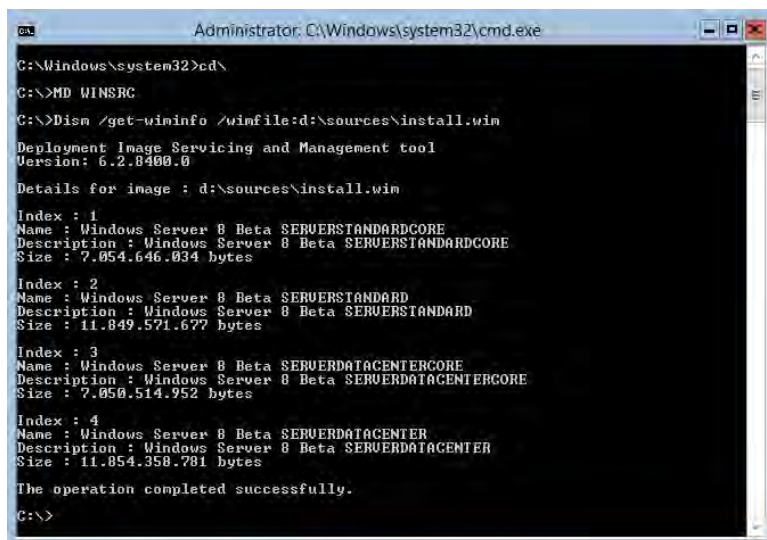
espaço em disco seja mais caro. Recomendo o uso sob demanda do Windows Server 2012 R2 se seu problema estiver intimamente ligado a espaço em disco.

A utilização de recursos sob demanda é extremamente útil quando aplicado em máquinas virtuais com funções específicas, e pode ser um grande aliado em ambientes de alto custo alocados em tecnologia baseada em *storages* ou tierização.

Guarde bem a importância e as características da pasta `winSxS`, pois existe uma boa chance de ser objeto de questão de prova.

Instalando a interface gráfica em uma instalação Server Core:

1. Crie uma pasta para montarmos um arquivo WIM;
2. Coloque uma mídia ou ISO do Windows Server 2012 R2 para acessarmos o arquivo WIM;
3. Use o comando `Dism` para subir o arquivo WIN: `Dism /get-wiminfo /wimfile:<drive>:sources\install.wim`



```
Administrator: C:\Windows\system32\cmd.exe

C:\Windows\system32>cd\
C:\>MD WINSRC
C:\>Dism /get-wiminfo /wimfile:d:\sources\install.wim

Deployment Image Servicing and Management tool
Version: 6.2.8400.0

Details for image : d:\sources\install.wim

Index : 1
Name : Windows Server 8 Beta SERVERSTANDARDCORE
Description : Windows Server 8 Beta SERVERSTANDARDCORE
Size : 7.054.646.034 bytes

Index : 2
Name : Windows Server 8 Beta SERVERSTANDARD
Description : Windows Server 8 Beta SERVERSTANDARD
Size : 11.849.571.677 bytes

Index : 3
Name : Windows Server 8 Beta SERVERDATACENTERCORE
Description : Windows Server 8 Beta SERVERDATACENTERCORE
Size : 7.050.514.952 bytes

Index : 4
Name : Windows Server 8 Beta SERVERDATACENTER
Description : Windows Server 8 Beta SERVERDATACENTER
Size : 11.854.358.781 bytes

The operation completed successfully.

C:\>
```

4. Monte a imagem WIM conforme o exemplo do comando
`Dism : Dism /mount-wim /WimFile:
<drive>:\sources\install.wim /Index:<Index>
/MountDir:c:\WINSRC /readonly`
5. Após a montagem do arquivo WIM, abra o Power Shell e use o comando a seguir: `Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart -Source c:\WINSRC\windows\winsxs`
6. Caso você possua acesso à internet no momento da instalação, é possível utilizar o Windows Update em vez de apontar a origem dos binários: `Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart`

A pasta WinSxS

Esta pasta fica dentro do diretório de instalação do Windows Server 2012 R2 `C:\Windows\winsxs`, e também pode ser identificada como “Windows Side By Side”. Este diretório em

especial serve unicamente para armazenar as versões de arquivos que mantêm a compatibilidades de vários programas. A palavra que mais se adequa a este diretório seria repositório.

Tanto o Windows Server 2008 quanto as versões superiores, como o Windows Server 2012 R2, reduzem automaticamente o tamanho do `winSxS` usando métodos parecidos, que incluem processos internos, como desinstalação e exclusão de pacotes com componentes que foram substituídos por outros com versões mais novas. As versões anteriores de alguns componentes são mantidas no sistema por um tempo, permitindo a reversão, se necessário. Depois de certo período, esses componentes são removidos da instalação. É exatamente por esse motivo que a remoção ou compactação forçada não são recomendadas, porém sendo perfeitamente possível.

O repositório de componentes do Windows foi introduzido pela primeira vez no Windows XP para dar suporte aos códigos *assemblies* lado a lado. A partir do Windows Vista, foi aprimorado para acompanhar e fazer a manutenção de todos os componentes que formam o sistema operacional como um todo. Esses diferentes componentes do sistema operacional acompanham objetos, como arquivos, diretórios, chaves do registro e serviços e, em versões específicas de componentes, são reunidos em pacotes.

Esses pacotes são usados pelo Windows Update e ferramenta de linha de comando `DISM` para atualizar o Windows e seus componentes. Os componentes e pacotes usados em uma instalação do Windows são processados pelo repositório de componentes do Windows.

Determinar o tamanho do repositório é complicado pelo fato de que muitos dos arquivos são usados pelo Windows de diretórios de fora do repositório de componentes, usando uma técnica conhecida como link físico. Nesses casos, os arquivos de uma versão do

componente aparecem dentro e fora do dele. Usando o link físico, o Windows pode parecer manter várias cópias do mesmo arquivo, sem realmente ocupar o espaço adicional para várias cópias.

Use o seguinte código para analisar o tamanho do repositório de componentes WinSxS : `Dism.exe /Online /Cleanup-Image /AnalyzeComponentStore` .

A opção `/AnalyzeComponentStore` não é reconhecida no Windows 8 e versões anteriores.

```
C:\>dism /online /cleanup-image /analyzecomponentstore

Deployment Image Servicing and Management tool
Version: 6.3.XXXX.0

Image Version: 6.3.XXXX.0

[=====100.0%=====]

Component Store (WinSxS) information:

Windows Explorer Reported Size of Component Store : 4.98 GB

Actual Size of Component Store : 4.88 GB

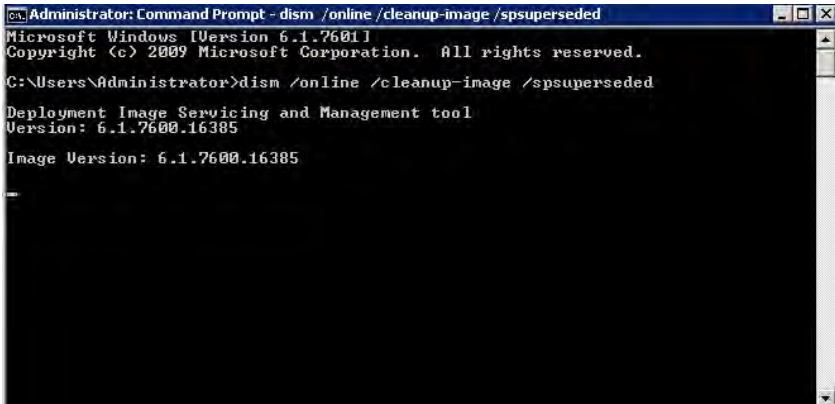
    Shared with Windows : 4.38 GB
    Backups and Disabled Features : 506.90 MB
    Cache and Temporary Data : 279.52 KB

Date of Last Cleanup : 2013-06-10 23:32:22

Number of Reclaimable Packages : 0
Component Store Cleanup Recommended : No

The operation completed successfully.
```

Para efetuar a limpeza dos dados do repositório WinSxS , pode-se usar o seguinte comando: `dism /online /cleanup-image /spsuperseded` . Após o uso do comando, será iniciado o processo de limpeza do repositório, como demonstrado pela próxima figura.



```
Administrator: Command Prompt - dism /online /cleanup-image /spsuperseded
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dism /online /cleanup-image /spsuperseded

Deployment Image Servicing and Management tool
Version: 6.1.7600.16385

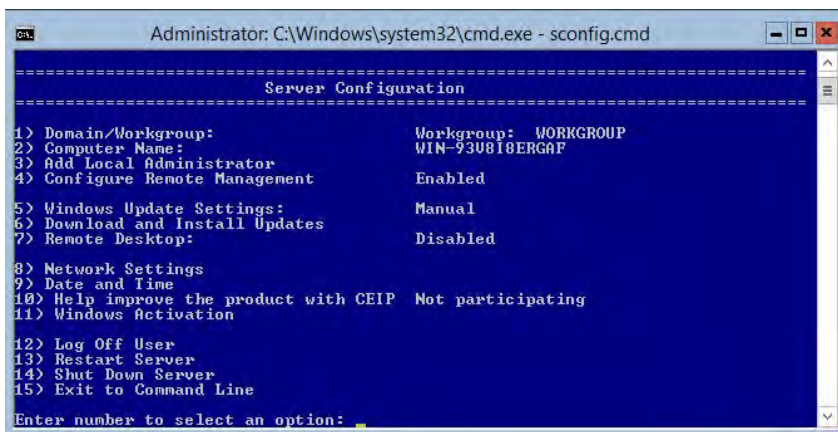
Image Version: 6.1.7600.16385

-
```

1.7 ACIONANDO O SCONFIG

Não tenho como negar: a utilização do Server Configuration (`sconfig`) é realmente muito interessante, em se tratando de configurações iniciais de um servidor em modo de instalação Server Core. No mundo real, este menu de letras brancas e fundo azul pode ser utilizado também para configurações iniciais de servidores com o Hyper-V Server 2012 R2, que não possui interface gráfica nativa.

O `sconfig` não é uma novidade e se fez presente desde o lançamento do Windows server 2008. A próxima figura demonstra o formato dessa janela de configurações.



O `sconfig` possui extensão `.cmd`, portanto trata-se de uma ferramenta de comando (*command*). Ele permite que o administrador de redes configure itens essenciais ao funcionamento do servidor em ambiente de rede e administração remota, como por exemplo, o item 7 (Remote Desktop) ou ainda atividades mais simples como o boot de um servidor.

Sua interface é bem simples e objetiva. O `sconfig` é, sem sombra de dúvidas, muito útil em situações nas quais o servidor não pode ser convertido para modo gráfico, como no caso do Hyper-V Server 2012 R2 e Windows Server 2008 R2.

1.8 MINIMAL SERVER INTERFACE

Você pode ser cobrado durante a prova pelo modo de instalação mínima de interface, conhecido também pelos especialistas Microsoft como Mini Server ou Minimal Server Interface. Este tipo de instalação fornece a interface gráfica de modo reduzido, apresentando acesso apenas ao Gerenciador do Servidor, ao prompt de comando e ao PowerShell.

Este recurso auxilia também com a segurança e desempenho do

servidor, mantendo algumas telas gráficas em especial, sendo um “meio termo” para a administração. Você pode ser cobrado com a prova 70-410 pela existência do Mini Server, e muito provavelmente será cobrado pelos comandos de transição do modo gráfico para o modo Server Core. A instalação Minimal Server permite acesso ao MMC (Microsoft Management Console), o Server Manager e alguns itens do Painel de Controle.

Para remover a interface do usuário, pode-se utilizar o Power Shell da seguinte forma: `Uninstall-WindowsFeature Server-Gui-Mgmt-Infra -restart .`



Quando efetuamos a remoção da interface gráfica, o Windows não aplica de imediato a configuração. Será necessário reiniciar o servidor e aguardar até que todas as diretrizes de funcionamento sejam aplicadas. A próxima figura demonstra bem esta atividade.

Em nosso treinamento EAD, temos vídeos passo a passo do processo, incluindo mensagens de erro que podem ser extremamente úteis com o processo de configuração da interface gráfica.



É sempre bom lembrar de que todas as versões anteriores do Windows Server 2012 e Windows Server 2012 R2, que oferecem suporte a remoção da interface gráfica, não permitem o processo reverso. Ou seja, uma vez convertido, não é possível desfazer o processo.

Caso você precise converter a instalação Server Core de um servidor com o Windows Server 2008 R2 para interface gráfica, será necessário primeiro efetuar o Upgrade para o 2012 ou 2012 R2, e então instalar a interface gráfica. É um processo demorado que exige uma janela de manutenção e, pelo menos, um backup confiável.

INTRODUÇÃO AO ACTIVE DIRECTORY (ADDS)

2.1 SUBINDO O AMBIENTE

Posso afirmar aqui que o conceito sobre a administração de servidores é extremamente amplo e precisa ser estudado a fundo, considerando-se o tamanho atual da empresa, seu parque atual de máquinas, seu tamanho atual em usuários e seu crescimento médio ao longo do tempo. Todos os planos para aquisição de novas tecnologias devem ser considerados para melhor aproveitamento do orçamento técnico.

Outro ponto importante a ser considerado para provas Microsoft é a necessidade de “subirmos o ambiente” do zero, ou seja, criar um ambiente limpo e sem problemas relacionados ao cotidiano — como instalações malfeitas, ação de vírus e usuários mal-intencionados e problemas de hardware em geral. Subir um ambiente do zero é começar a elaboração da estrutura de forma a facilitar o trabalho dentro do ambiente. É raro o momento em que você fará a subida do ambiente do zero, pois, geralmente, quando é contratado, o administrador de redes fará manutenção em algo que já está em produção. Lembre-se de que tudo o que fizermos em laboratório funciona sem problemas, mas no mundo real você pode se deparar com situações mais complexas que exijam mais estudo e dedicação.

A administração de servidores pode exigir um único administrador de redes ou uma equipe de administradores de redes. Tudo dependerá de sua organização e crescimento. Se a organização dos servidores que controlam o domínio for bem feita, os servidores de atualizações estiverem no lugar correto, e os servidores de DNS forem bem configurados, a administração do ambiente Microsoft será uma experiência simples e duradoura.

Neste capítulo, falaremos do conceito relacionado ao Active Directory Domain Services (ADDS) e sua estrutura funcional básica. Essa etapa permitirá não só o conhecimento para atender a prova, mas também o necessário para atuar em ambientes funcionais.

Para subir um ambiente baseado em um controlador de domínio do zero, é interessante saber que são necessários certos requisitos mínimos. Lembre-se de que será necessário que pelo menos um de seus servidores seja um servidor de DNS. Caso sua rede não possua nenhum DNS ativo, durante a instalação do controlador de domínio ele será automaticamente promovido também como servidor de DNS.

Para subir o ambiente, é necessário conhecer antes os atalhos e painéis relacionados ao funcionamento do Windows Server 2012 R2, cuja estrutura gráfica é bem similar ao Windows 8.1, incluindo a ausência do menu iniciar como era conhecido em seus antecessores. Acredito que para quem vê pela primeira vez o Windows Server 2012 R2, não há muita dificuldade. Porém para quem já atua com o Windows Server 2008 ou um de seus antecessores, é possível estranhar muito essa nova aparência. A navegabilidade não cai em provas do MCSA, mas ajudará muito em relação ao uso e facilidades com o Windows Server 2012 R2.

Novo ambiente

Ao final da instalação do Windows Server 2012 R2, é criado automaticamente um usuário chamado Administrador (*Administrator*, em inglês, se a mídia possuir esse idioma como padrão). Aqui as instalações mantêm o mesmo padrão de seu antecessor, o Windows Server 2008 e Windows Server 2003.

Nas versões anteriores ao Windows Server 2008 R2, você definia a senha da conta Administrador, durante o processo de instalação. Já no Windows Server 2012 R2, a senha da conta Administrador é definida após a instalação, durante o primeiro login. No Windows Server 2012 R2, o padrão de segurança de senha é exigido já no momento da criação do usuário Administrador.



A imagem mostra a tela de configuração do Windows Server 2012 R2 durante a criação da conta Administrador. O título da janela é "Configurações". Abaixo do título, há uma instrução: "Digite uma senha para a conta de administrador interna que você pode usar para entrar no computador." Existem três campos de entrada: "Nome do usuário" com o texto "Administrador" preenchido, "Senha" (campo vazio) e "Reinsirir senha" (campo vazio).

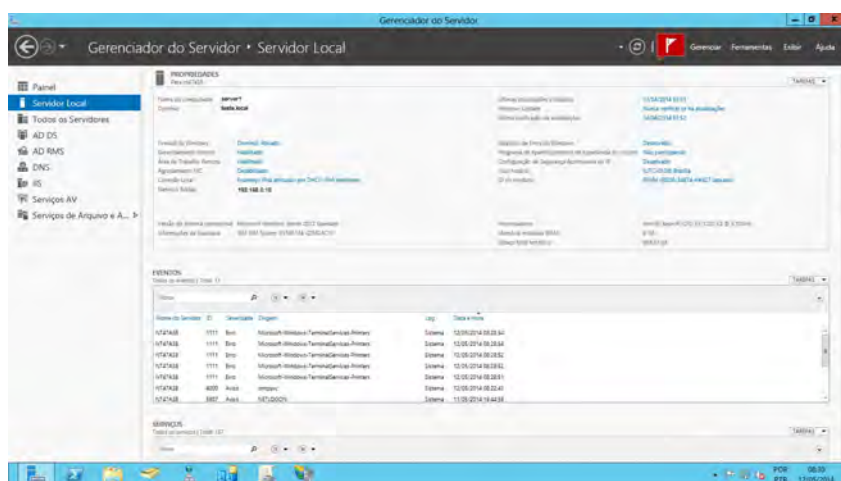
O Windows Server 2012 R2 mantém um ambiente personalizado para cada usuário. Por exemplo, se o usuário Administrador faz o login, altera algumas configurações do Windows e cria alguns atalhos na sua Área de trabalho. Estas alterações somente estarão disponíveis para o usuário Administrador e não estarão disponíveis para outros usuários que façam o login. Com isso, é possível manter um ambiente personalizado, onde cada usuário cria os seus próprios ícones e atalhos, e define as configurações que julgar mais adequadas para o seu trabalho diário.

2.2 GERENCIADOR DO SERVIDOR

Neste ponto, os administradores mais antigos sentem a mudança para o Windows Server 2012 R2, pois o gerenciador do servidor (*server manager*) teve uma mudança brusca de formato e design, porém, ao meu ver, está mais funcional e eficaz. Tudo dependerá do uso e de costume.

As tarefas de configurações iniciais estão mais simples e fáceis de visualizar, além de que é possível gerenciar serviços e servidores remotamente. Se seu objetivo é certificação, será obrigatório saber todos os novos caminhos. Entretanto, se seu objetivo é apenas o conhecimento aleatório, existem formas de acessar ferramentas já conhecidas através do painel de controle. Como nosso foco principal é o de passar nas provas, mantendo um conhecimento aplicado de qualidade, faremos a passagem por toda a nova interface.

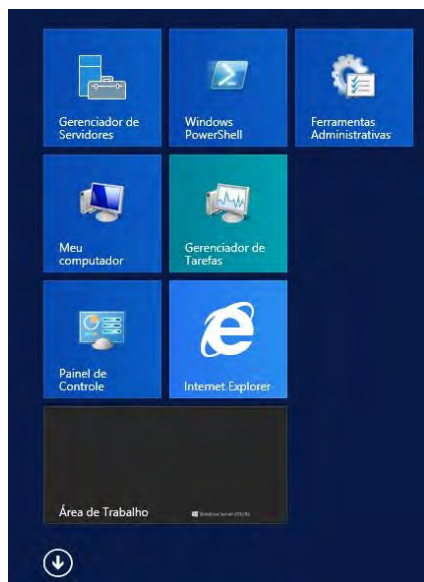
É possível gerenciar diversos servidores por meio de um único painel centralizado através de grupos de servidores. Os agrupamentos podem ser montados de forma simples e rápida, conforme veremos no decorrer deste livro.



Caso você feche o gerenciador do servidor, será possível retornar a ele pelo segundo ícone da esquerda para direita, na barra de ferramentas. Este ícone se parece com uma maleta e uma caixa azul, que representa um servidor com ferramentas administrativas:

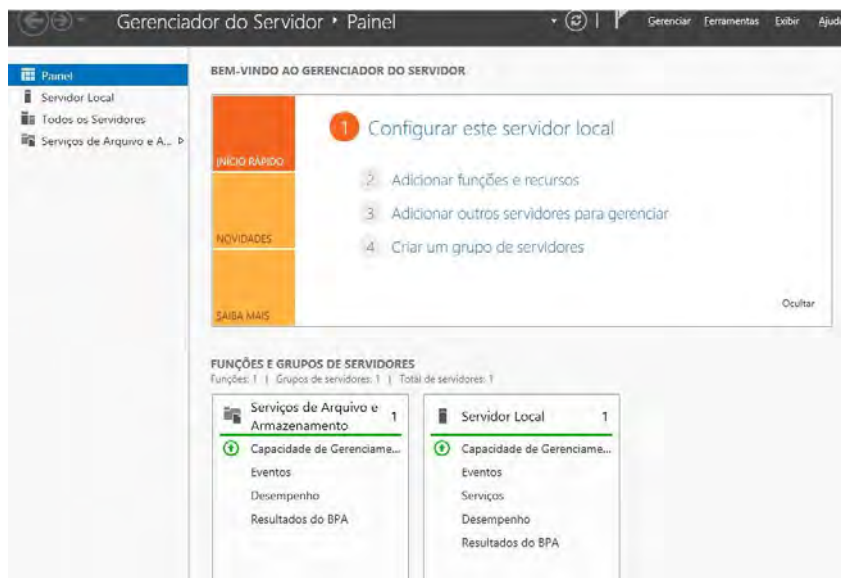


Se esse ícone for excluído, ainda é possível acionar o Gerenciador do servidor por meio da tela inicial, ou digitando `ServerManager.exe` através do executar (teclas de atalho `Winkey + R`). É importante lembrar de que este recurso está armazenado em `%systemroot%\system32\`, e pode ser necessário na prova 70-410 direcionar sua localização. Outra tecla de atalho de extrema utilidade é o `Winkey + X`, que abre um pequeno menu no canto esquerdo inferior da área de trabalho.

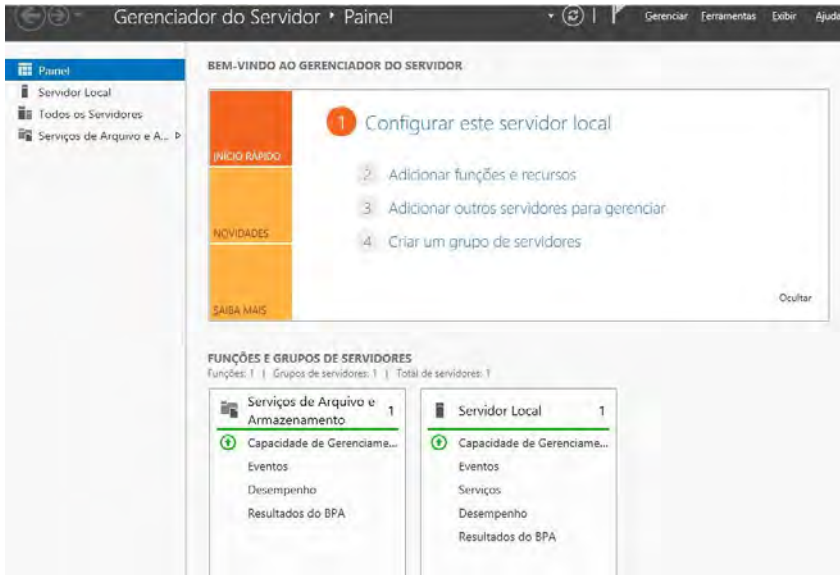


Esta mudança foi a mais interessante no ponto de vista deste autor, quando comparado a seu antecessor, o Windows Server 2008

e 2008 R2. O que antes era apenas um painel de controle de instalações, por assim dizer, agora se torna um painel mais robusto e recheado de novos recursos de gerenciamento.



Precisamos entender muito bem cada parte do gerenciador que será cobrado na prova 70-410, a fim de deixar claro como a remodelagem desta ferramenta deixou a vida dos administradores Microsoft mais fácil e interessante (sim, você precisará se adaptar). Logo no centro da tela, temos a informação de bem-vindo, onde encontraremos quatro passos básicos de configuração para o painel.



2.3 CONFIGURAR O SERVIDOR LOCAL

Permite-nos configurar o nome do servidor, colocar um IP, domínio, placas de rede, entre outras coisas de nosso cotidiano administrativo relacionadas ao servidor local. Demonstrarei cada uma das possibilidades logo nas próximas páginas.

Adicionar funções e recursos

É por aqui que faremos a adição de praticamente todos os recursos e funções de nosso servidor, como por exemplo, o WSUS para gerenciamento de atualizações ou o servidor de VPN.

Adicionar outros servidores para gerenciar: é aqui que a novidade mais interessante aparece, permitindo que eu gerencie outros servidores pelo mesmo painel de gerenciamento. Posso administrar servidores remotamente sem precisar acessá-los através de um console remoto. Sim, posso fazer instalação e remoção de funções e recursos em servidores que estejam em minha rede sem

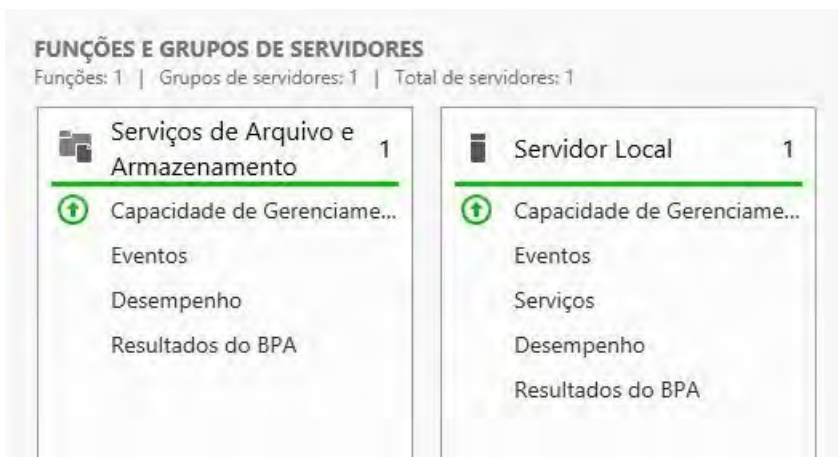
acessá-los pelo terminal. Posso gerenciar todo o meu parque de servidores por meio deste painel.

O Dotnet Framework 3.5 não deve ser baixado da internet, pois agora é uma feature (recurso) do próprio Windows Server 2012 e 2012 R2. Para efetuar sua instalação, é necessário fazê-lo por meio do Server Manager.

Criar um grupo de servidores

É possível criar um grupo de servidores com características específicas para facilitar o gerenciamento. Por exemplo, posso criar um grupo chamado de servidores ADDS, e ali adicionar todos os servidores que sejam controladores de domínio. Isso me permite instalar recursos e gerenciar uma gama maior de servidores de forma mais organizada e assertiva.

Funções e Grupos de Servidores nos permitem identificar detalhes importantes do dia a dia, como por exemplo, se um serviço específico está fora de operação, ou ainda medir o desempenho de um serviço relacionado a um servidor de nossa infraestrutura.



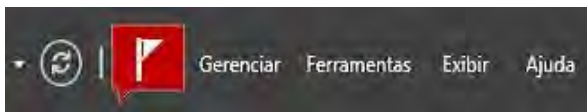
Teremos respectivamente quatro itens marcados para cada serviço ou atividade desempenhada pelo servidor:

- Capacidade de gerenciamento;
- Eventos;
- Desempenho;
- Resultado do BPA.

A área de gerenciamento específico permite escolher uma ação para um grupo de servidores ou ainda para configuração do servidor local com Windows Server 2012 R2. Esta tela ganha mais itens conforme criamos os grupos para gerenciamento.



A barra superior do Gerenciador do Servidor está muito parecida com a de um navegador Web, como o Internet Explorer, por exemplo. Do lado direito dessa barra, é possível encontrar alguns menus que permitem gerenciar o servidor, instalar funções e recursos e ainda acionar a ajuda do Windows. Do lado esquerdo, temos a opção de navegar pelas janelas anteriores já acessadas, bem como fazemos hoje no Internet Explorer quando precisamos volta para uma página visitada recentemente. Ainda na barra de configuração, é possível identificar um ícone parecido com uma bandeirola:

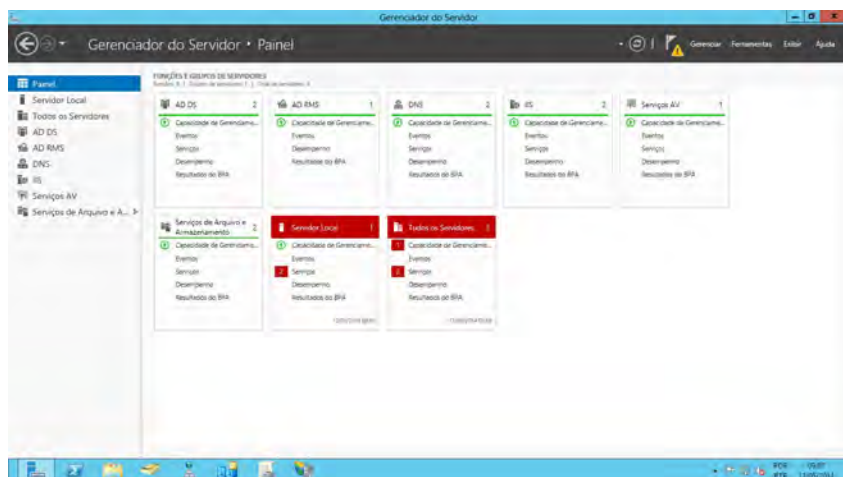


Neste ícone, temos alertas sobre tarefas administrativas pendentes que surgem após a instalação de alguma função ou recurso. Por exemplo, você pode instalar o recurso de ADDS, mas não promover o servidor a controlador de domínio. Isso gera um alerta dizendo que o recurso está instalado e pronto para uso, porém ainda não foi devidamente configurado.

Este ícone carrega você para o console Tarefas de Configurações Iniciais que lhe permite efetuar uma série de configurações, as quais normalmente são feitas logo após a instalação do Windows Server 2012 R2. A ideia deste console é fornecer, em um só local, todos os pré-requisitos para a funcionalidade básica das funções e recursos do Windows.

Através desse console, que será aberto automaticamente logo após o primeiro login ao fim da instalação do Windows Server 2012 R2, você pode configurar o fuso horário, a placa de rede, o agrupamento NIC Team, o nome do servidor, ingressar o servidor em um domínio, configurar opções das atualizações automáticas, habilitar a área de trabalho remota e configurar o Firewall do Windows. Esse console continuará sendo aberto todas as vezes que o servidor for reiniciado. É possível acessar esta janela clicando na tecla Winkey do teclado.

Este console permite a visualização das funções instaladas atualmente no servidor local, ou qualquer servidor remoto para o qual o administrador tenha acesso. Ele também permite a visualização não só das roles e features, mas também de eventos que possam surgir e representar potenciais problemas no servidor.



Uma grande novidade deste painel é a possibilidade de administrar servidores remotamente também com a instalação de funções e recursos, o que não era possível no Windows Server 2008 R2. Agora, é possível criar um grupo de servidores e, por meio dele, instalar e remover funções e recursos simplesmente clicando com o

botão direito no grupo e adicionando as funções desejadas.

Logicamente, existem algumas configurações específicas para este ponto quando tentarmos adicionar um servidor com Windows Server 2008 R2 para ser gerenciado através do painel do Windows Server 2012, mas é possível, sim, este formato de gerenciamento unificado.

DICA

Para este painel ficar disponível em um computador com o Windows 8 ou 8.1, basta instalar a ferramenta RSAT da própria Microsoft. Para quem já conhece o bom e velho Windows Server 2003, esta ferramenta seria um adminpack remodelado (opinião do autor). A Ferramenta RSAT contém uma série de consoles de administração para servidores Windows Server 2012 R2. Mais detalhes em: <https://www.microsoft.com/pt-br/download/details.aspx?id=28972>.

Teclas de atalho

Toda a interface gráfica sofreu mudança, e isso implica em uma adaptação do público técnico que fará a administração do servidor. É realmente interessante conhecer as teclas de atalho do Windows Server 2012 e 2012 R2 para facilitar sua vida no quesito de administração e mobilidade pelo sistema.

Separamos algumas teclas de atalho que farão grande diferença com o acesso a recursos já conhecidos. Elas não serão cobradas nas provas do MCSA para o Windows Server 2012 R2, porém podem aparecer nas provas do MCSA do Windows 8 e 8.1. Veja a lista a seguir com as teclas de atalho, sua função e uma observação,

respectivamente.

- Winkey + I — Barra de configurações: acesso mais rápido para desligar e reiniciar o servidor, além de nos levar ao painel de controle com grande agilidade.
- Winkey + C — Barra charmosa: a charm bar (barra charmosa) aparece todas as vezes que levamos o ponteiro do mouse no canto direito inferior da tela e permitimos acesso desde configurações até pesquisa de arquivos e programas.
- Winkey + Q — Pesquisa de aplicativos: localiza programas instalados em um servidor.
- Winkey + W — Pesquisa de configurações: localiza uma configuração específica efetuada.
- Winkey + F — Pesquisa de arquivos: localiza arquivos armazenados em unidade física ou lógica que esteja diretamente tachada a um servidor.
- Winkey + E — Windows Explorer: acessa de forma simples o Windows Explorer para localização e gestão de unidades lógicas (discos, pendrives, unidades de armazenamento em geral).
- Winkey + R — Executar: permite a execução de programas através do acesso a seus executáveis. Esta tecla está presente em diversas versões e edições do Windows, e já é uma velha conhecida.
- Winkey + P — Segundo monitor: acessa o compartilhamento de monitores em forma de segundo monitor ou de compartilhamento de tela.
- Winkey + X — Menu de acesso rápido: este menu possui diversas opções rápidas a elementos de configuração e verificação de logs do servidor local. Entre as opções, o que identifico como ponto de atenção são o acesso ao prompt em modo de

administração e o visualizador de eventos, porém existem diversas ferramentas disponíveis.

- Winkey + D — Desktop: quando pressionada, tudo o que estiver aberto será minimizado para a barra de tarefas deixando o desktop à mostra.
- Winkey + L — Bloqueia a máquina: bloqueia o servidor ou estação de trabalho sem a necessidade de passagem pelas clássicas telas do *CTRL+ALT+DEL*.
- Winkey + U — Central de facilidade de acesso: utilizado para acesso rápido a área de ferramentas de acessibilidade. Nesta tela temos ferramentas como o narrador, lupa, teclado virtual e alto contraste. Muito útil para administradores com características especiais, como um problema de visão, por exemplo.
- CTRL + Esc — Tela iniciar: tela de início do sistema com programas, recursos e ferramentas.
- Winkey + 1 — Programas da barra de tarefas: você pode usar a sequência de programas da barra de tarefas, sendo 1 para o primeiro programa, 2 para o segundo e assim sucessivamente. Em nosso caso, o gerenciador do servidor é nosso primeiro ícone, então, no primeiro momento, o *Winkey + 1* abrirá essa ferramenta. Se você mudar o programa, também muda a ação do atalho.
- CTRL + SHIFT + Esc — Gerenciador de tarefas: gerenciador de tarefas em execução do sistema operacional. Permite a verificação de recursos atualmente em atividade, consumo de memória, disco, processamento e rede. Muito mais completa e útil que sua antecessora.

2.4 INTRODUÇÃO AO ACTIVE DIRECTORY DOMAIN SERVICES (ADDS)

O Active Directory da Microsoft nasceu da necessidade de se ter um único local para armazenamento de objetos para compor uma estrutura de rede. Ele nasceu para cuidar da organização de usuários, impressoras, servidores e demais recursos comuns em uma estrutura de TI de uma empresa, seja ela de pequeno, médio ou grande porte.

A grande vantagem vislumbrada pelos administradores de redes é a unificação dos acessos através de um único usuário e senha. Um passo importante para controle de acesso a recursos e facilidade aos usuários, afinal, ninguém merece a árdua tarefa de decorar inúmeras senhas que mudam de tempos em tempos. Você fará os passos para instalação e configuração do ADDS nos laboratórios deste capítulo.

O AD foi implementado pelo Microsoft Windows 2000 Server em relação ao Windows NT Server 4.0 e, até hoje, é carro chefe da Microsoft quando pensamos em servidores. Todos os recursos que exigem ou necessitam de autenticação não funcionariam. Ou seja, podemos entender que, sem ele, quase todas as aplicações que possuem regras e políticas não funcionariam como se deve.

Imagine um Proxy que libere ou bloqueie conexões com a internet baseado em autenticação de usuário, liberando acesso para o usuário A e bloqueando do usuário B. Sem o controlador de domínio e o Active Directory, não seria possível identificar tais regras.

No Windows Server 2012 e 2012 R2, o Active Directory (ADDS) também é o elemento fundamental, sobre o qual é planejada e implementada toda a infraestrutura e os serviços de uma rede baseada no Windows Server 2012 R2. O grande concorrente da Microsoft nos tempos de nascimento do Windows NT já possuía algo parecido e bem estruturado com o atual Active Directory. A antiga Rede Novell também possui uma estrutura similar e bem

organizada, porém com a evolução tecnológica e o aprimoramento da estrutura de diretórios pelo Windows. Poucas empresas hoje ainda possuem a rede Novell em operação.

O ADDS nada mais é que um banco de dados que armazena todos os objetos de uma rede baseada em controladores de domínio. O Active Directory é armazenado em um arquivo chamado de `Ntds.dit` (guarde bem esse arquivo, pois será cobrado tanto na prova 70-410 como na 70-411), que está presente em dois locais diferentes dentro do controlador de domínio.

- `%SystemRoot%\NTDS\Ntds.dit`
- `%SystemRoot%\System32\Ntds.dit`

A cópia do `Ntds.dit`, que fica dentro da `System32`, só é usada quando você pretende adicionar um servidor com Windows Server 2012 R2 em um domínio com servidor Windows, onde a estrutura organizacional ainda está como Windows 2000. A disponibilidade deste arquivo permite que você execute o Assistente de Instalação do Active Directory (`Dcpromo.exe`) sem ter de usar o CD do sistema operacional Windows 2000 Server. Durante o processo de promoção, `Ntds.dit` é copiado do diretório `%SystemRoot%\System32` para o diretório `%SystemRoot%\NTDS`.

Falando de provas Microsoft, é possível que seja cobrado o conhecimento de ambos os lugares onde encontrar o `Ntds.dit`. É importante lembrar de que muitas empresas ainda possuem servidores legado Windows 2000 em operação e pretendem fazer sua migração para o Windows 2012 R2, gerando uma alta demanda pelo conhecimento específico. É possível mover o `Ntds.dit` através de um processo trabalhoso e arriscado que não será cobrado a primeiro momento pela prova 70-410, porém deve ser de seu conhecimento para a prova 70-412.

O Active Directory possui os seguintes elementos em sua estrutura lógica:

- Domínios
- Árvores
- Florestas
- Relações de confiança
- Objetos do Active Directory
- Unidades organizacionais
- Schema
- Sites

2.5 IMPLEMENTANDO CONTROLADORES DE DOMÍNIO NO WINDOWS SERVER 2012 R2

Para implementar um controlador de domínio, é necessário apenas seguir o assistente e efetuar a instalação. Contudo, é sempre recomendável utilizar boas práticas e ficar atento a alguns detalhes que pretendo discutir ainda neste capítulo. Quanto aos passos, fique tranquilo que o laboratório coloca todos os itens de forma simples e eficiente.

Um controlador de domínio é um repositório central que armazenará todos os objetos de uma rede, como usuários e computadores. Um controlador de domínio é usado para fornecer autenticação segura a recursos e serviços de forma simplificada, além de fornecer uma camada extra de segurança e facilidade de aplicação de configurações.

Imagine que você adicionou um servidor Proxy em sua rede para filtrar o conteúdo Web visto pelos usuários, e precisa configurar cerca de duas mil máquinas. Você pode configurar todas as máquinas de uma única vez através de uma política de grupo (GPO), ou ainda possuir diversos caminhos de configuração para

cada departamento.

Imagine que, em sua rede, existam cerca de doze servidores proxys diferentes, e cada grupo de usuários precisa sair por um específico. Trabalhar com redes onde existe o controle de domínio é realmente algo muito interessante, e torna a administração algo bem mais simples reduzindo a necessidade de uma grande equipe de TI e centralizando a administração e controle de acesso.

TIPOS DE AD

- **AD DS - ACTIVE DIRECTORY DOMAIN SERVICES:** serviço principal de instalação do AD e o mais utilizado pelas empresas. É o catálogo global e objetos em si.
- **AD LDS - ACTIVE DIRECTORY LIGHTWEIGHT DIRECTORY SERVICES:** é também chamado de ADAM Active Directory Application Mode e possui menos recursos que o AD DS. Foi utilizado no Windows Server 2003.
- **AD RMS - ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES:** aumenta a segurança da informação, uma vez que pode impedir que documentos e e-mails sejam lidos por usuários não autorizados.
- **AD CS - ACTIVE DIRECTORY CERTIFICATE SERVICES:** cuida do gerenciamento de certificados digitais de um domínio.
- **AD FS - ACTIVE DIRECTORY FEDERATION SERVICES:** também chamado de Serviço de federação do AD e Sing-On (SSO) para minimizar o número de senhas de logon a serem memorizadas pelo usuário. Com o SSO, uma única conta dá acesso a todos os serviços possíveis e autorizados.

Algo interessante que você deve saber sobre o ADDS é que a autenticação é feita pelos protocolos Kerberos, LDAP e, em alguns casos, pelo NTLM. Isso significa que qualquer software de terceiros,

como firewalls, proxys e demais, podem efetuar a leitura em um controlador de domínio aplicando permissões e configurações específicas para um determinado usuário ou grupo de usuários. Vou citar aqui softwares como Ocommon (Linux), para controle de chamados, e o proxy Endian (Linux).

Para um bom administrador de redes, tudo deve se comunicar de forma segura e eficaz, não importa a plataforma. A interoperabilidade sistêmica é a chave do sucesso para uma rede saudável. No link a seguir, é possível ver uma matéria da HTBRAZ sobre a autenticação de um Proxy Endian em um domínio com Windows Server 2012 R2. Para autenticar unidades open externas, use sempre protocolos NTLM e LDAP (<http://htbraz.blogspot.pt/2012/12/proxy-autenticado-com-endian-251-em.html>).

The screenshot shows the 'Proxy HTTP: Autenticação' configuration window. The 'Autenticação' tab is selected. The 'Escolha o Método de Autenticação *' dropdown is set to 'Active Directory do Windows (NTLM)'. The 'Domínio de Autenticação *' field contains 'contoso.htb'. The 'Número de Processos Filhos de Autenticação *' is set to 20, and the 'TTL do cache de autenticação (em minutos) *' is set to 60. The 'Número de IPs diferentes por usuário *' is set to 0, and the 'TTL do cache de usuário/IP (em minutos) *' is set to 0. The 'Configurações específicas NTLM' section is expanded, showing the 'Nome de domínio do servidor AD *' as 'contoso', the 'Nome do servidor primário do AD (PDC) *' as 'htbraz-03454-teste', and the 'Endereço IP do servidor PDC do AD *' as '192.168.0.1'. There is also a button 'Ingressar no domínio AD' and a field 'Ingressar no Domínio'. The 'Nome do servidor secundário do AD (BDC)' and 'Endereço IP do servidor BDC do AD' fields are empty. A 'Salvar' button is at the bottom.

Para que o Active Directory (ADDS) possa ser instalado, transformando um Servidor Membro (Member Server) em Controlador de Domínio (DC - Domain Controller), dois pré-requisitos básicos devem ser atendidos:

- Um volume formatado com o sistema de arquivos NTFS;
- Acesso a um servidor DNS padrão Windows 2000 Server, Superior ou compatível com este padrão.

O volume NTFS evoluiu muito da época do Windows NT, e é necessário para gravar os arquivos do Active Directory. Se não houver um volume formatado com o sistema de arquivos NTFS, o assistente de instalação do Active Directory será cancelado. Coloco esta recomendação apenas para deixar registrada essa exigência, mas é muito pouco provável que alguém utilize FAT ou FAT 32 em partições de um servidor ainda hoje.

O sistema de arquivos NTFS é amplamente usado nos sistemas operacionais da Microsoft há muito tempo, e sua primeira aparição foi no Windows NT (Server / Workstation). No que se trata de provas, é necessário conhecer bem as características do NTFS, pois a 70-410 exige domínio dos detalhes deste sistema de arquivos e pode confundir quem tenta efetuar a prova.

O Active Directory apresenta alguns elementos individuais, que devem ser entendidos em sua íntegra, pois praticamente seu funcionamento se mantém através dos dias até sua atual versão, o Windows Server 2012 R2. Entendendo estes elementos você poderá oferecer suporte não só à versão mais atual, mas a versões anteriores do Windows Server. Estes elementos fazem a composição da estrutura lógica do AD e serão cobrados em todas as provas do MCSA e MCSE.

Domínios

É um agrupamento lógico de contas e recursos, os quais compartilham políticas de segurança. As informações sobre os diversos elementos do domínio (contas de usuários, contas de computador, grupos de usuários, políticas de segurança etc.) estão contidas no banco de dados do Active Directory. A composição de seu nome é chamada de *Canonical Name* (CN) e, por boa prática, deve conter um nome composto separado por ponto e diferente de um nome público.

Árvores

Uma árvore é um agrupamento ou arranjo hierárquico de um ou mais domínios do Windows Server 2012 R2, os quais compartilham um espaço de nome. Imagine que você possui uma estrutura para cada departamento da empresa `sbrubles.local`. Observe que o domínio `sbrubles.local` possui uma divisão hierárquica para cada departamento.

1. `Rh.sbrubles.local`
2. `Dp.sbrubles.local`
3. `Assistência.sbrubles.local`

DICA

Este tipo de uso é adequado não para departamento, mas para filiais diferentes que possuem a necessidade de diferenciação. Se houver uma hierarquia muito complexa, será exigida uma janela de manutenção maior em caso de mudança.

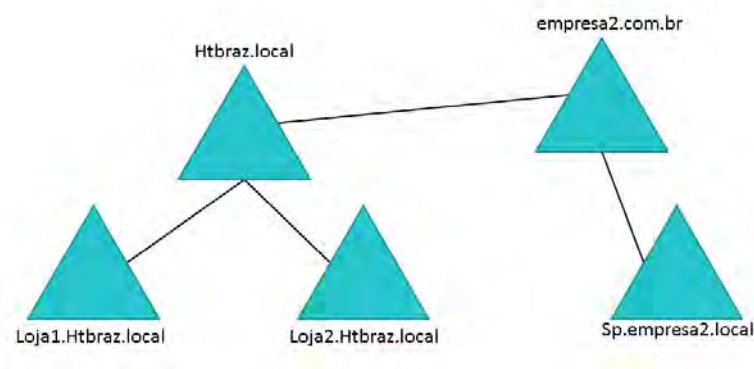


Figura 2.14: Elementos do AD

Uma floresta é um conjunto de domínios que confiam uns nos outros.

Relações de confiança

As relações de confiança possibilitam a comunicação entre domínios diferentes, permitindo que um usuário da empresa A efetue login com todos os seus dados, customização e personalização em uma rede de uma empresa B. Imagine que sua empresa foi comprada por uma multinacional, porém tudo continuará da mesma forma, com o mesmo domínio, e-mail e demais atividades rotineiras, porém agora com o compartilhamento de recursos.

No Windows Server 2012 R2 (bem como no Windows 2000 Server, Windows Server 2008 e no Windows Server 2012 R2), as relações de confiança são criadas automaticamente entre os domínios de uma árvore de domínios de forma bidirecionais. Ou seja, se o domínio paulista.htbraz.local confia no domínio

barafunda.htbraz.local , isso significa que o domínio barafunda.htbraz.local também confia no domínio paulista.htbraz.local . Esta questão despenca nas provas do MCSA e MCSE, valendo sua releitura diversas vezes.

Objetos do Active Directory

São todos os usuários, computadores, grupos e elementos que compõem o Active Directory. O conhecimento sobre os objetos do AD será cobrado principalmente por questões de replicação de políticas de grupo com a prova 70-410 e entre sites diferentes pela prova 70-411.

Unidades organizacionais

As unidades organizacionais (OU) são contêineres de objetos e funcionam como se fossem um grande Windows Explorer dentro do Active Directory. Logicamente, este conceito é simplista perto da real importância das OUs, mas serve muito bem para entender seu funcionamento. Durante o treinamento, teremos oportunidade de criar e excluir objetos dentro das OUs, e entender melhor sua estrutura e funcionamento.

Schema

Quando pensamos em organização da infraestrutura, é necessário falar sobre o esquema (*Schema*) de funcionamento do Catálogo Global (*Global Catalog*), pois é este mecanismo que define o que será ou não gravado. Os atributos de cada objeto copiados para dentro do Catálogo Global são aqueles mais utilizados para a realização de pesquisas no Active Directory, por exemplo, nome do usuário, nome de compartilhamento e tipo da impressora e assim por diante.

A definição de quais atributos são armazenados no Catálogo

Global, e quais não são é feita no Schema do Active Directory. Conforme mostrarei mais adiante, o Schema é como se fosse (na prática, eu considero que é) a definição da estrutura do banco de dados do Active Directory

Sites

Quando nos referimos ao termo *site*, é na verdade uma localização física diferente da unidade matriz. Quando criamos um site pelo Active Directory Sites and Services, é implantada uma configuração específica de replicação do catálogo global. Isso significa que, dentro dessa estrutura de rede, existe uma hierarquia e uma organização lógica.

Este é um dos itens mais interessantes de todo o conteúdo relacionado ao MCSA. De todas as consultorias que fiz Brasil afora, posso contar nos dedos quem tem as configurações de sites bem estruturada e bem configurada. Posso afirmar sem medo que este item deveria ser mais bem explorado dentro de diversas empresas de pequeno e médio porte. Isso significa que existe um amplo campo de manutenção dos sites e serviços que ainda precisam amadurecer.

Quando todo o ambiente está bem configurado, raramente apresenta problemas, o que demonstra que uma estrutura bem montada apresentará pouquíssimo esforço administrativo por parte de replicação do catálogo global, relação de confiança ou até mesmo funcionamento do Active Directory.

Este recurso é cobrado de forma mais extensa pela prova 70-412, e é utilizado para representar a estrutura física da rede da empresa. As informações sobre a topologia da rede, replicação e range de endereços, contidas nos objetos site e link entre sites, são usadas pelo Active Directory para a criação automatizada de configurações de replicação otimizadas, sempre procurando reduzir o máximo possível do tráfego pelos links de WAN. Este conteúdo é

intensamente cobrado nas provas 70-411 e 70-412.

IMPORTANTE

O nível funcional da floresta e do domínio acompanham a versão do AD. Se você já possui uma rede com pelo menos um controlador de domínio Windows Server 2003, não será possível elevar o nível funcional sem sua despromoção. Na prática, você não pode ter o nível funcional do ambiente com o Windows Server 2012 se seu controlador de domínio é Windows Server 2003.

Existe uma prática muito interessante para preparar um ambiente com nível funcional Windows Server 2003 para receber um controlador de domínio com Windows Server 2012 ou 2012 R2. A próxima figura traz uma dica importante sobre o assunto.

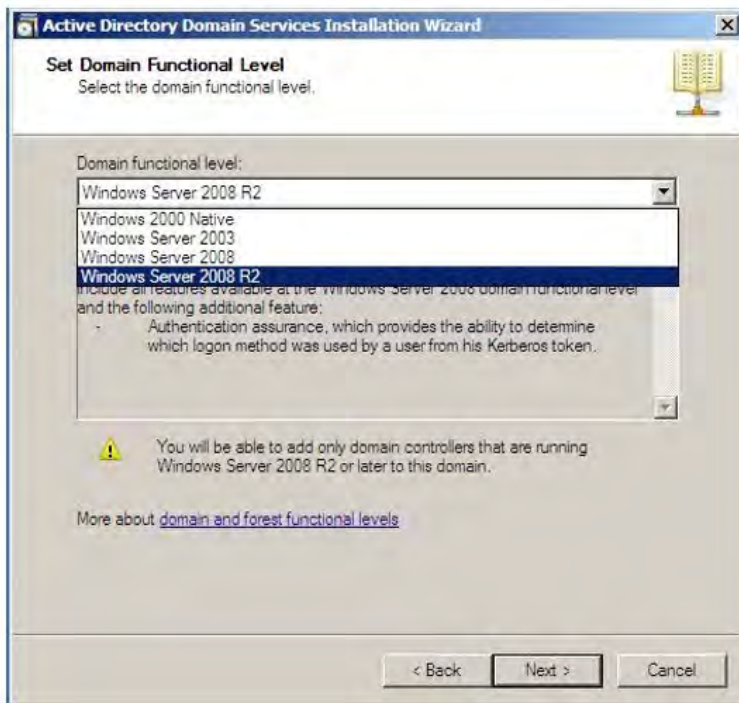


Figura 2.15: Níveis de funcionalidade

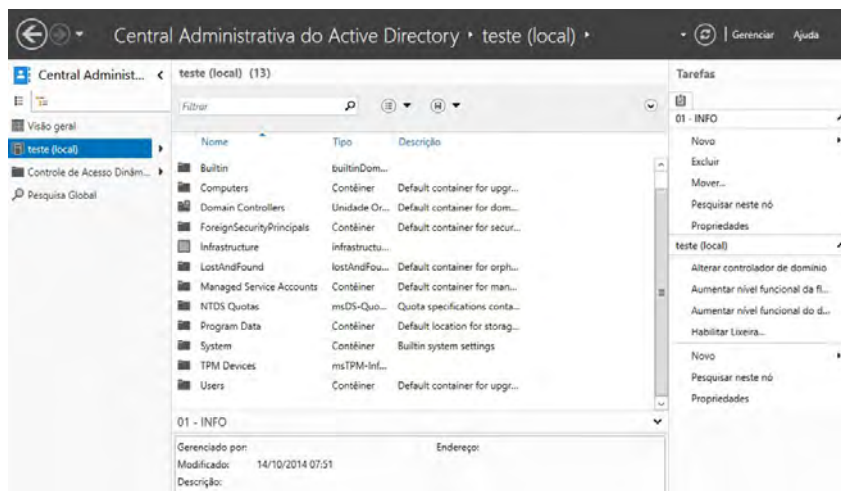
Os níveis funcionais determinam os recursos de domínio ou floresta dos Serviços de Domínio Active Directory (AS DS) disponíveis. Também determinam os sistemas operacionais Windows Server que podem ser executados em controladores de domínio no domínio ou na floresta.

No entanto, os níveis funcionais não afetam os sistemas operacionais que podem ser executados em estações de trabalho e servidores membros associados ao domínio ou à floresta.

Abordaremos com mais ênfase esse processo quando

estudarmos para a prova 70-412. Neste momento, apenas lembre-se de que o nível funcional da floresta deve ser por padrão compatível com o controlador ativo da rede. Se você tiver trinta controladores de domínio Windows Server 2012 R2 e um com Windows Server 2003, então o nível funcional da floresta será o mais baixo, ou seja, será Windows Server 2003. Para preparar um ambiente Windows Server 2003 para receber um controlador de domínio Windows Server 2008 ou 2012, será necessária a utilização do Adprep (que comentaremos mais à frente).

Quando você inicia a promoção de um servidor como controlador de domínio onde não existem outros controladores de domínio, será criada a floresta e sua composição primária, aqui demonstrada pela central administrativa do Active Directory. Esta composição primária cria algumas unidades organizacionais automaticamente, e é por meio desta composição que você deve iniciar a construção da estrutura de departamentos da empresa.



Grupos criados automaticamente:

- Builtin

- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- LostAndFound
- Managed Service Accounts
- NTDS Quotas
- Program Data
- System
- TPM Devices
- Users

Boas práticas para subir um AD:

- Desenhe o tamanho de sua estrutura citando os servidores que conterão as FSMOs de domínio e as FSMOs de floresta;
- Quanto mais simples for a estrutura, mais fácil será sua manutenção, porém nem sempre será a forma mais correta, segura ou rápida de trabalhar;
- Sempre tenha mais de um controlador de domínio, pois ter um só é o mesmo que não ter nenhum;
- Use nomes compostos diferentes da convenção padrão da internet. Isso permitirá futuramente adicionar um servidor de correio eletrônico como o Exchange, por exemplo, sem se preocupar com a propagação de nomes DNS. Acredite, não se preocupar com isso é um verdadeiro tiro no pé para um futuro que pode não ser tão distante. Não use domínios internos com as convenções .com , .br ou qualquer item da lista de domínios públicos disponível pela internet para evitar problemas de acesso. Exemplo:
 - Não usar: `eduardopopovici.com.br` (não é recomendado e dará problemas de acesso).
 - Usar: `eduardopopovici.local` (sem problemas)

de acesso).

- Desenhe os grupos e identifique quais políticas serão criadas antes da aplicação na prática;
- Evite aplicar políticas diretamente ao *Default Domain Policie*.

2.6 IMPLEMENTANDO CONTROLADORES DE DOMÍNIO PELO IFM

Este tipo de instalação é útil quando existe um link de baixa velocidade ou alta latência entre filiais e matriz. Quando instalamos os Serviços de Domínio Active Directory (AD DS) para um novo controlador de domínio que se encontra em uma localidade física de difícil acesso com links de baixa velocidade, podemos usar um método de instalação a partir de mídia de DC ou DVD, chamado de técnica IFM, ou *Install From Midia*.

Você pode reduzir significativamente o tráfego de replicação que é iniciado durante a instalação de um controlador de domínio adicional em um domínio do Active Directory. A redução do tráfego de replicação reduz o tempo que é necessário para instalar o controlador de domínio adicional.

Este recurso foi implementado no Windows Server 2008 e mantido como diferencial pelo Windows Server 2012 R2, incluindo uma versão melhorada da ferramenta `Ntdsutil`. O `Ntdsutil` é uma ferramenta já conhecida dos administradores de redes que pode ser usada para criar as mídias de instalação para um controlador de domínio adicional.

O método IFM usa os dados da mídia de instalação para instalar o AD DS, o que elimina a necessidade de replicar cada objeto de um controlador de domínio do parceiro.

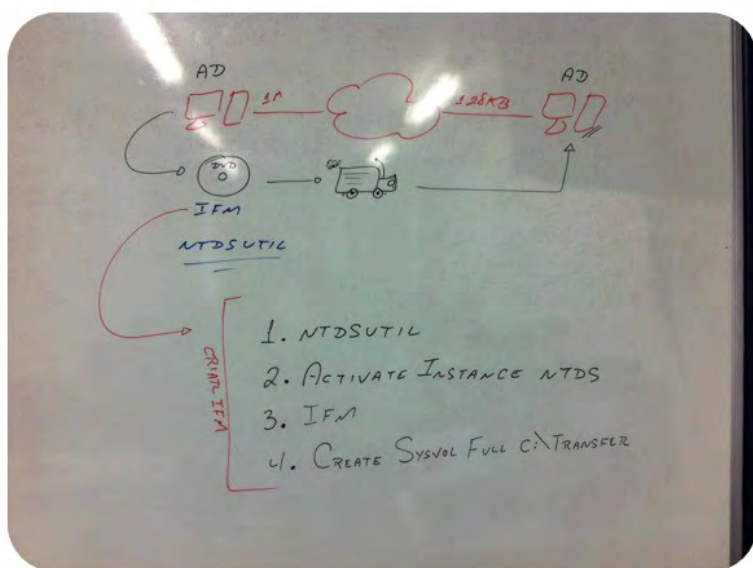


Figura 2.17: IFM

Você precisa usar a ferramenta `Ntdsutil.exe` para criar mídia de instalação para os controladores de domínio adicionais que estiver criando em um domínio. É possível minimizar a replicação de dados do diretório pela rede, usando a opção Instalar da Mídia (IFM). Isto ajuda a instalar, de maneira mais eficiente, controladores de domínio em sites remotos.

O IFM está disponível a partir do Windows Server 2008 até as versões mais atuais. Deve-se trabalhar sempre com o conceito de origem e destino, lembrando de que é necessário que haja uma infraestrutura de redes ativas para o funcionamento do IFM.

No entanto, os objetos que foram modificados, adicionados ou excluídos desde que a mídia de instalação foi criada devem ser replicados. Se o suporte de instalação foi criado recentemente, a quantidade de replicação que é necessária é consideravelmente

menor do que a quantidade de replicação que é necessária para uma instalação normal AD DS.

É importante lembrar de que a técnica de instalação do controlador de domínio através do IFM não exclui a necessidade de um link de comunicação com o domínio principal. Na verdade, esta técnica apenas facilita a cópia dos dados do Active Directory que não precisam ser trafegados.

DICA

Fique atento ao detalhe da instalação de controladores de domínio com o IFM. Existem diversas questões que citam lentidão e latência em um pequeno cenário que pode ser útil a implementação por mídia removível. A próxima figura demonstra os passos simplificados para uso do IFM.

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ntdsutil
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds"
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create sysvol full c:\transfer\IFM\
Creating snapshot...
Snapshot set {4202ef37-8b8d-4109-91b3-de7ce45f8d30} generated successfully.
Snapshot {4ecfc830-93b1-49b3-af53-cdd0f1aed42f} mounted as C:\$SNAP_201508051324_VOLUME#\
Snapshot {4ecfc830-93b1-49b3-af53-cdd0f1aed42f} is already mounted.
Snapshot {4ecfc830-93b1-49b3-af53-cdd0f1aed42f} is already mounted.
Initiating DEFRACTIONMENTATION mode.
Source Database: C:\$SNAP_201508051324_VOLUME#\Windows\NTDS\ntds.dit
Target Database: c:\transfer\IFM\Active Directory\ntds.dit

Defragmentation Status (% complete)
0 10 20 30 40 50 60 70 80 90 100
|---|---|---|---|---|---|---|---|---|---|
.....

Copying registry files.
Copying c:\transfer\IFM\Registry\SYSTEM
Copying c:\transfer\IFM\Registry\SECURITY
Copying SVSOL...
Copying c:\transfer\IFM\SVSOL\green.net
Copying c:\transfer\IFM\SVSOL\green.net\Policies
Copying c:\transfer\IFM\SVSOL\green.net\Policies\31B2F340-0160-11D2-945F-00C04FB984F9
Copying c:\transfer\IFM\SVSOL\green.net\Policies\31B2F340-0160-11D2-945F-00C04FB984F9\GPT.INI
Copying c:\transfer\IFM\SVSOL\green.net\Policies\31B2F340-0160-11D2-945F-00C04FB984F9\MACHINE
Copying c:\transfer\IFM\SVSOL\green.net\Policies\31B2F340-0160-11D2-945F-00C04FB984F9\MACHINE\Microsoft
Copying c:\transfer\IFM\SVSOL\green.net\Policies\31B2F340-0160-11D2-945F-00C04FB984F9\MACHINE\Microsoft\Windows NT
Copying c:\transfer\IFM\SVSOL\green.net\Policies\31B2F340-0160-11D2-945F-00C04FB984F9\MACHINE\Microsoft\Windows NT\
ecedit
```

Figura 2.18: IFM

- Servidor de origem:
 1. Cmd com permissões administrativas
 2. ntdsutil

```
3. activate instance ntds
4. ifm
5.         create         sysvol         full
           c:\Transfer\IFM\
```

- Servidor de destino:

Rode o Wizzard de instalação do AD DS

2.7 PESQUISAR OBJETOS NO ACTIVE DIRECTORY

Grande parte da rotina administrativa consiste em gerenciar objetos do Active Directory. Isso significa que você precisa conhecer bem questões simples, como localizar um usuário dentro de sua estrutura antes mesmo de alterar suas propriedades. Vejo alguns administradores de redes estudando para provas de certificação como MCSA e MCSE sem mesmo saber os passos mais simples para localização de objetos em um controlador de domínio.

No Windows Server 2012 e Windows Server 2012 R2, é possível pesquisar usuários de três formas diferentes, sendo duas através da área gráfica pelo Active Directory Users and Computers e através do Active Directory Administrative Center, e uma pelo prompt de comando pela ferramenta `dsquery`. Nas versões mais antigas, como o Windows Server 2008 R2 ou o Windows 2000, é possível a pesquisa de duas formas diferentes, sendo uma com o Active Directory Users and Computers e a outra pelo prompt de comando.

2.8 FSMO

As FSMO são divididas em dois grupos: nível de floresta (2

FSMO) e em nível de domínio (3 FSMO).

FSMO de Florestas

- **Schema Master**

O Schema é o coração do Active Directory. Ele é composto de objetos e atributos que modelam o Active Directory. É pelo Schema que dizemos, por exemplo, que o objeto do tipo `USUÁRIO` terá os atributos `NOME`, `ENDEREÇO`, `TELEFONE` etc. Como o esquema pode ser customizado e deve ser o mesmo em toda a floresta Windows, a regra Schema Master se encarrega de evitar conflitos entre os DCs.

- **Domain Tree (Domain Naming Master)**

Se você adiciona um novo domínio em uma floresta (por exemplo, se você adiciona um domínio filho), o nome desse domínio deve ser único na floresta. Esta é a regra responsável por assegurar isto e evitar conflitos entre outros domínios.

FSMO de Domínio

- **PDC**

Como o nome já diz, uma das funções desta regra é emular um PDC NT 4.0 para manter a compatibilidade com servidores legados (por exemplo, BDCs NT 4.0) e clientes mais antigos. Mesmo que você migre todo seu ambiente para Windows 2000 ou 2003, esta regra ainda é importante, pois é responsável por tratar alterações de contas de usuários, *lockouts* de contas, relações de confianças com outros domínios e pelo sincronismo do

relógio no domínio.

- **RID**

Qualquer DC pode criar novos objetos (usuários, grupos, contas de computadores). Cada objeto deve possuir um identificador único, conhecido como SID. O SID do objeto é construído usando o SID do domínio, mais um ID relativo (RID). Porém, após criar 512 objetos, um DC precisa contatar o RID Master para conseguir mais 512 RIDs (atualmente, um DC contata o RID Master quando ele possui menos de 100 RIDs disponíveis). Isto evita que dois objetos diferentes tenham o mesmo RID em todo o domínio.

- **Infrastructure**

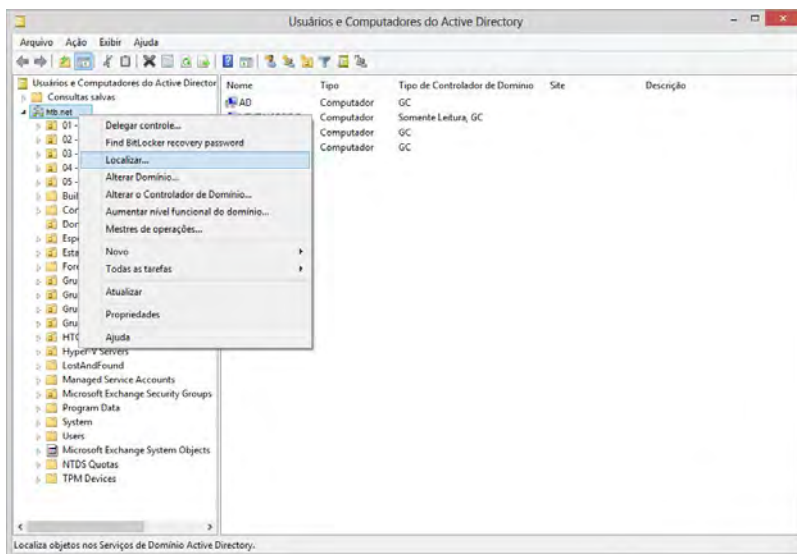
Esta regra é muitas vezes conhecida apenas como cosmética, já que sua função é se assegurar que o Display Name de usuários pertencentes a um grupo sejam atualizados caso este atributo seja alterado. Ele é mais importante em ambientes que possuem vários domínios, pois vai assegurar que todos os grupos que um determinado usuário pertença vai refletir o Display Name correto.

2.9 USANDO A INTERFACE DO WINDOWS

Grande parte da administração será feita por meio de interface gráfica, salvo momentos em que o servidor está em modo de instalação Server Core. Bom, alguns de vocês podem pensar em instalar a interface gráfica, efetuar a mudança e depois retornar para o modo Server Core. Bem, a ideia é boa, mas não é bem assim que funciona, principalmente em servidores com o Windows Server

2008 e 2008 R2 que não suportam essa ação, ou em servidores com o Windows Server 2012 e 2012 R2 que suportam a ação, mas não podem ser reiniciados ou desligados fora de uma janela de manutenção.

1. Abra o Gerenciador do Servidor (Server Manager). No Windows 2012, este item está localizado em *Tools* (ferramentas), já no Windows Server 2008 pode ser acessado pelas ferramentas administrativas no botão *Iniciar*.
2. Abra *Usuários e Computadores* do Active Directory.
3. É possível efetuar a pesquisa através do domínio todo, pela árvore de console. Clique com o botão direito do mouse no nó do domínio e, em seguida, clique em *Localizar*. A próxima figura exemplifica bem esta ação.



4. Se souber em qual unidade organizacional o usuário está, na árvore de console, clique com o botão direito do mouse na unidade organizacional e clique em *Localizar*.
5. Em *Nome*, digite o nome do usuário que deseja localizar.

6. Clique em *Localizar Agora*.

A pesquisa por objetos do Active Directory não exige credenciais administrativas. É uma prática recomendada de segurança que você execute qualquer tipo de pesquisa com um usuário sem credenciais administrativas.

Para abrir Usuários e Computadores do Active Directory:

1. No Windows Server 2008, clique em *Iniciar*, depois em *Painel de Controle*, clique duas vezes em *Ferramentas Administrativas* e, em seguida, duas vezes em *Usuários e Computadores* do Active Directory. No Windows Server 2012 e 2012 R2, abra o *Server Manager*, selecione *Tools*, e depois *Active Directory Users and Computers*.
2. Clique com o botão direito do mouse no nó do domínio e, em seguida, clique em *Localizar*.
3. Clique em *Localizar agora* para acessar mais opções da localização.
4. Digite o nome do usuário ou computador que deseja encontrar e clique em *Localizar agora*.
5. Você também pode pesquisar usando critérios de pesquisa parciais. Por exemplo, o retornará todos os objetos cujos nomes comecem com a letra **O**, como Operadores de Cópia.
6. Use a guia *Avançado* para obter opções de pesquisa mais sofisticadas.
7. Para localizar um usuário, você também pode clicar em *Localizar objetos* no Active Directory na barra de ferramentas.

Usando uma linha de comando para localizar usuários:

1. Abra o prompt de comando.

2. Digite: `dsquery userparâmetro` .

Localizar uma pasta compartilhada:

1. Abra *Usuários e Computadores* do Active Directory.
2. Na árvore de console, clique com o botão direito do mouse no nó do domínio e, em seguida, clique em *Localizar*.
3. Na lista *Localizar*, clique em *Pastas Compartilhadas*.
4. Na guia *Pastas Compartilhadas*, em *Nome*, digite o nome da pasta que deseja localizar.
5. Clique em *Localizar Agora*.

Localizar uma impressora:

1. Abra *Usuários e Computadores* do Active Directory.
2. Na árvore de console, clique com o botão direito do mouse no nó do domínio e, em seguida, clique em *Localizar*.
3. Na lista *localizar*, clique em *Impressoras*.
4. Na guia *Impressoras*, em *Nome*, digite o nome da impressora que deseja localizar.
5. Clique em *Localizar Agora*.

Localizando grupos:

Aqui segue a mesma linha de raciocínio da localização dos usuários. Utilizaremos duas formas diferentes de localização, sendo uma pela interface gráfica e outra pela linha de comando.

Localizando Grupos utilizando a interface do Windows:

1. Abra *Usuários e Computadores* do Active Directory.
2. Na árvore de console, clique com o botão direito do mouse no nó do domínio, e clique em *Localizar*.
3. Na guia *Usuários*, vá em *Contatos e Grupos*, depois em *Nome*, e digite o nome do grupo que deseja localizar.
4. Clique em *Localizar Agora*.

Localizando Grupos utilizando o prompt de comando:

1. Abra o prompt de comando.
2. Digite: `dsquery group parâmetro`

Localizando controladores de domínio:

1. Abra o prompt de comando.
2. Digite: `dsquery server Parâmetro`

Localizando os servidores responsáveis pelas FSMO:

1. Abra o prompt de comando.
2. Digite: `Netdom query FSMO`

Localizando uma unidade organizacional:

1. Abra *Usuários e Computadores* do Active Directory.
2. Na árvore de console, clique com o botão direito do mouse no nó do domínio e, em seguida, clique em *Localizar*.
3. Na lista *Localizar*, clique em *Unidades Organizacionais*.
4. Digite o nome da unidade organizacional que deseja localizar e clique em *Localizar Agora*.

DICA

É possível ainda personalizar o painel de detalhes do *snap-in* Usuários e Computadores do Active Directory com os objetos do seu diretório de modo mais eficiente. Use o comando *Adicionar/Remover Colunas* através do menu *Exibir* na parte superior da janela para adicionar colunas ao painel de detalhes.

É interessante lembrar de que nem todos os atributos ficam disponíveis para exibição simplificada, mas certamente será possível encontrar colunas bem úteis para exibição, como por exemplo, o Nome de Logon do Usuário.

OBJETOS DO AD

Sabe-se que o Active Directory é o banco de dados de diretórios do Windows Server desde sua primeira versão, até os tempos atuais com o Windows Server 2012 R2. E é nele que são armazenados todos os objetos de uma rede baseada em controladores de domínio. O AD DS fica localizado exatamente em um arquivo chamado `ntds.dit`. É exatamente neste arquivo que se encontra toda a base de dados de nossa rede.

Um serviço de diretório é um serviço de rede, o qual identifica todos os recursos disponíveis em uma rede que podem ser especificados, como: contas de usuários, pastas compartilhadas, grupos, computadores, impressoras, contatos e GPOs. O serviço de diretório é responsável por cada usuário, pasta compartilhada, servidor e dispositivo dentro de uma rede (dentro de uma determinada abrangência).

A estrutura do Active Directory armazena objetos em unidades organizacionais conhecidas como OU, assimilando-se ao Windows Explorer. As unidades organizacionais recebem as políticas de grupo (GPO) e replicam suas configurações para computadores, usuários e demais objetos, portanto, sua organização e criação são de extrema valia e importância.

Lembre-se de que a prova cobrará de você situações fáceis de se resolver, como por exemplo, a administração de um ambiente pequeno ou sem muitos detalhes. Porém, o mundo real lhe dará

situações complexas que muitas vezes apresentam janelas de manutenção, paradas estratégicas e muito conhecimento técnico para recuperação.

3.1 AS CONTAS DE USUÁRIO

Todo usuário de nossa rede precisa comprovar sua autenticidade. Isso significa que precisa validar suas credenciais de acesso para utilizar recursos de nossa rede. Entenda o termo usuário como qualquer ser humano ou dispositivo que possua um papel de interação direta com o sistema. Isso significa que uma aplicação de backup pode possuir um usuário em nossa rede, assim como um firewall que precise validar regras com base em usuários criados no Active Directory.

Todo usuário criado em nossa estrutura de rede baseada em controladores de domínio possui a permissão de leitura dos objetos. Essa permissão indica que o usuário é um dado estruturado armazenado pelo Active Directory. O AD nada mais é do que um banco de dados.

As contas de usuário são objetos usadas com muita frequência no gerenciamento do Active Directory, seja no Windows Server 2012 R2 ou em suas versões anteriores, consistindo em todas as informações que definem um usuário. Tais informações são denominadas atributos, que serão cobrados na íntegra pela prova 70-411. Os atributos são números de telefone, e-mail, endereço, nome, entre outros itens.

É importante a definição dos atributos e de seu preenchimento correto para integrações futuras, como a integração do Microsoft Lync para vídeo conferência ou até mesmo algo mais simples, como o Exchange Server para disparo de e-mails. Com dados mais concisos do banco de dados do AD, é possível, por exemplo, que o

Ao criarmos um usuário, seis atributos são definidos, sendo que apenas dois são configurados pelo administrador de redes. O `cn` e `SamAccountName` são os únicos dois objetos configurados pelo administrador de redes, sendo que o `cn` é o nome completo do usuário, e `SamAccountName` é o nome de logon do usuário (que são coisas bem distintas), e os outros quatro são configurados pelo serviço de diretório, `Instance Type`, `objectCategory`, `objectClass`, `objectSid`.

[illegible]

Em versões mais antigas, tais como o Windows 2000 Server e Windows Server 2003, utilizávamos a ferramenta Active Directory Users and Computers (que também está presente em versões mais novas), para gerenciamento de usuários, criação, mover, excluir, alterar atributos e localizar. Porém, no Windows Server 2012 R2, usamos o Active Directory Administrative Center. Veja bem, o Active Directory Users and Computers ainda está presente e pode, sim, ser utilizado, mas como você pretende realizar a prova 70-410, é necessário conhecer a fundo o Active Directory Administrative Center.

O ADAC (ou Active Directory Administrative Center) é uma nova ferramenta de trabalho, com novos recursos, novas possibilidades e um ambiente todo remodelado. É através do ADAC que podemos, por exemplo, ativar a lixeira de objetos do Active Directory. Para quem já efetuou o processo de ativação da lixeira do AD com o Windows Server 2008 R2, sabe que se trata de um processo complexo e trabalhoso. O ADAC veio para facilitar a administração dos objetos do Active Directory.

Cada conta de usuário possui quatro tipos de nomes associados: um nome de logon de usuário, um nome de logon do usuário anterior ao Microsoft Windows 2000, um nome de logon principal do usuário e um nome distinto relativo do LDAP (Lightweight Directory Access Protocol). O LDAP é um protocolo de autenticação muito usado para leitura do Active Directory por sistemas externos como firewalls, sistemas open como Linux e Unix, e ainda sistemas proprietários desenvolvidos dentro de linguagens específicas.

O nome de logon de usuário

Deve ser exclusivo dentro da floresta na qual a conta de usuário foi criada, o que significa que, onde existe um usuário com o logon

epopovi , não poderá existir outro. Uma técnica muito interessante para a criação de usuários é de mesclarmos nomes e sequências de letras do sobrenome. Coloquei a seguir alguns exemplos muito comuns para a criação de usuários:

- Nome do usuário: Eduardo Popovici
- Logins possíveis:
 - Epopovi - Primeira letra do nome e as seis últimas letras do sobrenome.
 - Edupopov - Três primeiras letras do nome e as últimas quatro do sobrenome.
 - Eduardo.popovici - Nome ponto sobrenome.

IMPORTANTE

Cada empresa possui sua política interna para a criação dos nomes de usuários. Entretanto, quando iniciar o levante de um ambiente do zero, considere alguns fatores para desenvolver as regras, como por exemplo, a facilidade de assimilação pelos usuários da rede, a resposta por quem recebe a mensagem e a questão do recebimento de SPAMs pelos e-mails, pois é muito provável que a conta de e-mail seja a mesma que seu usuário.

Evite colocar nomes de departamento para usuários, pois quando este deixa o quadro de funcionários, seja por férias, demissão ou qualquer outro motivo, a administração se torna mais demorada e problemática. Estude a política interna da empresa e, caso não exista nenhuma, busque frameworks como o MOF (Microsoft Operational Framework) para ajudar com a organização e desenvolvimento de políticas.

- **Nome de logon anterior ao Windows 2000:** é usado

para fazer logon em um domínio do Windows onde os computadores executam sistemas operacionais anteriores ao Windows 2000, usando um nome como o formato *Nome do Domínio\Nome do Usuário*. Também é possível utilizar este nome para fazer logon em domínios a partir de computadores que executam o Windows 2000 ou o Windows XP, ou Windows Server 2003.

Em algumas florestas com domínios diferentes, onde existe relação de confiança, é necessário usar o formato *domínio\usuário* para se conectar. Por exemplo, caso um professor da Htbraz da Avenida Paulista precise ministrar treinamentos na Faculdade Htbraz da Barra Funda, será necessário efetuar logon com as credenciais da unidade da Paulista, informando também o domínio.

- **Nome de logon principal de usuário:** consiste do nome de logon do usuário e do sufixo do nome principal do usuário, unidos pelo símbolo de arroba @ . Este nome principal carrega o usuário e o domínio separado pelo símbolo da arroba (por exemplo, `epopovi@htbraz.local`). Estes dados podem ser acessados no momento da criação do usuário ou ainda após sua criação, pelo Active Directory Users And Computer ou pelo Active Directory Administrative Center, clicando-se com o botão direito no usuário, e depois em propriedades.
- **Nome distinto relativo do LDAP:** este nome é usado para adicionar usuários à rede a partir de um script ou linha de comando. Identifica com exclusividade o objeto em seu recipiente pai. Arrisco inclusive a dizer

que este nome é um dos mais importantes quando pretendemos autenticar ferramentas open a nosso controlador de domínio, como por exemplo, ferramentas de abertura de chamado, como OTRS e Ocommon, e até ferramentas de chat, como OpenFire.

A configuração do Canonical Name (CN) é muito utilizada para leitura do AD. Caso seja necessário autenticar uma ferramenta externa no controlador de domínio, use o CN como nome de objetos e o DC como partes do domínio. Por exemplo, o usuário `epopovi` que está na OU `users` dentro do domínio `htbraz.local` terá sua escrita em nome distintivo como `CN=epopovi,CN=users,DC=htbraz,DC=local`.

IMPORTANTE

É sempre uma boa prática não usar usuários com permissão administrativa dentro do dia a dia, para evitar o comprometimento dos dados em caso de infecção por vírus e worms. É recomendado também que firewalls, bancos de dados e ferramentas que exijam autenticação utilizem um usuário específico que possua permissão apenas de leitura ao Active Directory.

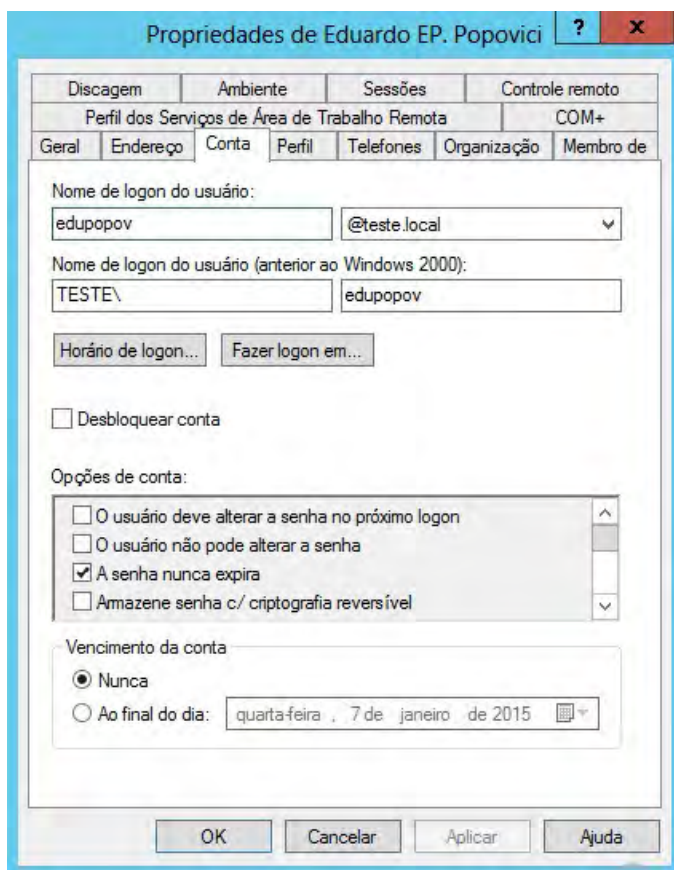
3.2 PROPRIEDADES DO USUÁRIO

A maior parte das configurações do dia a dia é feita no objeto usuário, então neste momento daremos ênfase aos trabalhos em suas propriedades. As abas que mais usaremos diariamente e nas provas do MCSA são Conta, Perfil, Membro de Controle Remoto e

Discagem.

- **Conta** — Utilizado para configurações gerais do usuário, como expiração, horário de logon, nome de conta e demais informações.
- **Perfil** — Usado para direcionar o perfil de usuário para um servidor específico, ou ainda a execução de um script específico.
- **Membro de** — Utilizado para atribuição de usuários em grupos específicos com regras unificadas.
- **Controle Remoto** — Libera ou bloqueia acesso remoto para um determinado usuário sem afetar as configurações do grupo.
- **Discagem** — Atua como configurador de acesso externo ao ambiente interno, como um acesso através de VPN ou modem dial up apenas para o usuário, sem `htbrazr` em todo o grupo.

A aba chamada de Conta de Usuário permite a visualização dos nomes vistos no início deste capítulo, além de permitir a configuração de controle de horário de logon, local de logon e o vencimento da conta. É possível também habilitar configurações mais simples, como por exemplo, a possibilidade de não ser necessário a troca de senha, que é útil em caso de usuário sistêmico (usuário criado para autenticação de um firewall, proxys, antivírus ou gerenciadores de banco de dados — tudo que necessite de autenticação).



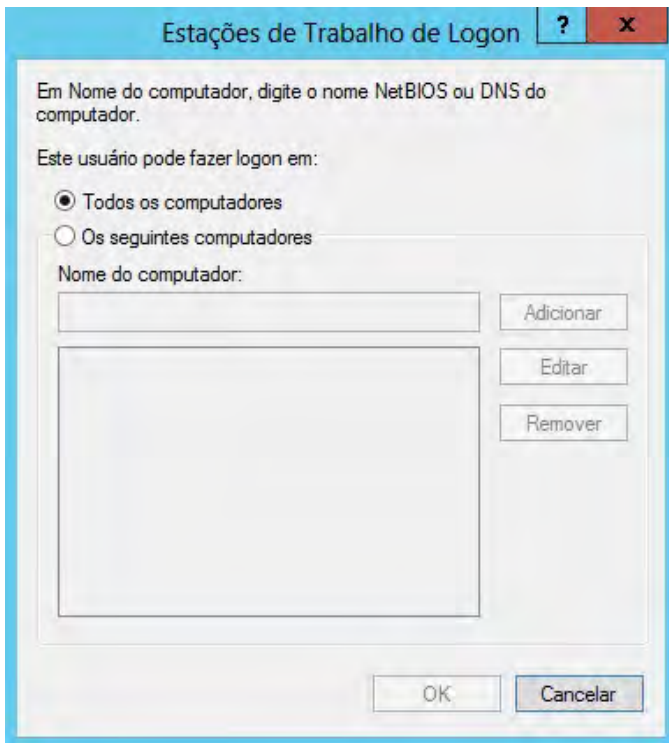
Ainda nas propriedades do usuário, é possível controlar o horário em que será possível efetuar o logon e se haverá a necessidade de uso de um equipamento específico. Este item é particularmente útil quando haverá acesso por prestadores de serviço com pouco acesso e a equipamentos de uma única sala, ou ainda para evitar que sejam feitas horas extras sem a devida autorização. A figura adiante ajuda a definir qual equipamento o usuário poderá efetuar logon na rede.

Gosto muito deste recurso para limitar um departamento onde existem funcionários com uma ação específica, como um Call

Center ou um laboratório de escola de tecnologia.

A associação do usuário ao equipamento é feita pelo nome do host (*host name*) armazenado no servidor de DNS. Para localizar um nome de equipamento, caso você possua em mãos apenas o endereço IP da estação, pode utilizar o comando `Tracert` a fim de identificar o nome registrado no servidor DNS. O comando `Ping` com opção `-a` também permite a resolução do nome do equipamento.

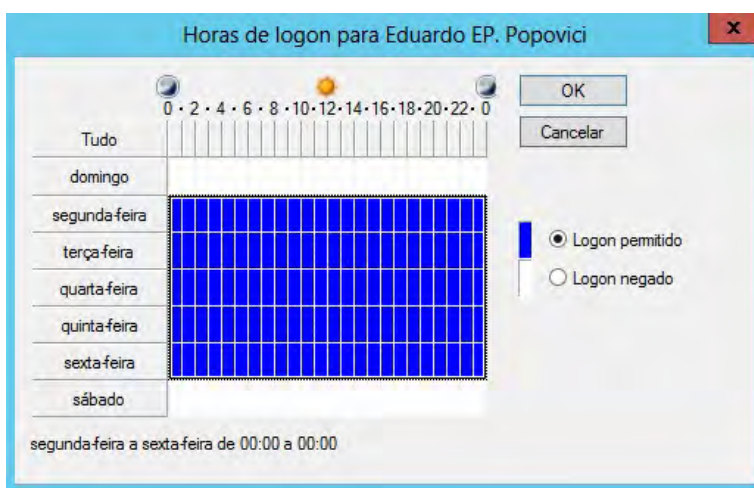
- `Ping <endereço IP> -a`
- `Tracert <endereço IP>`



É possível que seja cobrado de você nas provas e no mundo real o conhecimento sobre a forma como é atribuído a permissão de

logon baseado em horário. Este controle tem sido atribuído cada vez mais em empresas que pretendem controlar gastos em folha de pagamento e evitar processos por trabalho extra sem a devida autorização e ciências dos responsáveis.

A próxima figura apresentada demonstra que o usuário Eduardo EP. Popovici pode efetuar logon apenas de segunda-feira a sexta-feira em horário livre, porém seu acesso será negado aos sábados e domingo.



O vencimento da conta permite atribuir uma data de expiração para momentos em que um determinado usuário finaliza um contrato de permanência, ou até mesmo para um terceiro que tem data certa para ir embora do local de acesso.

3.3 UNIDADES ORGANIZACIONAIS (OU)

As unidades organizacionais são utilizadas para organizar os objetos do Active Directory, e devem ser organizadas conforme a necessidade da empresa. Contudo, é aconselhável perder um pouco mais de tempo nesta organização para evitar mudanças futuras.

Como as Unidades Organizacionais permitem o recebimento de políticas de grupo, é possível assimilar regras de utilização de recursos da rede apenas movendo usuários para uma determinada OU. Em resumo, a unidade organizacional é um tipo diretamente útil de objeto de diretório contido em sendo recipientes do Active Directory, nos quais é possível “guardar” usuários, grupos, computadores e outras unidades organizacionais. Uma unidade organizacional não pode conter objetos de outros domínios.

3.4 GRUPOS DE TRABALHO

A utilização dos grupos veio para simplificar a administração, permitindo conceder permissões para recursos para mais de um usuário por vez. Para uma denominação mais técnica podemos definir o termo grupo como sendo um conjunto de contas de usuário e/ou de computadores com a intenção de facilitar a administração.

Existem basicamente dois grupos de usuários que seguem a seguintes características:

- **Grupos de segurança:** são usados para atribuir direitos e permissões de usuário a grupos, onde direitos determinam o que os membros do grupo de segurança podem fazer em um domínio ou floresta; já as permissões determinam quais recursos um membro de um grupo pode acessar na rede. São os grupos que mais utilizaremos aqui e em praticamente todo o estudo para o MCSA.
- **Grupos de distribuição:** utilizados em aplicações de e-mail, como o Microsoft Exchange, para enviar e-mail para conjunto de usuários. Este grupo não tem recursos de segurança, desta forma, não é possível conceder permissão. Em resumo, só use caso você possua uma

estrutura de e-mail.

DICA

Conhecer a aplicação prática destes dois grupos evita pegadinhas no momento da prova e permite a você alcançar pontuações mais altas. Fique atento no momento da prova aos enunciados que podem misturar características de ambos os grupos. Isso faz com que você confunda a resposta.

3.5 ESCOPOS DE GRUPOS DE TRABALHO

A escolha do escopo dos grupos permite controlar a propagação de modificações entre domínios e florestas, permitindo um melhor gerenciamento da largura de banda entre filiais e sucursais, além de prover segurança adicional com o tráfego dos dados entre servidores. Tudo o que for relacionado à replicação envolve tráfego de dados e, dependendo do tamanho da floresta e da qualidade do link entre as filiais, isso pode realmente ser um problema. Após a escolha entre grupo de segurança e grupo de distribuição, é necessário marcar o tipo de escopo desse grupo, que recebe a divisão de grupos universais, grupos globais e grupos de domínio local.

Grupos universais

Como o próprio nome sugere, são grupos que podem ser utilizados em qualquer parte de um domínio ou da árvore de domínios, e podem conter membros, grupos e usuários de quaisquer domínios. Em resumo, podem conter contas de usuários, outros grupos universais e grupos globais de qualquer domínio; podem ser membros dos grupos locais do domínio ou grupos

universais de qualquer domínio e receber permissões para recursos localizados em qualquer domínio.

Quando o nível de funcionalidade do domínio está configurado como Windows 2000 Nativo, Windows Server 2003, Windows Server 2008 ou Windows Server 2012 R2, um grupo universal pode ser colocado como membro de um outro grupo universal, e permissões podem ser atribuídas em qualquer domínio.

Um grupo pode ser convertido de universal para global, ou de universal para local do domínio. Nos dois casos, esta conversão somente pode ser feita se o grupo universal não tiver como um de seus membros outro grupo universal.

É importante citar que o cache da associação de grupo universal permite que o controlador de domínio armazene em cache informações de associação de grupo universal para usuários. Isto permite que controladores de domínio executando o Windows Server, seja ele 2008 ou 2012 R2, armazene localmente as associações de grupos universais, permitindo que um usuário de uma empresa faça seu login em outra empresa da mesma rede apenas alterando dados de domínio. Trocando em miúdos, o usuário precisará apenas colocar no momento de logon seu domínio principal e seu usuário separado por uma barra (*domínio\usuário*).

Vamos ao esquema prático para melhor entendimento. Imagine que o usuário Luiz da filial SP, do departamento de auditoria, ficará alocado na filial RJ por uma semana. Suas credenciais de acesso devem ser mantidas com o menor esforço administrativo possível.

O cache da associação de grupo universal elimina a necessidade de um servidor de catálogo global em cada site de um domínio, minimizando o uso da largura de banda de rede, já que um controlador de domínio não precisará replicar todos os objetos localizados na floresta. Reduz também os tempos de logon, já que os

controladores de domínio de autenticação nem sempre precisam acessar um catálogo global para obter informações de associação de grupo universal.

Se um usuário se conectar em uma filial, a consulta daquele objeto é feita imediatamente em seu controlador de origem. Em uma rede pequena ou em uma floresta de domínio único, todo e qualquer controlador de domínio existente age como servidores de catálogo global virtual. Isso significa que todos eles podem responder a qualquer autenticação ou solicitação de serviço.

Essa condição especial para florestas de domínio único ocorre intencionalmente. As solicitações de autenticação não exigem o contato com um servidor de catálogo global como acontece quando há vários domínios, e um usuário pode ser membro de um grupo universal existente em um domínio diferente.

IMPORTANTE

Os grupos universais devem ser muito bem planejados, pois o retrabalho é complexo e pode afetar uma grande parte da organização em questão da segurança e tráfego de dados. Em redes baseadas no Windows Server 2003, não devem ser feitas alterações frequentes nos membros de um grupo universal, uma vez que este tipo de ação causa um volume elevado de replicação no Active Directory.

Porém, já no Windows Server 2008 ou Windows Server 2012 R2, foram implementadas modificações, as quais permitem fazer cache das informações dos grupos universais, nos servidores de catálogo global. Com isso, são replicadas somente as alterações feitas nos grupos universais, e não todas as informações contidas no grupo. Assim, o volume de tráfego de replicação foi reduzido consideravelmente em relação ao que ocorria no Windows Server 2003.

Grupos globais

Um grupo global é “global” quanto aos locais onde ele pode receber permissões de acesso. Ou seja, um grupo global pode receber permissões de acesso em recursos (pastas compartilhadas, impressoras etc.) de qualquer domínio de uma árvore de domínios.

Em resumo, esses grupos podem conter contas de usuários e grupos globais do mesmo domínio; somente pode conter membros do domínio no qual o grupo é criado; podem ser membros de grupos universais e grupos locais do domínio, de qualquer domínio; pode ser membro de qualquer grupo global, do mesmo domínio; e podem receber permissões para recursos localizados em qualquer

domínio.

Grupos locais do domínio

São grupos que somente podem receber permissões para os recursos do domínio onde foram criados, porém podem ter grupos e usuários de outros domínios como membros. Em resumo, podem conter membros de qualquer domínio; somente podem receber permissões para recursos no domínio no qual o grupo foi criado; podem ser membro de grupos locais do próprio domínio.

IMPORTANTE

Um grupo pode ser convertido de local para universal, desde que o grupo não tenha como seu membro um outro grupo local.

3.6 ALTERANDO O ESCOPO DOS GRUPOS

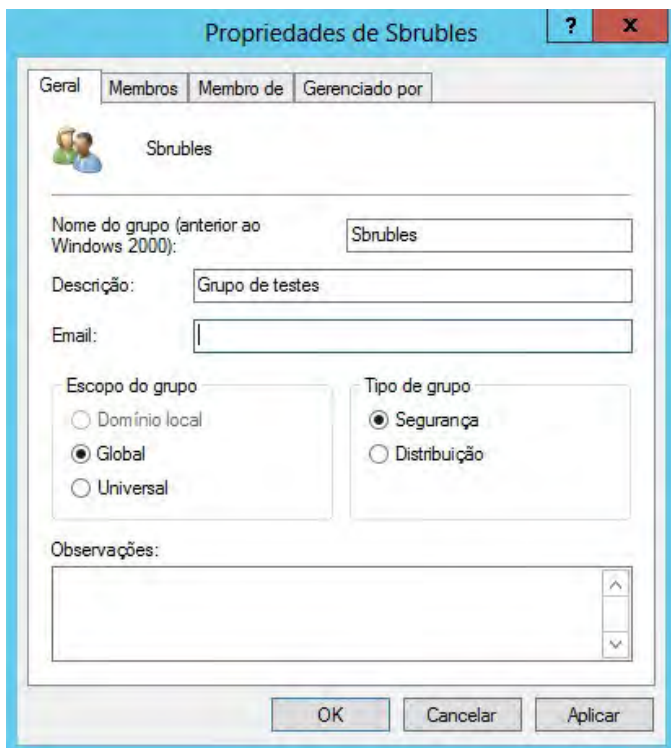
É necessário realçar detalhes importantes relacionados à troca de escopo de grupos já existentes dentro da estrutura funcional, pois a mudança de um grupo global para universal (ou vice-versa) pode ajudar muito a controlar a quantidade de tráfego e a segurança da estrutura do Active Directory. Este processo é muito comum e pode ser necessário pelo tamanho da infraestrutura.

Agora que você entendeu bem a diferença entre os grupos universais, globais e locais, vamos a um ponto importante, que é a mudança do tipo desses grupos após sua criação. Estes passos exigem uma simetria específica e, inclusive, são itens que podem ser cobrados pelas provas 70-410 e 70-411.

Para transformar grupos locais em globais, por exemplo, é necessário antes transformá-los em grupos universais e, somente depois, para grupos globais. Não é possível fazer essa passagem diretamente.

Ok, você dirá, então vamos a um ponto importante: esta regra não funcionou comigo em algum momento do dia. Quando isso não acontece, o problema é com o sistema operacional? Já encontrei casos em que essa regra se tornava pífia e não era possível fazer a mudança, e durante o *troubleshooting* notei que o grupo que eu tentava mudar era membro de outro grupo com escopo diferente.

Por exemplo, imagine que você quer alterar o escopo de um grupo global para universal. Esta conversão só será feita (permitida pelo sistema) quando o grupo que você deseja alterar não for membro de outro grupo com escopo global. Fique atento a esta informação, pois existem questões na 70-410 que abordarão este ponto. Para acessar esta tela a seguir, use o botão direito do mouse em cima do grupo que deseja alterar e, em seguida, clique em *Propriedades*.



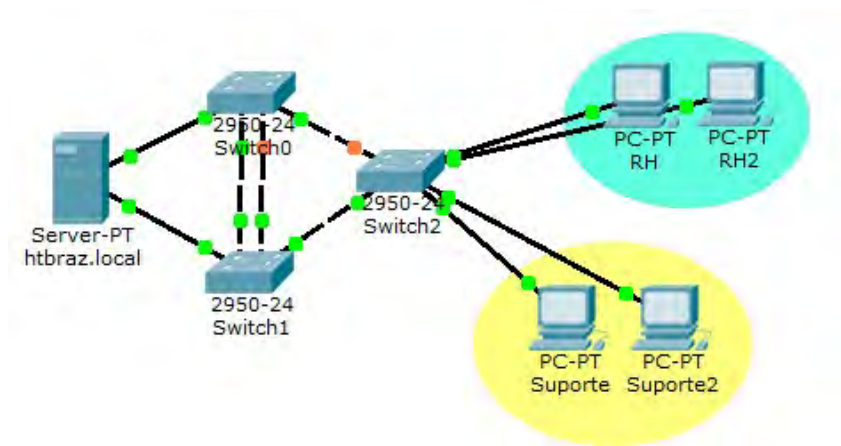
3.7 DELEGANDO ACESSOS NO ACTIVE DIRECTORY DOMAIN SERVICES

A delegação de acesso a objetos e recursos do Active Directory é um ponto de extrema importância para a administração do Windows como um contexto geral. Existem momentos em que a administração é segmentada permitindo a usuários de departamentos cuidarem de seus próprios usuários. Ou ainda, permite a possibilidade de atribuição de permissões específicas a usuários de uma célula mais baixa, como suporte de primeiro nível ou equipe de *help desk*. Para entender melhor, farei a abordagem em um cenário que segue a seguinte linha de raciocínio:

Você é agora o administrador de redes da empresa Sbrubles S/A.

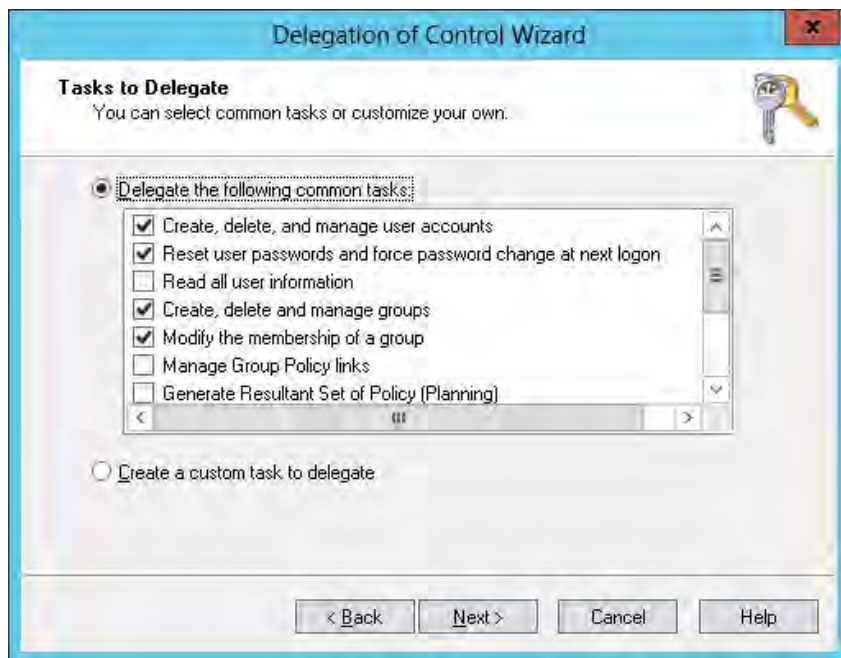
Sua organização possui três controladores de domínio com Windows Server 2012 R2, onde a floresta está com o nível funcional Windows Server 2008 configurado. A Sbrubles S/A possui cerca de mil usuários e mais de cem departamentos diferentes, espalhados por várias filiais conectadas através de um link MPLS de 512 MB. Você recebe ordens de permitir ao departamento de RH a gestão das contas de usuário da unidade organizacional RH. Quais procedimentos devem ser efetuados para cumprir esta tarefa?

O que nos interessa neste enunciado é a visualização do cenário de forma simplificada e reduzida, como por exemplo, a existência do departamento de RH que precisa receber um permissionamento único e dedicado a uma situação específica. A figura a seguir demonstra o cenário (de forma bem simplificada), no qual ignoramos os mil usuários e focamos apenas no local a se aplicar o permissionamento.



Este enunciado é um modelo que criei para representar uma típica questão de prova oficial, em que o texto cansativo retira o foco da pergunta e confunde o candidato. Este pequeno cenário coloca que é necessário atribuir permissões específicas a um grupo de usuários para que possa alterar um objeto em especial. Através

do assistente de delegação de controle, é possível direcionar as ações de alguns usuários sobre objetos específicos, como criar e apagar usuários, resetar senhas e ainda modificar permissões.

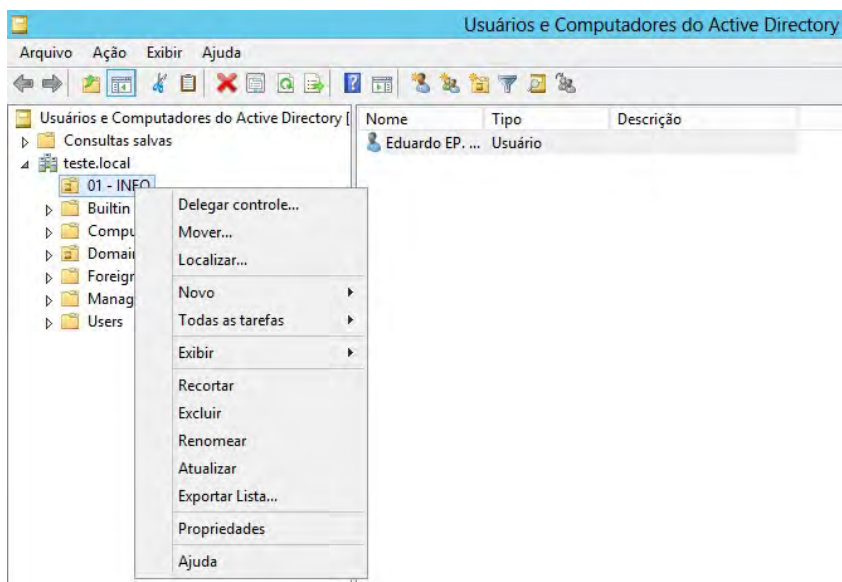


A customização do ambiente proporciona uma excelente oportunidade de controle de acesso, e deve ser seguida à risca com a devida documentação. Por meio deste assistente, podemos configurar regras simples que permitem a sua equipe de primeiro nível resetar senhas de usuários, sem a possibilidade de modificar a estrutura das unidades organizacionais. Ou ainda, pode permitir a um departamento gerenciar seus próprios usuários sem afetar os demais objetos do Active Directory.

A tarefa de organizar e regradar o uso dos recursos lógicos da TI é sim uma tarefa que exige planejamento e dedicação que leva tempo. E mesmo não sendo cobrada com tanto ênfase pelas provas do MCSA do Windows Server 2012 R2, ainda é uma excelente forma

de delegar controles específicos.

Tal delegação pode ser feita tanto pelo Active Directory Administrative Center quanto pelo Active Directory Users and Computer. Você pode ser questionado em algum momento de como acionar o Wizard, então lembre-se deste ponto em especial. A figura a seguir demonstra o acionamento do assistente através do Usuários e Computadores do Active Directory em um ambiente de testes com Windows Server 2012 R2 em idioma português Brasil. Nosso laboratório está com os termos em língua inglesa, porém você deve se adaptar ao cenário de provas.



ADMINISTRAÇÃO POR LINHA DE COMANDO

Administração por linha de comando será cobrado pela 70-410

Há muito tempo já utilizamos alguns comandos para a administração local, seja para a criação de usuários, troca de endereçamento IP, mapeamento de redes e demais atividades. Tudo o que é feito pela área gráfica do Windows fica disponível para utilização também por meio da linha de comando.

Apesar de não ser cobrado em provas oficiais, é muito útil a criação de pequenos arquivos `.BAT` para efetuar uma rotina simples de mudança de IP de uma interface de rede. Para entender a utilidade de scripts e administração por linha de comando, avalie o seguinte cenário.

Imagine um representante comercial que possui em sua casa uma rede wifi com distribuição de endereços baseado em DHCP. Esse representante comercial trabalha em uma empresa multinacional que tem endereçamento fixo para seu notebook com dados de Gateway. Este representante possui um notebook com Windows 8 instalado.

Todas as vezes que este representante comercial se desloca do

trabalho para casa, precisa alterar todas as configurações do adaptador de rede para poder usar a internet e, quando retorna ao trabalho no dia seguinte, deve novamente alterar as configurações para poder acessar a rede da empresa. Não existe a possibilidade de a empresa alterar sua estrutura interna para disponibilizar o DHCP. Como resolver este problema de forma fácil e rápida?

Este pequeno cenário pode ser resolvido apenas com uma alteração de configurações de rede, que acaba consumindo tempo e obrigando nosso usuário a possuir conhecimento mais “amplo”. Para resolver este paradigma de forma rápida, poderíamos criar dois scripts de rede, sendo que um altera as configurações do adaptador para a rede da empresa e outro com a alteração de volta para DHCP que seria usado pelo cliente em sua casa.

Depois bastaria salvar estes scripts na área de trabalho do usuário com o nome de HOME e WORK , onde HOME deveria ser executado quando estivesse em casa e WORK quando estivesse no trabalho. Uma ação muito simples que pouparia muito tempo e esforço administrativo pelo lado de clientes mais habituados, e pouparia esforço da equipe de suporte com orientações a um cliente com menos conhecimento técnico para efetuar a operação sozinho.

A administração por linha de comando faz tudo o que a administração visual faz, porém pode ser executada sequencialmente em formato de arquivos de lote, chamados de arquivos .BAT e arquivos de script, seja em PowerShell ou VBA. Existem provas mais simples chamadas de MTA, que atuam diretamente nessa questão de comandos básicos para *troubleshooting*. E se me permitem um comentário, são excelentes para atuar em formato de termômetro.

Significa que, se você não consegue passar nas provas do MTA, nem tente fazer as provas do MCSA, pois existe uma chance enorme de fracasso. As provas do MCSA possuem um nível de dificuldade

de numeração 300 em um total de 500, já as provas da certificação MTA possuem um nível de dificuldade 100 de um total de 500. São extremamente simples e direcionadas ao público acadêmico (faculdade/universidade).

Veremos agora alguns comandos relacionados ao cotidiano de administração de estações de trabalho e servidores.

- `Ipconfig` — Usado para visualização de configurações de rede e primeiro *troubleshooting* de estações que não recebem endereçamento IP através de DHCP. Para conhecer todos os seus parâmetros, utilize o `/?` após o comando `Ipconfig /?`.
 - `/all` — Mostra todas as informações.
 - `/release` — Libera o endereço utilizado.
 - `/renew` — Solicita um novo endereço.
 - `/flushdns` — Limpa o cache DNS.
 - `/registerdns` — Atualiza concessões DHCP e renova as conexões de DNS.
 - `/displaydns` — Mostra o cache de DNS local.

O `Ipconfig` é um dos primeiros comandos aprendidos pela equipe de suporte, porém o que poucas pessoas sabem é que sua variação de parâmetros permite identificar incidentes relacionados ao cache de DNS, perda de conectividade e concessões de endereçamento. É um comando muito útil que pode ser executado pela equipe de linha de frente antes do acionamento de analistas de segundo e terceiro nível.

- `Ping` — Comando usado para teste de conectividade sob uso do protocolo ICMP: `Ping <endereço IP ou nome do host>`.

O `Ping` utiliza pacotes ICMP para teste de conectividade entre estações de trabalho. Uma estação de trabalho que não recebe um

Ping pode ter os dados bloqueados pelo firewall do Windows, ou até mesmo um firewall externo. Os parâmetros a seguir complementam a funcionalidade do Ping e serão de grande utilidade para *troubleshooting* durante o cotidiano. Estes comandos são cobrados nas primeiras provas do MCSA do Windows 8 e Windows Server 2012 R2, então é bom conhecê-los.

Parâmetro	Ação
-t	Dispara contra o host especificado até ser interrompido. Para ver as estatísticas e continuar, pressione <i>Control+Break</i> ; para parar, pressione <i>Control+C</i>
-a	Resolve endereços para nomes de host
-n count	Número de requisições de eco a serem enviadas
-l size	Envia o tamanho do buffer
-f	Ativa o sinalizador <i>Don't Fragment</i> (não fragmentar) no pacote (somente IPv4)
-i TTL	Vida útil
-v TOS	Tipo de serviço (somente IPv4). Essa configuração foi preterida e não entra em vigor no campo de tipo de serviço no Cabeçalho IP
-r count	Grava a rota dos saltos de contagem (somente IPv4)
-s count	Carimbo de data/hora para saltos de contagem (somente IPv4)
-j host-list	Rota ampliada de origens com lista de hosts (somente IPv4)
-k host-list	Rota restrita de origens definida na lista de hosts (somente IPv4)
-w timeout	Tempo limite em milissegundos a aguardar para cada resposta
-R	Usa cabeçalho de roteamento para testar também a rota (somente IPv6). Para RFC 5095, o uso deste cabeçalho de roteamento foi substituído. Alguns sistemas podem remover as solicitações de eco se este cabeçalho for usado
-S srcaddr	Endereço de origem a ser usado
-4	Força o uso do IPv4
-6	Força o uso do IPv6

- **Tracert** — Comando utilizado para teste de

conectividade de verificação de saltos entre um ponto A e um ponto B: Tracert <endereço IP ou host> .

- Arp — Usado para verificação das tabelas de conversão de endereços IP, sendo útil para descobrir, por exemplo, um endereçamento MAC de uma estação de trabalho ou servidor após a execução do comando Ping : Arp -a .

Parâmetro	Ação
-a	Exibe entradas ARP atuais interrogando os dados de protocolo atuais. Se <i>inet_addr</i> for especificado, somente os endereços IP e físicos do computador especificado serão exibidos. Se mais de uma interface de rede usar ARP, serão exibidas as entradas para cada tabela ARP
-g	O mesmo que -a
-v	Exibe as entradas ARP atuais no modo detalhado. Todas as entradas inválidas e entradas na interface de loopback serão mostradas
inet_addr	Especifica um endereço internet
-N if_addr	Exibe as entradas ARP para cada interface de rede especificada por <i>if_addr</i>
-d	Exclui o host especificado por <i>inet_addr</i> . O <i>inet_addr</i> pode ser marcado com o caractere * para exclusão de todos os hosts
-s	Adiciona o host e associa o endereço internet <i>inet_addr</i> ao endereço físico <i>eth_addr</i> . O endereço físico é passado como 6 bytes hexadecimais separados por hífens. A entrada é permanente
eth_addr	Especifica um endereço físico
if_addr	Caso esteja presente, especifica o endereço internet da interface cuja tabela de conversão de endereços deve ser modificada. Caso contrário, é usada a primeira interface aplicável

- Route Print — Usado para visualizar a tabela de roteamento interna do Windows: Route print .

```

C:\Users\Administrador>route print

Lista de interfaces
=====
14...02 b3 96 28 fa 6c .....Microsoft Failover Cluster Virtual Adapter
12...00 15 5d 2f 14 00 .....Adaptador de Rede Microsoft Hyper-U
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP
15...00 00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP #2
=====

Tabela de rotas IPv4
=====
Rotas ativas:
Endereço de rede      Máscara      Ender. gateway      Interface      Custo
0.0.0.0               0.0.0.0       192.168.0.1         192.168.0.10   261
127.0.0.0             255.0.0.0     No vínculo          127.0.0.1      306
127.0.0.1             255.255.255.255 No vínculo          127.0.0.1      306
127.255.255.255       255.255.255.255 No vínculo          127.0.0.1      306
192.168.0.0           255.255.255.0 No vínculo          192.168.0.10   261
192.168.0.10          255.255.255.255 No vínculo          192.168.0.10   261
192.168.0.255         255.255.255.255 No vínculo          192.168.0.10   261
224.0.0.0             240.0.0.0     No vínculo          127.0.0.1      306
224.0.0.0             240.0.0.0     No vínculo          192.168.0.10   261
255.255.255.255       255.255.255.255 No vínculo          127.0.0.1      306
255.255.255.255       255.255.255.255 No vínculo          192.168.0.10   261
=====

Rotas persistentes:
Endereço de rede      Máscara      Ender. gateway      Interface      Custo
0.0.0.0               0.0.0.0       192.168.0.1         Padrão
=====

Tabela de rotas IPv6
=====
Rotas ativas:
Se destino de rede de métrica      Gateway
1      306 ::1/128                      No vínculo
1      306 ff00::/8                      No vínculo
=====

Rotas persistentes:
Nenhuma

```

- Shutdown — Utilizado para resetar ou desligar uma estação de trabalho ou servidor. Para conhecer todos os parâmetros do shutdown, use o `?/` : Shutdown `-f -r` .
- Net user — Utilizado para criação, remoção e visualização de usuários locais: Net user .

```
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>net user
Contas de usuário para \\AD-AMB-TEST
-----
Administrador          Convidado          edupopov
krbtgt
Comando concluído com êxito.

C:\Users\Administrador>
```

- Hostname — Usado para verificação do nome do equipamento: hostname .

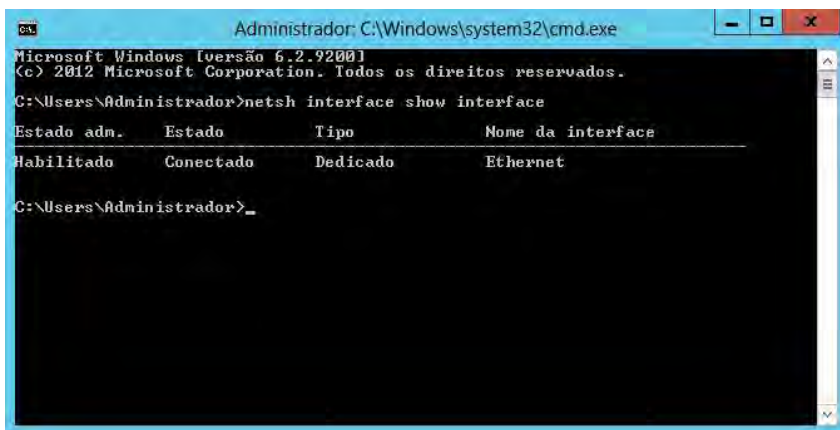
```
Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [versão 6.2.9200]
(c) 2012 Microsoft Corporation. Todos os direitos reservados.
C:\Users\Administrador>hostname
AD-AMB-TEST
C:\Users\Administrador>
```

- Netsh — Ferramenta de extrema flexibilidade permitindo a troca de endereços IP, configuração de interface de rede, configuração de firewall e demais configurações. É realmente um dos comandos mais úteis e interessantes que utilizamos. Para conhecer todas as ações possíveis, use o parâmetro /? .

Faremos aqui a utilização de ações rápidas mais usuais, que podem ser cobradas na prova e que, com certeza, serão cobradas de

você no mundo real:

- Configurar placa de rede: `netsh interface ip set address "Rede Local" gateway = 10.0.0.1 gwmetric = 2`
- Alteração de IP na interface para endereço DHCP: `netsh interface ip set address name="Rede Local" source=dhcp`
- Listar as interfaces de rede: `netsh interface show interface`



```
Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [versão 6.2.9200]
(c) 2012 Microsoft Corporation. Todos os direitos reservados.
C:\Users\Administrador>netsh interface show interface

Estado adm.   Estado      Tipo        Nome da interface
-----
Habilitado    Conectado   Dedicado    Ethernet

C:\Users\Administrador>_
```

- Renomear interface de rede: `netsh interface set interface Ethernet newname="CPD07"`
- Desativar placa de rede: `set interface name="Conexão Ethernet com Fio" admin=DISABLED`
- Ativar placa de rede: `set interface name="Conexão Ethernet com Fio" admin=ENABLE`

Esta atividade é muito comum quando em uma ponta do suporte está o especialista e, em outra, o técnico novato ou cliente com pouca ou nenhuma experiência. O simples fato de ativar uma placa de redes pode se tornar um verdadeiro desafio, facilmente resolvido com um script que efetua o processo. Você pode criar um script que ativa uma interface de rede, ou encaminhar a um cliente através de e-mail que será lido em outro equipamento, copiado a um pen drive e executado no computador onde a interface está desativada. Muito simples e útil. Também útil para o cenário no qual o usuário possui um modem 3G conectado e informa que o acesso à internet só ocorre desta forma, não sendo possível navegar pela rede interna.

- Alterando o DNS da placa de rede: `netsh interface ip set dns "Rede Local" source=static addr=200.200.200.200 register=PRIMARY`
- Reset de configuração de rede: `netsh winsock reset`

O comando `netsh winsock reset` permite “limpar as configurações de rede”, por assim dizer. Ele reseta todas as configurações de rede (útil quando não for possível requisitar um IP ao DHCP Server).

- Resetar configurações de Firewall: `netsh firewall reset`

Muito útil em situações nas quais o firewall recebeu uma série de modificações e agora precisa retornar a seu estado original. Muito comum quando aproveitamos o hardware de servidores em forma de um servidor legado que será realocado para outra atividade. Imagine um servidor que oferecia suporte a uma aplicação e que agora será realocado para outra atividade distinta, na qual as portas de acesso serão completamente diferentes. Antes de retirar um servidor legado, é interessante efetuar a limpeza das configurações do firewall.

- Ver as configurações atuais do firewall: `Netsh firewall show config`
- Habitando gerenciamento remoto: `Netsh advfirewall set currentprofile settings remotemanagement enable`
- Criação de regras do firewall do Windows com liberação de portas e aplicações:
 - `netsh advfirewall firewall add rule name="My Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes`
 - `netsh advfirewall firewall add rule name="My Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes remoteip=157.60.0.1,172.16.0.0/16,LocalSubnet profile=domain`
 - `netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow`

```
◦ netsh advfirewall firewall add rule  
  name="Block Type 13 ICMP V4"  
  protocol=icmpv4:13,any dir=in  
  action=block
```

4.1 POWERSHELL

O Windows PowerShell é um shell de linha de comando e linguagem de script, baseado em tarefas e muito similar ao utilizado hoje por plataformas open, como o Linux. Sua criação foi direcionada especialmente para a administração de sistemas baseados em Windows, por exemplo, o Windows Server 2012 R2.

É possível instalar o PowerShell com comandos mais limitados para versões como Windows Server 2003 por meio de um pacote específico. Criado em uma estrutura .NET, o Windows PowerShell ajuda os Administradores de Rede e até usuários a controlar e automatizar a administração do sistema operacional Windows e os aplicativos que são executados em Windows. O PowerShell também está presente no Windows 8, 8.1 e 10.

Os comandos incorporados do Windows PowerShell são chamados `cmdlets` (*commandlets*), e permitem que o administrador de redes gerencie computadores e servidores em uma empresa pela linha de comando. O PowerShell também pode ser usado para administração de ambientes com servidores Exchange para envio e recebimento de e-mails, fornecendo uma forma fácil e rápida para importação e exportação de usuários, relatórios e administração geral. É uma ferramenta extremamente útil e completa que é, inclusive, cobrada diretamente em todas as provas do MCSA do Windows Server 2012 R2 e no MCSA do Windows 8.

Ao contrário da maioria dos shell scripts que aceita e retorna textos, o Windows PowerShell é compilado sobre o CLR (Common

Language Runtime) do .NET Framework e sobre o .NET Framework, e aceita e retorna objetos do .NET Framework. Essa alteração fundamental no ambiente apresenta ferramentas e métodos totalmente novos para o gerenciamento e a configuração do Windows.

O Windows PowerShell versão 4.0 vem de forma nativa no Windows Server 2012 R2 e Windows 8.1, porém é possível a instalação de uma versão mais antiga em sistemas operacionais anteriores por meio de um pacote de atualizações. Adiante segue uma lista de sistemas operacionais que apresentam suporte à instalação do PowerShell 2.0:

- Windows Server 2008 com Service Pack 1
- Windows Server 2008 com Service Pack 2
- Windows Server 2003 com Service Pack 2
- Windows Vista com Service Pack 2
- Windows Vista com Service Pack 1
- Windows XP com Service Pack 3

O Windows 7 pode receber a instalação do PowerShell 3.0 que é nativo do Windows Server 2012 e Windows 8.

Recursos inclusos no Windows PowerShell são:

- Commandlets (cmdlets) para a execução de tarefas comuns, como gerenciamento de registro, serviços, processos e logs de eventos, usando a instrumentação de gerenciamento do Windows.
- Uma linguagem de script baseada em tarefas e suporte para scripts existentes e ferramentas de linha de comando.
- Simplificada, a navegação baseada em comandos do sistema operacional permite aos usuários navegar pelo registro e outros repositórios de dados usando as

mesmas técnicas usadas para navegar pelo sistema de arquivos.

- Recursos de manipulação de objetos potentes. Objetos que podem ser diretamente manipulados ou enviados para outras ferramentas ou bancos de dados.
- Interface extensível. Provedores de software independentes e desenvolvedores empresariais podem criar ferramentas padronizadas e utilitários para administrar seus softwares.

IMPORTANTE

Design consistente. Como os `cmdlets` e os repositórios de dados do sistema usam sintaxes comuns e convenções de nomenclatura, os dados podem ser compartilhados facilmente e a saída de um `cmdlet` pode ser usada como a entrada para outro `cmdlet`, sem a necessidade de reformatação ou manipulação.

Os `cmdlets` são organizados de forma simples como um verbo-substantivo em termos da língua inglesa. Segue uma relação de alguns exemplos de formatos de `cmdlets` e sua função original.

Verbo	Função	Comando	Explicação
Get	Obter	Get-Location	Obter o diretório atual
Set	Alterar	Set-Location	Alterar o diretório atual. Este comando pode ser utilizado para modificar propriedades gerais de usuários através do substantivo <i>ADUser</i>
Copy	Copiar	Copy-Item	Copiar arquivos
			Remover um arquivo ou diretório. Também pode

Remove	Remover	Remove-Item	excluir usuários quando utilizado com o substantivo <i>ADUser</i>
Move	Mover	Move-Item	Mover um arquivo
Rename	Renomear	Rename-Item	Renomear um arquivo
New	Criar um novo	New-Item	Criar um novo arquivo vazio ou diretório. Este comando também pode ser utilizado para criação de usuários com o substantivo <i>ADUser</i>
Unlock	Desbloqueia	Unlock-ADAccount	Desbloqueia uma conta de usuário quando ela é bloqueada depois de exceder o número aceito de tentativas de login incorretas
Set	Alterar	Set-ADAccountPassword	Redefine a senha de uma conta de usuário
Set	Alterar	Set-ADAccountExpiration	Modifica a data de expiração de uma conta de usuário
Enable	Ativa	Enable-ADAccount	Habilita uma conta de usuário
Disable	Desativa	Disable-ADAccount	Desabilita uma conta de usuário

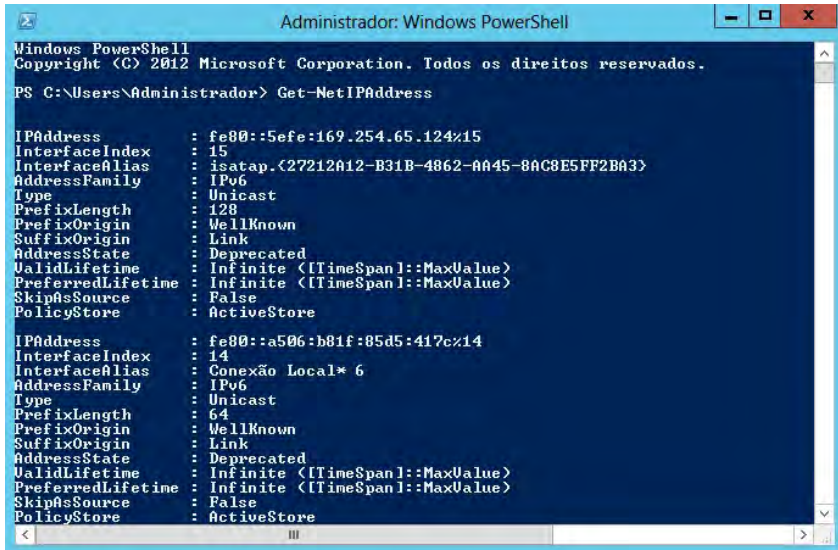
Para se adaptar com os comandos do PowerShell, é possível, por exemplo, efetuar testes para obtenção de informações do equipamento, como endereço IP, protocolos e portas utilizados por um programa e diversas outras ações. Efetue os comandos a seguir em ordem, e note a apresentação do resultado na tela de seu computador. O primeiro comando utilizado pelo PowerShell efetua a criação de um usuário chamado Fulano da Silva com a solicitação de senha através de um prompt.

```
New-ADUser "Fulano Silva" -AccountPassword (Read-Host -AsSecureString "Digitar senha") -Department IT
```

O comando a seguir apresenta informações completas de todas as interfaces de redes disponíveis no computador onde é executado. Este comando mostra desde endereçamento IP ao tipo de tráfego e o prefixo da interface. É usado para *troubleshooting* mais completo

quando alguma aplicação apresenta problemas. Existem comandos mais simples e objetivos caso você precise apenas verificar o endereçamento IP de um servidor ou estação de trabalho.

Get-NetIPAddress



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. Todos os direitos reservados.

PS C:\Users\Administrador> Get-NetIPAddress

IPAddress      : fe80::5efe:169.254.65.124%15
InterfaceIndex : 15
InterfaceAlias  : isatap.{27212A12-B31B-4862-AA45-8AC8E5FF2BA3}
AddressFamily   : IPv6
Type            : Unicast
PrefixLength    : 128
PrefixOrigin    : WellKnown
SuffixOrigin    : Link
AddressState    : Deprecated
ValidLifetime   : Infinite <[TimeSpan]::MaxValue>
PreferredLifetime : Infinite <[TimeSpan]::MaxValue>
SkipAsSource    : False
PolicyStore     : ActiveStore

IPAddress      : fe80::a506:b01f:85d5:417c%14
InterfaceIndex : 14
InterfaceAlias  : Conexão Local* 6
AddressFamily   : IPv6
Type            : Unicast
PrefixLength    : 64
PrefixOrigin    : WellKnown
SuffixOrigin    : Link
AddressState    : Deprecated
ValidLifetime   : Infinite <[TimeSpan]::MaxValue>
PreferredLifetime : Infinite <[TimeSpan]::MaxValue>
SkipAsSource    : False
PolicyStore     : ActiveStore
```

O comando a seguir é mais específico e apresenta em sua tela apenas configurações do adaptador de redes disponível como seu nome, ID, tipo, servidor DNS e endereçamento IP.

Get-NetIPConfiguration



```
Administrador: Windows PowerShell

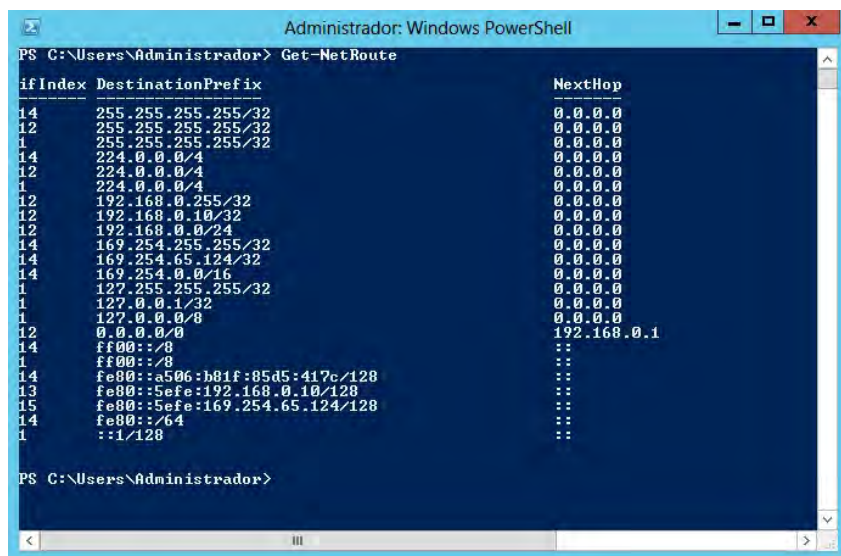
PS C:\Users\Administrador> Get-NetIPConfiguration

InterfaceAlias : Ethernet
InterfaceIndex  : 12
InterfaceDescription : Adaptador de Rede Microsoft Hyper-V
NetProfile.Name : teste.local
IPv4Address     : 192.168.0.10
IPv4DefaultGateway : 192.168.0.1
DNSServer       : 127.0.0.1

PS C:\Users\Administrador>
```

O comando `Get-NetRoute` apresenta as rotas configuradas em um servidor e seus caminhos, exatamente como em qualquer equipamento roteador. O Windows pode conhecer redes e sub-redes se nele for configurado de forma correta.

Get-NetRoute



```

PS C:\Users\Administrador> Get-NetRoute

ifIndex DestinationPrefix NextHop
-----
14      255.255.255.255/32      0.0.0.0
12      255.255.255.255/32      0.0.0.0
1       255.255.255.255/32      0.0.0.0
14      224.0.0.0/4             0.0.0.0
12      224.0.0.0/4             0.0.0.0
1       224.0.0.0/4             0.0.0.0
12      192.168.0.0/24          0.0.0.0
12      192.168.0.10/32         0.0.0.0
12      192.168.0.0/24          0.0.0.0
14      169.254.255.255/32      0.0.0.0
14      169.254.65.124/32       0.0.0.0
14      169.254.0.0/16          0.0.0.0
1       127.255.255.255/32      0.0.0.0
1       127.0.0.1/32            0.0.0.0
1       127.0.0.0/8             0.0.0.0
12      0.0.0.0/0               192.168.0.1
14      ff00::/8                ::
1       ff00::/8                ::
14      fe80::a506:b81f:85d5:417c/128 ::
13      fe80::5efe:192.168.0.10/128 ::
15      fe80::5efe:169.254.65.124/128 ::
14      fe80::/64               ::
1       ::1/128                 ::
  
```

O comando `Get-NetTCPConnection` permite a visualização das conexões ativas e suas respectivas portas de acesso. Muito útil em situações nas quais a aplicação precisa de uma conexão específica através de uma determinada porta. Hoje é muito comum aplicações como ERPs e CRMs usarem saídas por portas determinadas.

Get-NetTCPConnection


```

Administrador: Windows PowerShell
PS C:\Users\Administrador> Get-NetTCPConnection

LocalAddress      LocalPort RemoteAddress
-----
::1               56572   ::1
::1               49337   ::1
::               49206   ::
::1               49201   ::1
::1               49192   ::1
::               49189   ::
::               49165   ::
::               49158   ::
::               49157   ::
::1               49155   ::1
::1               49155   ::1
::1               49155   ::1
::               49155   ::
::               49154   ::
::               49153   ::
::               49152   ::
::               47001   ::
::               9389    ::
::               5985    ::
::               593     ::
::               464     ::
::               445     ::
::               135     ::
::               88      ::
::1               53      ::
127.0.0.1         54577   127.0.0.1
192.168.0.10      54561   192.168.0.10
192.168.0.10      54554   192.168.0.10
0.0.0.0           49206   0.0.0.0
  
```

O comando a seguir demonstra o uso do PowerShell para identificação de usuários e seu último logon efetuado permitindo a validação da data de sua última atividade. Muito utilizado em empresas em que a comunicação não é boa quanto ao desligamento de funcionários. Este comando pode consumir tempo de processamento dependendo do tamanho de sua estrutura física e quantidade de usuários.

`Get-ADUser -Filter * -Properties "LastLogonDate" | sort-object -property lastlogondate -descending | Format-Table -property name, lastlogondate -AutoSize`

```

Administrador: Windows PowerShell
PS C:\Users\Administrador> Get-ADUser -Filter * -Properties "LastLogonDate" | sort-object -property lastlogondate -descending | Format-Table -property name, lastlogondate -AutoSize

name                lastlogondate
-----
Administrador       08/12/2014 14:38:27
Eduardo EP. Popovici 14/10/2014 07:53:26
Convidado
krbtgt
PS C:\Users\Administrador>
  
```

O comando `New-ADUser` permite a inclusão de um usuário ao Active Directory, e deve ser utilizado com o apontamento completo de sua unidade organizacional e domínio. Pelo comando a seguir, é possível identificar que o usuário `Fulano` foi criado na unidade organizacional `Informática` dentro do domínio `treinamento.htbraz`. Nos laboratórios serão demonstrados todos os passos para a criação de grupos e usuários, além de sua ativação e atribuição de senhas.

```
New-ADUser -Name "Fulano da Silva" -DisplayName "Fulano Silva e Silva" -GivenName Fulano -Surname Silva -Path "OU=Informatica,dc=treinamento,dc=htbraz"
```

DICA

Para ir bem no mundo real e nas provas da Microsoft, é importante praticar através dos laboratórios e simulados. Sem estes itens, é muito difícil fixar o conhecimento adquirido.

O comando exemplificado a seguir usa o PowerShell em um servidor Exchange para validar estatísticas de uso da caixa dos usuários efetuando sua gravação em um arquivo de extensão `.CSV`. Muito útil e eficiente, este comando permite a aquisição de um relatório preciso do consumo das caixas.

O comando é complexo e gera o arquivo em extensão `.CSV`, já colunado e separado, evitando o manuseio mais complexo por Excel, tornando a vida dos usuários e administradores muito mais simples. Note que os próximos exemplos utilizam exatamente o verbo da tabela anterior acompanhado por um substantivo.

Como não temos em nosso laboratório uma estrutura preparada para o Exchange Server, não teremos uma resposta positiva para

este comando, ficando apenas como exemplo de como pode se tornar útil e complexo uma boa escrita em PowerShell.

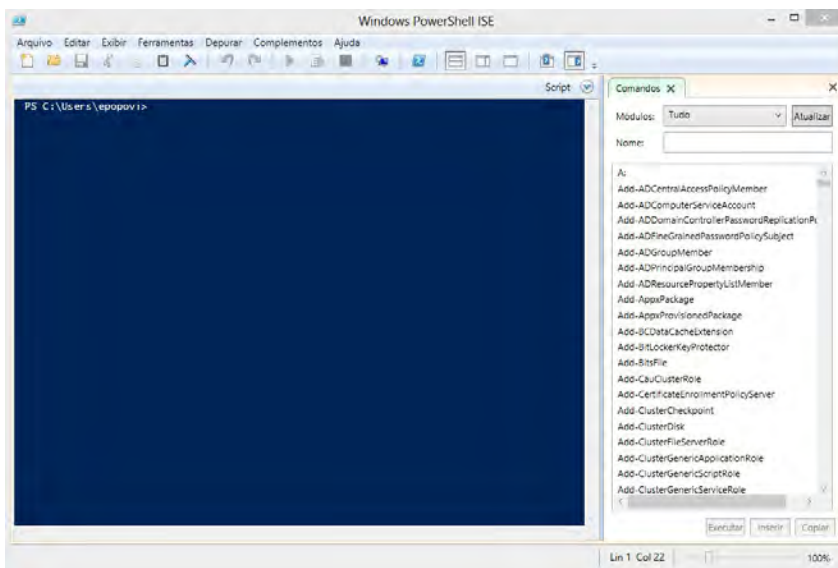
```
Get-Mailbox | Get-MailboxStatistics | where {$_.ObjectClass -eq "Mailbox"} | Sort-Object TotalItemSize -Descending | ft @{label="User";expression={$_.DisplayName}},@{label="Total Size (MB)";expression={$_.TotalItemSize.Value.ToMB()}},@{label="Items";expression={$_.ItemCount}},@{label="Storage Limit";expression={$_.StorageLimitStatus}} -auto > \\192.168.0.1\PastaCompartilhada\LogExchange.csv
```

4.2 POWERSHELL ISE

O PowerShell ISE é exatamente o mesmo PowerShell, porém com uma interface de assistência na qual é possível depurar, gravar e salvar scripts através de uma interface gráfica amigável. Muito usado por iniciantes e experts em scripts do PowerShell.

O PowerShell ISE apresenta de forma nativa um corretor ortográfico da sintaxe de linha de comando, permitindo que você corrija scripts prontos de forma simplificada. Você pode usar itens de menu e atalhos de teclado para executar muitas das tarefas que executaria no Console do Windows PowerShell. Por exemplo, ao depurar um script no Windows PowerShell ISE, para definir um ponto de interrupção de linha, clique com o botão direito do mouse na linha de código e, em seguida, clique em *Ativar/Desativar Pontos de Interrupção*.

Para acionar o PowerShell ISE, é possível utilizar as teclas de atalho `Winkey + R` (abre o executar) no Windows 8 ou Windows Server 2012, e depois digitar `powershell_ise.exe`. A tela do PowerShell ISE é mais completa e rica em detalhes, ficando no canto direito da tela os commandlets e no topo a barra de ferramentas que permite executar scripts. Para baixar e atualizar os manuais de apoio sobre o PowerShell ISE, use o commandlet `update-help`.



Será cobrado de você nesta primeira prova do MCSA, a 70-410, o conhecimento básico sobre Windows PowerShell e PowerShell ISE. Porém, conforme seus estudos avançarem dentro da certificação, a cobrança alcançará níveis mais complexos, como por exemplo, a instalação de uma controladora HBA de um Storage em um servidor com Hyper-V Server 2012 R2 através de linha de comando, ou a administração de um servidor em ambiente Server Core.

É importante frisar aqui que a extensão dos scripts de PowerShell será salva como `.ps1`, e sua execução pode ser efetuada clicando com o botão direito sobre o arquivo e selecionando *Run with PowerShell*.

4.3 CSVDE

O `csvde` é uma ferramenta já conhecida e cobrada em questões relacionadas ao MCSA, em que sua principal funcionalidade é

importar e exportar conteúdo do Active Directory, em algum momento muito útil para trabalhar com um grande volume de inserções através de arquivos de texto.

Imagine uma pequena empresa de eventos que precisa cadastrar cerca de dois mil promotores em um Active Directory de um fabricante automotivo. Eles não possuem acesso ao Active Directory e precisam fornecer um arquivo detalhado com o nome, login e e-mail dos promotores por meio de um arquivo de extensão `.csv`, facilmente gerado por programas como Excel e Access. O administrador de redes, por sua vez, precisa apenas validar o arquivo `.csv` e importar para uma unidade organizacional específica dentro do domínio. Veja a próxima figura.

```
csvde -f c:\objetos.csv  
csvde -d "ou=RH,dc=htbraz,dc=net" -f c:\RH.csv  
csvde -r objectClass=user -f c:\usuariosOnLine.csv  
csvde -r objectClass=Computer -f c:\usuariosOnLine.csv
```

O `csvde` é uma ferramenta baseada em linha de comando que exporta ou importa objetos do Active Directory para uma Unidade Organizacional a partir de um arquivo de dados separados por vírgula (`.csv`). Muitos aplicativos fabricados por terceiros são capazes de exportar ou importar dados de arquivos `.csv`, tornando o `csvde` útil para interoperabilidade com outros aplicativos, como bancos de dados, sistemas de chamados, controles de estoque ou planilhas.

Entretanto, sua principal limitação é que ele não pode modificar objetos existentes do Active Directory. O `csvde` pode apenas criar novos objetos, como por exemplo, quando usado para criar um conjunto de novas contas de usuários, mas sem poder modificar as

propriedades das que são criadas depois. Também é possível usar `csvde` para exportar propriedades de objetos, como uma lista de usuários e seus endereços de e-mail.

Para exportar os objetos de um controlador de domínio usando `csvde`, é necessário especificar pelo menos o nome do arquivo `.csv` para o qual os dados serão exportados. Com apenas o nome do arquivo especificado, todos os objetos no domínio serão exportados, sem exceção. Esta operação pode levar horas dependendo da quantidade de objetos existentes.

`csvde -f filename`

IMPORTANTE

O `csvde` não pode editar objetos do Active Directory. É preciso tomar muito cuidado nas questões relacionadas a prova para não haver confusão com a ferramenta `Ldifde`, que possui esta característica.

A sintaxe básica para usar `csvde` de forma a criar objetos é:

`csvde -i -f <nome_do_arquivo> -k`

Parâmetro	Ação
-d RootDN	Especifica o nome distinto do contêiner a partir do qual a exportação começará. O padrão é o domínio
-p SearchScope	Especifica o escopo da pesquisa em relação ao contêiner especificado pela opção <i>-d</i> . A opção <i>SearchScope</i> pode ser <i>base</i> (somente este objeto), <i>onelevel</i> (objetos dentro deste contêiner) ou <i>subtree</i> (este contêiner e todos os subcontêineres). O padrão é <i>subtree</i>
-r Filter	Limita os objetos retornados àqueles que correspondem ao filtro. O filtro se baseia na sintaxe de consulta do protocolo LDAP
-l ListOfAttributes	Especifica os atributos a serem exportados. Use o nome LDAP para cada atributo e separe-os com vírgulas

4.4 LDIFDE

A ferramenta `Ldifde`, diferentemente da `csvde`, permite exportar, criar, modificar ou excluir objetos de um controlador de domínio com o AD DS instalado. Sua flexibilidade pode ajudar muito com administrações em larga escala, muito usadas quando empresas são assimiladas por outras e precisam de sua base de objetos migrada.

Um arquivo LDIF é baseado em texto, com blocos de linhas de programação que englobam uma única operação, como criar ou modificar um objeto de usuário. Cada linha na operação especifica algo sobre essa operação, como um atributo ou o tipo de operação. Uma linha em branco separa várias operações dentro desse arquivo, em que para cada operação em um arquivo, a linha `changetype` define a operação a ser realizada. Os valores válidos são `add`, `modify` ou `delete`. A seguir está um modelo de Script utilizado pelo `Ldifde`.

Estas ferramentas não são uma novidade e pertencem aos pré-requisitos para o MCSA tanto do Windows Server 2012 R2 quanto para suas versões anteriores, como o Windows Server 2008, por exemplo. Veja a próxima figura com um resumo rápido.

```
dn: CN=Bonnie Kearney,OU=Employees,OU=User Accounts,DC=adatum,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Bonnie Kearney
sn: Kearney
title: Operations
description: Operations (London)
givenName: Bonnie
displayName: Kearney, Bonnie
company: Contoso, Ltd.
sAMAccountName: bonnie.kearney
userPrincipalName: bonnie.kearney@adatum.com
mail: bonnie.kearney@adatum.com
```

Figura 4.12: Ldifde



4.5 DISM

A ferramenta de linha de comando `dism` é uma velha conhecida por quem presta as provas da Microsoft relacionadas a sistemas operacionais, como o MCSA do Windows 8 e até mesmo o

MCSA do Windows 7. A ferramenta `dism` não é uma novidade e será cobrada em uma enorme gama de provas Microsoft. Essa ferramenta de linha de comando será cobrada nas provas 70-410 e 70-411.

Ela é uma dos principais itens de apoio do Windows Server quando nos referimos a gerenciamento de imagens e implantações sistêmicas. A ferramenta de linha de comando `dism` é, na verdade, um gerenciador de imagem de implantação que monta um arquivo de imagem do Windows em seu formato `.wim` ou um disco rígido virtual, em formato `.vhd` ou `.vhdx`. O administrador de redes que utiliza esta ferramenta também poderá instalar, desinstalar, configurar e atualizar recursos e pacotes em imagens off-line (desligados), do Windows e imagens off-line do ambiente de pré-instalação do Windows (Windows PE).



```
Deployment Demos (run as Administrator) Send Feedback

DISM OPTIONS:

/English           - Displays command line output in English.
/Format            - Specifies the report output format.
/WinDir            - Specifies the path to the Windows directory.
/SysDriveDir       - Specifies the path to the system-loader file named
                    BootMgr.
/LogPath           - Specifies the logfile path.
/LogLevel          - Specifies the output level shown in the log (1-4).
/NoRestart         - Suppresses automatic reboots and reboot prompts.
/Quiet            - Suppresses all output except for error messages.
/ScratchDir        - Specifies the path to a scratch directory.

For more information about these DISM options and their arguments, specify an
option immediately before /?.

Examples:
DISM.exe /Mount-Wim /?
DISM.exe /ScratchDir /?
DISM.exe /Image:C:\test\offline /?
DISM.exe /Online /?

Press any key to continue . . .
```

O conhecimento sobre a utilização da ferramenta de linha de comando DISM é de grande utilidade, sendo inclusive cobrada em diversas provas, incluindo o MCSA do Windows Server 2012 2. Para um exemplo mais concreto, imagine que sua empresa possua um ambiente com cerca de 80 desktops, todos usando o Windows 7.

Você recebe a tarefa de, em poucas horas, subir um novo sistema operacional em todos os desktops. Esse novo sistema operacional será o Windows 8.1. Será necessário utilizar essa ferramenta de linha de comando para executar esta tarefa.

A próxima tabela descreve as opções e argumentos do `dism` e sua estrutura de funcionamento prático. Em especial, para a prova 70-410, utilize o `dism` para remover e instalar a interface gráfica do Windows quando não houver permissão de trabalho com o PowerShell.

Veja a seguir as suas opções:

Opção/argumento	Descrição
<code>/Append-Image</code>	Adiciona uma imagem a um arquivo <i>.wim</i> e permite comparação de novos arquivos com os recursos no arquivo <i>.wim</i> existente, especificado pelo argumento <code>/ImageFile</code> . Armazena somente uma única cópia de cada arquivo exclusivo para que cada arquivo só seja capturado uma única vez
<code>/Apply-Image</code>	Aplica uma imagem a uma unidade especificada
<code>/Capture-CustomImage</code>	Capta as mudanças de arquivos incrementais com base no arquivo específico <i>install.wim</i> para um arquivo novo, <i>custom.wim</i> , para uma imagem <i>WIMBoot</i> . Não é possível capturar um diretório vazio
<code>/Cleanup-Mountpoints</code>	Exclui todos os recursos associados a uma imagem montada que foi corrompida. Esse comando não desmonta imagens já montadas, nem exclui imagens que possam ser recuperadas com o comando <code>/Remount-Image</code>
<code>/Export-Image</code>	Exporta uma cópia da imagem especificada para outro arquivo
<code>/Get-MountedImageInfo</code>	Lista as imagens que estão atualmente montadas e as informações sobre a imagem montada, como se a imagem é válida, permissões de leitura/gravação, local de montagem, caminho do arquivo montado e índice da imagem montada

Separamos os principais parâmetros, porém o `dism` possui uma enorme gama de opções e argumentos, sendo utilizado principalmente para a administração de ambientes e imagens. Recomendo que você use como prática constante o `dism` e seu conteúdo. Este comando é tão importante que é cobrado em outras provas Microsoft como a 70-680 (Windows 7), 70-687, 70-688 (ambas do Windows 8.1), 70-411 e 70-412 (ambas do Windows Server 2012 R2). Foque neste comando o máximo que puder.

4.6 NETSH

O `netsh`, ou Network Shell, é um utilitário de linha de comando em sistemas operacionais Microsoft Windows proveniente do Windows NT que mantém até hoje sua funcionalidade. Ele é encontrado a partir do Windows NT, porém ganhou força a partir do Windows 2000, permitindo até hoje a configuração local ou remota dos parâmetros de rede, firewall e usuários em estações de trabalho locais e servidores. Não é necessário possuir permissões administrativas específicas para executar alguns dos comandos relacionados ao `netsh`, porém para outros, sim.

Veja as opções do `netsh` :

Comando	Descrição
<code>netsh interface ip show config</code>	Exibir Configuração atual de IP
<code>netsh interface show interface</code>	Exibir estado dos adaptadores de rede
<code>netsh wlan show interface</code>	Exibir estado do adaptador sem fio
<code>netsh interface ipv6 show address</code>	Exibir endereço com o protocolo <i>ipv6</i>

netsh advfirewall set currentprofile state on	Ativar firewall do Windows
netsh advfirewall set currentprofile state off	Desativar firewall do Windows
netsh interface ipset address "RedeLocal" gateway = 10.0.0.1 gwmetric= 2	Configurar nome da interface de rede para <i>RedeLocal</i> e o Gateway <i>10.0.0.1</i> com métrica <i>2</i>
netsh interface ipset address name="RedeLocal" source=dhcp	Configurar nome da interface de rede para <i>RedeLocal</i> e o modo <i>DHCP</i>
set interface name="ConexãoEthernet com Fio" admin=DISABLED	Desativar a interface de rede chamada <i>ConexãoEthernet com Fio</i> . O mesmo comando pode ser utilizado para habilitar a interface, porém com o parâmetro <i>ENABLE</i>
Netsh firewall show config	Exibe a configuração atual do firewall do Windows
Netsh advfirewall set currentprofile settings remotemanagement enable	Habilita o gerenciamento remoto em estações e servidores
netsh advfirewall firewall add rulename="MyApplication" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes	Criação de regra de entrada de um programa específico no Firewall do Windows

É comum o uso do `netsh` em arquivos `.bat` em forma de scripts para troca rápida de configurações de interface de rede. Imagine um usuário que possui uma configuração específica em sua casa e outra na empresa, sendo necessário reconfigurar seu notebook todas as vezes que se desloca de um lugar para o outro. É possível criar scripts que, com um duplo click, alterem configurações de IP, Gateway, DNS etc.

4.7 SLMGR

O `slmgr.vbs` é utilizado para validação das licenças instaladas em uma estação de trabalho ou servidor com sistema operacional

Microsoft. Por ele também é possível trocar a chave de licença sem a necessidade da formatação do equipamento ou reinstalação do sistema operacional. Porém, é necessário possuir permissões administrativas.

Este comando apresenta funcionamento positivo tanto em prompt de comando quanto pela console do Power Shell. O exemplo permite a troca de chave de ativação do Windows. A tabela a seguir apresenta alguns parâmetros mais usados para o `slmgr.vbs` que podem ser cobrados em sua prova.

Veja as opções:

Parâmetros	Descrição
-ipk	Troca da chave do Windows
-ato	Status da ativação do sistema operacional
-dli	Exibe informações do tipo de licença atualmente instalada
-xpr	Exibe a data de validade da licença instalada
-cpky	Limpa a chave do produto do registro, evitando ataque de divulgação
-rearm	Rearma (renova) a licença de testes por mais 60 dias

```
slmgr.vbs -ipkXXXXXX-XXXXX-XXXXX-XXXXX
```

4.8 NETDOM

O comando `netdom` é utilizado para a administração geral de estações de trabalho e servidores, permitindo a identificação de dados relacionados ao controlador de domínio, troca de nome de estações, associação de recursos e demais configurações. O `netdom` não é algo novo e, assim como o `netsh` visto anteriormente, é encontrado em versões anteriores do Windows Server.

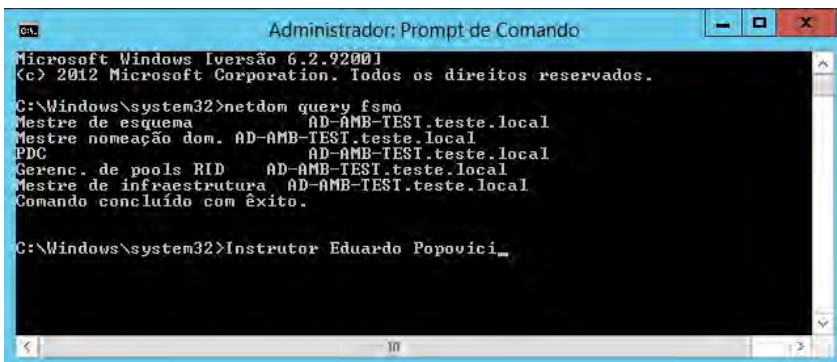
O `netdom` fica disponível assim que a função de controlador de domínio é instalada (ADDS), ou quando em uma estação de

trabalho é disponibilizada a ferramenta de administração remota RSAT .

IMPORTANTE

O `netdom` depende da instalação do ADDS e é usado para gerenciamento de características administrativas de redes baseadas em domínio. Sua ação é aplicada em computadores a partir do Windows NT até o Windows Server 2012 R2. No exemplo da figura a seguir, todas as FSMOs estão instaladas no mesmo servidor. Existem momentos em que é possível transferir as FSMOs fazendo com que fiquem em servidores diferentes para aumentar a resiliência do ambiente. Essa prática pode ser aplicada levando-se em consideração a carga de rede e requisições ao controlador de domínio.

O comando de maior utilidade para administradores iniciantes em ambiente já em produção é o `netdom query fsmo` que permite identificar qual servidor possui responsabilidade para as FSMOs. É muito importante saber onde estão alocadas as FSMOs relacionadas a florestas e domínios em seu ambiente



```
Administrador: Prompt de Comando
Microsoft Windows [versão 6.2.9200]
(c) 2012 Microsoft Corporation. Todos os direitos reservados.

C:\Windows\system32>netdom query fsmo
Mestre de esquema          AD-AMB-TEST.teste.local
Mestre nomeação dom.      AD-AMB-TEST.teste.local
PDC                        AD-AMB-TEST.teste.local
Gerenc. de pools RID      AD-AMB-TEST.teste.local
Mestre de infraestrutura   AD-AMB-TEST.teste.local
Comando concluído com êxito.

C:\Windows\system32>Instrutor Eduardo Popovici_
```

Figura 4.15: O comando `netdom query fsmo`

As vantagens do uso do `netdom` são:

1. Adiciona uma conta de servidor ou estação de trabalho ao domínio.
2. Gerencia os nomes primários e alternativos para um computador.
3. Ingressa em um servidor membro ou estação de trabalho a um domínio.
4. Move um servidor membro ou estação de trabalho para um novo domínio.
5. Consulta o domínio para informações como participação e confiança.
6. Remove um servidor ou estação de trabalho do domínio.
7. Renomeia um computador do domínio e sua conta de domínio correspondente.
8. Redefine a conexão segura entre uma estação de trabalho e um controlador de domínio.
9. Redefine a senha da conta de computador para um controlador de domínio.
10. Estabelece, verifica ou redefine uma relação de confiança entre domínios.
11. Verifica a conexão segura entre uma estação de trabalho e um controlador de domínio.

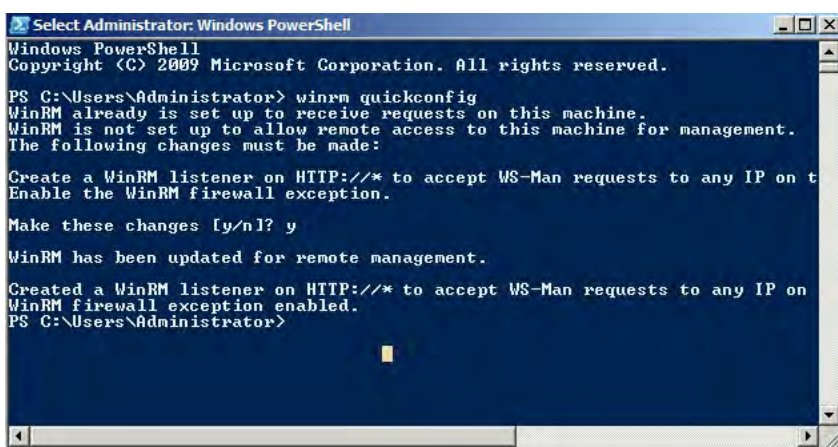
4.9 WINRM

O `winrm` pertence à lista de comando antigos da Microsoft que recebe foco nas versões atuais do Windows, sendo na verdade o gerenciamento remoto do Windows (`winrm`). É a implementação da Microsoft do protocolo WS-Management que fornece uma forma segura de se comunicar com computadores locais e remotos usando serviços web.

O gerenciamento remoto do Windows pelo `winrm` não é novo.

Ele é um componente do servidor que estiver ativo. No entanto, devo observar que ambos os computadores devem ter winrm instalado e ativado com eles para trabalhar e recuperar informações de um sistema remoto.

É possível ativar o winrm pelo comando winrm quickconfig , que habilitará a comunicação remota com outros servidores ou estações de trabalho com o RSAT instalado. Será necessária a elevação de permissionamento para executar o quickconfig .



```
Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> winrm quickconfig
WinRM already is set up to receive requests on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:
Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on t
Enable the WinRM firewall exception.
Make these changes [y/n]? y
WinRM has been updated for remote management.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on
WinRM firewall exception enabled.
PS C:\Users\Administrator>
```

Figura 4.16: O comando winrm

DICA

Este comando costuma cair na prova, fique atento.

4.10 COMMANDLETS DO POWERSHELL

O Windows PowerShell é um shell script de linha de comando baseado em tarefas de administração, criado especialmente para a administração geral de sistemas, seja ele um sistema operacional

(como o Windows Server) ou de uma aplicação específica (como o Microsoft Exchange). Os comandos incorporados ao Windows PowerShell são chamados pela literatura oficial de `cmdlets` ou `commandlets`, e permitem que você gerencie os computadores em sua empresa da linha de comando.

A prova 70-410 não exige pleno domínio de todos os `commandlets`, porém exigirá que conheça o necessário para trabalhar com a instalação Server Core e também com a instalação baseada em ambiente gráfico (GUI).

O PowerShell está em sua versão 4.0 e mantém seu desenvolvimento em estrutura de linguagem .NET, com o intuito de ajudar os profissionais de TI e usuários a controlarem e automatizarem a administração do sistema operacional Windows e os aplicativos que são executados em Windows.

A versão 4.0 do PowerShell traz três melhorias essenciais em comparação com as anteriores, que são:

- Suporte para fluxo de trabalho e depuração de script remotamente;
- Suporte de atualização da versão 3.0 para 4.0 (caso seja possível);
- Correções de bugs e melhoria de desempenho.

IMPORTANTE

A versão 1.0 do PowerShell pode ser instalada no Windows Server 2003 e Windows XP desde que possua o Microsoft.NET Framework 2.0. Entretanto, não apresentam compatibilidade com todos os `commandlets` disponíveis atualmente com a versão 4.0 nativas do Windows Server 2012 e Windows 8.

Os commandlets que você deve se lembrar e utilizar com frequência são responsáveis por situações corriqueiras efetuadas geralmente pelo Server Manager, como por exemplo, a instalação e remoção de funções e recursos de um servidor. Para trabalhar com o PowerShell, é necessário compreender o conceito básico dos comandos.

Commandlets	Descrição
Install-WindowsFeature	Instala funções e recursos do Windows Server
Uninstall-WindowsFeature	Remove funções e recursos do Windows Server
get-help	Apresenta o help de apoio aos commandlets do PowerShell
Get-NetTCPConnection	Mostra todas as conexões ativas, seus endereços e portas
Clear-DnsClientCache	Limpa o cache de DNS da estação
New-NetIPAddress	Adiciona um novo endereço IP ao equipamento
Get-NetIPAddress	Mostra os dados das interfaces de rede presentes no equipamento
Get-NetIPConfiguration	Mostra informações relevantes sobre o equipamento
Get-NetRoute	Lista todas as rotas criadas no equipamento e suas métricas
Get-Location	Obter o diretório atual (<i>Get</i> = obter)
Set-Location	Alterar o diretório atual (<i>Set</i> = Informar; configurar)
Copy-Item	Copiar arquivos
Remove-Item	Remover um arquivo ou diretório
Move-Item	Mover um arquivo
Rename-Item	Renomear um arquivo
New-Item	Criar um novo arquivo vazio ou diretório

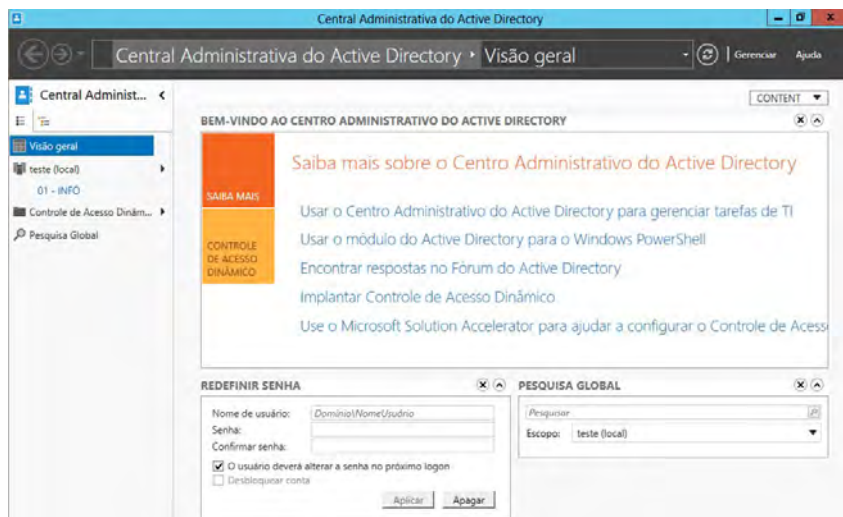
ACTIVE DIRECTORY ADMINISTRATIVE CENTER (ADAC)

Em versões mais antigas do Windows, como o Windows Server 2003 e Windows Server 2008, os administradores podem gerenciar e publicar informações em seus ambientes usando o Active Directory Users and Computers. Porém, com a chegada do Windows Server 2008 R2, foi possível assimilar uma nova forma de trabalho e administração do ambiente. Além do uso da ferramenta Active Directory Users and Computers, os administradores podem gerenciar seus objetos de serviço de diretório usando o novo Centro Administrativo do Active Directory.

O Active Directory Administrative Center permite a administração do domínio e suas atividades corriqueiras, como criação de objetos, localização de usuário e troca de senhas, além de executar ações corriqueiras da administração do domínio. O ADAC também é uma ferramenta de interface de usuário do PowerShell, no qual os administradores podem aprender e otimizar cmdlets voltados ao AD DS usando o PowerShell history.

Conforme as ações são realizadas, os comandos equivalentes serão mostrados para o usuário no visualizador do PowerShell history, permitindo aos administradores criar scripts automatizados, reduzindo o tempo para realizar tarefas. O Active

Directory Administrative Center apresenta os códigos em PowerShell de suas ações, permitindo ao usuário copiar e aprender durante suas atividades rotineiras.



Ao abrir sua interface gráfica, é possível identificar de forma rápida uma maneira objetiva para a troca de senhas de um usuário através de seu login, sem a necessidade de sua localização pelo Active Directory Users and Computers. O Active Directory Administrative Center também pode ser instalado em computadores com Windows 8 e Windows 8.1 por meio de um conjunto de ferramentas chamado de RSAT para administrar um domínio remotamente, equivalendo ao Admin Pack do Windows Server 2003.

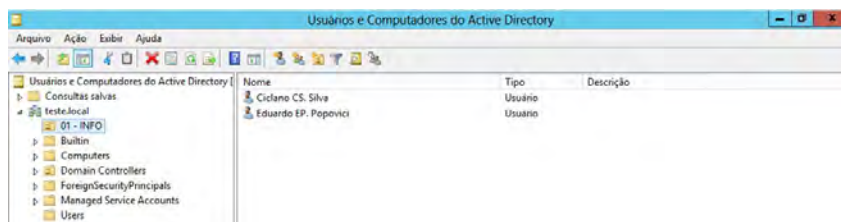
A criação de usuários está mais completa e rica em dados logo em sua área inicial, além de manter o design mais limpo e otimizado nas opções. Uma das características mais interessantes é que a opção de Exclusão Acidental está de fácil acesso, diferente do Windows Server 2008 R2, que ficava escondida nas propriedades do Active Directory Users and Computers.

A próxima figura demonstra a criação do usuário Ciclano Silva (csilva) com a marcação da opção de proteger contra exclusão accidental. Caso essa marcação esteja ativa, a conta não poderá ser apagada de forma simples. Caso você receba uma mensagem de erro ao tentar apagar um objeto, será necessário desmarcar a caixa de exclusão accidental (se não me engano, tem uma questão de prova que apresenta essa mensagem de erro).

É interessante que você utilize tanto ferramentas já consagradas pelos administradores quanto as novas de mercado. As novas ferramentas sempre são cobradas em provas, e possuem recursos e facilidades de uso que não eram contemplados em ferramentas antigas. Entretanto, as ferramentas mais antigas permitem a assimilação profissional pelo mercado de trabalho, que muitas vezes ainda tem servidores com Windows 2000 ou Windows Server 2003 instalados.

Saber lidar com ambas as ferramentas é sempre muito interessante. O Active Directory Administrative Center equivale ao Active Directory Users and Computers do Windows Server, porém

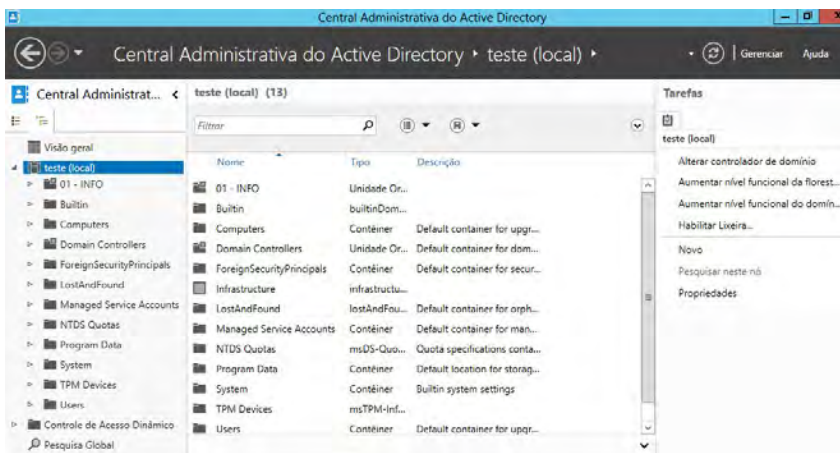
com diversos recursos diferentes. A figura a seguir demonstra o Active Directory Users and Computers.



5.1 LIXEIRA DO ACTIVE DIRECTORY

No Windows Server 2008 R2, era possível acionar (com muito custo) a lixeira do Active Directory através de LDAP, permitindo a recuperação de objetos excluídos há algum tempo. O processo agora está infinitamente mais simples e, com um único clique, é possível configurar a recuperação da lixeira do AD.

É muito provável que você seja cobrado pela prova 70-410 sobre a utilização deste excelente recurso de recuperação de objetos excluídos. Note que a próxima figura apresenta o botão **Habilitar Lixeira** no canto direito superior, quando selecionamos o controlador de domínio pelo Active Directory Administrative Center.



IMPORTANTE

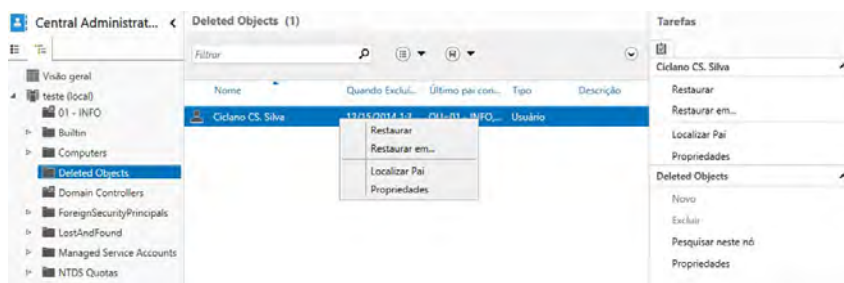
O processo de ativação da lixeira do AD é irreversível e será necessário efetuar o refresh na página do Active Directory Administrative Center. Objetos excluídos do Active Directory (AD) ficam disponíveis por até 180 dias na lixeira, permitindo sua fácil recuperação.

Você pode encontrar alguma dificuldade caso possua apenas parte do ambiente atualizado, como por exemplo, recuperações em uma floresta com Windows Server 2012 com o Exchange Server 2007. Em muitos casos, versões mais antigas do Exchange não recuperam a conta excluída em formato de caixa da mesma forma. A floresta deve estar pelo menos como Windows Server 2008 R2 para ser possível o uso da lixeira do AD.

Após a habilitação da lixeira do AD, é possível identificar uma nova unidade organizacional chamada Deleted Objects .



Ali ficam armazenados objetos excluídos do domínio como usuários e computadores. Em caso de exclusão acidental, é possível recuperar usuários e configurações específicas de acesso como horário de logon e permissões. A recuperação de objetos excluídos é feita de forma simples, pelo botão direito do mouse, permitindo a restauração no local de origem do objeto, ou ainda em local específico à escolha.



5.2 GERENCIAMENTO DE CONTAS DE USUÁRIO

Para gerenciar e administrar contas de usuários, seja por meio da linha de comando ou pela área gráfica, é necessário conhecer as ferramentas disponíveis no Windows Server. Algumas possuem características específicas, como o Active Directory Administrative Center, discutido há pouco neste livro.

Um objeto de usuário no AD DS é muito mais do que apenas propriedades relacionadas à identidade de segurança, ou à conta do usuário. Ele é a base da identidade e do acesso no AD DS. Portanto, processos consistentes, eficientes e seguros relativos à administração das contas de usuário são a base do gerenciamento da segurança corporativa.

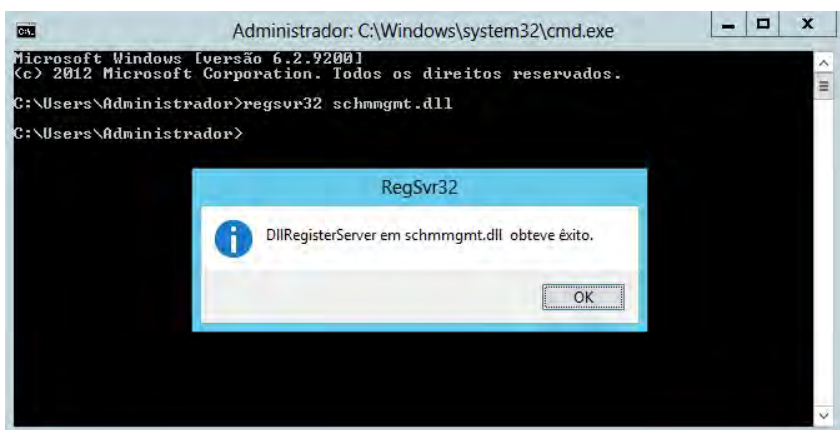
Grande parte da administração dos objetos do AD DS é administrada por ferramentas disponíveis no controlador de domínio, e acessíveis através da ferramenta RSAT em desktops com Windows 8 e Windows 8.1. Trabalharemos grande parte da rotina administrativa com as ferramentas:

Ferramenta	Descrição
Usuários e computadores do Active Directory	É um velho conhecido dos administradores de redes Microsoft, e gerencia a maioria dos recursos cotidianos comuns, incluindo usuários, grupos, computadores e OUs (unidades organizacionais). É provável que ele seja o snap-in mais usado por um administrador do Active Directory. Recebeu a partir do Windows Server 2008 a opção de proteção de exclusão acidental
Serviços e sites do Active Directory	Esta ferramenta gerencia replicação, topologia de rede e serviços relacionados. Será de extrema validade quando configurar a replicação entre controladores de domínio. Caso você precise forçar uma replicação, é aqui que devemos trabalhar as configurações
Domínios e relações de confiança do Active Directory	Este snap-in permite configurar, e mantém relações de confiança e o nível funcional da floresta. Você fará uso deste snap-in principalmente na prova 70-412, em que ambientes maiores apresentam uma complexidade maior. É possível resolver problemas de confiança entre domínio diferentes e florestas. No mundo real, é muito usado quando existe a fusão de empresas nas quais suas florestas precisam receber um certo nível de confiança e interoperabilidade
Snap-in Esquema do Active Directory	Esse snap-in examina e modifica a definição dos atributos e objetos de classe do Active Directory. Ele é o plano gráfico do AD DS, e é raramente exibido e ainda mais raramente alterado. Portanto, o snap-in Esquema do Active Directory não é instalado por padrão. Para ativá-lo, é necessário validar um arquivo .dll chamado de <i>schmmgmt.dll</i>

IMPORTANTE

Para registrar este arquivo .dll , é necessário utilizar o comando `regsvr32 schmmgmt.dll` em um prompt de comando com permissões administrativas. Este item possivelmente será cobrado de você na prova 70-410, então é muito interessante conhecer o processo de validação desse arquivo .dll .

A prova 70-410 pode cobrar de você não só o conhecimento sobre a funcionalidade desse arquivo `.dll` , mas também a forma com que é possível registrar tais arquivos com a ferramenta de linha de comando `regsvr32` . A ferramenta de linha de comando `Regsvr32` é na verdade um utilitário que registra ou cancela o registro de controles OLE, como por exemplo, os controles relacionados às bibliotecas DLLs e ActiveX no Registro do Windows. O `Regsvr32.exe` está instalado na pasta `%systemroot%\System32` a partir do Windows XP e versões posteriores do Windows. É um comando bem antigo que se faz presente em versões atuais do sistema.



Para utilizar os recursos de registro da `schmmgmt.dll` , siga os passos a seguir após efetuar o logon em um controlador de domínio:

1. Abra o prompt de comando.
2. Digite `regsvr32 schmmgmt.dll` , e pressione *Enter*.
3. Este comando registrará o arquivo `schmmgmt.dll` no computador.
4. Use as teclas de atalho `winkey + X` ; clique em *Executar* e digite `mmc /a` ; clique em *OK* ou pressione *Enter*.
5. No menu *Arquivo* dentro do `mmc` , clique em

Adicionar/remover snap-in e, em seguida, clique em *Adicionar*.

6. Em *Snap-ins Autônomos Disponíveis*, clique duas vezes em *Esquema do Active Directory*, clique em *Fechar* e em *OK*.
7. Para salvar esse console, clique em *Salvar*, no menu *Arquivo*.
8. Em *Salvar em*, aponte para o diretório `systemroot\system32`.
9. Em *Nome do arquivo*, digite `schmmgmt.msc` e clique em *Salvar*.
 - A versão de 64 bits é `%systemroot%\System32\regsvr32.exe`.
 - A versão de 32 bits é `%systemroot%\SysWow64\regsvr32.exe`.

As ferramentas de linha de comando para administração de usuários existem desde as primeiras versões do Windows Server, podendo ser cobradas pela prova 70-410 e também pela 70-411, que trata mais da parte de administração. Não faremos uma abordagem muito específica neste momento, porém é importante conhecer cada comando e sua funcionalidade básica.

Ferramenta	Descrição
Dsadd	Use para criar novos objetos
Dsget	Use para exibir objetos e as respectivas propriedades
Dsmode	Use para editar objetos e as respectivas propriedades
Dsmove	Use para mover objetos
Dsquery	Use para consultar objetos no AD DS que correspondem aos critérios fornecidos
Dsadd	Use para excluir objetos

É interessante lembrar de que, embora as contas do Active Directory sejam o foco da prova 70-410, você também pode armazenar contas de usuário no banco de dados SAM (gerenciador

de contas de segurança) local de cada computador, habilitando o logon e o acesso local aos recursos locais.

As contas de um controlador de domínio são armazenadas no banco de dados do AD DS (`ntds.dit`) e mantêm um cache local na estação em que houve o logon. Caso uma estação tenha problemas com um cabo de rede, por exemplo, qualquer usuário que possua cache local conseguirá efetuar o logon, porém não receberá atualizações até que a rede seja restabelecida.

As ferramentas de linha de comando anteriores são aplicáveis a contas armazenadas em controladores de domínio, e não se aplicam a contas locais armazenadas no arquivo `SAM` . A seguir, temos um bom exemplo do comando `dsadd` , adicionando um computador na unidade organizacional `Computer`.

```
dsadd computer cn=desktop45,ou=computers,dc=dominio,dc=teste
```

IMPORTANTE

Todo computador que adentra o domínio entra automaticamente na pasta `Computer` e, caso você deseje customizar essa opção, será necessário utilizar o comando `Redircmp.exe` . Este item tem boas chances de ser cobrado na prova 70-410, então fique atento. Para alterar o local de entrada dos computadores do domínio, utilize o comando:

```
redircmp ou=OutraOU,DC=domínio,dc=tete
```

Aqui temos alguns exemplos mais práticos da ação dos comandos e suas diretrizes primárias.

- **CSVDE** — Este comando trabalha com importação ou exportação de dados de um domínio utilizando um

arquivo .csv .

Csvde -d "ou = marketing, dc = contoso, dc = com" -f marketingobjects.csv -d indica a raiz (superior) de uma consulta específica.

CSVDE -i -f input.csv

Csvde -f output.csv

- Dsadd — Cria objetos.

dsadd user CN = Eduardo, DC = saopaulo, DC = Contoso, DC = net

- Dsmode – Modifica objetos.

dsmode computer CN = MemberServer1, CN = computadores, DC = Microsoft, DC = Com CN = MemberServer2, CN = computadores, DC = Microsoft, DC = net

- Dsrms – Remove objetos.

dsrm-subárvore - exclude - noprompt -c "OU = Marketing, DC = Contoso, DC = Com"

- Dsmove – Renomeia objetos.

dsmove "CN = Celso Lima, OU = Informatica, DC = Contoso, DC = Com" - newname "Eduardo Popovici"

- Dsquery – Localiza objetos.

dsquery user OU = Informatica, DC = Contoso, DC = Com -o upn-name Popovici *-desativado

- Dsget – Exibe propriedade de um objeto.

dsquery computer OU = Test, DC = Contoso, DC = Com-name tst * | dsget computador - desc

- Ldifde – Cria / modifica / apaga objetos.

ldifde -f exportou.ldf -s Servidor1 -d "dc=Export,dc=com" -p subtree -r "(objectCategory=organizationalUnit)" -l "cn,objectclass,ou"

5.3 CANAIS DE SEGURANÇA

Em algum momento do dia, um equipamento perde a comunicação com o Active Directory, afetando sua relação de segurança entre a conta do computador local e o controlador de domínio. Os sintomas são os mais diversos e mais comuns do que se imagina.

Durante a prova, pode ser cobrado a resolução desse problema de forma simplificada, que é a saída e entrada novamente no domínio pela estação de trabalho. Este processo redefine a relação de segurança da conta do computador local e, apesar de não ser recomendado pelos administradores de redes, funciona muito bem.

Para a prova e para o mundo real, usaremos formas mais inteligentes de corrigir este problema, pois todas as vezes que removermos um equipamento do domínio e o recolocarmos, é gerado um novo SID desse computador. O SID é um registro do computador dentro do controlador de domínio, e nele estão contidas associações, senhas e regras do objeto.

Para redefinir o canal de segurança sem a necessidade de retirar o computador do domínio (que causa a perda do SID), use o snap-in Usuários e Computadores do Active Directory, `DsMod.exe`, `NetDom.exe` ou `NLTest.exe`, e siga os seguintes passos:

1. Clique com o botão direito do mouse em um computador e clique em *Redefinir Conta*;
2. Clique em *Sim* para confirmar sua escolha;
3. Reingresse o computador no domínio e reinicie o computador.

É possível reintegrar um computador também pela linha de comando utilizando o `Dsmod`. Muito útil quando o servidor está funcionando sob uma instalação Server Core. Para efetuar a reintegração do computador, use o comando conforme demonstrado a seguir.

1. Em um prompt de comando, digite o seguinte comando:
`dsmod computer "ComputerDN" -reset .`
2. Reingresse o computador no domínio e reinicie o computador. Para redefinir o canal de segurança usando `NetDom.exe`, digite o seguinte comando em um prompt de comando, no qual as credenciais pertencem ao grupo local Administradores do computador: `netdom reset MachineName /domain DomainName /User0 UserName /Password0 {Password |*} .`

IMPORTANTE

A administração de um controlador de domínio envolve todos os objetos, seja em linha de comando ou em ambiente gráfico. Conhecer ambas as formas é um diferencial importante.

Esse comando redefine o canal de segurança tentando redefinir a senha no computador e no domínio. Portanto, ele não exige reingresso ou reinicialização. Para redefinir o canal de segurança usando `NLTest.exe`, no computador em que perdeu sua relação de confiança, digite o seguinte comando em um prompt de comando:

```
NLTEST /SERVER:SERVERNAME  
/SC_RESET:DOMAIN\DOMAINCONTROLLER .
```

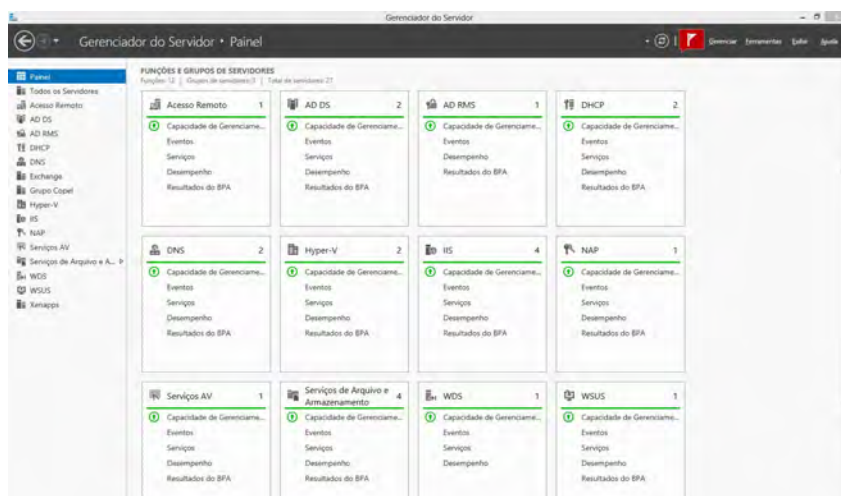
Você também pode usar o Windows PowerShell com módulo Active Directory para redefinir uma conta de computador. O exemplo a seguir demonstra como redefinir o canal de segurança entre o computador local e o domínio no qual é feito seu ingresso. Você deve executar este comando no computador local: `Test-ComputerSecureChannel -Repair .`

É possível redefinir uma conta de computador local utilizando o PowerShell, e o comando a seguir pode ser cobrado em uma prova direcionada para o MCSA. Pratique cada comando e lembre-se sempre do que faz cada parâmetro antes de efetuar a prova 70-410.

```
invoke-command -computername CPD07 -scriptblock {reset-computermachinepassword}
```

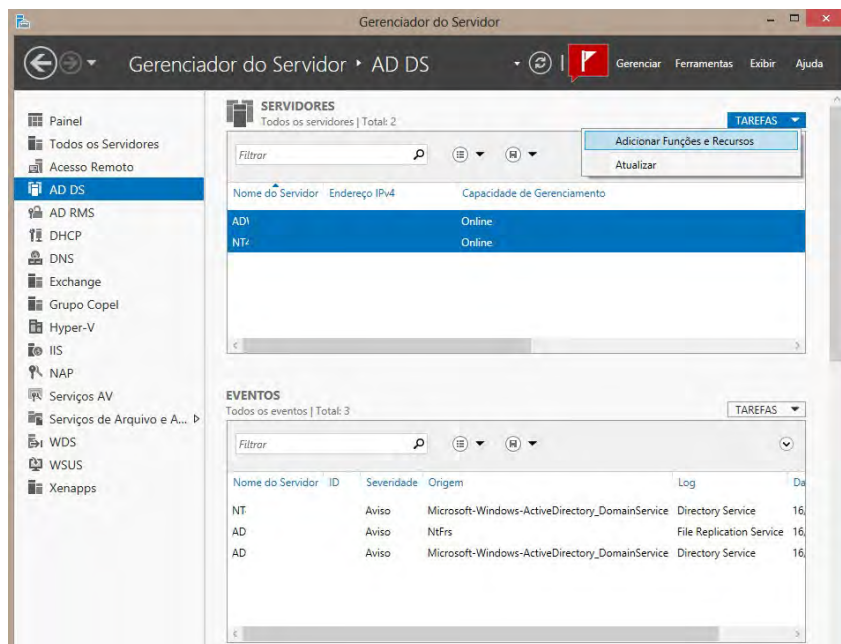
5.4 ADMINISTRAÇÃO CENTRALIZADA

É possível agrupar servidores para efetuar uma gestão mais eficiente e de forma centralizada como demonstrado pela figura a seguir. A criação de grupos de servidores é uma novidade muito interessante e que permite ao administrador de redes uma visão mais rápida do ambiente como um todo.



Essa figura foi feita em um ambiente real e funcional com o Windows Server 2012 R2. Note a composição da existência de grupos onde existem mais de um servidor por função ou atividade, como por exemplo, o IIS que está com quatro servidores ativos, ou o AD que está com dois servidores ativos. É possível instalar funções e

recursos em diversos servidores de uma única vez dentro de um grupo de servidores. A figura a seguir demonstra a facilidade de adicionar tais funções e recursos.



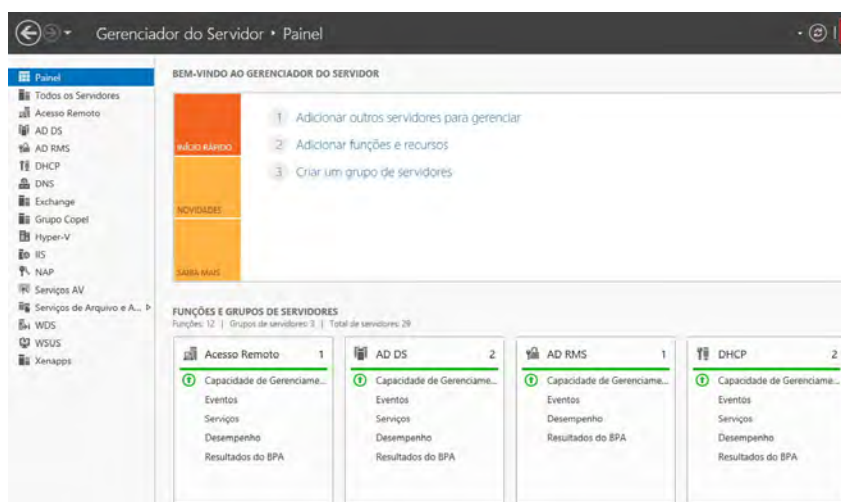
Para criar grupos de servidores pelo RSAT instalado em uma estação de trabalho, ou por qualquer servidor com o Windows Server 2012 R2 instalado, e as devidas permissões administrativas, siga os passos:

1. Abra o gerenciador do servidor.
2. No menu *Gerenciar*, logo no centro da tela, clique em *Criar Grupo de Servidores*.
3. Na caixa de texto *Nome do grupo de servidores*, digite um nome amigável para seu grupo de servidores, como *Servidores de Contabilização*.
4. Adicione servidores à lista *Selecionado do pool de servidores* ou adicione outros servidores ao grupo usando as guias *Active*

Directory, *DNS* ou *Importar*. Para obter mais informações sobre como usar essas guias, consulte *Adicionar servidores ao Gerenciador do Servidor* neste tópico.

5. Quando tiver terminado de adicionar servidores ao grupo, clique em **OK**. O novo grupo é exibido no painel de navegação do *Gerenciador do Servidor* no grupo *Todos os Servidores*.

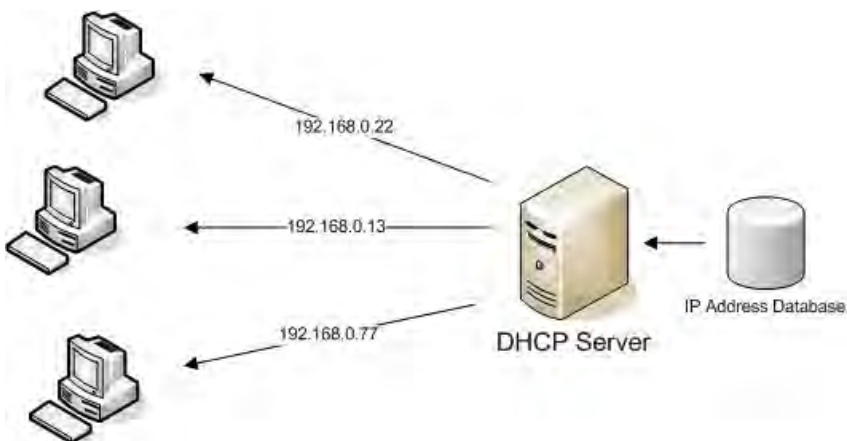
A figura a seguir demonstra bem a facilidade de criação de grupos de servidores.



DHCP

Imagine que sua equipe de suporte, composta por exatas três pessoas, precise configurar mais de dois mil equipamentos com o endereço IPV4 de uma determinada rede de classe B, em menos de oito horas. Seria extremamente cansativo, e até mesmo inviável, por mais produtivos que possam ser seus especialistas e técnicos de campo.

Existem formas mais inteligentes de configurar um grande número de estações de trabalho, ou até mesmo de instalar sistemas operacionais e replicar atualizações automáticas do Windows. O DHCP é o primeiro passo dessa inteligência e deve ser conhecido por todos que desejam alcançar qualquer certificação sobre Windows Server ou estações de trabalho.



Todas as provas do MCSA abordam o DHCP de forma única, ou seja, a cada momento teremos níveis de dificuldade diferentes para cada situação. Nesta primeira prova, será cobrado de você o conhecimento sobre a implementação do servidor DHCP, incluindo questões de filtragem de endereços, reserva de IPs, criação de escopos e o conhecimento sobre superescopos. Nas próximas páginas deste livro, tratarei não só o conceito do DHCP, mas também sua configuração em servidores que possuam o Windows Server 2012 R2 instalado.

O DHCP é um dos recursos mais antigos que existem quando falamos em servidores, e em tempos atuais se tornou algo comum inclusive em roteadores Wifi de diversos fabricantes. Com a quantidade de dispositivos que entram em nossa realidade hoje em dia, é irreal ou impensado não possuir um destes servidores dentro da infraestrutura de redes, seja ela grande ou pequena. O grande perigo de trabalhar com endereçamentos estáticos está exatamente no fato da empresa crescer sem aviso prévio.

Imagine que hoje a empresa que você suporta possui apenas vinte computadores e, em menos de seis meses, receba cerca de seiscentos dispositivos. As estruturas aumentam e diminuem de tamanho rapidamente, dependendo de como está o mercado de um país ou da relação econômica atual de seu negócio. Tudo fica contemplado em seu planejamento estratégico, porém não espere que a diretoria compartilhe esse dado.

A comunicação da TI ainda é muito falha para pequenos e médios negócios, gerando exatamente esse ruído operacional. Manter uma estrutura confiável de DHCP funcionando não é nenhum monstro de sete cabeças, e pode ser feita rapidamente por aqueles que possuem o conhecimento específico. Considere os seguintes termos chaves, *Failover* e *Balanceamento de Carga*.

O termo Dynamic Host Configuration Protocol, ou mais

conhecido como DHCP, é na verdade um Protocolo de configuração dinâmica de host, fornecendo as estações de trabalho um endereço dinâmico dentro da rede da empresa. É um protocolo construído com base em serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host, máscara de sub-rede, Default Gateway (Gateway Padrão), número IP de um ou mais servidores DNS, número IP de um ou mais servidores WINS e sufixos de pesquisa do DNS. O protocolo DHCP é, na verdade, um padrão de fato, criado em meados de outubro de 1993 com sua normatização através da RFC 2131 sobre IPV4.

O banco de dados do servidor DHCP no Windows Server 2012 R2 é dinâmico e é atualizado quando os clientes DHCP são atribuídos, ou quando liberam os respectivos parâmetros de configuração TCP/IP. Como o banco de dados DHCP não é um banco de dados distribuído, como o banco do servidor WINS, a manutenção do banco de dados do servidor DHCP é menos complexo.

Por padrão, o backup do banco de dados DHCP e das entradas de registro relacionadas é feito automaticamente em intervalos de 60 minutos, podendo ser alterado através da chave de registro: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCP\Parameters`. O backup do DHCP pode ser encontrado em `systemroot\System32\Dhcp\Backup`.

Quando sei que preciso usar um servidor DHCP em minha rede? Essa é a pergunta que deve ser feita antes de se instalar e configurar efetivamente a solução do DHCP. Separamos algumas opções que seguem muito além do simples fornecimento de endereços IP pela rede.

É importante quebrar a ideia de que o servidor DHCP serve apenas para distribuir endereços. Ele também serve para:

1. Aumentar tolerância a falhas, dividindo escopos de DHCP.
2. Eliminar atualizações manuais de registros de DNS, configurando atualização dinâmica e atualização dinâmica segura.
3. Permitir administração remota dos servidores DHCP, configurando as portas do Firewall do Windows.
4. Evitar servidores DHCP não autorizados na sua rede, autorizando servidores DHCP em AD DS.
5. Aplicar diretivas de acesso à rede para integridade do cliente, configurando DHCP com proteção de acesso à rede.
6. Automatizar o gerenciamento de dispositivos que têm endereços IP estáticos, criando reservas de DHCP.
7. Suportar várias sub-redes com um servidor DHCP configurando agentes de retransmissão DHCP.
8. Evitar reconfiguração de DHCP em um novo servidor migrando uma infraestrutura DHCP existente.
9. Balancear a carga nos servidores DHCP usando a função 80/20 para escopos.
10. Centralizar o gerenciamento de dois ou mais servidores DHCP como um sistema único, agrupando os servidores DHCP.

Para configurar uma rede utilizando o DHCP, é necessário definir alguns parâmetros como os que apresentarei a seguir.

Servidor DHCP

Qual sistema operacional será utilizado, que em nosso caso será o Windows Server 2012 R2. A configuração é a mesma para equipamentos que estão inseridos ao domínio ou não.

É possível efetuar uma série de configurações que permite manter o controle de acesso em redes segmentadas como uma rede privativa ou uma rede Guest para acesso de visitantes. O

procedimento de autorização no Active Directory é uma medida de segurança para evitar que servidores DHCP sejam introduzidos na rede sem o conhecimento do administrador.

Cliente DHCP

É qualquer dispositivo de rede capaz de obter as configurações do TCP/IP a partir de um servidor DHCP, seja um notebook, desktop, tablet ou celular, independentemente de seu sistema operacional legado. Você pode ter um tablet com Android conectado a uma rede e recebendo endereçamento IP de um servidor com Windows Server 2012 R2. O padrão de distribuição independe de fabricante, e são direcionados através de regras internacionais chamadas de RFC.

Escopo

Um escopo é o intervalo consecutivo completo dos endereços IP possíveis para uma rede (por exemplo, a faixa de 192.168.0.100 a 192.168.0.200, na rede 192.168.0.0 e máscara 255.255.255.0). Os escopos definem qual range de IP será distribuído pela rede.

Por exemplo, imagine que você tem uma rede de classe C com máscara 255.255.255.0, significando que você possui 254 endereços válidos. Você decide criar um escopo que distribuirá endereços do 100 ao 200. Ou seja, o endereço 192.168.0.100 ao 192.168.0.200 será distribuído para estações de trabalho que estejam com a configuração dinâmica. A próxima figura demonstra a configuração ativa de um servidor em produção com escopos criados, além do superescopo, que discutiremos mais adiante.

Para criar um novo escopo DHCP siga quatro passos simples:

1. Abra o snap-in *Console de Gerenciamento Microsoft* (MMC) para DHCP encontrado em *Tools* do Server Manager.

2. Na árvore de console, clique duas vezes no servidor DHCP que você deseja configurar.
3. Clique com o botão direito do mouse em IPv4 ou IPv6, e clique em *Novo Escopo*.
4. Siga as instruções do *Assistente para Novos Escopos*.

Durante a utilização do DHCP com redes mais antigas, baseadas em florestas com nível funcional Windows Server 2003, pode surgir um problema quando você utiliza o DHCP em combinação com o DNS, usando zonas integradas com o Active Directory no DNS. As zonas integradas ao Active Directory aceitam somente atualizações dinâmicas seguras. O problema surge quando o servidor DHCP cria um registro para um cliente antigo do Windows.

Como as zonas integradas somente aceitam atualizações dinâmicas seguras — isto é, de computadores autenticados no domínio e computadores com estas versões antigas não tem conta no domínio (portanto, não são autenticados no domínio) —, para contornar o problema, o servidor DHCP registra as informações no DNS em seu próprio nome, ou seja, no nome do servidor DHCP. O inconveniente deste procedimento é que o servidor DHCP torna-se o dono destes registros. Porém, os registros destes clientes mais antigos podem tornar-se órfãos, se uma das condições a seguir acontecer:

1. Se o servidor DHCP for substituído por um servidor de reserva, ou se o escopo for migrado para outro servidor DHCP. Com isso, os registros criados para clientes antigos continuarão tendo como dono o servidor antigo, que não existe mais. Ou seja, é lixo que vai se acumulando no DNS.
2. Se o cliente for atualizado para uma das versões mais novas do Windows (2000, XP ou 2003), o servidor DHCP continuará sendo o dono dos registros, porém não mais vai atualizá-los, pois agora “julga” que o próprio cliente é capaz de fazê-lo.

A solução mais simples seria migrar todos os clientes para versões mais novas do Windows, como por exemplo, o Windows 7 ou Windows 8. Outra opção é adicionar as contas de todos os servidores DHCP para o grupo `DnsUpdateProxy`.

Quando um membro do grupo cria um registro dinamicamente no DNS, não são atribuídas configurações de segurança ao registro, ou seja, o servidor DHCP não será mais o dono do registro. Isso evita que o registro fique “órfão”. Quando um outro computador qualquer modificar este registro, ele vai se tornar o dono do registro. Esta é a situação desejável quando você tem um cliente com versões mais antigas do Windows.

Neste caso, com a conta do servidor DHCP no grupo `DnsUpdateProxy`, quando o DHCP for criar os registros para o cliente mais antigo, o servidor DHCP não será configurado como dono do registro. O cliente é atualizado para uma versão mais atual do Windows. Quando o cliente tentar atualizar os registros, ele vai se tornar o dono do registro, que é o que deve acontecer com as versões mais novas do Windows. É importante citar esse tipo de configuração, pois a grande maioria das empresas ainda atua com ambiente híbrido.

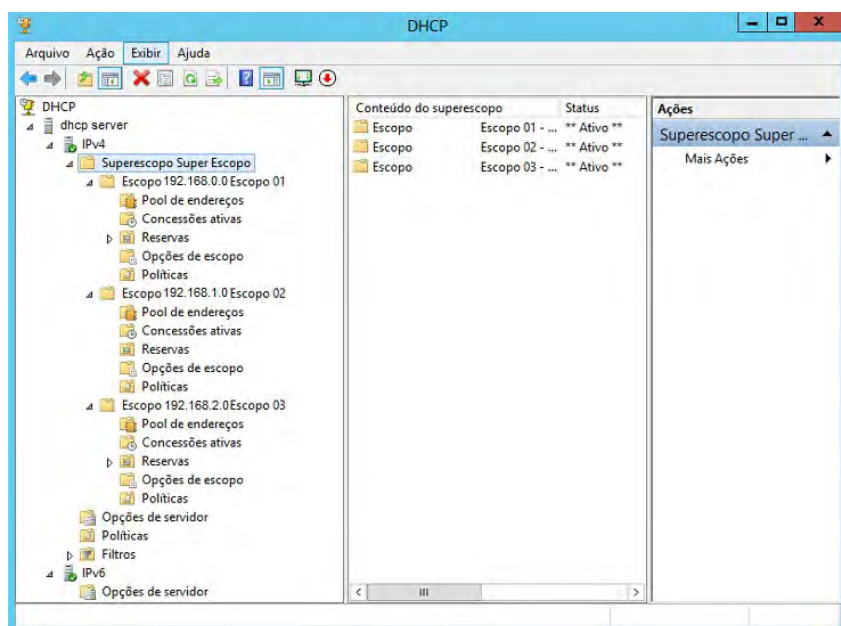
Superescopo

Um superescopo é um agrupamento administrativo de escopos que pode ser usado para oferecer suporte a várias sub-redes IP lógicas na mesma sub-rede física. É possível distribuir a segmentação de redes através de endereços diferentes, porém é necessário um roteador disponível para a tarefa.

Os superescopos contêm somente uma lista de escopos associados ou escopos filho que podem ser ativados em conjunto. Por exemplo, se todos os computadores devem receber o mesmo número IP de Default Gateway, este número tem de ser configurado

em cada escopo, individualmente. Não tem como fazer esta configuração no superescopo e todos os escopos (que compõem o superescopo) herdarem estas configurações.

O mais interessante sobre o superescopo é que pode ser utilizado para aquisição de mais equipamentos de trabalho, sem a necessidade de modificação imediata da estrutura de infraestrutura. Ou ainda, é possível segmentar departamentos por sub-rede ou segmentar filiais e sucursais de uma empresa por sub-rede. A utilização deste recurso depende muito da criatividade do administrador de redes e disposição de ativos de hardware.



Intervalo de exclusão

Um intervalo de exclusão é uma sequência limitada de endereços IP dentro de um escopo, excluído dos endereços que são fornecidos pelo DHCP. Os intervalos de exclusão asseguram que quaisquer endereços nesses intervalos não são oferecidos pelo

servidor para clientes DHCP na sua rede. Por exemplo, dentro da faixa 10.10.10.100 a 10.10.10.150, na rede 10.10.10.0/255.255.255.0 de um determinado escopo, você pode criar uma faixa de exclusão de 10.10.10.120 a 10.10.10.130. Os endereços da faixa de exclusão não serão utilizados pelo servidor DHCP para configurar os clientes DHCP.

Pool de endereços

Após definir um escopo DHCP e aplicar intervalos de exclusão, os endereços remanescentes formam o pool de endereços disponíveis dentro do escopo. Endereços em pool são qualificados para atribuição dinâmica pelo servidor para clientes DHCP na sua rede.

No nosso exemplo, onde temos o escopo com a faixa 10.10.10.100 a 10.10.10.150, com uma faixa de exclusão de 10.10.10.120 a 10.10.10.130, o nosso pool de endereços é formado pelos endereços de 10.10.10.100 a 10.10.10.119, mais os endereços de 10.10.10.131 a 10.10.10.150.

Concessão

Uma concessão é um período de tempo especificado por um servidor DHCP durante o qual um computador cliente pode usar um endereço IP que ele recebeu do servidor DHCP (diz-se atribuído pelo servidor DHCP). Uma concessão está ativa quando ela está sendo utilizada pelo cliente.

Geralmente, o cliente precisa renovar sua atribuição de concessão de endereço com o servidor antes que ela expire. Uma concessão torna-se inativa quando ela expira ou é excluída no servidor. A duração de uma concessão determina quando ela vai expirar e com que frequência o cliente precisa renová-la no servidor. Por padrão, a concessão é mantida em oito dias, porém pode sofrer

mudanças do administrador.

Reserva

Você usa uma reserva para criar uma concessão de endereço permanente pelo servidor DHCP. As reservas asseguram que um dispositivo de hardware especificado na sub-rede sempre pode usar o mesmo endereço IP. A reserva é criada associada ao endereço de hardware da placa de rede, conhecido como MAC-Address.

No servidor DHCP, você cria uma reserva, associando um endereço IP com um endereço MAC. Quando o computador (com o endereço MAC para o qual existe uma reserva) é inicializado, ele entra em contato com o servidor DHCP. O servidor DHCP verifica que existe uma reserva para aquele MAC-Address e configura o computador com o endereço IP associado ao Mac-Address.

Caso haja algum problema na placa de rede do computador e a placa tenha de ser substituída, mudará o MAC-Address e a reserva anterior terá de ser excluída e uma nova reserva terá de ser criada, utilizando, agora, o novo Mac-Address. A figura a seguir representa uma janela de reserva de estações.

6.1 TIPOS DE OPÇÃO

Tipos de opção são outros parâmetros de configuração do cliente que um servidor DHCP pode atribuir aos clientes. Por exemplo, algumas opções usadas com frequência incluem endereços IP para gateways padrão (roteadores), servidores WINS (Windows Internet Name System) e servidores DNS (Domain Name System). Geralmente, esses tipos de opção são ativados e configurados para cada escopo.

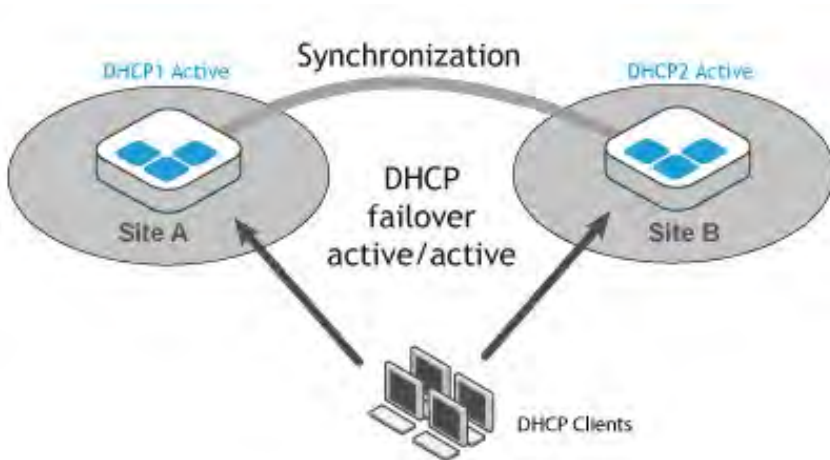
É possível direcionar detalhes de trabalho oferecidos para cada tipo de escopo informando ao usuário qual será seu servidor de DNS primário ou Gateway ativo, facilitando muito o direcionamento de tráfego de rede e carga de trabalho de analistas e administradores de redes. O console de Administração do serviço DHCP também permite a você configurar tipos de opção padrão que são usados por todos os escopos adicionados e configurados no

servidor.

DHCP Failover

A Microsoft disponibilizou a partir do Windows Server 2012 a possibilidade de criação de um Failover de servidores DHCP, permitindo que haja distribuição de endereços IP mesmo que um dos servidores fique indisponível. É possível balancear a carga de endereços entre servidores ou apenas trabalhar de forma ativo-passivo entre eles.

O DHCP Failover será cobrado em quase todas as provas do MCSA do Windows Server 2012 R2, então prepare-se muito bem com os detalhes dessa configuração. É interessante realçar que o DHCP Failover suporta no máximo dois servidores DHCP, e pode ser implementado através de console gráfico ou pelo PowerShell.



A regra chamada de 80/20 (velha conhecida pelas equipes de infraestrutura), criada pela Microsoft, se trata de uma boa prática para configuração de um balanceamento de carga, seja ele em ambientes mais complexos quanto ao balanceamento de endereços IP através do DHCP Failover.

O intuito desta técnica é o de equilibrar a quantidade de requisições e respostas entre servidores de uma rede, ou seja, direcionar e até limitar a carga de trabalho e o uso de um determinado servidor DHCP. O administrador de redes pode dividir os endereços do escopo entre os dois servidores DHCP, utilizando como receptor de requisições um servidor com 20% da carga, e para o outro servidor 80% da carga.

Este tipo de técnica é conhecido como DHCP Failover ativo-ativo (80/20). Outra forma de se utilizar é a técnica do ativo-passivo, que demanda 0% de uso para um dos servidores enquanto o outro assume 100% da carga. Essa técnica deixa um servidor completamente em espera até que o outro apresente problemas.

A prova 70-410 exige que você domine características mais simples em relação ao conceito de DHCP, deixando para a prova 70-412 a cobrança de configurações avançadas sobre o assunto.

O Windows Server 2012 e 2012 R2, diferente de seu antecessor, suporta 2 servidores em estado de Failover. No Windows Server 2008 R2, era necessário a criação de um Cluster de Failover e, só então, a inserção de servidores. Era possível também dividir os

escopos do DHCP.

Já com o Windows Server 2012 e 2012 R2, é possível criar todo o sistema de Failover sem a necessidade de um Cluster. É importante lembrar de que este ponto, apesar de introdutório neste conteúdo, é visto a fundo pela prova 70-412.

A próxima figura demonstra bem a clara diferença de formato de atuação do Windows Server 2008 R2 para o Windows Server 2012 e 2012 R2:



Automatic Private IP Addressing (APIPA)

No Microsoft Windows 98, houve a introdução de uma funcionalidade extremamente interessante, chamada de APIPA. Esta funcionalidade está presente em versões mais antigas, passando pelo Windows 2000, Windows ME, Windows XP, Windows Vista e em versões mais novas como o Windows 7, Windows 8, Windows 8.1 e Windows 10, além de toda a família de sistemas operacionais para servidores como o Windows Server 2003 até o Windows Server 2012 R2.

Este sistema de fornecimento de endereços automáticos é

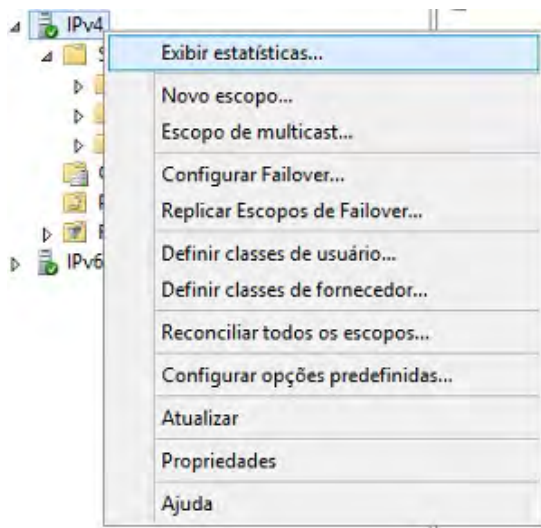
acionado quando não é identificado um servidor DHCP disponível. Imagine que um cliente corporativo dentro de sua estrutura de redes, com um notebook ou tablet, esteja com as configurações especificadas para obter um endereçamento TCP/IP a partir de um servidor DHCP automaticamente.

Pelo processo padrão, a estação cliente é inicializada e envia um broadcast solicitando um endereço de redes. Porém, para nosso pequeno cenário, nosso usuário não consegue se comunicar com um servidor DHCP. Antes mesmo de iniciar o *troubleshooting* (passos para solucionar o problema), é interessante entender que é a funcionalidade APIPA que assume a tentativa de aquisição de endereçamento.

Neste pequeno cenário o Windows, aciona o recurso da APIPA, e atribui um endereço de forma automática. Este endereço está na faixa de endereçamento 169.254.0.0/255.255.0.0. O endereçamento iniciado por 169 é um dos endereços especiais reservados para uso em redes internas Microsoft. Ou seja, este não seria um endereço de rede válido para a internet.

6.2 ESTATÍSTICAS DO DHCP

As estatísticas do DHCP podem ser extremamente úteis para entender configurações simples de tempo concessão, ou até mesmo da necessidade de criação de novos escopos de rede. Toda a área de estatísticas é apresentada ao se acionar o escopo com o botão direito do mouse em cima do servidor responsável pela distribuição de endereços IP, conforme demonstrado pela próxima figura. Esta visualização permite uma visão detalhada de seu ambiente, e com toda certeza será cobrado como conhecimento base para especialistas.



É importante se atentar ao crescimento da empresa ou corporação em que atua, pois caso acabem os endereços disponíveis, as estações de trabalho não receberão um endereço válido quando houver a necessidade. A próxima figura demonstra as opções disponíveis em uma configuração de escopo baseada em IPV4 trabalhando em broadcast.

Descrição	Detalhes
Hora de início	01/12/2014 14:24:14
Tempo de atividade	380 horas, 59 minutos, 38 segundos
Descobertas	983
Ofertas	983
Ofertas Atrasadas	0
Solicitações	4037
Acks	198031
Nacks	406
Recusas	1
Liberações	172
Escopos totais	3
Escopos com atraso configurado	0
Total de endereços	660
Em uso	61 (9%)
Disponível	599 (90%)

Essa figura apresenta um resumo informativo de todos os

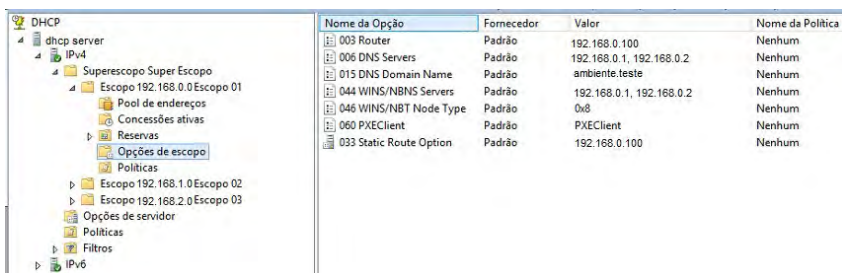
endereços disponíveis dentro de um superescopo de rede, descrevendo que ainda estão disponíveis cerca de 599 endereços (90%) de um total de 660 endereços. Apenas para constar, essa figura não representa um laboratório de testes, mas um ambiente real de trabalho em produção.

É possível notar pela figura que o tempo médio de atividade deste servidor é de mais de 380 horas com cerca de 4037 solicitações, que pelo entendimento representa uma baixa carga de trabalho. Este servidor é utilizado atualmente para manter também outras máquinas virtuais em atividades pelo Hyper-V do Windows Server 2012 R2. Particularmente, utilizo servidores DHCP como ponto de apoio, pois raramente usam todo o hardware apenas para atender requisições de endereço.

6.3 OPÇÕES DE ESCOPO

É através das configurações de escopo que podemos transferir informações importantes às estações de trabalho, como por exemplo, a possibilidade de atuação com servidores WSUS, pela entrada 060. Cada entrada de configuração possui uma numeração única, oferecendo em determinado momento uma rota para um determinado item como um roteador ou proxy, ou até mesmo um servidor WSUS e informações de domínio.

Recomendo uma boa configuração das opções de escopo e atenção a este ponto para que seus usuários não acabem ficando fora da rede por algum motivo “desconhecido”. Quando configuramos um ambiente do zero, estas opções ficam em branco e disponíveis.



Lembre-se de que este item será cobrado não só pela prova 70-410, mas também pela prova 70-411, pois está ligado exatamente como as estações de trabalho requisitam endereços pela rede. É este formato de solicitação que mantém funcionando o boot por PXE das estações de trabalho para servidores WDS.

Servidores WDS são responsáveis por distribuir imagens do Windows através da rede para uma instalação remota. Muitas empresas customizam as instalações do Microsoft Windows para atender uma demanda específica, seja ela relacionada a segurança ou apenas economia de tráfego e rede para a replicação de imagens .win .

Apesar de comentar sobre o WDS neste livro, não farei a abordagem mais aprofundada, visto que trata-se de um assunto específico para a prova 70-411. Recomendo que você, leitor, pratique sempre laboratórios práticos para consolidar tudo o que o conteúdo teórico lhe apresenta.

DNS

O DNS, ou Domain Name System, é um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à internet, intranet ou rede corporativa e privada. Ele baseia-se em nomes simplificados, permitindo a associação de nomes textuais aos endereços IP públicos ou privados. É de extrema importância e largamente utilizado em quase todos os itens relacionados a redes de computadores.

Em virtude ao banco de dados de DNS ser distribuído, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele. Este tipo de servidor usa como porta padrão a 53, e sua primeira implementação surgiu com o codinome DNS-Berkeley para BSD UNIX 4.3. O Windows NT, em sua versão 4.0, apresentou a primeira versão do DNS dentro da gama de produtos Microsoft, baseando-se nas RFCs 882 e 883, posteriormente atualizadas para as RFCs 1034 e 1035.

A prova 70-410 cobrará de você conceitos básicos sobre o DNS e a transferências de zonas. São as zonas de DNS que armazenam os dados relacionados às estações de trabalho, seus nomes e seus endereçamentos, mantendo uma maior disponibilidade de todo o ambiente. Questões relacionadas ao DNS são cobradas em todas as provas do MCSA.

É possível a colocação de diversos servidores DNS dentro de

uma estrutura de rede, seja ela interna ou externa, com ou sem autenticação e de plataforma aberta ou fechada. É muito comum a comunicação de servidores Microsoft com DNS se conversarem com servidores de plataforma aberta utilizando o BIND.

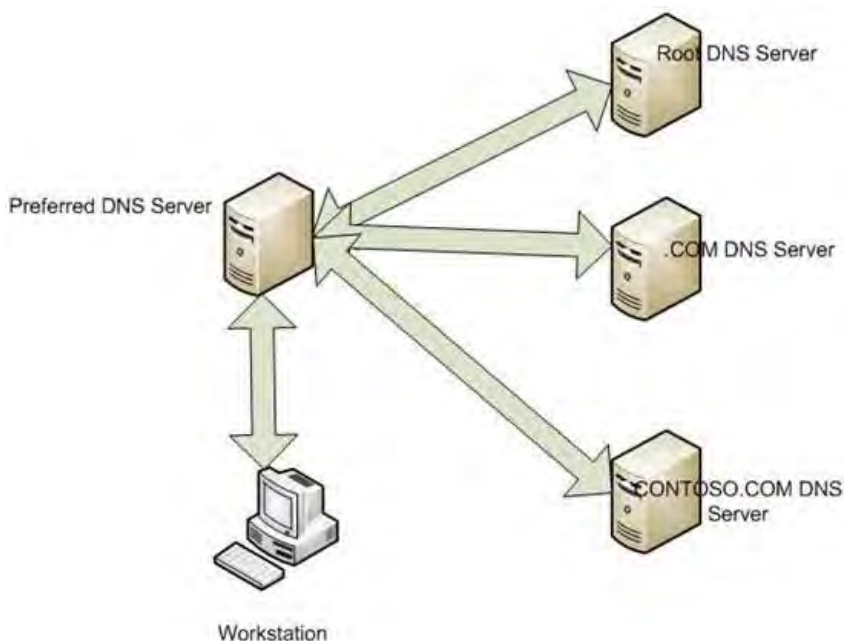
O DNS é usado de forma simplificada dentro de empresas para direcionar um nome a um endereço IP através de uma aplicação, facilitando a vida dos analistas, técnicos e também de usuários. Imagine que você configurou uma aplicação de web para abertura de chamados, onde o acesso é feito com a digitação do endereço IP 192.168.0.12:8080 em seu navegador. Todos os usuários passam a usar a ferramenta com tais dados e tudo segue seu curso.

Porém, em algum momento dessa realidade, é necessário a troca do endereço IP dessa aplicação. O tempo em que seus usuários levarão para se adaptar a essa mudança dobra e muito ruído operacional surgirá, além do aumento de ligações para a equipe de primeiro nível, gerando um volume de atendimentos fora do contexto.

Vamos mudar agora a forma de trabalhar com o cenário que apresentei. Em vez de configurar a aplicação de abertura de chamados como o endereço 192.168.0.12:8080, vamos entregar a ele um endereço baseado em DNS que será <http://sistema.chamados>. Este nome aponta para o endereço 192.168.0.12:8080 de forma transparente ao usuário. Caso seja necessário a troca de endereço, o ruído operacional será infinitamente menor, visto que a mudança envolve apenas questões técnicas de configuração e propagação. Seu usuário continuará utilizando o mesmo endereço <http://sistema.chamados>.

Qualquer aplicação web ou site pode ser encontrado tanto pelo seu endereçamento IP quanto pelo seu nome, porém é indiscutível a facilidade com que o nome é assimilado pelos usuários e ambiente operacional. Dê sempre preferência a esse modelo de utilização. A

figura a seguir demonstra a funcionalidade do DNS quando uma estação cliente requisita através de seu navegador web um dado domínio.



É possível notar que o servidor com autoridade de um domínio possui os registros originais que associam aquele domínio a seu endereço de IP, seja IPV4 ou IPV6. Toda vez que um domínio adquire um novo endereço, essas informações devem ser adicionadas a pelo menos dois servidores autoritativos, onde um deles será o servidor autoritativo principal e o outro, o secundário.

Isso é feito para minimizar o risco de perda de informações originais do endereço daquele domínio. É altamente recomendável que você possua mais de um servidor DNS em sua rede (sempre no mínimo 2). Costumo dizer que, se você possui apenas um servidor DNS e um controlador de domínio, é o mesmo que não possuir nenhum, pois se houver um problema não será possível efetuar uma

rápida resolução e tudo para de funcionar.

IMPORTANTE

É considerado uma boa prática que o servidor com o AD DS instalado também seja um servidor de DNS ativo. Isso agiliza a leitura e escrita, além de permitir uma rápida verificação e atualização de dados dentro da estrutura do domínio. Não é possível subir um controlador de domínio em uma rede sem antes possuir um servidor de DNS. Caso você não possua um servidor de DNS quando subir o controlador de domínio, será efetuado automaticamente durante o processo de configuração do Domain Controller.

7.1 DNS REVERSO

Este recurso chamado de DNS reverso é geralmente configurado em operadoras de link de internet, e permitem a validação de origem de disparo de e-mails. O DNS atua resolvendo o nome do domínio de um host qualquer para seu endereço IP correspondente, mas o DNS Reverso resolve o endereço IP, buscando o nome de domínio associado ao host.

Ele efetua o processo contrário efetuado pelo DNS, servido como uma espécie de “prova real” de sua existência. Caso não seja configurado, seu impacto mais forte é encontrado dentro de estruturas de envio e recebimento de e-mail para usuários da internet.

Os servidores que utilizam o DNS Reverso conseguem verificar a autenticidade de endereços, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS. Isto

evita que alguém utilize um domínio que não lhe pertence.

Durante o decorrer deste capítulo, veremos alguns comandos de validação de servidores DNS. Até a data de criação deste livro, existiam cerca de treze servidores DNS raiz espalhados pelo mundo e, sem eles, a internet não funciona. Destes treze servidores, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa com réplicas localizadas por todo o mundo, inclusive no Brasil desde 2003. Um servidor de réplica de DNS possui uma base somente leitura em forma de cópia perfeita do DNS principal.

IMPORTANTE

Quando uma alteração de DNS é efetuada, seja ela dentro ou fora da empresa, é necessário um período de replicação que pode chegar a até 72 horas, dependendo do país e região. Este número é muito relativo, pois pode ser personalizado pelo administrador de redes visando economia de tráfego e banda. Nunca troque um nome de DNS de servidores de e-mail no meio da semana durante períodos de trabalho intenso, pois isso causará grandes problemas.

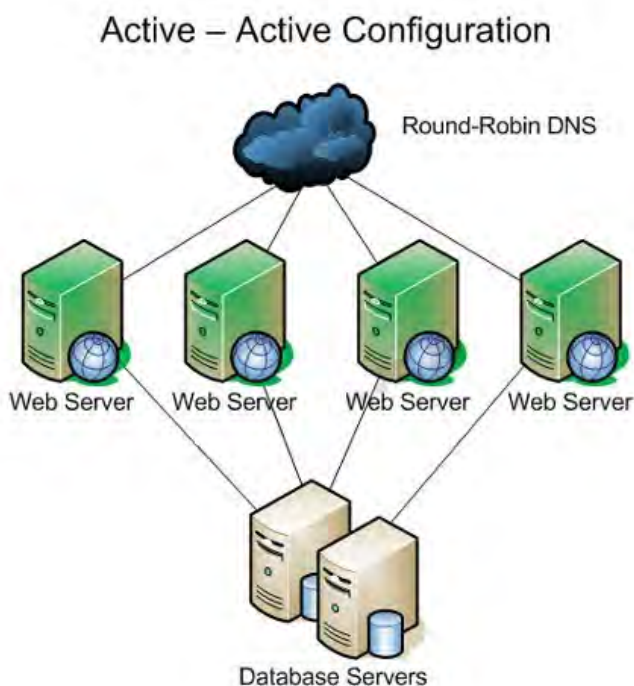
7.2 ROUND-ROBIN DNS

O Round-Robin DNS é uma técnica de distribuição de carga de balanceamento de requisições de DNS, também considerado como técnica de tolerância a falhas e provisionamento de múltiplos servidores anfitriões. É possível aplicar esta técnica a diversos tipos de servidor que dependem diretamente do serviço de DNS, como por exemplo, servidores Web e servidores de FTP.

Em sua forma mais simples, a implementação da técnica de

Round-Robin DNS consiste em responder a pedidos de DNS não só com um único endereço IP, mas uma lista de endereços IP de vários servidores que hospedam serviços idênticos. A ordem em que os endereços IP da lista são devolvidos é a base de funcionamento do Round-Robin, que funciona como um chaveador.

A cada resposta DNS, a sequência de endereço IP na lista é permutada onde normalmente os clientes IP básicos tentam conexões com o primeiro endereço de voltar de uma consulta DNS. Assim, em diferentes tentativas de conexão, os clientes receberão serviços de provedores diferentes, distribuindo a carga geral entre os servidores. A próxima figura demonstra o funcionamento simplificado da técnica de Round-Robin DNS



Não existe um processo padrão para decidir qual endereço será

usado pelo aplicativo requerente, e alguns resolvers tentam listar novamente a lista de servidores para dar prioridade a chamada. Alguns clientes de desktop tentam endereços alternativos depois de um tempo limite de conexão de 30-45 segundos. Quando um servidor web sai de operação, o Round-Robin direciona a requisição para o segundo servidor, e assim sucessivamente.

O sintoma mais comum do uso desta técnica é quando o usuário digita um endereço em seu navegador e, ao pressionar a primeira vez a tecla `Enter`, é apresentado um erro de acesso. Porém, quando pressiona novamente a tecla `Enter` ou pressiona a tecla `F5` para atualizar a pesquisa, o site é carregado normalmente. O primeiro `Enter` levou o usuário para um servidor Web indisponível, já o segundo foi chaveado para o próximo servidor ativo dentro da estrutura, que é na verdade um clone balanceado do que está fora de operação.

A técnica de Round-Robin DNS é usada para carregar os pedidos e requisições de DNS em forma de equilíbrio entre um número determinado de servidores web. Por exemplo, uma empresa tem um nome de domínio e três cópias idênticas do mesmo site que reside em três servidores, com três endereços IP diferentes (cada servidor com seu IP único).

Quando um usuário acessa a página inicial, ele será enviado para o primeiro endereço IP. O segundo usuário que acessa a página inicial será enviado para o próximo endereço IP, e o terceiro usuário será enviado para o terceiro endereço IP. Em cada caso, uma vez que o endereço de IP é dado para fora, que vai para o fim da lista. O quarto utilizador, por conseguinte, vai ser enviada para o primeiro endereço de IP, e assim por diante. Este balanceamento de carga é utilizado em sites de comércio eletrônico, ou sites que recebem milhares de acesso por minuto.

IMPORTANTE

É possível utilizar tanto o modo ativo-ativo quanto o modo ativo-passivo para esquemas de balanceamento de carga de servidores. Geralmente, a decisão é influenciada pela quantidade de licenças disponível relacionada à aplicação que recebe o balanceamento.

TCP/IP

8.1 IPV4

Independentemente de seu escopo de projeto, nos dias de hoje toda conexão de rede existente conhecida depende de regras de tráfego. O principal protocolo é hoje o IP (ou Internet Protocol) em sua versão de número quatro (IPv4), contendo quatro octetos que dividem os bits de segmentação de rede e sub-rede.

O IPV4 possui uma estrutura bem desenhada com um melhor gerenciamento de rotas, resultando em um maior tráfego de rede dimensionado pela internet. Apesar de ser muito funcional, o verdadeiro calcanhar de Aquiles do protocolo IPV4 é sua quantidade de endereços disponíveis por classe aplicada. O IPV4 possui cerca de cinco classes com disponibilidade de uso efetivo de apenas três (A, B e C), exigindo a configuração precisa de segmentação para seu funcionamento.

Se você configura uma rede com um protocolo considerado de classe A, será necessária a criação de uma rota até os computadores de uma classe B ou C. As classes não se comunicam diretamente e, por padrão, seguem uma normatização de tamanho baseado na quantidade de bits de cada Octeto.

O endereçamento IPV4 possui uma regra de uso de bits através de uma máscara de sub-rede. Por exemplo, você configura uma estação de trabalho com o endereço 192.168.0.4 e a máscara de sub-

rede 255.255.255.0. Isso significa que os três primeiros octetos representam a rede em que a estação está alocada.

Por padrão, cada classe de rede possui uma quantidade específica de estações por rede dependendo da quantidade de bits alocado. A máscara 255.255.255.0 comporta 254 equipamentos dentro de uma rede. Porém, quando emprestamos um bit da máscara, esse valor pode mudar drasticamente. Imagine que agora usaremos a máscara 255.255.254.0, onde o terceiro octeto foi modificado de 255 para 254. Isso faria com que a quantidade de máquinas aumentasse de 254 para 510 por rede, sem a necessidade de um roteador.

É possível especificar a quantidade de equipamentos dentro de uma rede ou sub-redes através da máscara de sub-redes. Você pode colocar um endereço 10.0.0.4 como disponível apenas para 510 máquinas quando utiliza a máscara 255.255.254.0.

O protocolo IPv4 é um protocolo usado exclusivamente para uso em redes de comutação de pacotes (todos os dados trafegados são colocados em forma de empacotamento) independentemente de seu escopo de projeto, podendo ser utilizado tanto em redes públicas como em redes privadas. O IPV4 representa a aplicação de integridade dos dados e são suportados por um protocolo de transporte de camada superior, como o Transmission Control Protocol (TCP). A composição do protocolo é conhecida como TCP/IP, unindo protocolos de camadas diferentes em um modelo conhecido como modelo TCP de cinco camadas.

Aos estudantes de conteúdo aprofundado relacionado a redes de computadores, recomendo algumas horas de estudo nos modelos como OSI e TCP, além de modelos de tráfego unicast , broadcast e multicast , que mesmo não sendo cobrados diretamente nas provas, acabam aparecendo em conceitos uniformes dentro da realidade sistêmica Microsoft e não Microsoft.

O endereçamento IPv4 usa um total de 32-bits (separado em 4 octetos W.X.Y.Z) para compor os endereços de rede, o que limita o espaço de endereçamento em exatos 4.294.967,296 endereços. O esgotamento dos endereços IPv4 dentro das redes públicas ocorreu em 3 de fevereiro de 2011, mesmo tendo recebido um significativo atrasado devido às técnicas de tratamento e segmentação de tráfego, como o projeto de rede classful, Classless Inter-Domain Routing, e tradução de endereços de rede (NAT).

A NAT, ou Network Address Translate, traduz endereços WAN para endereços de LAN (simplificando a explicação), e pode ser usada para recursos como VPN, DirectAccess e, até mesmo em alguns casos, para disparo de e-mail. Esta limitação do protocolo IPv4 estimulou o desenvolvimento de uma nova versão, porém chamada de IPv6. O IPv4 reserva blocos de endereços especiais para redes privadas (18 milhões de endereços) e endereços em modo de multicast (270 milhões de endereços).

É muito comum o uso de endereçamento IPV4 em redes do tipo LAN e uso de IPV6 em redes do tipo WAN, porém isso não é obrigatório. Nada impede que você utilize dentro da rede interna endereços de rede IPV6.

É importante lembrar de que a prova não cobrará de você o conceito sobre as normas e desenvolvimento das versões do IPV4. Entretanto, é necessário entender o ponto principal de comunicação entre dispositivos de rede baseado em endereçamento IP. Você deve estudar para a prova tanto os comandos quanto telas gráficas para troca de IPV4 e IPV6.

A seguir, temos um comando que permite a configuração da interface de rede. Neste exemplo, a interface de nome Rede Local, recebe a configuração de Gateway 10.0.0.1 com métrica de número 2.

```
netsh interface ip set address "Rede Local" gateway = 10.0.0.1 gwmetric = 2
```

Grande parte das mudanças de endereço e configuração será feita pela ferramenta de linha de comando `netsh`. Você pode alterar com esta ferramenta todos os itens que geralmente são identificados pela área gráfica, como endereço IP, gateway, servidores DNS e até o tipo de endereço com fixo e dinâmico. É uma ferramenta de extrema validade cobrada em provas Microsoft desde o Windows 2003 até os dias atuais.

8.2 IPV6

IPv6 é a versão mais atual do Protocolo de Internet, substituindo na WAN e na WEB o protocolo IPv4, devido seu esgotamento. Porém nem todo equipamento oferece o devido suporte ao protocolo.

Vamos a um exemplo: imagine que sua rede possui roteadores de um fabricante como Cisco do modelo 1841, que está com o IOS antigo. Os equipamentos mais antigos exigem a atualização do sistema e uma janela de manutenção envolvendo, além de uma equipe especializada, o risco do equipamento não funcionar; envolve risco e custo que muitas empresas não pretendem arcar a primeiro momento.

O protocolo IPV6 foi oficialmente publicado como funcional para fabricantes como Cisco, D-Link, TP-Link (etc.), e desenvolvedores de sistemas operacionais como Microsoft e Apple em 6 de junho do ano de 2012, sendo fruto de esforços de uma grande equipe de pesquisadores do IETF devidamente documentadas RFC 1752.1 e RFC 2460.2. Então, me pergunto: se sua divulgação foi efetuada em 2012, por que as empresas até agora não estão adaptadas?

Os equipamentos legados consomem muito da estrutura atual e, em sua grande maioria, não estão documentados. Isso significa que ninguém sabe o que o equipamento efetivamente faz e como reconfigurar sem impacto. Os equipamentos legados são um grande problema em muitas empresas que cresceram sem planejamento de forma rápida.

Outra característica que tem contribuído para o esgotamento dos endereços IP é a internet das coisas. Hoje diversos dispositivos fazem acesso à internet sem a interação humana, consumindo endereçamentos que antes eram utilizados por nós, seres humanos. A internet das coisas é um termo utilizado dentro do panorama mundial para representar a existência de equipamentos conectados diretamente a internet, como drones, câmeras, veículos e até mesmo geladeiras com tecnologia mais refinada.

O protocolo IPV6 está sendo implantado de forma gradual dentro da estrutura da internet, e deve funcionar lado a lado com o protocolo IPv4 por muito tempo, em uma situação conhecida tecnicamente por "pilha dupla" ou *dual stack*. Esta foi a forma mais útil e interessante de fazer com que o custo diminuísse ou, pelo menos, levasse mais tempo para se adaptar à realidade do mercado de tecnologia da informação. Porém, em longo prazo, o IPV6 tem como objetivo substituir completamente o IPv4, que “só” suporta cerca de 4 bilhões (4×10^9) de endereços IP, contra cerca de $3,4 \times 10^{38}$ endereços do novo protocolo IPV6.

Um grande “problema” para a entrada definitiva do IPV6 em diversas redes LAN e WAN é a incompatibilidade de equipamentos como Switches, roteadores e bridges, além do custo efetivo e risco em se modificar uma estrutura funcional legada. Existem muitos destes equipamentos sem a devida atualização e manutenção, fazendo com que sua troca se torne extremamente cara e difícil de ser efetuada.

Esse cenário torna o *dual stack* não só uma boa alternativa, mas sim algo necessário. Algo interessante a ser notado é que, no IPv6, o responsável pela fragmentação do pacote é o equipamento host que envia o datagrama, e não os roteadores e switches de camada três, como no caso do protocolo IPv4 (conhecer o conceito de datagrama pode ajudar em provas do MCSA e MCSE).

O endereçamento no IPv6 trabalha basicamente com 128 bits, que é enorme se comparado com os 32 bits de trabalho do já antigo IPV4. O endereçamento IPV6 inclui também um prefixo de rede e o sufixo de host, significa que sua estrutura é mais elaborada e única, permitindo uma quantidade enorme de endereços disponíveis, permitindo atender tanto seres humanos e suas conexões como as “coisas” conectadas a uma rede. Algo curioso e muito interessante é que no IPV6 não existem classes de endereços, como acontece hoje no IPv4 e suas classes A, B, C, D e E, o que não impede de termos endereços reservados.

Um endereço padrão IPv6 é composto por um campo único chamado `provider ID`, um outro campo chamado `subscribe ID`, um outro chamado `subnet ID` e um chamado `node ID`. O `node ID` (ou identificador de interface) possui respectivamente 64 bits, e é formado a partir do endereço físico da placa de rede (MAC) no formato EUI 64 bits. É bom lembrar de que os endereços IPv6 são normalmente escritos como oito grupos de quatro dígitos hexadecimais, diferente dos limitados quatro octetos do IPV4. Por exemplo:

```
2000:0CC5:5B1B:0108:1313:802E:0370:4444
```

Se um grupo de vários dígitos seguidos for 0000, pode ser omitido. Essa omissão de endereçamento só pode ser feita uma única vez dentro do protocolo IPV6 e, acredite, será cobrado pela prova 70-410. Em nosso exemplo, fica da seguinte forma:

```
2000:0CC5:5B1B:0000:0000:0000:0000:4444 . E é o mesmo
```

endereço IPv6 que 2000:0CC5:5B1B:4444 .

O endereçamento IPV6 pode ser mapeado para o IPV4, e são usados por roteadores que suportam ambos os protocolos, permitindo a existência de um túnel IPV4 através da estrutura IPV6 (existem técnicas relacionadas a esse mapeamento como 6to4 e Teredo, ambos cobrados ao longo do MCSA do Windows Server 2012 e do Windows 8).

Estes endereços são construídos de forma automática pelos roteadores quando atualizados pelo fabricante. Para tal, os 128 bits do IPv6 ficam assim divididos:

- Campo de 80 bits colocado a '0' (zero), 0000:0000:0000:0000:0000 ...
- Campo de 16 bits colocado a '1' (um), ... FFFF ...
- Endereço IPv4 de 32 bits

Já endereços IPv6 mapeados para IPv4:

- ::FFFF:

O comando `Netsh` com o parâmetro `interface` permite a administração tanto de endereçamento IPV4 quanto endereçamento IPV6, e pode ser muito útil durante a configuração de servidores em modo Server Core, ou ainda pode se tornar útil para a criação de scripts e até de arquivos `.bat` . Para conhecer as características do comando, digite:

```

C:\Users\epopovi>netsh interface /?
Os seguintes comandos estão disponíveis:

Comandos neste contexto:
6to4      - Altera para o contexto 'netsh interface 6to4'.
?         - Exibe uma lista de comandos.
dump      - Exibe um script de configuração.
help      - Exibe uma lista de comandos.
httpstunnel - Altera para o contexto 'netsh interface httpstunnel'.
ipv4      - Altera para o contexto 'netsh interface ipv4'.
ipv6      - Altera para o contexto 'netsh interface ipv6'.
isatap    - Altera para o contexto 'netsh interface isatap'.
portproxy - Altera para o contexto 'netsh interface portproxy'.
set       - Define informações de configuração.
show      - Exibe informações.
tcp       - Altera para o contexto 'netsh interface tcp'.
teredo    - Altera para o contexto 'netsh interface teredo'.

Os seguintes subcontextos estão disponíveis:
6to4 httpstunnel ipv4 ipv6 isatap portproxy tcp teredo

Para exibir a ajuda relacionada a um comando, digite o comando seguido
de um espaço e digite ?.

C:\Users\epopovi>

```

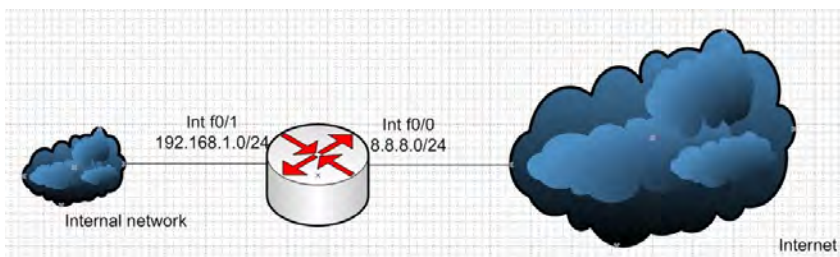
Você será cobrado na prova tanto pelo conhecimento da troca de endereçamento através de linha de comando quanto pela utilização simplificada do PowerShell, que neste capítulo trataremos pelo laboratório.

8.3 NAT

A Network Address Translation, ou simplesmente NAT, é uma técnica usada para que um endereço interno de uma rede possa efetuar contato com um endereço interno da rede. É uma técnica muito eficiente para comunicação de um IP público de internet para um IP interno da rede. Seu uso é direcionado geralmente para acesso remoto através de recursos como VPN, ou tunelamentos específicos como ISATAP.

A grande maioria de pequenos empresários e comerciantes não tem recursos necessários para adquirir um link dedicado com IP

fixo. Ou seja, contratamos o pacote de internet com uma empresa provedora com fornecimento de um link com de IP dinâmico (muda de tempos em tempos). Isso indica que não podemos digitar o IP do nosso link em uma ferramenta com o terminal services e acessar diretamente o roteador, pois o endereço pode mudar a qualquer momento.



Se o IP muda a cada hora, por exemplo, não é possível criar uma rota direta para dentro da estrutura da empresa, a não ser que o administrador de redes vincule um "nome" (DNS) ao endereço IP daquele momento. É aí que entram os provedores de DNS como o FreeDns. Ele válida de tempos em tempos o IP que está disponível em nosso link e vincula um nome, fazendo a ponte direta para a "porta de casa," ou seja, para a porta do roteador (é um provedor de DNS dinâmico).

O serviço de DNS é fundamental para que a internet exista, pois sem ele nenhum computador encontraria a origem de um nome. Seu conceito extrapola ainda mais a base quando falamos de DNS reverso, que é a validação do DNS pelo provedor de acesso, extremamente útil para estruturas que possuam disparo de e-mail, como o Exchange Server ou o Smart Mail, por exemplo.

O DNS reverso é visto em detalhes pelas provas relacionadas ao Exchange Server 2013 e precisa de um IP fixo e do apoio da operadora de dados que oferece o link. Esta é uma das formas de validar se um determinado servidor é realmente quem diz ser

quando dispara uma mensagem específica. Para esta prova, não será cobrado de você detalhes sobre o DNS reverso.

O DNS (ou Domain Name System, que traduzindo diretamente da língua inglesa significa Sistema de Nomes de Domínios) é responsável por fazer com que uma página de internet seja apontada para um determinado servidor e seu endereço IP. Ou seja, ele traduz um endereçamento IP para um nome comum com caracteres alfanuméricos. Ele é o principal motivo de você não precisar digitar os endereços IP em seu navegador Web e utilizar nomes simples, como por exemplo, www.google.com.br.

Ele é chamado de serviço de resolução de nomes e segue regras devidamente documentadas por documentos chamados RFC 882 e 883 (com atualização pelas RFCs 1034 e 1035). Tais documentos representam as regras de funcionamento dos serviços de DNS para todos os sistemas operacionais que necessitem utilizar recursos de tráfego de rede, ou seja, tudo hoje conhecido em forma de equipamento.

E o que tem a ver a NAT com a explicação relacionada ao DNS? Simples, a NAT é utilizada em grande maioria para que uma estação de trabalho acesse um determinado servidor através do endereço IP de um link ou de um nome DNS, seja por meio de IP fixo ou dinâmico. A dificuldade quanto a configuração fica a critério do analista de redes. Para nossa realidade, podemos entender que o NAT faz parte do servidor RRAS (VPN).

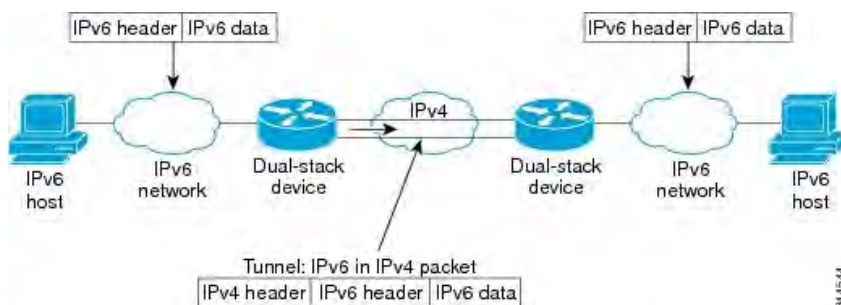
Para que você possa utilizar o servidor NAT, para fornecer conexão à internet para a rede da sua empresa, você deve ter um servidor com o RRAS instalado e habilitado. Esta técnica não é nova, e é cobrada desde a prova 70-216 até as mais atuais, como a 70-410.

O servidor onde está o RRAS deve ser o servidor conectado à

internet. O componente de tradução de endereços faz parte da funcionalidade do NAT e será habilitado, assim que o NAT for configurado no RRAS.

8.4 ISATAP

O protocolo ISATAP, ou Intra-Site Automatic Tunnel Addressing Protocol, é um mecanismo de transição IPv6. É utilizado para transmitir pacotes IPv6 entre nós *dual-stack* em uma rede IPv4. Este protocolo é configurado geralmente em roteadores de borda, porém pode ser utilizado de diversas formas diferentes, dependendo da situação.



Ao contrário do protocolo 6over4 (6to4), o ISATAP usa IPv4 como uma rede sem difusão de acesso múltiplo (NBMA) pela camada de enlace de dados virtual (pensando em modelo OSI de 7 camadas), de modo que ele não exige a infraestrutura de rede IPv4 subjacente para suportar o modo de tráfego *multicast*. Ele trabalha basicamente trafegando dados IPV6 entre túneis IPV4.

O 6over4 é um protocolo com o mesmo fim, porém mais antigo que pode ser encontrado facilmente em equipamentos legado. Já o protocolo ISATAP pode ser configurado em equipamentos que possuam sistema operacional Microsoft que possua desde o Windows XP até o Windows 8.1 e Windows Server

2012 R2. Recomendo fortemente o conhecimento do conceito técnico de ambos os protocolos para as provas do MCSA e MCSE, lembrando de que este conceito também pode ser encontrado pela cobrança das provas do Windows 7 e a certificação MCTS e MCTIP.

DICA

A prova não cobrará de você a configuração direta do ISAPA, porém lembre-se de que, caso apareça algum cenário de configuração entre redes IPV4 com protocolos IPV6, é o ISATAP ou o 6to4 que faz a transição. Sei que o contexto é mais complexo que aparenta, mas a prova 70-410 é básica, então somente a base será cobrada.

Para saber mais sobre o padrão de protocolo ISATAP, recomendo a visita em <http://www.isatap.org/>.

VOLUMES DE DISCO

Toda vez que efetuamos a instalação de um sistema operacional, a unidade de armazenamento recebe uma preparação relacionada a índices e formatos, referentes ao conteúdo ali gravado. Essa preparação é chamada de formatação, e assimila um “formato” de trabalho que leva em consideração a disposição das trilhas, setores e cluster do disco rígido, ou ainda do endereçamento de células de um disco SSD.

Um disco e um volume são itens diferentes, e é necessário conhecer a forma de trabalho relacionada a cada elemento. Por exemplo, você pode trabalhar com um disco de padrão SAS com uma formatação do tipo NTFS, e nele trabalhar com volumes dinâmicos.

O conceito de volume de disco não é algo novo e pode ser encontrado em materiais da época do Windows XP e a prova 70-272. São ferramentas importantes e sua utilização é conceitual para entender qualquer sistema operacional nos dias de hoje.

Trabalhamos basicamente com discos básicos e discos dinâmicos, onde os dinâmicos fornecem recursos que os básicos não oferecem, como a capacidade de criar volumes que estendam vários discos (volumes estendidos e distribuídos) e a capacidade de criar volumes tolerantes a falhas (volumes espelhados e RAID-5). Todos os volumes dos discos dinâmicos são conhecidos como volumes dinâmicos.

A prova 70-410 pode questionar você em algum ponto sobre a situação em que um analista não consegue montar um RAID de disco do tipo 1 em um servidor com o Windows Server 2012 R2. Nesse questionamento, é possível identificar que ambos os discos onde há essa tentativa de montar o RAID não estão em formato dinâmico. A resposta é simples, converta ambos os discos para dinâmico. Esse tipo de pergunta pode afetar a forma com que a prova se segue, e muitas vezes demonstra não a questão do conhecimento técnico em si, mas da interpretação de texto.

Existem seis tipos de volumes de disco aplicáveis a um servidor com o Windows Server 2012 R2 instalado:

- Dinâmicos
- Simples
- Estendidos
- Distribuídos
- Espelhados
- RAID-5

Os volumes espelhados e RAID-5 são tolerantes a falhas, e estão disponíveis somente em computadores executando sistemas operacionais a partir do Windows 2000 Server até o Windows Server 2012 R2. Entretanto, você pode usar um computador que esteja executando o Windows XP Professional, Windows Vista Business, Windows 7 Pro e Windows 8 Pro para criar remotamente volumes espelhados e RAID-5.

É possível converter um disco básico que contenha partições de sistema ou de inicialização em disco dinâmico, porém, após sua conversão, essas partições se tornarão sistemas simples ou volumes de inicialização (depois que o computador for reiniciado).

Você não pode marcar um volume dinâmico existente como ativo. Você pode converter um disco básico que contenha a partição

de inicialização (que contenha o sistema operacional) em um disco dinâmico. Depois que o disco for convertido, a partição de inicialização se tornará um volume de inicialização simples (depois que o computador for reiniciado).

Para entender melhor a funcionalidade entre um disco e outro, podemos determinar que um disco básico usa partições primárias, partições estendidas e unidades lógicas para organizar dados de forma simplificada. Em especial, nesta versão do Windows, discos básicos possuem quatro partições primárias ou três partições primárias e uma estendida.

A partição estendida pode conter várias unidades lógicas (há suporte para até 128 unidades lógicas). As partições de um disco básico não compartilham ou dividem dados com outras partições. Cada partição em um disco básico é uma entidade separada no disco.

DICA

É possível que você seja cobrado sobre a quantidade de unidades lógicas relacionadas a discos básicos e discos dinâmicos, portanto fique atento a este dado em especial.

Os discos dinâmicos podem conter aproximadamente 2.000 (dois mil) volumes dinâmicos funcionando como partições primárias usadas em discos básicos. É realmente um número bem alto quando comparado com o disco básico. Em algumas versões do Windows, você pode combinar discos rígidos dinâmicos separados em um único volume dinâmico (chamados de extensão), distribuir dados entre vários discos rígidos (chamados de distribuição) para aumento de desempenho, ou duplicar dados entre vários discos

rígidos (chamados de espelhamento) para aumento de confiabilidade.

É possível converter um disco básico em um disco dinâmico e vice-versa tanto pela ferramenta de linha de comando `diskpart` como pela área gráfica, como o Gerenciador de Disco — Disk Management.

IMPORTANTE

Não faça a conversão em discos básicos que contenham várias instalações do Windows, pois, após a conversão, os sistemas não inicializarão corretamente. Caso isso aconteça, será necessário utilizar a ferramenta de linha de comando `bcdboot` para remontar o índice de inicialização do sistema e, acredite, dará bastante trabalho.

Se existir o caso em que você precise converter um disco básico para dinâmico, utilize os seguintes passos:

1. Faça o backup de todos os volumes do disco que você deseja converter de dinâmico em básico.
2. Para obter mais informações sobre como fazer backup de volumes, consulte *Tópicos Relacionados*.
3. Abra o *Gerenciamento do Computador* (local).
4. Na árvore de console, clique em *Gerenciamento do Computador* (local), clique em *Armazenamento* e, em seguida, em *Gerenciamento de Disco*.
5. Clique com o botão direito do mouse no disco dinâmico que você deseja converter em básico e, em seguida, clique em *Excluir Volume* para cada volume do disco.
6. Quando todos os volumes do disco forem excluídos, clique

com o botão direito do mouse no disco e, em seguida, clique em *Converter em Disco Básico*.

É possível efetuar os mesmos passos através da ferramenta de linhas de comando `diskpart` e, acredite, você será cobrado pela prova a pelo menos conhecer essa ferramenta. Siga os passos a seguir em uma máquina virtual ou laboratório para efetuar a conversão. Nunca execute os comandos de conversão de disco em servidores em produção sem o devido backup. Faça o backup de todos os volumes do disco que você deseja converter de dinâmico em básico.

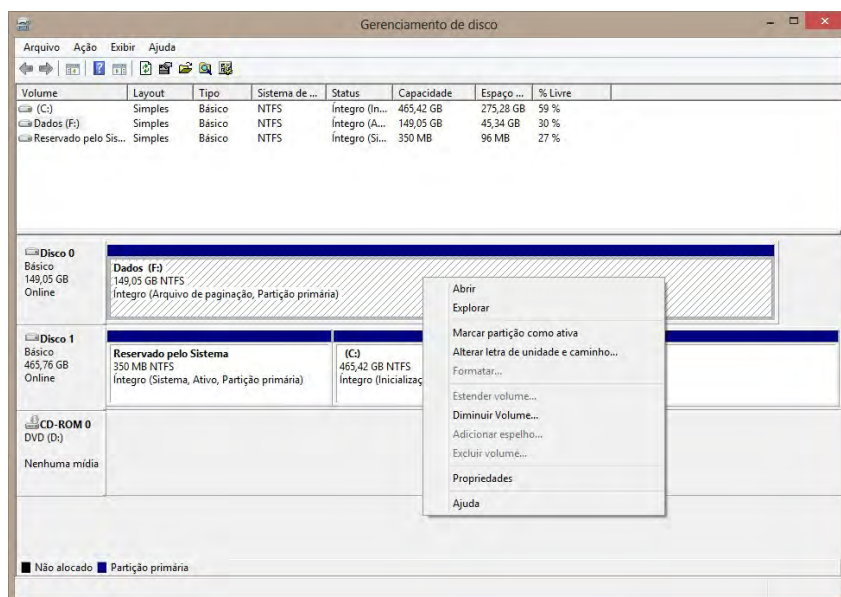
Para obter mais informações sobre como fazer backup de volumes, consulte *Tópicos Relacionados*.

1. Abra o prompt de comando e digite `diskpart` .
2. No prompt `diskpart`, digite `list disk` .
3. Anote o disco dinâmico que você deseja converter em básico.
4. No prompt `diskpart`, digite `select diskn` .
5. No prompt `diskpart`, digite `detail diskn` .
6. Para cada volume do disco, no prompt `diskpart`, digite `select volume=n` .
7. Em seguida, digite `delete volume` .
8. No prompt `diskpart`, digite `select diskn` .
9. Especifique o número do disco que você deseja converter em básico.
10. No prompt `diskpart`, digite `convert basic` .

9.1 GERENCIADOR DE DISCO — DISK MANAGEMENT

O gerenciador de discos, ou Disk Management, pode ser encontrado pelas teclas de atalho `Winkey + X` , ou dentro do painel de controle em *Sistema e Segurança, Ferramentas Administrativas* e

Criar e formatar partições do disco rígido. É possível também digitar `diskmgmt.msc` no executar do Windows para abrir o *Gerenciador de Discos*. A figura a seguir demonstra a tela do *Gerenciador de Discos* e sua estrutura básica.

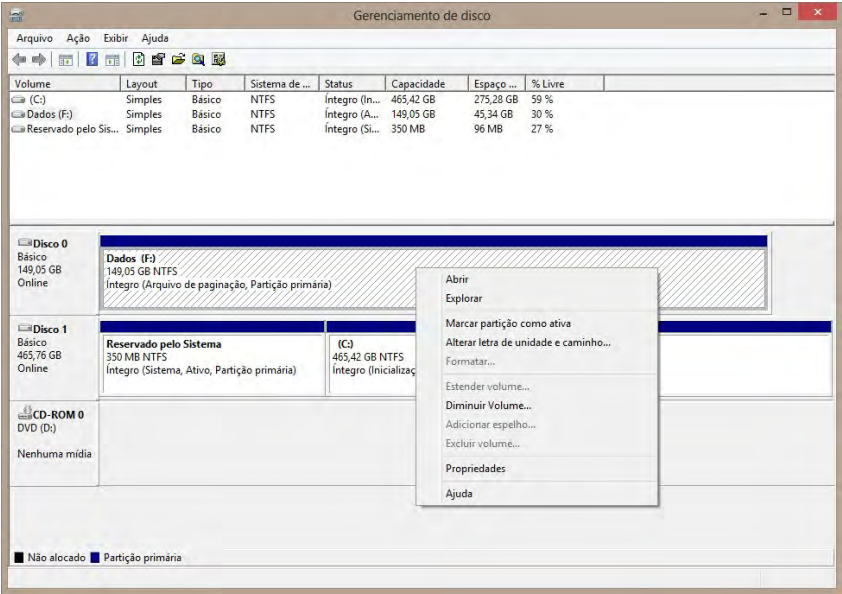


O *Gerenciador de Discos* é dividido em duas etapas. A parte superior mostra as unidades lógicas identificadas, e a parte inferior os discos físicos ou discos virtuais atribuídos ao sistema. É possível identificar os discos e seu espaço tanto na parte superior da janela quanto na parte inferior.

Note que a imagem possui dois discos, aqui interpretados como disco 0 e disco 1. O disco 1 está com o sistema operacional possuindo uma partição reservada pelo sistema, e uma segunda partição de instalação do Windows Server 2012 R2. O disco 0 é um disco secundário e possui dados diversos, como arquivos de texto, programas instalados e demais recursos relacionados a aplicações.

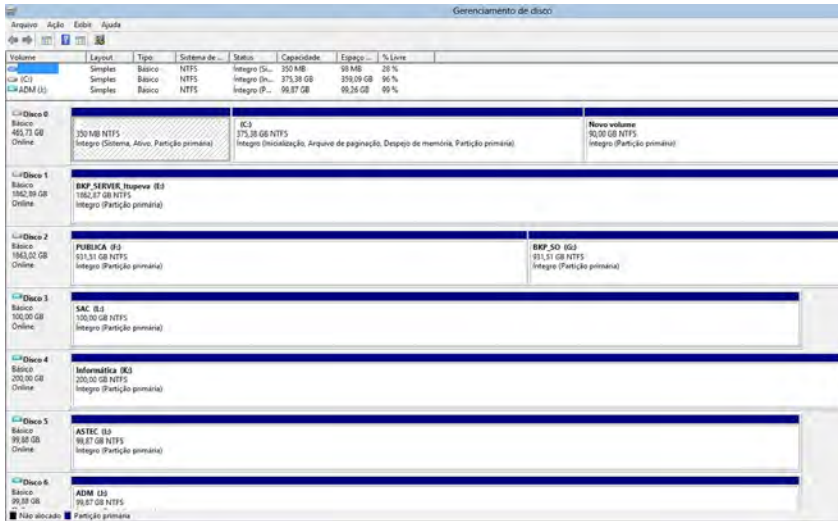
No disco 0, é possível identificar duas etapas, uma do lado

esquerdo da tela representado aqui pela palavra **Online** , e a segunda parte, representada aqui pela palavra **Dados** acompanhado da unidade (**F:**).

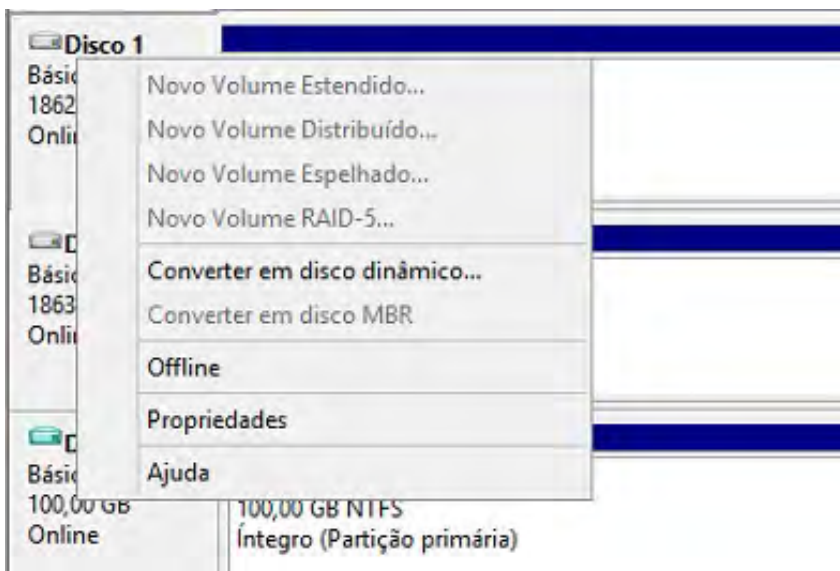


Você precisa entender que o disco 0 se trata de um disco físico ou partição física, aqui demonstrado pela cor cinza. Caso você perceba que se trata de uma cor azul, estaremos falando de um VHD ou VHDX montado em forma de unidade. É um arquivo VHDX interpretado em forma de disco lógico. Ele não existe fisicamente, porém o Windows reconhece e atribui ao arquivo uma letra de unidade, ficando disponível ao usuário como se fosse um disco compartilhado.

A figura a seguir demonstra esse processo. Nela, o disco 3, disco 4, disco 5 e disco 6 são na verdade discos montados em um servidor de arquivos. Neste processo, foi direcionado um tamanho para cada departamento com uma facilidade extra de backup dos dados.



Para converter um disco físico básico em dinâmico, basta clicar em cima dele com o botão direito do mouse e, em seguida, clicar em converter. É neste momento que também podemos montar os níveis de resiliência como volume estendido, distribuído, espelhado e RAID-5. Tais recursos estão disponíveis apenas em discos dinâmicos e não em discos básicos.



O gerenciamento de discos é o ponto crítico dentro da montagem de um servidor, pois é por meio dessa estrutura que nos preparamos para falhas futuras. Por exemplo, imagine que você possui em um servidor três discos, sendo um para o sistema operacional e os outros dois para dados de um servidor de arquivos. Você faz então um espelhamento entre os discos de dados aumentando o nível de resiliência para o dobro.

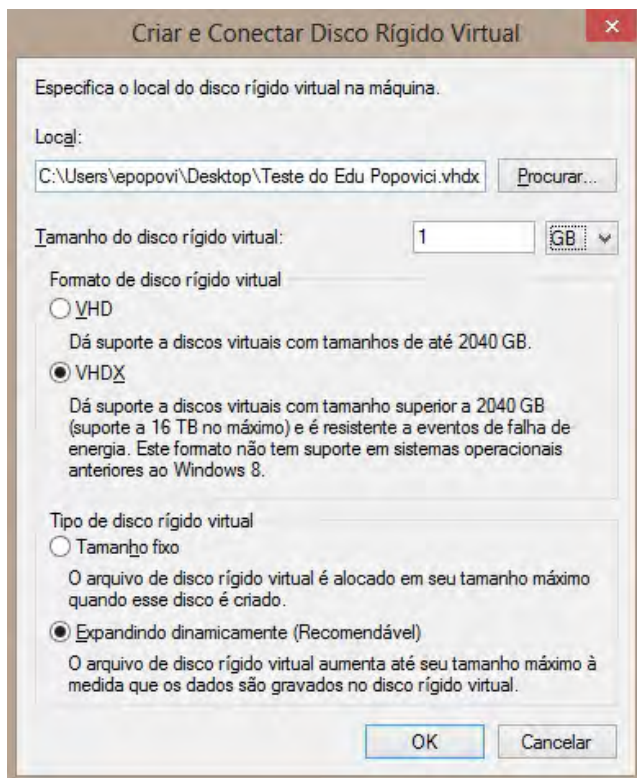
Se um dos discos que estiver no modo dinâmico queimar fisicamente, o outro assume o funcionamento sem que haja perda de dados. É uma excelente resposta para quem não possui dinheiro suficiente para comprar um *storage* profissional.

É possível ainda criar uma unidade lógica baseada em um arquivo VHD ou VHDX e, através desse arquivo, subir uma unidade lógica. Imagine que você precisa fazer um backup do Outlook e dados pessoais de um diretor ou supervisor, por exemplo. Você pode facilitar o processo criando um arquivo VHD em um servidor de arquivos onde somente aquele diretor ou supervisor terá

o compartilhamento ativo de forma a não ultrapassar um determinado limite. A vantagem desse modelo está na facilidade de se executar o backup e de movimentar o arquivo VHD em comparação a outras unidades.

Para criar um arquivo VHD ou VHDX em forma de unidade lógica, siga os seguintes passos:

1. Abra o *Gerenciador de Discos*.
2. Selecione um disco físico qualquer.
3. Na parte superior da tela, clique em ação.
4. Selecione *Criar VHD*.
5. Especifique o local onde o VHD será criado e o tamanho máximo dele. Em meu exemplo, usei um disco de 1GB, mas você pode ficar à vontade para escolher o tamanho nos limites do tipo do arquivo.
6. Escolha expandindo dinamicamente, assim o disco crescerá conforme recebe os dados. Veja a próxima figura para entender como a sua tela deve ser preenchida.



7. Após preencher todos os dados pressione **OK**.
8. Note que o disco foi anexado automaticamente, porém está desativado e marcado com uma seta vermelha apontando para baixo.



9. Clique com o botão direito do mouse no disco (que em meu caso é o disco 2), e em seguida clique em inicializar disco.
10. Marque a opção **GPT** (Tabela de Partição GUID) e pressione

OK.

11. Após a inicialização do disco, note que a unidade ainda não está formatada. O disco está presente, porém precisa de um formato para ser reconhecido pelo sistema operacional. Clique com o botão direito do mouse em *Não alocado*, e depois em *novo volume simples*.
12. O assistente que é aberto vai auxiliar com a criação da partição. Pressione o *Avançar*.
13. Mantenha o tamanho da unidade em MB. Como utilizei um exemplo de 1 GB, o próprio assistente alocou 8 MB para sistema e liberou 990 MB para uso efetivo. Apenas pressione o *Avançar*.
14. Escolha a letra disponível, que em meu caso é a *E:*, e pressione o *Avançar*.
15. Mantenha a formatação em sistema de arquivos *NTFS* e pressione o *Avançar*.
16. Conclua o assistente para que a unidade seja disponibilizada para uso com a formatação concluída.
17. Vá até o Windows Explorer e veja sua unidade pronta para uso.

9.2 DISKPART

O `diskpart` é uma ferramenta de linha de comando utilizada para gerenciamento de discos. Para os mais antigos na área de TI, é possível criar um paralelo de comparação com o antigo `fdisk` do saudoso Dos 6.22.

Mas a comparação fica apenas na questão de ambos serem utilizados para linha de comando, pois o `diskpart` é mais poderoso e cheio de recursos que seu antecessor, sendo inclusive cobrado em provas do MCSA tanto do Windows 8 quanto Windows Server 2012 R2. Fique atento com este comando para todas as provas do MCSA.

IMPORTANTE

Quando o comando `diskpart` for usado como parte de um script, é recomendável que você conclua todas as operações do comando ao mesmo tempo como parte de um único script do `diskpart`. Você pode executar seus scripts consecutivos, mas aguarde pelo menos quinze segundos entre cada um deles para que haja um desligamento completo da execução anterior antes de uma nova execução do comando `diskpart` em scripts sucessivos. Caso contrário, os scripts sucessivos poderão falhar.

Você pode incluir uma pausa entre os scripts consecutivos do `diskpart`, adicionando o comando `/t 15` de tempo limite ao seu arquivo em lotes junto com seus scripts do `diskpart`. É possível carregar uma pequena lista de parâmetros do `diskpart` pelo parâmetro `help`, dentro do seu gerenciador. Este gerenciador é carregado através do prompt de comando `cmd`, conforme demonstrado pela figura a seguir.



O `diskpart` é uma ferramenta rica em comandos, porém os

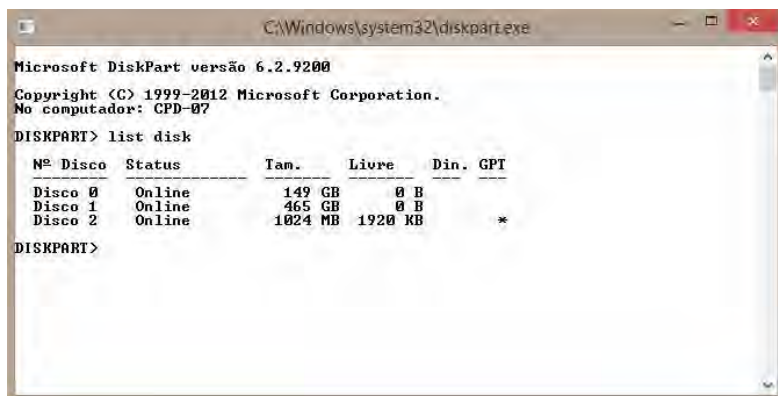
mais comuns cobrados em provas de certificação são os listados pela tabela a seguir.

Comando	Funcionalidade
list disk	Exibe uma lista de discos e informações sobre eles, como tamanho, quantidade de espaço livre disponível, se o disco é básico ou dinâmico e se usa o tipo de partição de MBR (registro de inicialização principal) ou tabela de partição GUID (GPT). O disco marcado com um asterisco (*) tem foco
select disk	Seleciona o disco especificado, onde n é o número do disco, e concede foco a ele
detail disk	Exibe as propriedades do disco selecionado e os volumes desse disco
select volume	Seleciona o volume especificado, onde n é o número do volume, e concede foco a ele. Se nenhum volume for especificado, o comando select listará o volume atual com foco. Você pode especificar o volume por número, letra de unidade ou caminho de ponto de montagem. Em um disco básico, a seleção de um volume também fornece o foco de partição correspondente
delete volume	Exclui o volume selecionado. Não é possível excluir o volume do sistema, o volume de inicialização ou qualquer volume que contenha o arquivo de paginação ou despejo de memória ativo
convert basic	Converte um disco dinâmico vazio em disco básico

IMPORTANTE

O diskpart identifica não apenas discos físicos, mas também unidades lógicas montadas, como por exemplo, arquivos VHD e VHDX. É possível inclusive, por meio do diskpart, identificar os discos que possuem sua partição em formato GPT.

Discos GPT possuem suporte para partições acima dos 2 TB padrões, utilizados em sistemas NTFS. O comando `list disk` permite trazer inclusive o status do disco, tamanho espaço livre e se está em formato dinâmico. A próxima figura demonstra bem o funcionamento do comando.



```
C:\Windows\system32\diskpart.exe

Microsoft DiskPart versão 6.2.9200
Copyright (C) 1999-2012 Microsoft Corporation.
No computador: CPD-07

DISKPART> list disk

   Nº Disco  Status      Tam.      Livre   Din.  GPT
-----
Disco 0     Online        149 GB      0 B
Disco 1     Online        465 GB      0 B
Disco 2     Online       1024 MB   1920 KB      *
```

9.3 DISCO GPT

O GPT, também conhecido como Tabela de Partição Guid, é um modelo de organização de dados de um disco que tende a substituir o modelo chamado MBR. É na verdade uma arquitetura que evoluiu diretamente da MBR, porém apresentando maior resiliência e

confiabilidade. A estrutura de discos GPT é um novo layout relativo ao particionamento de discos rígidos ou volumes de disco baseado em VHD ou VHDX (lembre-se das páginas anteriores quando criamos e montamos o VHD).

O GPT traz muitos benefícios comparativamente ao tradicional MBR (Master Boot Record), dos quais se destacam:

1. Suporte para partições acima dos 2 TB (ou seja, 2^{64} blocos, um máximo de 1 ZB). De referir que no Windows, devido ao sistema de ficheiros NTFS, este tamanho está limitado para 256TB.
2. Apesar de poderem ser criadas um número ilimitado de partições, o GPT suporta 128 partições primárias.
3. Melhor estrutura/organização ao nível das partições.
4. Possui mecanismos para detecção de dados e partições corrompidas.
5. Aumenta a probabilidade de recuperação de dados, na existência de sectores do disco danificados, uma vez que tem um cabeçalho secundário (Secondary GPT Header) que funciona como backup da tabela de partições.
6. O campo Protective MBR funciona ao estilo do MBR, mas com suporte para 64 bits. Esta área funciona como “mecanismo” de retrocompatibilidade.

DICA

Fique atento a perguntas de prova que resolvem situações relacionadas ao tamanho do disco. Geralmente, elas acompanham situações onde o usuário precisa de uma partição específica de 3TB, e uma das respostas é exatamente a conversão de um disco MBR para GPT.

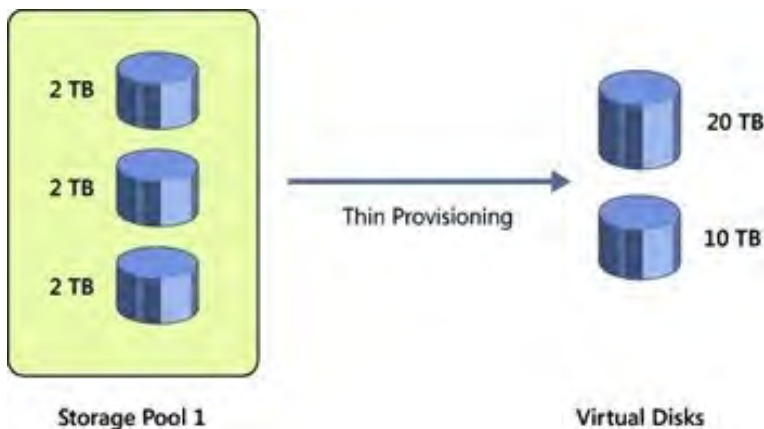
9.4 STORAGE POOL

O Storage Pool é uma técnica utilizada para criação de unidades lógicas de tamanho único usando mais de um disco físico. É uma técnica que se parece muito com o RAID, porém tem inúmeras características mais interessantes.

Para entender o conceito do Storage Pool, imagine que você possua um servidor de arquivos com 4 discos de 500 GB, totalizando 2 TB. Você precisa de duas unidades lógicas de 1,5 TB, em que tais unidades ocupem os 4 discos. Com o Storage Pool, posso transformar diversos discos em uma única unidade lógica ou criar diversas unidades lógicas com poucos discos.

Essa técnica é geralmente utilizada com Storages SAN por questões de performance, mas pode ser utilizada em equipamentos de pequeno e médio porte, geralmente direcionado com o Hyper-V. Os laboratórios deste capítulo farão o acompanhamento para a criação do Storage Pool de forma simples e direta.

Seu conceito deve ser dominado, pois é cobrado em praticamente todas as provas do MCSA do Windows Server 2012. É importante citar aqui que o Storage Pool não é algo novo e está presente também em versões anteriores do Windows, como por exemplo, o Windows 7.



O Storage Pool foi desenvolvido para flexibilizar o armazenamento em forma de custo-benefício, com alta disponibilidade de forma escalável para implantações (virtuais ou físicos) críticos do dia a dia. É possível utilizar discos menores com velocidades diferentes para geração de uma única unidade lógica sem a necessidade de drives HBA. Isso significa que é possível utilizar hardware mais antigo de forma econômica para montagem de um ambiente virtual.

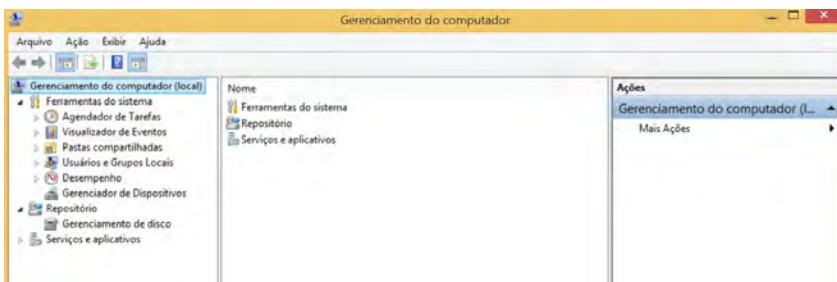
A utilização do Storage Pool permite integração com diversas ferramentas Microsoft já consolidadas como:

- Failover Cluster Manager
- Server Manager
- Windows PowerShell
- Windows Management Instrumentation (WMI)

COMPUTER MANAGEMENT — GERENCIADOR DO COMPUTADOR

Antes de começar os estudos dentro do mundo de permissionamento, precisamos entender que existe um local dentro do Gerenciamento do Computador que nos mostra uma visão geral do que está ativo, como pastas compartilhadas, usuários conectados e até quais arquivos estão sendo acessados naquele exato momento.

O Computer Management é uma ferramenta de extrema validade e pode ser acessado rapidamente pelas teclas de atalho Winkey + X , conforme demonstrado pela próxima figura:



Neste momento, é interessante saber que podemos localizar por meio do ícone de pastas compartilhadas três atividades, sendo elas

os Compartilhamentos, as Sessões e os Arquivos abertos. Tudo o que está compartilhado no computador é apresentado pela pasta de compartilhamento, assim como seu local de origem e número de concessões ativas. As sessões apresentam quais usuários estão conectados ao servidor, assim como seu endereçamento IP (facilmente localizado pelo comando `Arp -a`, como visto nos capítulos anteriores). Os arquivos abertos apresentam os arquivos que estão sendo lidos, copiados e modificados pelos usuários.

A figura a seguir pode ajudar a demonstrar essa área em especial:



Antes de iniciar as atividades relacionadas ao compartilhamento de pastas e arquivos, é interessante saber onde é possível ver esse compartilhamento ativo e suas características. Este recurso é muito útil em servidores de arquivos em que um departamento inteiro precisar utilizar um mesmo arquivo com limitação de acesso.

Imagine que uma pasta possui permissão para acesso simultâneo de duas pessoas. Ambas as pessoas estão ausentes da empresa e uma terceira precisa do acesso. Você precisa desconectar os usuários ausentes para que o terceiro funcionário efetue o acesso. Este modelo de situação pode ser cobrado de você nas provas, e é gerenciado através da área de sessões das pastas compartilhadas.

10.1 PERMISSÕES NTFS E COMPARTILHAMENTO

Vimos anteriormente que o NTFS é um sistema de arquivos desenvolvido na época do Windows NT pela Microsoft. Sua intenção era de substituir o sistema FAT, que não servia como sistema de arquivos devido diversas limitações e falta de recursos.

O sistema de arquivos NTFS permitiu que se fosse possível trabalhar questões de segurança que antes não eram disponíveis pelo sistema de arquivos FAT. O NTFS, em sua versão 5.0, trouxe inúmeras melhorias; entre elas estão a criptografia de arquivos, quotas de usuário, gerenciamento e otimização melhorados.

As permissões NTFS são usadas quando queremos limitar de fato as permissões dos usuários a pastas e arquivos. Diferente das permissões de compartilhamento, caso um usuário esteja com uma sessão estabelecida localmente na máquina que possui o arquivo ou a pasta, ele não conseguirá acessar o documento, dependendo da permissão que foi aplicada para ele. Desta forma, podemos restringir o acesso a dados tanto na rede quanto localmente.

Em um servidor de arquivos, o acesso a uma pasta pode ser determinada por dois conjuntos de entradas de permissão: o conjunto de permissões de compartilhamento em uma pasta e o conjunto de permissões de NTFS na pasta influenciando sobre todos os arquivos ali contidos. As permissões de compartilhamento são geralmente usadas para gerenciar computadores com sistemas de arquivos FAT32, ou outros que não usam o sistema de arquivos NTFS, além de possuírem um caminho reduzido diretamente para o acesso, ignorando a herança.

As permissões de compartilhamento e as permissões de NTFS são independentes no sentido de que nenhuma altera a outra. As permissões de acesso final em uma pasta compartilhada são

determinadas levando-se em consideração as entradas de permissão de compartilhamento e de NTFS. As permissões mais restritivas são aplicadas em seguida.

DICA

Permissões são somadas, porém permissões restritivas tem prioridade sobre qualquer outra. Imagine que você deixe explícito um grupo de usuários com acesso negado e outro grupo de usuários com permissão de leitura a uma determinada pasta (chamaremos de grupo A e grupo B, respectivamente). Então, você adiciona o usuário `epopovi` a ambos os grupos como parte da rotina administrativa. A permissão efetiva seria acesso negado, pois existe uma restrição explícita de negação.

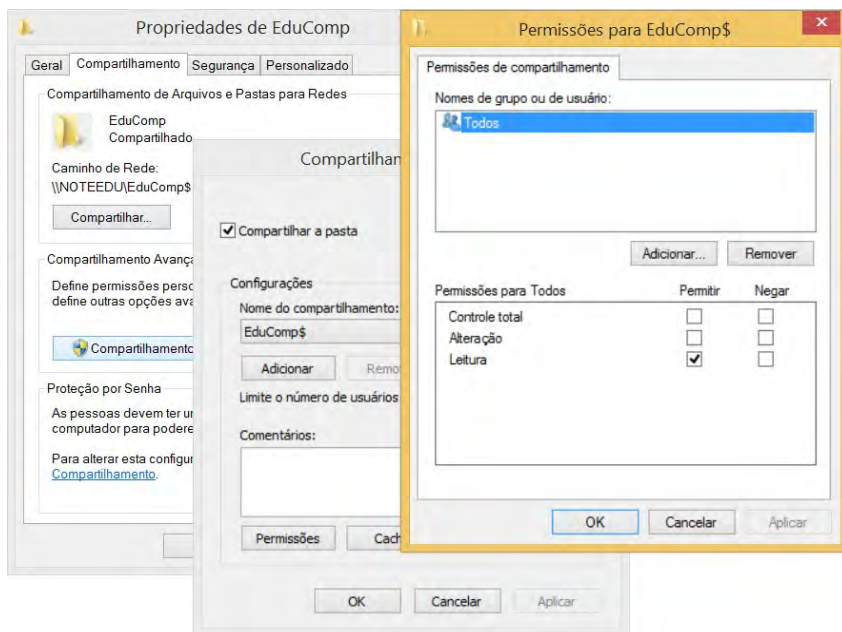
IMPORTANTE

As permissões NTFS, assim como as permissões de compartilhamento, são cumulativas. E assim como nas permissões de compartilhamento, nas permissões NTFS negar tem prioridade sobre qualquer permissão.

Quando um usuário pertence a vários grupos com diferentes permissões (quer seja permissões de compartilhamento ou NTFS), a permissão efetiva é a soma das permissões.

- NEGAR tem prioridade sobre permitir.
 - Permissões de compartilhamento
- SOMA: leitura + modificar + negar leitura = negar Leitura
 - Permissões NTFS
- SOMA: modificar + controle total + modificar = controle total
 - Compartilhamento e NTFS = negar Leitura (a mais restritiva)

Para ficar claro a diferença, veja que a seguir temos uma pasta chamada EduComp , que está compartilhada como \\NOTEEDU\EduComp\$. As propriedades dessa pasta permitem validar que seu compartilhamento está com permissão de leitura para todos os usuários da rede. Porém, pela presença do símbolo de \$, somente aquele que souber o caminho completo poderá efetuar o acesso.



O guia de Segurança trabalha com permissões NTFS e o guia de Compartilhamento trabalha com permissões relacionadas ao compartilhamento pela rede. As permissões de compartilhamento básicas são leitura, alteração e controle total, com as premissas de permitir ou negar uma determinada ação.

Já pelo guia de segurança é possível configurar permissões como controle total, modificar, ler & executar, listar conteúdo da pasta, leitura, gravar e permissões especiais.

10.2 HERANÇA DE PERMISSÕES

O conceito de herança funciona de forma simples. Depois de definirmos as permissões em uma pasta pai, os novos arquivos e subpastas nela criados herdam essas permissões. Ou seja, se você criar uma ramificação de vinte subpastas, por padrão as permissões da pasta raiz serão herdadas para toda a estrutura de diretórios. Para

que eles não herdem as permissões, é necessário selecionar a opção de remoção de herança nas propriedades da pasta.

Cuidado, muito cuidado ao habilitar ou desabilitar heranças em pastas que contenham muitas subpastas e arquivos, pois a replicação dessa configuração pode afetar toda a estrutura de uma única vez. Para configurar a herança, clique com o botão direito do mouse no arquivo ou no subpasta que deseja configurar, depois clique em *Propriedades*, guia *Segurança*, e em *Avançado* desmarque a caixa de seleção incluir permissões herdáveis provenientes do pai deste objeto.

Permissões





Compartilhamento

Auditoria

Acesso Efetivo

Para obter informações adicionais, clique duas vezes em uma entrada de permissão. Para modificar uma entrada de permissão, selecione-a e clique em Editar (se disponível).

Entradas de permissão:

Tipo	Entidade de segurança	Acesso	Herdado de	Aplicável a	
	Permitir	Administradores (Note...	Controle total	C:\	Esta pasta, subpastas e arquivos
	Permitir	SISTEMA	Controle total	C:\	Esta pasta, subpastas e arquivos
	Permitir	Usuários (NoteEdu)\Usu...	Ler & executar	C:\	Esta pasta, subpastas e arquivos
	Permitir	Usuários autenticados	Modificar	C:\	Esta pasta, subpastas e arquivos

Adicionar

Remover

Exibir

Desabilitar herança

☐ Substituir todas as entradas de permissão de objetos filho por entradas de permissão herdáveis desse objeto

IMPORTANTE

Observe que, caso as opções na coluna *Permitir* estejam marcadas, porém sem permissão para modificação, e tentarmos alterá-las clicando com o mouse, nada acontece. Isso significa que a pasta "herdou" as permissões do objeto pai.

Esse é o comportamento padrão mantido pelos sistemas operacionais Microsoft desde o Windows 2000 Server até o Windows Server 2012 R2. Cuidado com pequenos cenários de prova que tenham algo semelhante e a resposta seja direcionada ao desativamento da herança. Esse tipo de questão pode cair tanto na prova 70-410 quanto na prova 70-411 do MCSA.

10.3 SHADOWN COPY (CÓPIA DE SOMBRA)

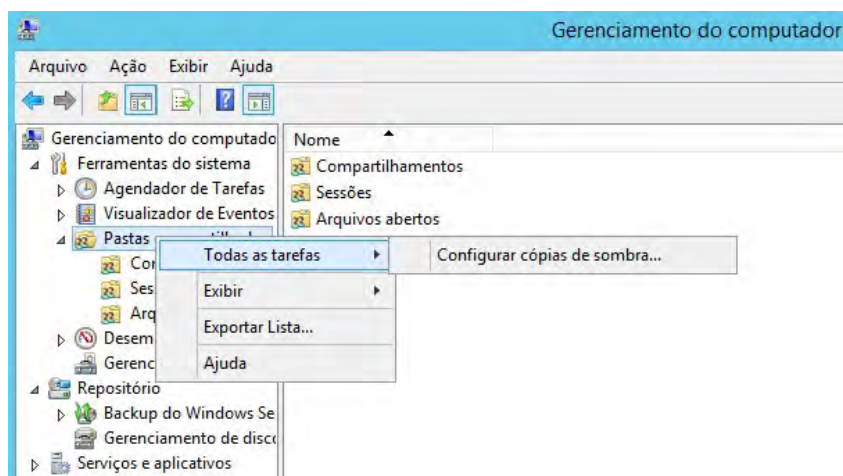
O recurso de cópia de sombra não é uma novidade, mas será cobrado de você nas provas do Windows Server 2012 R2 devido sua grande utilidade e facilidade para recuperação de arquivos através dos próprios usuários. É uma ferramenta de extrema qualidade operacional que está presente desde o Windows Server 2003.

O recurso de Shadown Copy, ou cópias de sombra, realizam cópias datadas de arquivos que estão localizados em recursos compartilhados, como um servidor de arquivos, por exemplo. Com as cópias de sombra, os usuários podem exibir pastas e arquivos compartilhados do modo em que existiam em datas e momentos anteriores, funcionando como uma fotografia de um determinado arquivo.

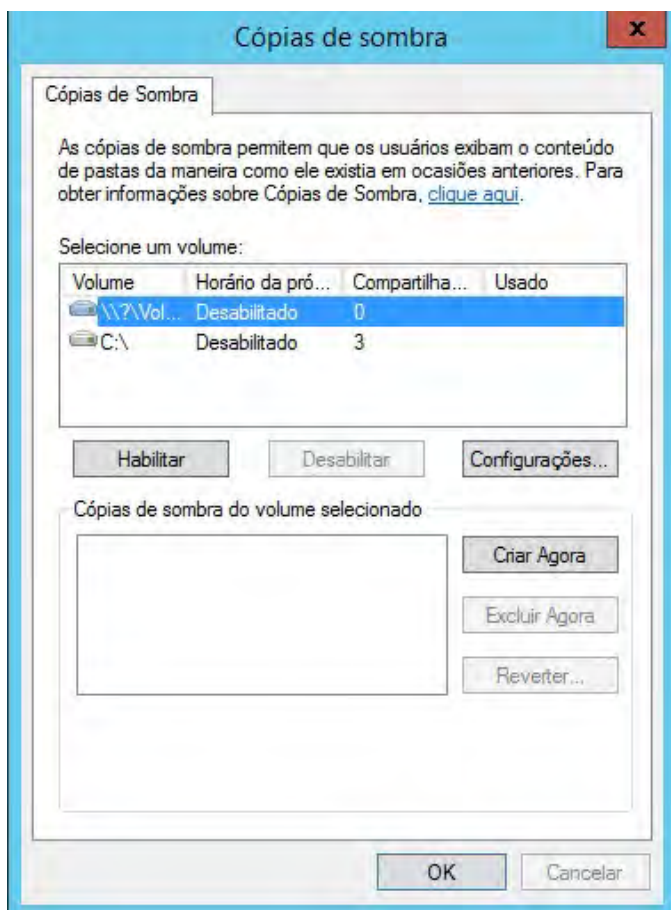
É o primeiro ponto de recuperação antes do restore de backup

que pode poupar muito tempo e recursos de sua equipe técnica. Isso porque pequenas modificações não necessitam de restores mais complexos.

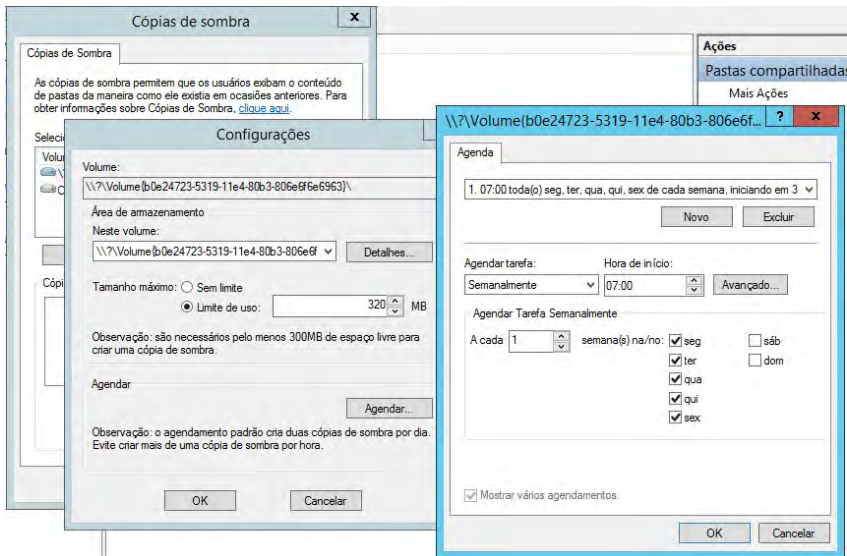
Para configurar a cópia de sombra, é necessário abrir o *Gerenciamento do Computador*, clicar com o botão direito em *Pastas compartilhadas*, depois *Todas as Tarefas*, e então configurar cópia de sombra, conforme demonstrado pela próxima figura.



A cópia de sombra é aplicada em um volume permitindo que os dados ali contidos possuam uma cópia espelho dentro do próprio servidor. A próxima figura ilustra a aplicação das cópias de sombra e a possibilidade de configuração de quantidade de vezes em que a cópia é gerada e nos dias da semana. É possível direcionar os detalhes através do botão de configurações.



Cuidado com o acionamento do recurso de cópia de sombra, pois ele consumirá uma grande quantidade de disco e recursos relacionados a espaço. Caso haja um grande consumo de disco, pode se fazer necessário o aprimoramento da configuração. A próxima figura demonstra exatamente a configuração das cópias de sombra em questão de tamanho máximo utilizado e agendamento para a geração da sombra.



Com o recurso de cópia de sombra, a autonomia dos usuários em questão de recuperação de seus arquivos aumenta muito, reduzindo a necessidade da interação da equipe de suporte. Os usuários terão acesso para executar as seguintes tarefas:

- Se você excluir acidentalmente um arquivo, poderá abrir uma versão anterior dele e copiá-lo para um local seguro desde que não atualizado pelo agendamento da sombra;
- Se você acidentalmente substituir um arquivo, poderá recuperar uma versão anterior do arquivo, porém o número de versões depende da quantidade de “fotografias no tempo” que você criou;
- Comparar versões de um arquivo enquanto trabalha. Você pode usar versões anteriores quando quiser verificar as mudanças entre versões de um arquivo.

A prova colocará você em uma situação de cobrança dos detalhes sobre o funcionamento da ferramenta Shadown Copy. Ai

vão algumas dicas importantes que devem ser estudadas a fundo para a prestação da prova 70-410:

- Quando você restaurar um arquivo, as permissões de arquivo não serão alteradas. As permissões permanecerão as mesmas que eram antes de o arquivo ser restaurado. Quando você recuperar um arquivo que foi acidentalmente excluído, as permissões de arquivo serão definidas para as permissões padrão do diretório. Ou seja, se você recuperar um arquivo para uma determinada pasta, o arquivo absorve suas permissões (essa é uma questão clássica e confunde com relação as permissões NTFS).
- A opção cópias de sombra de pastas compartilhadas está disponível em todas as edições do Windows Server 2008 R2 e Windows Server 2012 R2. Portanto, mesmo que o enunciado não seja relacionado ao servidor mais atual, a resposta é a mesma. Entretanto, é bom lembrar que a interface gráfica do usuário não está disponível para a opção de instalação Server Core, ou como gostam de chamar, Núcleo de Servidor. Para criar cópias de sombra para computadores com uma instalação Núcleo do Servidor, você precisa gerenciar esse recurso remotamente de outro computador (lembre-se do ADAC e o comando `winrm quickconfig`).
- A criação de cópias de sombra não substitui a criação de backups regulares, portanto nunca deixe de efetuar continuamente os backups pelo gerenciador de backups do Windows. A cópia de sombra permite a rápida recuperação de arquivos baseado em um momento no tempo, e não em uma cópia de segurança. Então, fique

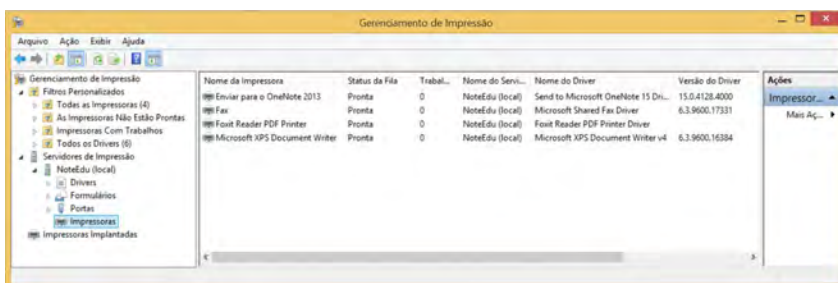
atento a perguntas que excluem o backup convencional.

- Quando os limites da área de armazenamento forem atingidos, a cópia de sombra mais antiga será excluída para abrir espaço para que outras cópias de sombra sejam criadas. Depois que uma cópia de sombra for excluída, ela não poderá ser recuperada, ou seja, nesse ponto você precisará do restore do backup.
- O local de armazenamento, a alocação de espaço e o agendamento podem ser ajustados para se adequarem às suas necessidades. Na página *Propriedades do Disco Local*, na guia *Cópias de Sombra*, clique em *Configurações*, ou pelo *Gerenciamento do computador* na área de pastas compartilhadas. Conheça ambas as formas de chegar a área de configuração das cópias de sombra.
- Há um limite de 64 cópias de sombra por volume que podem ser armazenadas. Quando esse limite for atingido, a cópia de sombra mais antiga será excluída e não poderá ser recuperada.
- As cópias de sombra são somente leitura. Não é possível editar o conteúdo de uma cópia de sombra.
- Só é possível habilitar cópias de sombra de pastas compartilhadas por volume — isto é, não é possível selecionar pastas e arquivos compartilhados específicos de um volume para serem copiados e não copiados.

10.4 SERVIDOR DE IMPRESSÃO

É muito comum usarmos um servidor dedicado para cuidar de nossas impressoras, seja pela facilidade do gerenciamento de

impressões ou da configuração de pooling de impressoras dedicadas para uma determinada atividade. Outra grande vantagem de utilizarmos os recursos de um servidor de impressão é o direcionamento de gestão de memória e disco para cache de impressões. Vá até o executar e digite `printmanagement.msc` para acionar o painel de gerenciamento de impressoras, conforme demonstrado pela próxima figura.



O gerenciador de impressão permite uma visão aprimorada dos recursos de um servidor, como por exemplo, a criação de spoolers de impressão, gerenciamento e backup de drivers de impressoras, gestão de impressões e portas específicas (úteis em configurações de impressoras de cupom fiscal).

Apesar de não ser cobrado diretamente dentro de provas de certificação, o acesso a este gerenciador pode ser solicitado, então guarde o `printmanagement.msc`. Você pode ser questionado sobre a criação de spoolers de impressão e, antes de sairmos configurando este recurso, é interessante entender seu funcionamento.

Os spoolers de impressão, também conhecidos como *print pooling*, são usados para distribuir impressões sequencialmente para diversas impressoras. Imagine uma grande empresa que possui cerca de 20 impressoras. Toda vez que uma estiver ocupada, a próxima da fila recebe e imprime o trabalho.

Um pool de impressão é uma impressora lógica conectada a várias impressoras através de várias portas do servidor de impressão, acessíveis pelo painel de controle ou pelo Gerenciador de impressões `printmanagement.msc`. Isso é útil em uma rede com grande volume de impressão, pois diminui o tempo que os usuários devem esperar por seus documentos.

Um pool de impressão também simplifica a administração, pois várias impressoras podem ser gerenciadas a partir da mesma impressora lógica em um servidor. No laboratório, você receberá os dados de como efetuar a criação de um pool de impressoras. Lembre-se de que as perguntas relacionadas a este recurso podem garantir pontos importantes para a obtenção da prova 70-410.

Você deve considerar algumas coisas para a prova e o gerenciamento de impressoras:

- Todas as impressoras em um pool devem usar o mesmo driver.
- Já que os usuários não saberão qual impressora no pool imprimirá determinado documento, certifique-se de que todas as impressoras no pool estão localizadas no mesmo local.

GPO — GROUP POLICYS

As Group Polycys, tratadas neste conteúdo simplesmente por GPO, são capazes de mudar configurações de equipamentos e navegadores, restringir ações e até mesmo distribuir aplicações em seu ambiente de redes em estações que contenham o Windows instalado. As vantagens são muitas, e podem ser aplicadas em sites, domínios e *organizational units* (conhecidas como OUs).

Se você criou uma OU para cada departamento da sua empresa, poderá fazer diferentes configurações de GPO para cada departamento, incluindo a mudança de senhas de usuários locais, como um administrador local. Ou ainda, o direcionamento de configurações de uma estação para um proxy, e até mesmo a cópia de arquivos para uma determinada estação de trabalho.

As políticas de grupo, que tratarei como GPO daqui por diante, possuem três estados básicos de funcionamento:

- **Ativada (*Enable*):** especifica que aquele item será ativado.
- **Desativada (*Disable*):** especifica que aquele item será desativado.
- **Não configurado (*Not configured*):** deixa a opção neutra, nem ativa e nem desativa o item, ou seja, fica como está agora. Esta é a configuração padrão.

O interessante é que, quando uma GPO está marcada como não

configurada, significa que existem padrões de configuração ativos pelo sistema operacional que não receberam a personalização do usuário. Ou seja, existem regras ativas para uma determinada ação, porém nenhuma customização foi efetuada.

Indo mais a fundo dentro do conceito, podemos definir uma GPO como um objeto que contém uma ou mais configurações de política que aplicam definições de configuração para usuários, computadores ou ambos. Os modelos de GPO são armazenados dentro da SYSVOL, enquanto os objetos contêineres de GPO são armazenados no Active Directory.

Os modelos administrativos (ou Administrative Templates) estão em formato de extensão `.adm` e `.admx`, sendo o `.admx` o usado pelo Windows Server 2012 R2. Os templates administrativos compõem uma série de configurações e modelos prontos que podem ser ativados de forma simplificada.

Outro ponto importante relacionado às regras e políticas é o fato da separação de configurações específicas pela área de preferências da política. Por exemplo, nas versões anteriores do Windows, as configurações do Internet Explorer ficavam dentro da estrutura da política, mas hoje são feitas através das preferências (*preferences*).

Vale saber como curiosidade que, por padrão, as políticas de grupo não redirecionam navegadores como Google Chrome e Firefox, porém é possível baixar e instalar modelos `.adm` e `.admx` para esse fim. Existem modelos específicos que permitem a administração e configuração de navegadores diversos por regras aplicadas aos domínios. Vale a dica de bons administradores de baixar e testar tais modelos que, mesmo não sendo utilizados em provas de certificação, são extremamente úteis para o dia a dia.

11.1 HIERARQUIA DAS GPOS

Um dos conhecimentos que será cobrado de você ao longo das provas do MCSA é o conceito sobre a hierarquia das políticas de grupo. A cobrança é indireta e pode vir bem camuflada dentro de uma questão na qual, após a aplicação de uma GPO, parte do ambiente funciona e outra não.

Por experiência, posso dizer que grande parte de as aplicações de GPO não apresentarem resultado positivo em ambientes específicos deve-se à hierarquia de aplicação. A hierarquia das GPOs pode ser aplicada em quatro níveis diferentes (em ordem):

- **Local** — São aplicados localmente em uma estação de trabalho ou servidor, geralmente em redes Workgroups pelo console mmc (abra o executar e digite mmc para acessar o console de políticas locais).
- **Sites** — É o mais alto nível em que todas as configurações efetuadas serão aplicadas a todos os domínios que fazem parte dele.
- **Domínios** — É o segundo nível direto, ou seja, as configurações feitas aqui afetarão todos os usuários e grupos dentro do domínio.
- **OUs** — É o nível mais baixo da aplicação das políticas. O que se aplica nas OUs afetará todos os objetos dentro dela, seja usuários ou computadores.

Você precisará saber quando aplicar uma determinada GPO dentro da cadeia hierárquica. Por exemplo, imagine uma empresa que possui três servidores Proxy diferentes, onde alguns departamentos possuem saída para a internet. Posso direcionar diversas OUs para que usem configurações personalizadas.

É importante lembrar de que as opções relacionadas às GPOS são cumulativas por padrão. Ou seja, se eu sou um usuário da OU RH, posso receber configurações que vem do site, domínio e da

minha própria OU RH. Isso pode causar um certo problema quando uma política interfere em uma ação específica de forma permissiva, e outra dentro da mesma ação, mas de forma negativa.

Imagine que você possui uma GPO no Domínio permitindo e outra GPO na OU negando um determinado acesso. Qual será aplicada? Temos aqui um conflito de permissões e, neste caso, a última a ser aplicada vale como prioritária.

É também interessante ressaltar que os usuários pertencentes ao grupo de administradores de domínio podem desabilitar o processamento das GPOs locais nos clientes que estejam executando sistemas operacionais cliente Windows e sistemas operacionais Windows Server. Assim, habilitam a configuração de política Desativar Processamento de Objetos de Políticas de Grupo Locais em um GPO de domínio.

Pode ser cobrado de você durante a prova algo relacionado ao tipo de permissão necessária para desativação do processamento, na qual a resposta é adicionar um determinado usuário ao grupo de Administradores do Domínio. Caso precise manter um mínimo de restrição de acesso a um determinado grupo de usuários, é possível adicionar um grupo específico ou usuário ao grupo Proprietários Criadores de Política de Grupo, e conceder permissão explícita ao grupo ou ao usuário para criar GPOs usando o GPMC.

IMPORTANTE

Você não pode vincular um GPO a um contêiner, mas pode vincular uma GPO a uma OU. Cuidado com perguntas que criem o panorama de vínculo de políticas. Entenda que existe uma grande diferença entre Unidades Organizacionais e contêineres.

Fique atento a perguntas que envolvam os filtros WMI. A filtragem WMI é o processo de personalização do âmbito de aplicação da GPO, optando por um filtro de Windows Management Instrumentation (WMI). Esses filtros permitem que os administradores apliquem as GPOs apenas para um determinado caso, por exemplo, computadores de modelos específicos, valores de memória RAM, software instalado, qualquer coisa disponível via consultas WMI. São extremamente úteis para a aplicação da política sob circunstâncias relacionadas a uma dependência física de hardware.

Algo interessante a ser ressaltado que pode ser cobrado de você tanto pelo MCSA do Windows Server 2012 quanto pelo MCSA do Windows 8 é que, a partir do Windows 8, houve a introdução de um novo recurso de atualização das diretivas de grupo. Este permite que um administrador possa forçar uma atualização de política de grupo em todos os computadores com contas em uma determinada unidade organizacional. Isso permite criar uma tarefa agendada no computador que executa o comando `GPUPDATE` dentro de 10 minutos, ajustado por um deslocamento aleatório para evitar sobrecarregar o controlador de domínio.

Nenhum dos contêineres padrão no domínio do AD DS podem ter GPOs vinculados a eles, exceto a UO de controladores de domínio e o próprio domínio. Todos os outros contêineres são apenas pastas.

Para vincular GPOs a fim de aplicar configurações e restrições, crie uma hierarquia de UOs e, em seguida, vincule GPOs a elas. Veremos ainda dentro deste capítulo os detalhes relacionados à herança de GPOs e suas características.

11.2 HERANÇAS DE GPOS

Utilizando ainda o exemplo anterior, o que aconteceria se configurássemos uma GPO para o domínio que muda a senha a cada 30 dias? Haveria um conflito de GPOs, pois no site está configurado para mudar a senha a cada 50 dias. Por isso, é importante entender como ocorrem as heranças de GPOs.

É muito comum falarmos de herança em aplicação de regras de permissionamento de acesso e políticas de grupo, pois esse tipo de recurso facilita muito a vida dos administradores de redes. O recurso de herança permite que um objeto receba uma configuração geral efetuada diretamente na estrutura de um controlador de domínio de forma simplificada.

Sem o recurso da herança, seríamos obrigados a efetuar a configuração da GPO em centenas ou milhares de objetos por vez. Isso não seria nada agradável, além de consumir muito tempo e esforço.

Por padrão, quem está mais próximo do objeto usuário tem preferência na aplicação da GPO sobre as configurações mais

genéricas. No nosso exemplo, a GPO do domínio será aplicada como prioritária.

Entretanto, o Administrador do Sistema pode alterar esse comportamento através de duas opções descritas a seguir:

- *Block Policy Inheritance* (Bloquear heranças de políticas): especifica que as configurações da GPO para um objeto não serão herdadas do nível superior. Isso é muito usado quando se tem uma OU dentro de outra e você quer aplicar uma configuração específica para aquela OU.
- *Force Policy Inheritance* (Forçar herança de políticas): especifica que você não permitirá que níveis filhos possam sobrescrever suas configurações de GPO. Por exemplo, sou administrador de um site da minha empresa, criei uma política de senha forte através de GPO com 9 caracteres e não quero que o Administrador do Domínio e nem o das OUs dos domínios possam sobrescrever minha política. Neste caso, crio minha GPO, aplico ao site e marco a opção de Force Policy Inheritance.

Para criar políticas locais, utilizamos o console chamado mmc . Mas para criarmos políticas em redes nas quais existem controladores de domínio, é necessário a utilização do GPMC (*Group Policy Management Console*). É possível utilizar o GPMC acessando o controlador de domínio, *Server Manager, Tools*, e então *Group Policy Management Console*, ou por meio de qualquer estação de trabalho com Windows 8 e a ferramenta RSAT.

IMPORTANTE

Com o Console de Gerenciamento de Política de Grupo, é possível editar GPOs e gerenciar sua aplicação no AD DS. Caso seja questionado pela prova, lembre-se de que a ferramenta a ser utilizada é o GPMC.

As configurações de usuário disponíveis são as mesmas entre todos os objetos de Diretiva de Grupo Local, fazendo com que muitas vezes existam conflitos de GPO. A partir da versão Windows Vista, é aplicado um método específico para resolver este tipo de conflito de GPOs. É utilizado o método de "última escrita wins".

Este resolve o conflito, substituindo qualquer configuração anterior com a última leitura de ajuste (mais atual). Isso significa que a *última escrita wins* faz com que a GPO válida real seja a última aplicada. Se você possui duas políticas definindo a quantidade de caracteres de senha, vale a última aplicada.

11.3 GPUPDATE

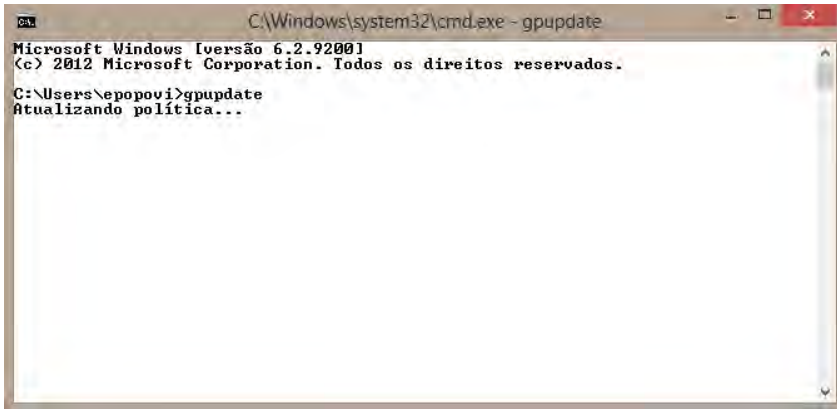
O `gpupdate` é um comando usado para forçar a atualização das políticas de grupo em uma determinada estação de trabalho. Ele pode ser de extrema utilidade quando pretendemos replicar atualizações de política sem a necessidade da reinicialização do equipamento ou do simples logoff do usuário.

A sintaxe do comando é simples e pode seguir este padrão:

```
gpupdate [/target:{computer|user}] [/force]
[/wait:value] [/logoff] [/boot] .
```

Faça um teste acessando o prompt de comando de sua estação

de trabalho e digitando `gpupdate /force` . A próxima figura ilustra a aplicação do comando.



O comando é muito útil e pode ser complementado por uma série de parâmetros, conforme descrito pela tabela a seguir. É muito provável que este comando seja cobrado pela prova 70-410, então estude-o bem. Veja a seguir os parâmetros e suas descrições.

- `/Target:{Computer | User}` — Especifica que somente as configurações de política são atualizadas.
- `/Force` — Reaplica todas as configurações de política. Por padrão, apenas configurações de políticas que foram alteradas são aplicadas.
- `/Wait:{valor}` — Define o número de segundos para aguardar a política processando para terminar. O padrão é 600 segundos. O valor '0' representa não esperar. O valor '-1' representa esperar indefinidamente. Quando o limite de tempo é ultrapassado, o prompt de comando reaparece, mas a política processando continua.
- `/Logoff` — Causa um logoff depois que as configurações foram atualizadas. Isto é necessário para extensões de cliente da política de grupo que não

processam políticas em um ciclo de ciclo de atualização, mas processam a política quando um usuário faz logon. Exemplos incluem instalação de software e redirecionamento de pastas do usuário. Esta opção não se aplica se não houver extensões chamadas que exijam um logoff.

- */Boot* — Causa a reinicialização do computador depois que as configurações de política de grupo são aplicadas. É necessário para extensões do cliente de política de grupo que não processam uma política em um ciclo de atualização de segundo plano atualização em segundo plano, mas processam uma política na inicialização do computador. Exemplos incluem instalação de software do computador. Esta opção não é aplicada se não houver extensões chamadas que exijam reinicialização.
- */Sync* — Faz com que o próximo aplicativo da política em primeiro plano seja feito de maneira síncrona. Aplicativos de primeiro plano de política ocorrem na inicialização do computador e no logon. Pode ser especificado para o usuário, computador do usuário ou ambos, usando o parâmetro */Target*. Os parâmetros */Force* e */Wait* serão ignorados se especificado.

DICA

Como alternativa para usar as configurações de conta de usuário individual, é possível utilizar GPOs para gerenciar essas configurações. Você pode definir as configurações de Redirecionamento de Pasta usando o Editor de Gerenciamento de Política de Grupo para abrir um GPO para edição e, em seguida, navegar até o nó Configuração do Usuário\Políticas\Configurações do Windows.

Lembre-se de que o redirecionamento da OU Computers de um Active Directory só pode receber um único direcionamento através do `redircmp`. Você deve executar o comando `redircmp` em um prompt de comando com permissões administrativas e não precisa da GPO para isso.

11.4 GPRESULT

Esta ferramenta de linha de comando permite retornar as configurações de diretiva de grupo ativas para um respectivo usuário ou computador específico dentro da estrutura de redes de um domínio. Os administradores de redes podem executar o `gpresult` em qualquer computador remoto dentro de seu escopo de gerenciamento. Por padrão, o `gpresult` retornará as configurações ativas no computador em que for executado.

Esta ferramenta de linha de comando é muito útil para identificar problemas em políticas, e pode ser cobrado pela prova 70-410 e 70-411. Você pode utilizar a ferramenta de linha de comando acompanhado de um sinal de maior e o nome de um arquivo `.txt`, gerando um arquivo de log bem detalhado. Veja a

seguir os parâmetros e suas descrições.

- `/s Computer` — Especifica o nome ou endereço IP de um computador remoto (não use barras invertidas). O padrão é o computador local.
- `/u Domain\User` — Executa o comando com as permissões de conta do usuário especificado por `Usuário` ou `Domínio\Usuário`. O padrão são as permissões do usuário que fez logon no computador que emite o comando.
- `/p Password` — Especifica a senha da conta de usuário especificada no parâmetro `/u`.
- `/user TargetUserName` — Especifica o nome de usuário do usuário cujos dados RSOP serão exibidos.
- `/scope {user|computer}` — Exibe o usuário ou os resultados do computador. Valores válidos para o parâmetro `/scope` são usados no computador. Se você omitir o parâmetro `/scope`, `gpresult` mostra as configurações tanto do usuário quanto do computador.
- `/v` — Especifica que a saída mostre informações detalhadas de diretiva.
- `/z` — Especifica que a saída mostre todas as informações disponíveis sobre a Diretiva de Grupo. Como esse parâmetro produz mais informações do que o parâmetro `/v`, redirecione a saída para um arquivo de texto quando utilizar esse parâmetro (por exemplo, `gpresult /z >diretiva.txt`).
- `/?` — Mostra a ajuda no prompt de comando.

HYPER-V

12.1 VIRTUALIZAÇÃO MICROSOFT

Alguns termos técnicos devem ser entendidos antes de adentrarmos o mundo das máquinas virtuais, como por exemplo, máquina host e unidade virtual.

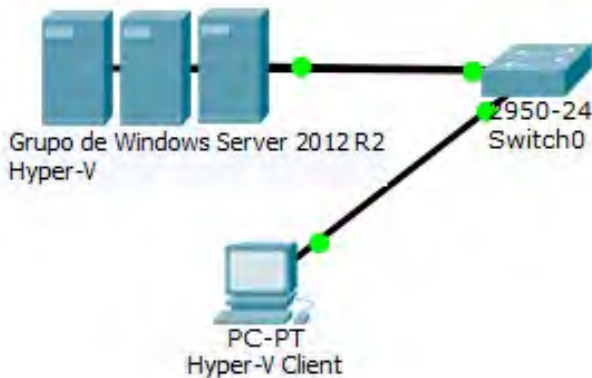
- **Máquina host:** servidor que comporta a virtualização e as máquinas virtuais.
- **Servidor legado:** servidor com uma aplicação antiga e *geralmente* não virtualizado.
- **VM:** a Máquina Virtual (ou Virtual Machine) é exatamente a emulação do hardware e a composição do sistema operacional, seja ele Microsoft ou não. É possível executar várias máquinas virtuais que estejam usando diferentes sistemas operacionais em um servidor de virtualização simultaneamente, desde que esse servidor de virtualização tenha recursos suficientes. Máquinas virtuais com sistemas open source podem necessitar de drivers específicos de redes para funcionar em um ambiente virtualizado Microsoft. No caso do Windows Hyper-V Server, é muito comum a necessidade da instalação de drivers de controladora HBA para comunicação com storages SAN.
- **Convidados de máquinas virtuais:** são máquinas

virtuais que funcionam como estações de trabalho, geralmente relacionadas à técnica chamada de VDI, ou virtualização de desktop. Quando os usuários entram em uma máquina virtual convidada remotamente usando a RDC (conexão de Área de Trabalho remota) ou uma sessão remota do console do Windows PowerShell, você precisa examinar de perto as propriedades do computador no qual o usuário está trabalhando para determinar se ele é uma máquina virtual ou uma máquina física tradicionalmente implantada.

Na teoria, a virtualização é fácil de se implementar, porém, na prática, existem inúmeras regras relacionadas a um manual de boas práticas que permite o funcionamento correto do ambiente. Por exemplo, a prática que recomenda a você que não implante um servidor de caixa de correio do Microsoft Exchange no mesmo computador que contenha uma função de controlador de domínio; ou ainda, a boa prática que recomenda a você que não implante uma instância de banco de dados do SQL Server 2012 no mesmo computador que contenha a função de controlador de domínio. Em vez disso, implante cada uma dessas cargas de trabalho em máquinas virtuais separadas, e depois execute essas máquinas virtuais como convidadas no mesmo servidor de virtualização.

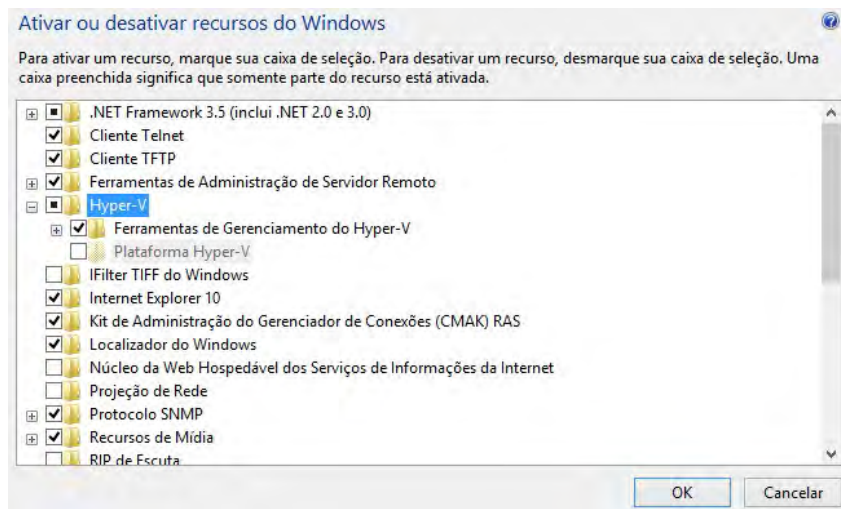
Você pode ser cobrado não só pela implantação do Hyper-V, mas pela melhor utilização de recursos e práticas recomendadas. Tais práticas afetam diretamente tanto o desempenho de servidores como o bom funcionamento do ambiente. Logo, devem ser levadas muito a sério durante a elaboração do escopo de projeto de implementação do Hyper-V.

12.2 CLIENT HYPER-V



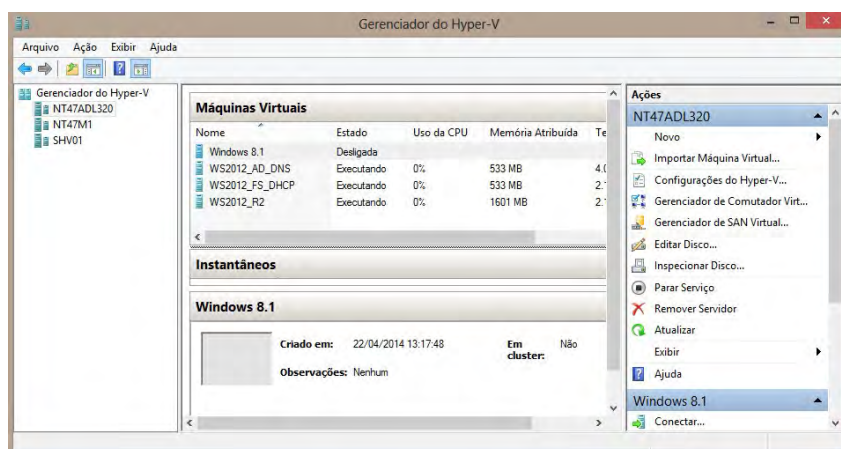
O cliente Hyper-V vem nativo com o Windows Server 2012, 2012 R2, Windows 8 e 8.1. É necessário instalar os componentes relacionados ao Hyper-V para que o Cliente de Acesso seja instalado.

A próxima figura ilustra essa instalação em uma estação com Windows 8.1. Já no Windows Server 2012 R2 o processo é efetuado através do Server Manager.



O cliente Hyper-V e o recurso do Hyper-V nos sistemas operacionais Windows 8 Pro e o Windows 8 Enterprise têm requisitos de processador um pouco diferentes que o Hyper-V nativo no Windows Server 2012 e Windows Server 2012 R2. Especificamente, com os sistemas operacionais cliente Windows 8, o computador deve ter uma plataforma x64 com suporte para SLAT segundo nível e Address Translation (conversão de endereços de segundo nível), e ter um mínimo de 4 GB de RAM. Isso é diferente do Hyper-V no Windows Server 2012, que não requer a SLAT.

O gerenciador do Hyper-V funciona como uma tela de conexão rápida aos servidores que possuem gerenciamento em máquinas virtuais. Notem que é possível gerenciar mais de um servidor por vez, conforme demonstrado aqui pela próxima figura. É possível também, pelo gerenciador do Hyper-V, verificar o consumo da CP e memória atribuída.



O principal componente que está disponível para o Hyper-V do Windows Server 2012 R2 que não está disponível para o Windows 8.1 é a migração de máquinas virtuais. O cliente Hyper-V também não dá suporte para aplicativos de publicação que são instalados na máquina virtual convidada para o menu Iniciar do sistema

operacional de gerenciamento. Esse era um recurso do Modo Windows XP no Windows 7, que usa o Windows Virtual PC.

12.3 REQUISITOS DE HARDWARE PARA O HYPER-V

O servidor no qual você planeja instalar a função Hyper-V deve atender aos seguintes requisitos de hardware:

- Plataforma x64 com suporte para virtualização assistida por hardware e prevenção de execução de dados.
- Capacidade de CPU suficiente para atender aos requisitos das máquinas virtuais convidadas.
- Uma máquina virtual hospedada no Hyper-V no Windows Server 2012 pode dar suporte a até 64 processadores virtuais.
- Deve possuir memória suficiente para dar suporte a todas as máquinas virtuais que devem ser executadas ao mesmo tempo, além de memória suficiente para executar o sistema operacional Windows Server 2012 host.
- O servidor deve ter, pelo menos, 4 GB de RAM.
- Uma máquina virtual hospedada no Hyper-V no Windows Server 2012 pode dar suporte a, no máximo, 2 terabytes (TB) de RAM.
- O desempenho do subsistema de armazenamento deve atender às necessidades de E/S (Entrada/Saída) das máquinas virtuais convidadas. Seja uma implantação local ou em redes SAN, talvez seja necessário inserir diferentes máquinas virtuais em discos físicos separados, ou implantar um RAID (*Redundant Array of Independent Disks*) de alto desempenho, uma SSD (unidade de estado sólido), uma SSD híbrida ou uma

combinação de todas essas três tecnologias.

- Os adaptadores de rede do servidor de virtualização devem ser capazes de dar suporte às necessidades de taxa de transferência de rede das máquinas virtuais convidadas. Você pode melhorar o desempenho da rede instalando vários adaptadores de rede e usando várias NICs (placas de interface de rede).

IMPORTANTE

O máximo de memória aceita por uma máquina virtual é de 2TB de memória RAM. Esse valor é especificamente relacionado à máquina virtual, e não ao hardware físico do servidor. Muito cuidado com questões que possam confundi-lo nessa relação de uso da memória RAM.

12.4 MEMÓRIA DINÂMICA

Na primeira versão apresentada do Hyper-V no Windows Server 2008, era possível atribuir uma quantidade estática de memória para máquinas virtuais, deixando em algum momento seu uso mal dimensionado. A menos que fossem tomadas precauções especiais para medir a quantidade exata de memória necessária para uma máquina virtual, a memória seria provavelmente alocada de maneira insuficiente ou excessiva, gerando o que chamamos de superdimensionamento ou dimensionamento degradado.

O recurso de memória dinâmica introduzido inicialmente pelo Windows 2008 R2 SP1 permite um melhor gerenciamento dessa memória alocada entre as máquinas virtuais, evitando a falha de alocação. É possível configurar um máximo e um mínimo de

memória disponível, fazendo com que as VMs trabalhem com maior equilíbrio e agilidade.

Posso permitir que uma máquina virtual receba prioridade de memória, ou ainda trabalhe permissão de solicitação de RAM adicional quando estiver atingindo seu pico de uso. A memória dinâmica será cobrada nas provas 70-410 e 70-412 em pequenos casos específicos, geralmente relacionados à falha ou à lentidão de máquinas virtuais. Fique atento a esse tipo de pergunta.

12.5 PAGINAÇÃO INTELIGENTE

Durante o processo de boot das máquinas virtuais, o consumo de memória RAM fica mais alto. O recurso de paginação inteligente atribui uma quantidade extra de memória apenas no período de boot da máquina virtual através de uma partição de disco para a memória temporária.

Esse processo permite a subida mais rápida e inteligente das máquinas virtuais. É possível configurar a paginação inteligente tanto pela área gráfica quanto pelo PowerShell, por meio do `cmdlet Set-VMemory`. Guarde bem este `cmdlet`, pois pode ser cobrado em questões relacionadas a servidores em modo de operação Server Core.

12.6 MEDIÇÃO DE RECURSOS

Por incrível que pareça, a medição de recursos de servidores com o Hyper-V instalado não pode ser feita pela área gráfica. Essa configuração deve ser feita apenas por PowerShell por meio dos seguintes `cmdlets`:

- `Enable-VMResourceMetering` — Inicia a coleta de dados para cada máquina virtual.

- `Disable-VMResourceMetering` — Desabilita a medição de recursos para cada máquina virtual.
- `Reset-VMResourceMetering` — Redefine contadores para medição de recursos de máquina virtual.
- `Measure-VM` — Exibe estatísticas de medição de recursos para uma máquina virtual específica.

12.7 ARQUIVOS DE ARMAZENAMENTO (VHD / VHDX)

Os discos virtuais podem ser tanto de extensão `.vhd` quanto `.vhdx`. A diferença entre esses arquivos é grande, principalmente em relação à resiliência e tamanho disponível.

O Windows Server 2008 introduziu o conceito de discos virtuais através de arquivos de extensão `.vhd`, sendo aprimorado agora no Windows Server 2012 o formato para `.vhdx`. É possível a conversão de discos `.vhd` para `.vhdx` sem a perda de dados através do Assistente para Edição de Discos Rígidos Virtuais, lembrando de que o sistema nativo deve ser Windows Server 2012 ou 2012 R2.

- VHDs com o formato `.vhdx` podem ter até 64 TB, enquanto VHDs com o formato `.vhd` estão limitados a 2 TB.
- VHDs com o formato `.vhdx` apresentam menos chances de serem corrompidos se o servidor de virtualização sofrer uma falta de energia inesperada.
- O formato `.vhdx` dá suporte a um alinhamento melhor quando implantado em um disco de setor grande.
- VHDs com o formato `.vhdx` podem conter VHDs dinâmicos e diferenciais maiores, o que significa que

esses VHDs apresentam melhor desempenho.

- Você pode criar discos de tamanho fixo ou dinâmicos de ambos os arquivos.

Para converter um VHD de tamanho fixo para dinâmico ou de dinâmico para fixo, siga os seguintes passos:

1. No console *Gerenciador do Hyper-V*, no painel *Ações*, clique em *Editar Disco*.
2. No *Assistente para Edição de Discos Rígidos Virtuais*, na página *Antes de Começar*, clique em *Avançar*.
3. Na página *Disco Rígido Virtual Local*, clique em *Procurar* e selecione o VHD que você deseja converter.
4. Na página *Escolher Ação*, clique em *Converter* e depois em *Avançar*.
5. Na página *Converter Disco Rígido Virtual*, escolha entre os formatos VHD e VHDX.
6. Na página *Converter Disco Rígido Virtual*, escolha entre *Tamanho Fixo* e *Expansão Dinâmica*. Se você também quiser converter o tipo de disco rígido, escolha o tipo apropriado e clique em *Avançar*.
7. Na página *Configurar Disco*, escolha o local de destino para o disco.

IMPORTANTE

Fique atento aos detalhes e diferenças entre os arquivos `.vhd` e `.vhdx`, pois serão cobrados pela prova 70-410 através de pequenas situações, como o tamanho do armazenamento, por exemplo.

Para criarmos um VHD de tamanho fixo, siga estas etapas:

1. Abra o console do *Gerenciador do Hyper-V*.
2. No painel *Ações*, clique em *Novo* e depois em *Disco Rígido*.
3. Na página *Antes de Começar do Assistente para Criação de Discos Rígidos Virtuais*, clique em *Avançar*.
4. No *Assistente para Criação de Discos Rígidos Virtuais*, na página *Escolher Formato de Disco*, clique em *VHD* ou em *VHDX* e depois clique em *Avançar*.
5. Na página *Escolher Tipo de Disco*, clique em *Tamanho Fixo* e depois em *Avançar*.
6. Na página *Especificar Nome e Local*, insira um nome para o VHD e depois especifique uma pasta na qual você deseja hospedar o arquivo VHD.
7. Na página *Configurar Disco*, escolha uma das seguintes opções:
 - Criar um novo disco rígido virtual em branco do tamanho especificado.
 - Copiar o conteúdo de um disco físico especificado. Com essa opção, você pode replicar um disco físico existente no servidor como um VHD. O VHD fixo terá o mesmo tamanho que o disco físico. Replicar um disco rígido físico existente não altera os dados nesse disco.
 - Copiar o conteúdo de um disco rígido virtual especificado. Com essa opção, você pode criar um novo disco rígido fixo com base no conteúdo de um VHD existente.

DICA

Você ainda pode utilizar o `cmdlet New-VHD` para criar arquivos VHD. Você pode ser cobrado na prova para este item, então vale a pena treinar sua utilização.

Algo que pode ser cobrado de você pela prova 70-410 é o uso de discos de conexão direta, que nada mais é que o acesso de uma máquina virtual em um disco físico. Esta técnica pode se fazer de extrema utilidade quando acompanhada do uso de unidades lógicas acompanhadas por storages e controladoras HBA, ou até mesmo armazenamento através de unidades lógicas iSCSI. É importante lembrar de que você deve deixar o disco off-line para usar esta técnica.

Para anexar discos físicos através do armazenamento com conexão direta, siga os seguintes passos:

1. Verifique se o disco rígido de destino está offline. Se não estiver offline, use o console de *Gerenciamento de Disco* no servidor de virtualização para colocá-lo offline.
2. Use o console *Gerenciador do Hyper-V* para editar as propriedades da máquina virtual existente.
3. Clique em um controlador IDE ou SCSI, clique em *Adicionar* e, em seguida, em *Disco Rígido*.
4. Na caixa de diálogo *Disco Rígido*, clique em *Disco Rígido Físico*. No menu suspenso, selecione o disco que você deseja usar como armazenamento com conexão direta.

12.8 INSTANTÂNEOS — SNAPSHOTS

Os atuais instantâneos, antigos *snapshots*, são momentos no tempo armazenados em uma linha de modificações. São simplesmente imagens estáticas de uma máquina virtual. Através de um instantâneo, é possível retornar a um ponto específico no tempo antes de uma determinada configuração.

Por exemplo, você pretende atualizar uma aplicação virtualizada, mas tem medo de que essa atualização comprometa o funcionamento da máquina virtual. Pode-se tirar um instantâneo do

momento em que ela funciona perfeitamente. Caso ocorra algum problema após a instalação da atualização, é possível retornar ao ponto no tempo em que tudo funcionava.

Apesar de extremamente úteis, os instantâneos não devem substituir os backups através do Windows Backup ou de ferramentas de terceiros. Instantâneos são armazenados no mesmo volume que os VHDs e, se esse volume falhar, tanto os instantâneos quanto o arquivo VHD serão perdidos. Os instantâneos são úteis para diversos momentos, mas não para serem backups de um ambiente.

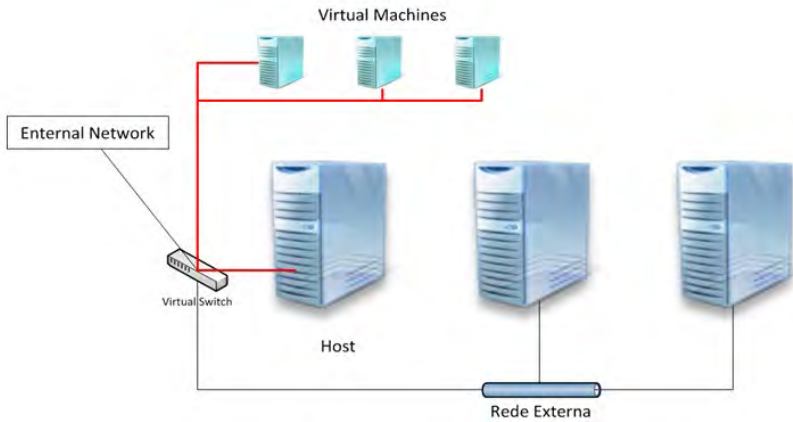
12.9 COMUTADOR VIRTUAL — SWITCH VIRTUAL

Para utilizar o Hyper-V, é necessário antes criar um comutador virtual. Ele fará a comunicação entre a LAN e WAN, ou entre a máquina host e as máquinas virtuais. O comutador virtual é peça fundamental para a comunicação das máquinas virtuais e até da segmentação do tráfego de rede e uso da banda disponível.

O comutador virtual Hyper-V é um switch de rede de camada 2 baseado em software (é um switch virtualizado), que está disponível no Gerenciador Hyper-V quando a função de servidor Hyper-V é instalada. Ele inclui funcionalidades gerenciadas e extensíveis para conectar máquinas virtuais a redes físicas e a redes virtuais, fornecendo imposição de política para níveis de segurança, de isolamento e de serviço.

O comutador virtual do Hyper-V 3.0 do Windows Server 2012 R2 recebeu uma série de recursos novos e aprimorados de isolamento de locatários, modelagem de tráfego, proteção contra máquinas virtuais mal-intencionadas e solução de problemas simplificada. Posso dizer com muita segurança que o comutador do

Hyper-V 3.0 recebeu atenção redobrada para se adequar ao cenário mundial de computação em nuvem que aflora no mundo da TI.



Por meio do comutador virtual, é possível trabalhar com três tipos de interfaces com situações distintas:

- **Externo:** é o comutador que mapeia uma rede para um adaptador de rede específico ou uma equipe de adaptadores de rede. O Windows Server 2012 R2 dá suporte ao mapeamento de uma rede externa para um adaptador de rede sem fio quando o serviço de rede local sem fio está instalado no servidor de virtualização, e este último possui um adaptador compatível.
- **Interno:** comutadores virtuais internos se comunicam entre as máquinas virtuais no servidor de virtualização e entre as máquinas virtuais e o servidor de virtualização propriamente dito.
- **Privados:** comutadores privados se comunicam apenas entre máquinas virtuais no servidor de virtualização. Você não pode usar comutadores privados para comunicação entre as máquinas virtuais e o servidor de virtualização propriamente dito.

DICA

Para que uma máquina virtual fale tanto com a rede externa quanto com a máquina host serão necessários dois comutadores virtuais de tipos diferentes. Esta dica pode ajudar muito em provas do MCSA em pequenas perguntas de casos específicos.

DESCRIÇÃO SOBRE OS SERVIDORES

Particularmente, tenho um carinho extra por este capítulo, pois em qualquer empresa existe uma máquina cumprindo fielmente o papel de servidor.

O termo *servidor* vem de servir para algo ou servir a algo. Significa que o equipamento que for alocado como servidor terá uma tarefa específica na rede da empresa.

Um erro muito comum é querer comparar um equipamento desktop com Windows Server instalado com um servidor feito para funcionar sem desligamento por 5 ou 6 anos. Não existe uma comparação direta com as tecnologias de um servidor para uma estação de um cliente, então vamos aos detalhes mais importantes em relação a esse tipo de equipamento.

Servidores são feitos para resistir a grandes horas de trabalho ininterruptas, e possuem uma série de recursos, como RAID por hardware, e redundância de peças, como fontes e memórias ECC. Nesta parte, veremos diversos modelos dos fabricantes HP, IBM, Dell e Cisco (sim, a Cisco tem uma linha de servidores).

Uma estrutura de servidores é direcionada de duas formas: ou o servidor é dedicado a alguma função, ou ele tem funções compartilhadas. Por exemplo, posso utilizar um servidor para fornecer endereços IP pelo DHCP e, ao mesmo tempo, esse servidor

fornece atualização de hora para as máquinas e também é meu servidor de arquivos.

Existem algumas boas práticas que vamos comentar nesta parte do livro que considero de extrema importância, como quando montar um servidor dedicado e quando compartilhar recursos.

Fabricantes

Escolher o fabricante do seu parque de servidores é importante, pois existe uma série de itens como suporte, contrato de garantia, manuais etc. que podem fazer a diferença em um atendimento em momento de crise, em que ocorre uma queima de uma peça, por exemplo. É importante lembrar de que o hardware de um servidor é diferente do hardware de um desktop adaptado com sistema operacional para servidores. A qualidade e desempenho das peças são muito diferentes.

Já trabalhei com diversos tipos de servidores de inúmeros fabricantes e algo que aprendi é que cada um é bom em algo. Alguns são excelentes em suporte pós-vendas, outros possuem uma alta gama de manuais e recursos para técnicos e analistas autodidatas. Já alguns deles fornecem maior agilidade para contratos de compra e afins.

Em resumo, você terá diversas experiências com todos os fabricantes, e isso pode ajudar a adotar uma linha de produtos como preferencial para seu dia a dia. No meu caso, gosto muito dos produtos da HP e, como segunda marca, trabalho com IBM. Porém, isso não me impede de trabalhar com outros fabricantes. Digamos que é uma preferência por marca pela facilidade com que assimilo os dados. Cabe a você localizar suas facilidades e se especializar.

13.1 TIPOS DE SERVIDORES



Quando começamos a elaborar um projeto, temos a árdua missão de juntar tudo o que sabemos sobre redes, hardware e bom senso para a escolha do melhor equipamento a determinada realidade do cliente.

Tratarei nesta seção o termo cliente como unidade externa de negócios. Ou seja, o cliente pode ser um departamento, um funcionário de outra comarca, ou até mesmo um cliente externo de suporte.

Perguntas antes de escolher o servidor

1. Quanto você pode gastar?
2. Para que será utilizado esse hardware?
3. Quais sistemas operacionais ele fornece suporte?
4. Quais são os processadores compatíveis?
5. Até quanto de memória podemos usar e qual é o modelo dela?

6. Vamos precisar de RAID? Qual?
7. Quantas placas de rede vem no servidor?

Quando você responder todas as perguntas, daí sim poderá escolher corretamente o fabricante e agregar os recursos ao ambiente de forma correta. Não se esqueça de que o cliente não compra equipamentos, mas sim a satisfação de suas necessidades. Investir em um equipamento de qualidade e custo adequado permite que seu usuário consiga trabalhar com a melhor percepção possível dentro de seu orçamento.

Servidores de mesa (torre)

Os servidores de torre são muito parecidos com desktops, e são indicados para empresas pequenas com até 100 usuários. Porém, por conhecimento do dia a dia, sei que essas máquinas podem trabalhar com bem mais do que isso.

São servidores relativamente baratos e que têm algumas funcionalidades bem interessantes, como RAID 0 e 1, placas de rede redundantes e, em alguns casos, um sistema que permite controlar o servidor quando ele está desligado. Sim, você leu certo, quando estiver desligado é possível controlar o servidor.

Você pode se deparar com o HP ProLiant ML110 Generation 7 (G7) sendo utilizado como servidor DHCP, servidor de impressão, AD ou até um servidor de arquivos. Esse equipamento é bem barato quando comparado com outro hardware, e possui uma configuração muito interessante a respeito de hardware.

Essa máquina aceita processadores de até 4-cores em plataforma Xeon, que é uma excelente notícia, pois esse processador da Intel é direcionado para servidores de alto desempenho. Esse equipamento suporta até o Intel® Xeon® E3-1280 (50GHz/4-core/8MB/95W, 1333, HT, turbo 1/2/3/4).

Apesar de ser fabricado pela HP, esse equipamento possui um chipset Intel® da série C200 e aceita até 16GB de memória RAM PC3-10600E em padrão ECC com Total 4 slots DIMM. Sua controladora de disco é a HP Embedded Smart Array B110i SATA RAID Controller (RAID 0/1/10), que, como diz sua especificação, permite RAID de disco de modelos SATA em modo 0, 1 e 10.

Porém, o que gosto realmente neste modelo de equipamento é a *iLO3 remote management support*. Esse servidor que parece um desktop (só parece) possui uma tecnologia chamada iLO, que permite o controle remoto do servidor mesmo quando ele está desligado. A iLO é configurada com um IP e fica ligada mesmo que os equipamentos estejam desligados. Ela é alimentada pela fonte ATX (que na verdade nunca desliga, mesmo que se computador esteja desligado).

É importante lembrar de que o computador pode estar desligado, porém conectado a tomada. Esse recurso não funciona caso o computador esteja fora da tomada, pois a fonte ATX precisa de acesso à energia elétrica, mesmo que em inatividade.



Neste servidor, é possível ver também um recurso chamado de

hot plug. A sacada do HD é fácil, através de gavetas, e não possui a necessidade de parafusos. Como concorrente direto para o ML 110 G7, temos o IBM X3100 m4, que é mais barato, porém mais chato para configurar alguns recursos, como o próprio RAID, por exemplo.

A HP tem um assistente que faz tudo de modo facilitado, chamado de Smart Start, e a IBM depende da boa e velha força braçal para este modelo. Porém, o valor entre um e outro é substancial, e pode variar em até R\$ 900,00 de diferença entre eles.



O IBM X3100 m4 é um servidor compacto com as mesmas características do HP ML 110 G7, porém com a fabricação IBM. Seu hardware é bem robusto e forte, sendo sua maior vantagem a expertise de anos de trabalho de um fabricante.

Este servidor permite a opção de trabalho com processadores até o E3-1200v2 e memórias DDR-3 ECC, até 1600 MHz; UDIMM de no máximo 32 GB. Uma excelente vantagem se comparado aos 16 GB de limite do ML 110 G7.

O ServeRAID-C100 padrão para IBM System x® suporta RAID-0 ou -1 ou RAID-0,-1 de hardware para HDDs hot-swap de 2,5 pol., modelo PSU redundante, que pode variar de modelo para modelo.

No momento da compra, você deve informar todas as especificações e não espere que o vendedor consiga te orientar. Outro ponto em questão de servidores é que você deve ser muito específico em todos os pontos e direcionando muitas vezes o modelo da controladora, a quantidade de memória, e até mesmo o tipo e fabricante da memória. Não é simples fazer a compra de um servidor com os fornecedores atuais que não possuem muita qualificação técnica. Todo cuidado é pouco.

O servidor da IBM possui suporte a até quatro unidades de disco rígido Serial ATA de baixo custo e alta capacidade, ou até oito unidades de disco rígido hot swap SAS/ SATA de 2,5 pol. que otimizam a flexibilidade da implementação. Como vimos no capítulo de discos, os HDs SAS são muito mais rápidos que os discos SATA.



Uma falha terrível deste modelo é que as gavetas de disco vêm contadas de fábrica, o que significa que, se você precisar adicionar um novo disco, vai precisar pagar uma pequena fortuna, pois essas gavetinhas plásticas não são vendidas separadamente. Só vêm com HDs novos que custam quase 4 vezes mais que os HDs compatíveis mais baratos.

Para fecharmos a comparação com um terceiro fabricante, é bom citar o Dell PowerEdge T110 II, que segue a mesma linha de trabalho da HP e IBM, com recursos bem interessantes para pequenas empresas de até 100 usuários ou que precisem de algo barato e funcional. O Dell PowerEdge T110 II pode vir com Processador Intel® Xeon® Quad-Core E3-1220V2 e até 16GB de memória RAM. O mais interessante é que possui a opção de RAID 5 se for adquirida com a controladora PERC S300.

Lembre-se de que o importante na hora de escolher um servidor é responder a algumas perguntas e estudar caso a caso onde um determinado hardware pode ser aplicado.

Servidores de rack

Sua empresa cresceu e agora você precisa de servidores mais fortes, mais parrudos e de melhor organização, pois precisa colocar mais equipamentos em uma mesma sala. Os servidores de rack foram criados para economizar espaço e ganharam uma unidade de medida toda personalizada, chamada de Unidade “U”.

Código	Altura da estrutura sem o pé, com pré + 40mm	Largura	Profundidades
RKSERV-16U	892mm	560mm	570-670-770-870-1000-1100-1200
RKSERV-20U	1072mm	560mm	570-670-770-870-1000-1100-1200
RKSERV-24U	1252mm	560mm	570-670-770-870-1000-1100-1200

24U			1000-1100-1200
RKSERV-28U	1445mm	560mm	570-670-770-870-1000-1100-1200
RKSERV-32U	1625mm	560mm	570-670-770-870-1000-1100-1200
RKSERV-36U	1805mm	560mm	570-670-770-870-1000-1100-1200
RKSERV-40U	1985mm	560mm	570-670-770-870-1000-1100-1200
RKSERV-44U	2165mm	560mm	570-670-770-870-1000-1100-1200

Quando queremos medir o tamanho de um servidor de hack, dizemos que ele tem uma ou mais Us. Por exemplo, o DL 380 G6 da HP possui 2Us de espaço no hack.

Esses hacks são um tipo de armários de aço que guarda servidores com uma maior segurança, também sendo utilizados para organizar o ambiente de TI. Seu tamanho é medido pela quantidade de U. Na tabela anterior, podemos ver um modelo de hack com 44U (que é bem grande).

O espaço “U” é uma unidade de espaço padrão usado em todos os fabricantes atuais de hacks pelo mundo, e é a forma mais ideal de medir e acertar um equipamento. Os servidores de hack são mais pesados, menos amigáveis quanto à colocação e exigem um manuseio mais cuidadoso. Entretanto, são excelentes para ocupar menos espaço, e sua organização final fica muito interessante.



A Cisco trabalha também com uma linha de servidores muito interessante e de alta desempenho, como o Cisco UCS C200 M2,

por exemplo. Esse equipamento pode trabalhar com discos SATA, SAS ou SSD. Lembrando de que, no momento da compra, isso deve ser informado pelo comprador, citando inclusive qual é o modelo da controladora que se quer colocar.

Em projetos que trabalhei com servidores Cisco, tive uma grande facilidade para conversar com o pré-vendas, pois notei que todos tinham um excelente conhecimento técnico e erros com entrega e equipamento errado não existiram.

Isso não acontece com outros fabricantes e, acredite, é frustrante conversar com um pré-vendas que não sabe o que está vendendo. E, pior ainda, quando sua compra vem errada, e o projeto para um novo ambiente trava e fica estagnado gerando custo e prejuízo.

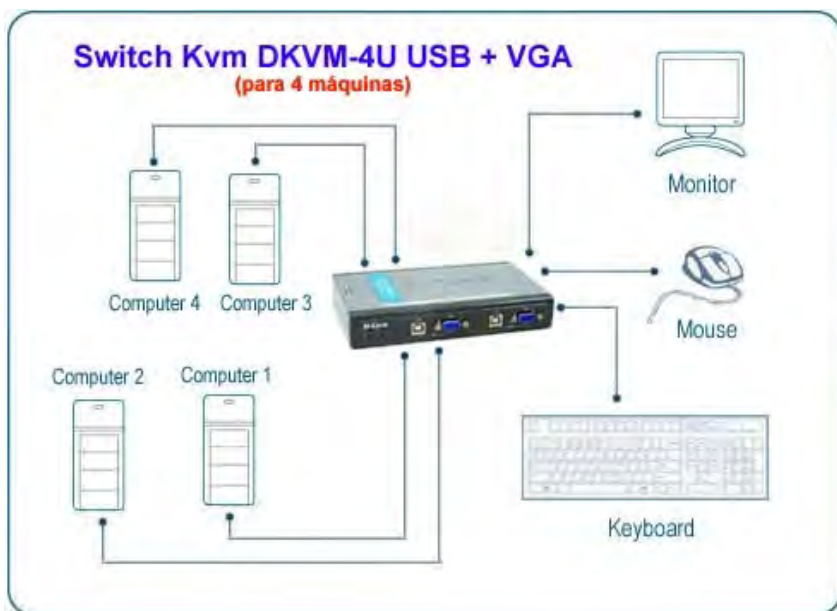


O Cisco UCS C200 M2 suporta RAID de discos 1, 5, 6, 10, 50 e 60, o que permite uma forma toda nova de trabalho para um pequeno ou médio empresário que esteja em expansão de negócios, precisando de uma plataforma parruda e confiável. Este servidor também possui a vantagem de trabalhar com até dois processadores físicos da linha Xeon da Intel (X5670, X5650, X5675, L5640, E5649,

E5645, E5640, E5620, E5506 ou E5606), permitindo um alto poder de processamento.

Servidores de hack costumam ser bem mais caros que servidores de torre, não só pelo formato compacto, mas por conter recursos tolerantes à falha de alta performance, como por exemplo, a duplicidade de controladores de disco e até duplicidade de fontes de energia. Quando um dispositivo para de funcionar, o outro assume a funcionalidade em tempo real.

Tudo aqui está duplicado. No que se trata de hardware, temos redundância de tudo. Mesmo que uma peça dê problemas, existe outra que não permite a parada completa do servidor (equipamento). Em muitos casos, dependendo do servidor, nem mesmo é necessário desligar tudo para substituir a peça danificada. Essa tecnologia se chama *Hot Swap*.



Os servidores de hack podem ser bem grande, parrudos e fazer

bastante barulho devido ao alto poder de refrigeração, como é o caso do HP DL560 G8. É um servidor com cara de poucos amigos, e que foi feito para alto poder de processamento e desempenho. Possui suporte ao Intel® Xeon® E5-4650 com seus 8-cores e atendendo até 64GB (4x8GB) PC3-12800R (DDR3-1600) de memória RAM.

Os servidores de hack não possuem monitores, nem mouses ou teclados, e geralmente devem ser acessado apenas pela rede ou iLO de conexão após serem configurados. Todo o gerenciamento é remoto, e foram criados para ter facilidade de colocação em volume. É muito utilizado em centrais de tecnologia e Data Centers.

Ainda é possível colocar um dispositivo chamado de monitor TFTP e um Switch KVM em uma sala onde existem muitos desses equipamentos. O Switch KVM pode receber acesso de um conjunto de mouse, teclado e monitor, e compartilhar com todos os servidores da sala. Seria como um botão seletor de equipamentos que permite um único conjunto de mouse, teclado e monitor acessarem milhares de servidores. É muito utilizado em ambientes nos quais o acesso físico é complicado e só acontece em último caso, quando o acesso pela rede é impraticável por um defeito ou configuração.

Servidores Blade



Quando falamos de servidores Blade (lâmina), estamos falando de servidores parrudos com alta disponibilidade, alta tolerância a falhas, alta performance e alto custo de compra e manutenção. Os servidores Blade são extremamente fortes e rápidos, e exigem um conhecimento profundo de hardware e configuração de redes.

São usados em sua grande maioria para virtualização com Hyper-V, XenServer e VMWare em camada zero (direto no hardware), além de trabalharem muito bem com banco de dados e principalmente com Cloud Computing.

Os servidores Blade podem variar muito de preço dependendo da estrutura que se está preparando a montagem e para que será utilizada. Tudo nesses servidores é tolerante a falhas e emite alertas por um painel informativo. Desde um cooler, até uma fonte e um módulo de memória são monitorados em tempo real, de temperatura até velocidade dos coolers.



São equipamentos magníficos de fato, e que são utilizados por médio, grandes e gigantes. Esses servidores são extremamente pesados, difíceis de configurar e exigem muito cuidado com o manuseio.

Algo importante que você deve saber sobre esse tipo de equipamento é que não recomendo a compra dele sem o atendimento pago por fora em forma de contrato estendido ou contrato de SLA diferenciado. Para uma empresa usar um servidor Blade, significa que o ambiente dela precisa ficar disponível quase que 24 horas, 7 dias na semana. Então, se uma peça queimar, precisa ser substituída rapidamente.

O grande problema é que, se você comprar um equipamento desses (que não é barato) e pagar à vista, a peça leva de 45 a 65 dias para chegar. Imagine se você espera queimar uma peça para fazer a troca; é inviável. Então, o que pode garantir que sua cabeça não role em um ambiente de crise é manter um contrato de manutenção atualizado e contendo a rápida troca de peças se necessário. Lembre-se de que estamos falando de um servidor que muitas vezes

custa o equivalente a um carro popular.



Os servidores Blade ficam conectados a uma caixa chamada *enclosure* que faz a conexão com o restante da rede. Um enclosure pequeno, como o c3000 da HP, pode armazenar até 8 lâminas pequenas do modelo BL460c, da geração 6 até a atual geração 8.

Todas as lâminas vêm com uma conexão em forma de barramento e a rede é fornecida através do enclosure, que utiliza conexões gigabit em malha para falar na rede. Vamos abordar mais a fundo os enclosures e detalhar essa parte de conexão em malha daqui há alguns instantes, mas por enquanto vamos focar nas lâminas.

Cada lâmina possui de 02 a 04 discos SAS ou SSD, que devem ser colocados em RAID 1 ou 5 dependendo do modelo. Porém, as mais comuns vêm com 02 discos e já vêm de fábrica com RAID 1.

Não é muito comum o uso dessas lâminas com muito espaço em disco, pois esses equipamentos geralmente são conectados a dispositivos maiores, chamados Storages, em uma rede de HDs chamada SAN (*Storage Área Network*), através de placas específicas, chamadas de placas HBA. Existem muitos outros modelos de placas, mas esta é bem comum e fácil de ser encontrada.

As placas HBAs são caras e podem custar mais do que uma motocicleta de baixa cilindrada zero Km, e não vêm com as lâminas de fábrica. Então, se for fazer um projeto de servidores que envolva Blades, lembre-se de cotar separadamente esse equipamento.

As lâminas são usadas para processamento e memória, e geralmente são poderosas nisso. Podem acomodar facilmente 32 núcleos de processamento com dois Intel® Xeon® E5-2670 de 8-cores, que significa que cada processador teria 16 núcleos cada, além de 256GB de memória RAM.

Cada enclosure da linha c3000 com lâminas BL460c G8 pode acomodar até 8 lâminas, então serial 256 núcleos de processamento e 2048 TB de memória RAM. Nada mal para uma única caixa com 8 lâminas.

Mas esse servidor também exige um preparo diferenciado em se tratando de energia elétrica, *nobreaks* e equipe de suporte, pois realmente é um verdadeiro monstro em tamanho, performance e dificuldade de manutenção. Se eu pudesse comparar esse equipamento com aviões, por exemplo, diria que esse é o Boeing dos servidores.

Complexo e difícil de lidar com tantos comandos e leds piscando, e informando situações de parada e queima. O enclosure c7000 da HP acomoda facilmente cerca de 16 lâminas e é utilizado para grandes ambientes.

Lidar com servidores Blade exige um profundo conhecimento de hardware, além de um excelente conhecimento em roteadores e switches e noções de virtualização. Então, para saber mais sobre esse modo tão fantástico de trabalho com servidores de alta disponibilidade, mãos à obra e vamos estudar.

A Fujitsu tem equipamentos excelentes, como o bx900, que fornece uma maneira mais rápida, mais simples e de menor custo para construir e executar uma infraestrutura de TI em sua organização de médio porte, filiais ou grande centro de dados. A família de sistemas PRIMERGY BX é projetada de modo que os componentes do chassi possam ser usados durante todo a família de outros modelos.

Blades de servidores, armazenamento e conexão podem ser adicionados ou substituídos sem cabeamento adicional ou esforço da administração. PRIMERGY servidores Blade foi desenvolvido para proporcionar o máximo de desempenho e redundância máxima, mas com apenas um espaço mínimo requisito e baixo consumo de energia.

Agilidade nos negócios é alcançada através de simples design modular e um grande número de recursos úteis que ajudam a reduzir o tempo de implantação de horas ou até mesmo apenas alguns minutos. Você pode usar milhares de aplicativos e um grande número de sistemas operacionais de certificados, e você pode organizar suas próprias combinações individuais de máquinas virtuais, armazenamento e lâminas de servidores, juntamente com uma seleção ampla de conexões internas e externas, tais como Ethernet, Fibre Channel, SAS e InfiniBand.

Como requisitos de negócio mudam, as Fujitsu PRIMERGY servidores Blade podem ser adaptados para atender às necessidades individuais de uma forma adequada. Quando escolher seu hardware, procure imaginar como será seu futuro e se poderá

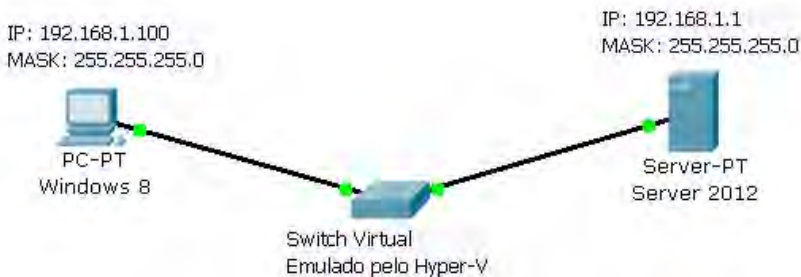
manter o mesmo fabricante.

Não é uma boa prática ter no mesmo ambiente equipamentos de fabricantes diferentes, apesar de funcionar até que razoavelmente bem. O motivo é muito simples: um fabricante tem tecnologias e melhorias embarcadas em seu hardware e que, apesar de parecidos em resultado final, são bem diferentes em questão de engenharia entre si. Não é recomendado misturar equipamentos de fabricantes diferentes devido à diferença dessas tecnologias embarcadas.

MONTANDO SEU LABORATÓRIO PRÁTICO NO HYPER-V

Para trabalhar com os laboratórios deste livro, recomendo que você monte um laboratório com o Hyper-V, seja com o Windows Server 2012 ou até mesmo com um desktop com o Windows 8, 8.1, ou ainda o Windows 10. Evite utilizar o Windows Server 2008, por questões unicamente acadêmicas. Lembre-se de que sua prova 70-410 envolve o conhecimento do Hyper-V baseado no Windows Server 2012 R2.

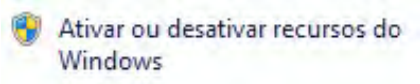
Vamos seguir um pequeno escopo básico de redes para entender o papel do Switch virtual do Hyper-V dentro do nosso ambiente simulado. Este Switch virtual tem um papel de extrema importância dentro dos laboratórios, e é o primeiro item a ser criado.



É muito importante tomar todos os cuidados para que seu ambiente virtual não interfira em seu ambiente real. Você não imagina a quantidade de paradas que ocorrem por alguém utilizar um notebook em sua rede com máquinas de teste que acabam interferindo no ambiente real, como quando levantamos um DHCP, por exemplo.

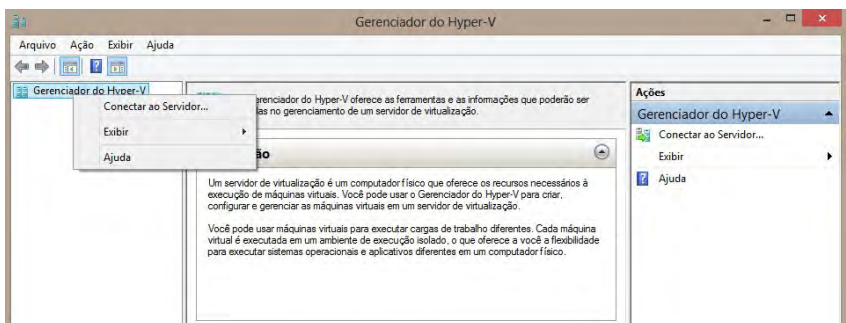
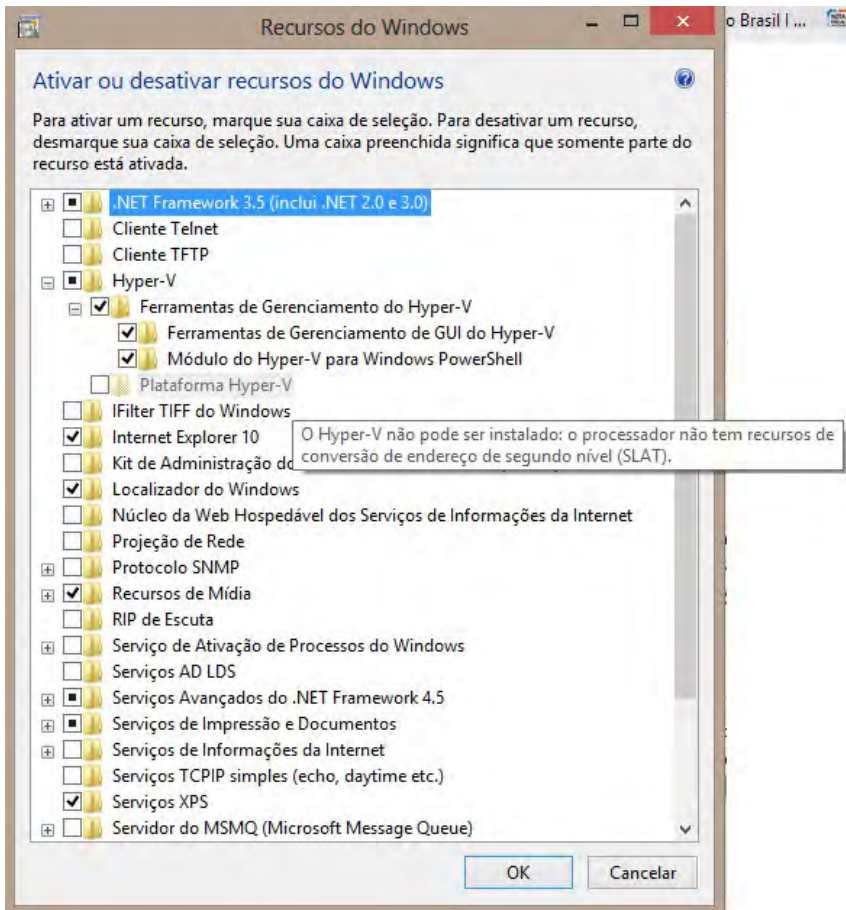
14.1 INSTALANDO O HYPER-V NO WINDOWS 8

No Windows 8 Pro, o Hyper-V é uma ferramenta nativa e pode ajudar muito no dia a dia do povo da TI. Para instalar essa ferramenta, você precisa acessar a charm bar (WIN + C), na parte de configurações, Painel de Controle e programas e Recursos.



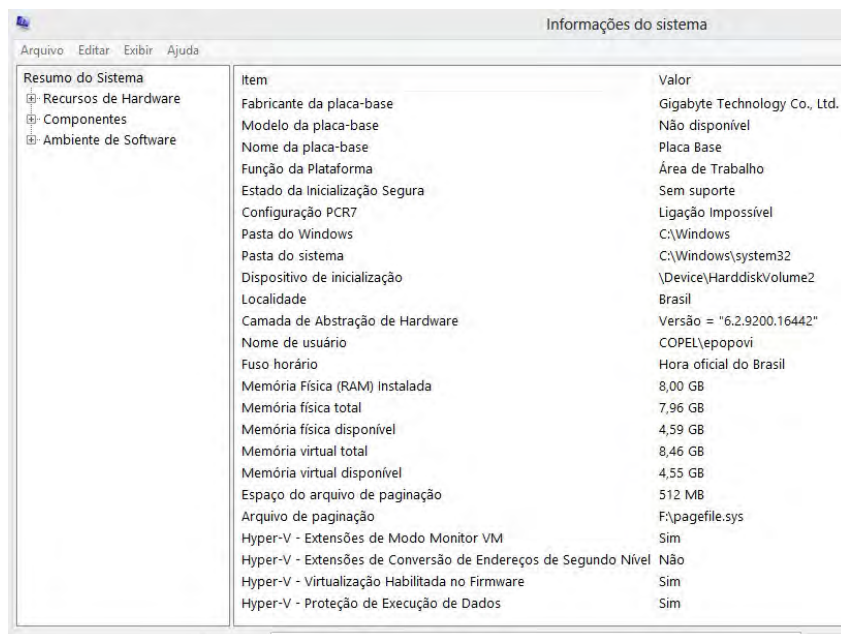
É importante lembrar de que seu processador deve dar suporte à virtualização e ser de geração de 64 bits para utilizar todos os recursos da solução. Você notará que, caso seu hardware não possua suporte a virtualização, o Hyper-V funciona apenas como gerenciador de um servidor virtual externo, e não poderá criar as máquinas virtuais.

Se a plataforma Hyper-V estiver desativada, você deve validar seu hardware. Nem todos os fabricantes disponibilizam ativamente o recurso de virtualização. Isso significa que em diversos casos será necessário acessar a bio do notebook, desktop ou até mesmo do servidor, e habilitar este recurso.



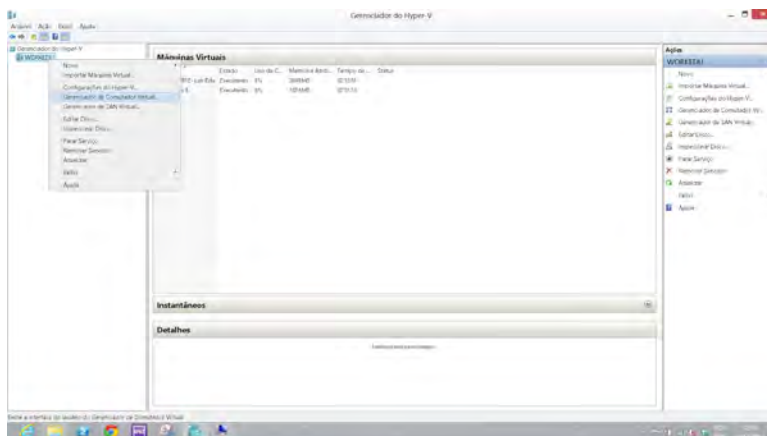
Dica de ouro

Use o comando `msinfo32` e, logo na tela inicial do resumo do sistema, aparece exatamente o que está habilitado para seu hardware. Não precisa instalar nenhum programa de terceiro. ;-)

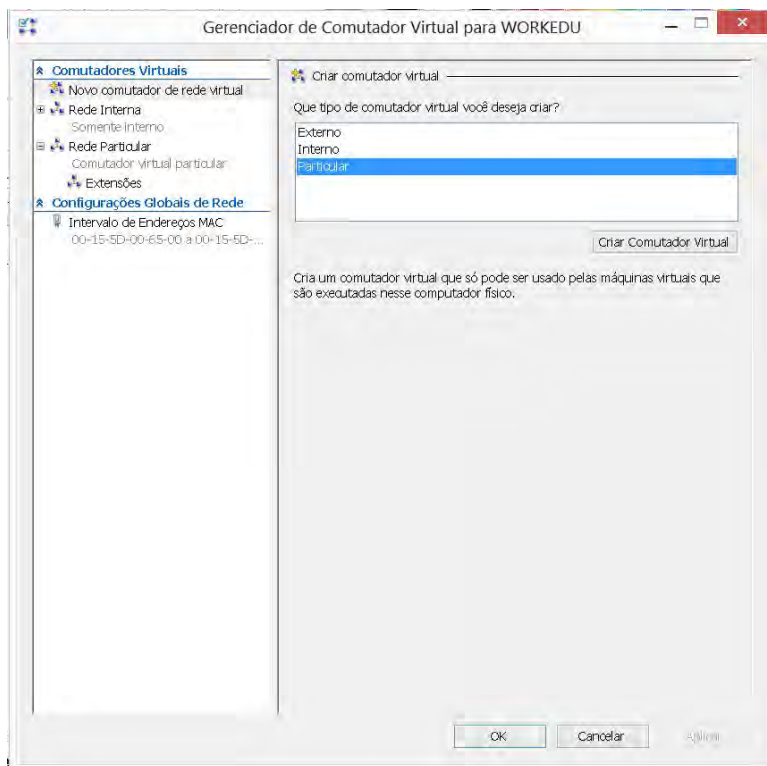


Item	Valor
Fabricante da placa-base	Gigabyte Technology Co., Ltd.
Modelo da placa-base	Não disponível
Nome da placa-base	Placa Base
Função da Plataforma	Área de Trabalho
Estado da Inicialização Segura	Sem suporte
Configuração PCR7	Ligação Impossível
Pasta do Windows	C:\Windows
Pasta do sistema	C:\Windows\system32
Dispositivo de inicialização	\Device\HarddiskVolume2
Localidade	Brasil
Camada de Abstração de Hardware	Versão = "6.2.9200.16442"
Nome de usuário	COPEL\epopovi
Fuso horário	Hora oficial do Brasil
Memória Física (RAM) Instalada	8,00 GB
Memória física total	7,96 GB
Memória física disponível	4,59 GB
Memória virtual total	8,46 GB
Memória virtual disponível	4,55 GB
Espaço do arquivo de paginação	512 MB
Arquivo de paginação	F:\pagefile.sys
Hyper-V - Extensões de Modo Monitor VM	Sim
Hyper-V - Extensões de Conversão de Endereços de Segundo Nível	Não
Hyper-V - Virtualização Habilitada no Firmware	Sim
Hyper-V - Proteção de Execução de Dados	Sim

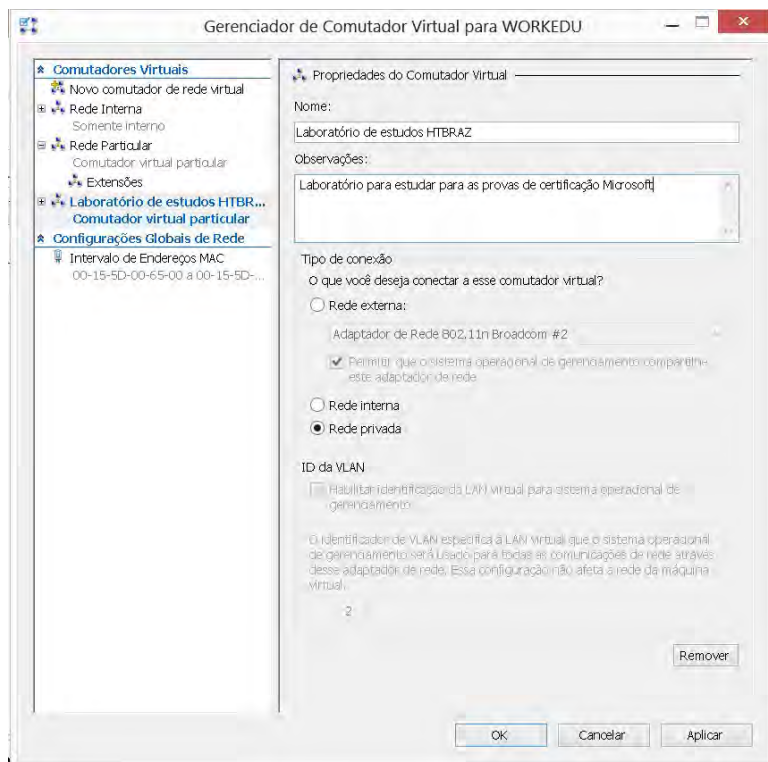
1. Clique com o botão direito no servidor Hyper-V (que no meu caso está como **WORKEDU**) e, em seguida, selecione *Comutador Virtual*.



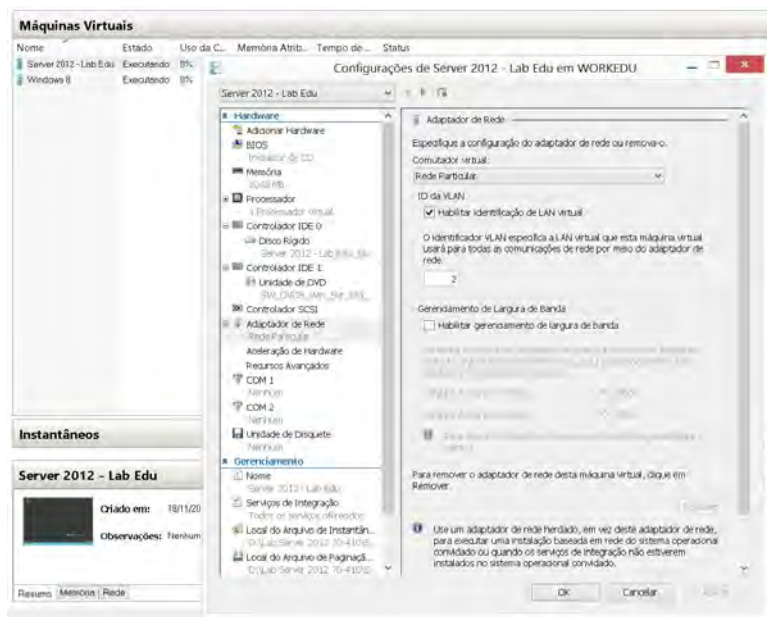
2. Localize e selecione a opção para *Novo comutador de rede virtual*, e depois marque do lado direito da janela o tipo de comutador chamado *Particular*.



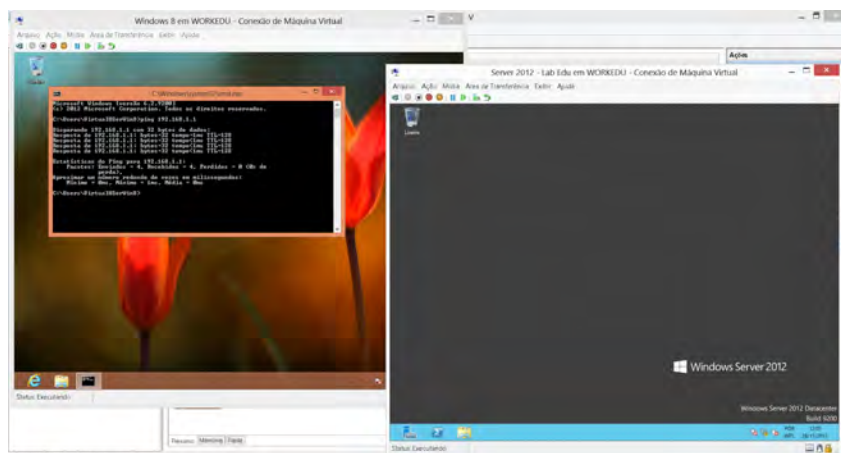
3. Preencha as propriedades do comutador virtual conforme a figura a seguir, ou use a criatividade, porém mantenha a opção *Rede Privada* marcada.



4. Agora clique nas máquinas virtuais (uma de cada vez), com o botão direito do mouse e escolha a opção de configurações. Quando a janela se abrir, escolha a opção chamada de *Adaptador de Redes*. Logo no início será apresentada a possibilidade de escolha do computador virtual. Agora marque a opção criada anteriormente.



Seguindo estes 04 passos, suas máquinas virtuais baseadas em Hyper-V se comunicam sem problema e o melhor de tudo, sem interferir em sua rede interna ou com o ambiente já em funcionamento. Se você configurou direitinho os IPs e as permissões, ambas as máquinas vão conversar numa boa.



Aproveitando a deixa, é sempre interessante conhecer as novidades do Hyper-V para cada distribuição ou versão. Então deixo aqui uma tabela bem interessante com os novos limites de funcionamento desta fantástica ferramenta de trabalho. É importante realçar que cada evolução da solução permite uma melhor flexibilidade e escalabilidade.

Novos limites do Hyper-V				
System	Resource	Maximum number		Improvement factor
		Windows 2008 R2	Windows Server 2012	
Host	Logical processors on hardware	64	320	5×
	Physical memory	1 TB	4 TB	4×
	Virtual processors per host	512	2,048	4×
Virtual machine	Virtual processors per virtual machine	4	64	16×
	Memory per virtual machine	64 GB	1 TB	16×
	Virtual disk capacity	2 TB	64 TB	32×
	Active virtual machines	384	1,024	2.7×
Cluster	Nodes	16	64	4×
	Virtual machines	1,000	8,000	8×

14.2 DICAS DE UTILIZAÇÃO DO HYPER-V

Muito se fala sobre virtualização, seja ela para usuários finais que descobriram uma forma de acessar seus jogos antigos por uma máquina virtual com um sistema mais antigo, ou até mesmo empresas que pretendem diminuir a utilização de espaço físico e melhorar o uso do hardware através de um dimensionamento aprimorado. Falar de virtualização não é exatamente uma novidade, porém vejo que a Microsoft vem fazendo muito bem a lição de casa e cada vez mais torna sua criação mais flexível e interessante.

O Hyper-V Server 2012 R2 é um sistema operacional criado para cuidar exclusivamente de máquinas virtuais e ambientes virtualizados e, acredite, é totalmente grátis. Você precisa apenas possuir o licenciamento das máquinas que serão instaladas neste

poderoso servidor.

Seus concorrentes diretos hoje (segundo o Gartner) são a VMWare e o XenServer. O gráfico a seguir, disponibilizado pelo próprio Gartner pelo seu site, demonstra exatamente a evolução de cada fabricante pelo mundo da virtualização no ano de 2010 até 2014. Isso demonstra a força e investimento da Microsoft para maturar essa fantástica ferramenta chamada Hyper-V.

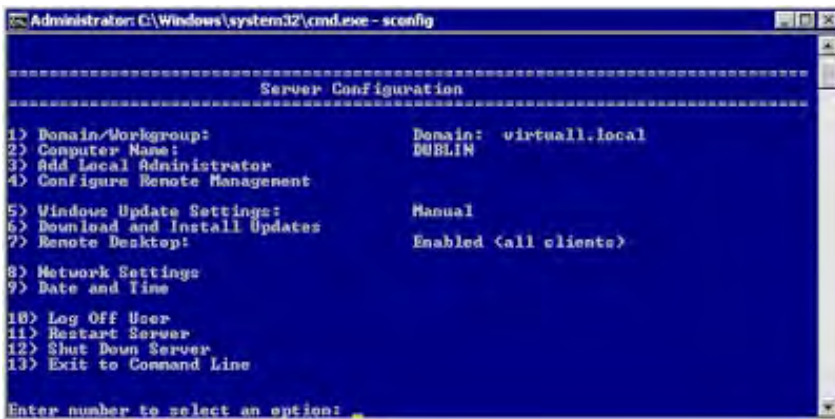


Cada solução possui diversas vantagens e desvantagens, que não serão comentadas aqui, pois nosso foco agora é atuar com os cmdlets de administração do Windows Hyper-V Server 2012 R2. Nesta postagem, faremos um apanhado geral através das linhas de

comando do PowerShell, permitindo conhecer cada vez mais essa excelente ferramenta.

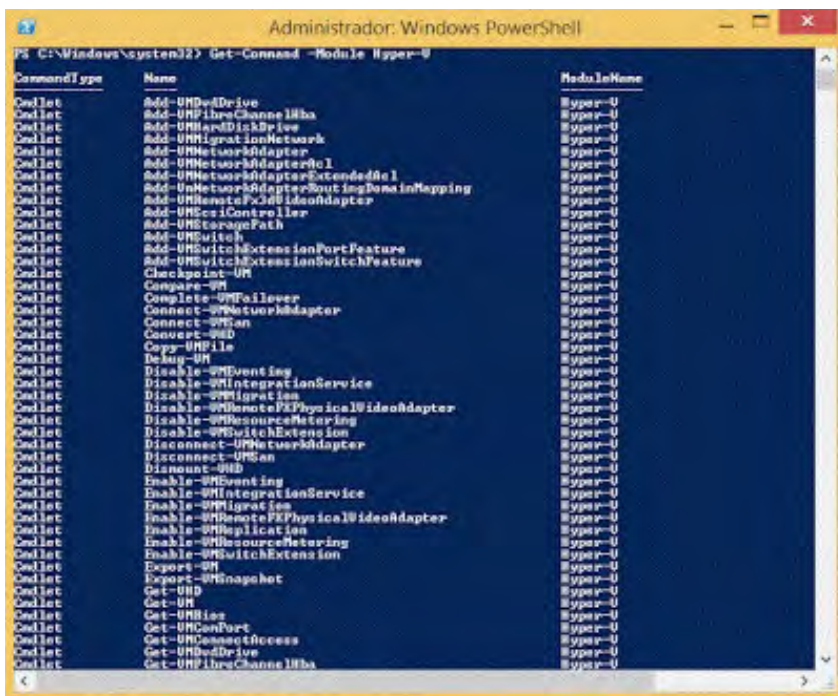
É interessante lembrar de que o Hyper-V está presente no Windows 8. Sua instalação está nativa pelo painel de controle desde que seus requisitos sejam contemplados. Antes de iniciar o trabalho com o Hyper-V, é interessante configurar o servidor com um *hostname*, um endereçamento IP e o tipo de rede que possui (Workgroup ou domínio). Use o comando `sconfig` para efetuar tais configurações de modo rápido e eficiente.

A próxima figura demonstra a tela de configuração do servidor pela ferramenta `sconfig` :

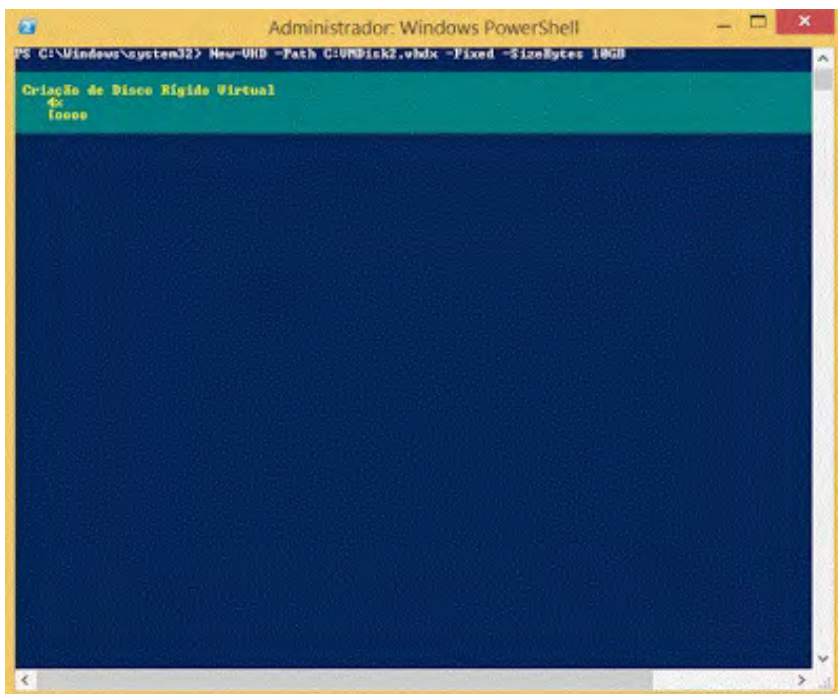


Alguns cmdlets do PowerShell para o Hyper-V:

- Instalar o Hyper-V e reinicia o servidor: `Install-WindowsFeature Hyper-V -Restart`
- Mostrar todos os cmdlets relacionados ao Hyper-V: `Get-Command -Module Hyper-V`



- Criar máquinas virtuais: `New-VM -Name "Debian Lenny" -MemoryStartupBytes 512MB -NewVHDPATH C:\VM\ubuntu1004.vhdx -NewVHDSIZEBYTES 10GB`
- Criar um disco VHD: `New-VHD -Path C:\VMDisk2.vhdx -Fixed -SizeBytes 10GB`



Após a execução do comando, é iniciado o processo de criação, que pode demorar um pouco dependendo muito da máquina host. Em um notebook com 16GB RAM e processador I7, levou cerca de 4 minutos para criar um VHDX de 10GB.

- Criar uma nova VM fazendo referência a um VHDX já existente: `New-VM -Name "AD_2012" -MemoryStartupBytes 512MB -VHDPATH C:\VMDisk2.vhdx`
- Iniciar uma VM: `Start-VM -Name "Windows 10"`
- Ver quais máquinas virtuais temos disponíveis: `Get-`

VM

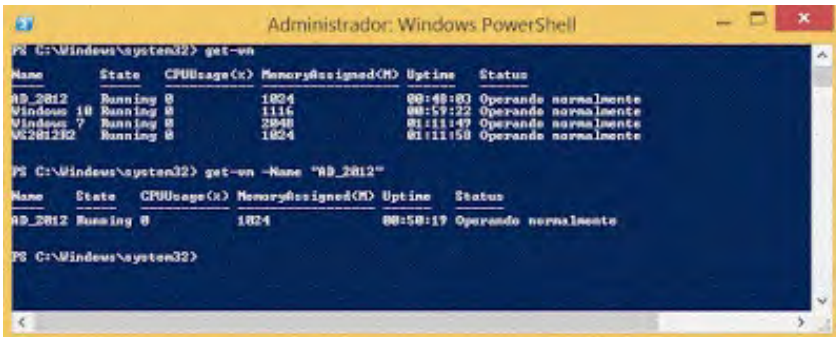


```
PS C:\Windows\system32> get-vm
```

Name	State	CPUUsage(%)	MemoryAssigned(M)	Uptime	Status
AD_2012	Running	0	1024	00:40:03	Operando normalmente
Windows 10	Running	0	1116	00:59:22	Operando normalmente
Windows 7	Running	0	2040	01:11:49	Operando normalmente
WS2012R2	Running	0	1024	01:11:50	Operando normalmente

```
PS C:\Windows\system32>
```

- Buscar informações de uma determinada máquina virtual: `get-vm -Name "AD_2012"`



```
PS C:\Windows\system32> get-vm -Name "AD_2012"
```

Name	State	CPUUsage(%)	MemoryAssigned(M)	Uptime	Status
AD_2012	Running	0	1024	00:50:19	Operando normalmente

```
PS C:\Windows\system32>
```

- Parar uma máquina virtual: `Stop-VM -Name "Ubuntu Server 2"`
- Listar os adaptadores de rede disponíveis: `Get-NetAdapter`
- Criar um Switch virtual em modo privado: `New-VMSwitch -Name "VMNetwork" -SwitchType Private`
- Remover uma máquina virtual: `Remove-VM -Name`

"Ubuntu 10.04"

SIMULADO

15.1 INSTALAÇÃO E CONFIGURAÇÃO

1.1) Que configuração mínima de hardware é necessária para instalação do Windows Server 2012?

- a) Processador 1.6 GHz 32 bits, 1024 MB RAM, 32 GB livres de disco, Super VGA (800 × 600) e acesso à internet
- b) Processador 1.6 GHz 64 bits, 1024 MB RAM, 80 GB livres de disco, Super VGA (1024 × 768) e acesso à internet
- c) Processador 1.6 GHz 64 bits, 512 MB RAM, 32 GB livres de disco, Super VGA (800 × 600) e acesso à internet
- d) Processador 1.6 GHz 32 bits, 512 MB RAM, 32 GB livres de disco, Super VGA (1024 × 768) e acesso à internet

1.2) Você é o administrador de redes da empresa Sbrubles LTDA. Esta empresa possui controladores de domínio com o Windows Server 2012 R2, e estações de trabalho com Windows 7, Windows 8 e Windows 8.1. Você pretende aumentar a segurança de alguns servidores através de instalações em modo Server Core. Quais Roles a seguir não estão disponíveis pela instalação Server Core? Marque todas as que se aplicam.

- a) Active Directory Certificate Services
- b) Active Directory Federation Services
- c) Network Policy and Access Services
- d) Active Directory Rights Management Services
- e) Remote Desktop Web Access
- f) DHCP Server
- g) Active Directory Domain Services
- h) Remote Desktop Gateway

1.3) Em uma empresa com três controladores de domínio,

duzentas estações de trabalho e quatro filiais, existe um servidor com uma instalação Server Core do Windows 2012 R2. Você, como administrador de redes, precisa ativar as ferramentas de migração de recursos e imagens usando o menor esforço administrativo possível. Qual dos comandos a seguir representa exatamente essa atividade?

- a) `dism.exe /mount-win /wimfile:c:\ServerHTB.win /index:4 /mountdir:c:\mount`
- b) `imagex.exe /image /wimfile:c:\ServerHTB.win /servermigration /mountdir:c:\mount`
- c) `dism.exe /image /wimfile:c:\ServerHTB.win /enable-feature /mountdir:c:\mount`
- d) Nenhuma das alternativas está correta

1.4) Você é o administrador de redes de uma consultoria que presta serviços para diversos clientes de forma remota. Você recebe o contato de um técnico de campo, informando que, em um servidor com Windows Server 2012 Datacenter, foi adicionado cerca de 6 TB de disco. Este técnico informa também que precisa de pelo menos um volume de 3 TB de disco disponível para uso de uma determinada aplicação. Qual das opções a seguir pode permitir a conclusão dessa tarefa?

- a) Converta os discos para o formato GPT
- b) Crie um pool de discos
- c) Converta os discos para o modo dinâmico
- d) Crie um VHD de 3 TB

1.5) Qual das edições do Windows Server 2012 R2 está limitada a até 15 usuários?

- a) Windows Server 2012 Datacenter
- b) Windows Server 2012 Standard
- c) Windows Server 2012 Essentials
- d) Windows Server 2012 Foundation

1.6) Qual das edições do Windows Server 2012 R2 está limitada a até 25 usuários?

- a) Windows Server 2012 Datacenter

- b) Windows Server 2012 Standard
- c) Windows Server 2012 Essentials
- d) Windows Server 2012 Foundation

1.7) Em quais edições do Windows Server 2012 R2 está disponível o modo de instalação Server Core? Marque todas as que se aplicam.

- a) Windows Server 2012 Datacenter
- b) Windows Server 2012 Standard
- c) Windows Server 2012 Essentials
- d) Windows Server 2012 Foundation

1.8) Qual dos itens a seguir é a ferramenta de configuração do servidor com as principais atividades administrativas?

- a) sconfig.cmd
- b) cmd.exe
- c) msinfo32.exe
- d) systeminfo
- e) sigverif.exe

1.9) Qual dos itens listados a seguir permite o carregamento do gerenciador de tarefas do Windows Server 2012 R2?

- a) sconfig.cmd
- b) cmd.exe
- c) msinfo32.exe
- d) systeminfo
- e) sigverif.exe
- f) taskmgr.exe

1.10) Os servidores com instalação em Modo Serve Core são limitados quanto à utilização de aplicações e programas diversos, porém possuem ferramentas nativas para sua administração e manutenção. Quais das ferramentas listadas a seguir possuem funcionalidade ativa em um servidor em modo de instalação Server Core?

- a) dxdiag
- b) regedt32
- c) notepad.exe
- d) sigverif
- e) mspaint

- f) cmd.exe
- g) calc
- h) taskmgr.exe

1.11) Imagine que você trabalha como um dos administradores de redes para a empresa HTBRAZ. A empresa possui diversos servidores, dentre eles controlador de domínio com o Active Directory instalado e configurado. Este servidor está com o Windows Server 2012 Standard Edition em modo de instalação Server Core. A empresa possui cerca de 30 estações de trabalho variando entre Windows 7, Windows 8 e Windows 8.1. A empresa possui ainda 3 servidores legado com Windows Server 2008 R2. Que comando a seguir me permite trocar o nome do servidor com a instalação em modo Server Core?

- a) netdom /renamecomputer %computername% /newname:HTB-SP-Core
- b) Get-NameComputer | Set-NameComputer %computername% /newname:HTB-SP-Core
- c) Set-Name -renamecomputer %computername% -HTB-SP-Core
- d) netdom %computername% /oldname:ServerCore01 /newname:HTB-SP-Cor e

1.12) A empresa HTBRAZ possui alguns servidores, dentre eles um Active Directory com Windows Server 2012 R2 Standard Edition em modo de instalação Server Core. Você é orientado pela diretoria da empresa a instalar um novo servidor, também em modo Server Core, que será utilizado posteriormente pela equipe de plataforma e sistemas. Que comando a seguir me permite ativar este novo servidor de forma simples e rápida?

- a) cscript c:\windows\system32\slmgr.vbs -dlv
- b) Get-Activation -ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
- c) cscript c:\Windows\system32\slmgr.vbs /ato
- d) cscript c:\windows\system32\slmgr.vbs -ipk XXXXX-XXXXX-XXXXX-XX XXX-XXXXX

1.13) Você recebe a tarefa de gerenciar o firewall de um servidor legado que recebeu a instalação do Windows Server 2012 R2 Standard em modo Server Core, porém essa administração será feita

remotamente. Quais opções temos disponíveis para habilitar a configuração de acesso remoto remota? Marque duas respostas.

- a) Netsh firewall show config | share services -remoteadmin enable
- b) Netsh.exe firewall set services remoteadmin enable ALL
- c) Sconfig com a opção 4
- d) Get-FirewallEnableRemote -admin

1.14) Você trabalha como administrador de redes na empresa HTBRAZ. A empresa possui alguns servidores, dentre eles um Active Directory com Windows Server 2012 Standard Edition em modo de instalação Server Core. Por uma questão administrativa, você recebeu a tarefa de passar da instalação Server Core para a instalação GUI, sem formatar o servidor. Que comando muda as formas de instalação do Windows Server 2012?

- a) Get-WindowsGraphics *gui* -install
- b) Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -restart
- c) Get-WindowsRoles *gui*
- d) Get-Install -WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -restart

1.15) Você trabalha como administrador de redes na empresa HTBRAZ. A empresa possui alguns servidores, dentre eles um Active Directory com Windows Server 2012 Standard Edition em modo de instalação Server Core. Por uma questão administrativa, você recebeu a tarefa de passar da instalação gráfica para a Server Core. Que comando pode utilizar para efetuar essa tarefa?

- a) Get-WindowsGraphics *gui* -remove
- b) Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -remove
- c) Get-WindowsRoles *gui* -remove
- d) Uninstall-WindowsFeature Server-Gui-Shell -remove

1.16) Você é o Administrador de redes da empresa HTBRAZ. Em uma nova instalação de um Servidor de aplicações, será necessário utilizar 2 partições de, pelo menos, 4TB de espaço cada. Que tipo de partição resolveria facilmente essa questão?

- a) MBR
- b) RAID 1
- c) GPT
- d) RAID 5

1.17) Qual dos tipos de sistemas de arquivos, usado no Windows Server 2012, é conhecido como resilientes, com verificação de dados e correção de erros?

- a) ReFS
- b) NTFS
- c) Ext3
- d) FAT
- e) FAT32
- f) Alternativas B e E estão corretas

1.18) Quantas partições podem ser criadas em um disco GPT pelo Windows Server 2012 R2?

- a) 512
- b) 64
- c) 32
- d) 128
- e) 1024
- f) 4

1.19) Qual é o tamanho máximo de uma partição em um disco GPT?

- a) 4 TB
- b) 8 TB
- c) 22 TB
- d) 1 ZB
- e) 12 ZB
- f) 18 ZB

1.20) Que tipo de disco pode ser modificado sem que o equipamento tenha de ser reiniciado?

- a) Estendido
- b) Dinâmico
- c) Simples
- d) Espelhado
- e) RAID 50

1.21) Qual das funções a seguir podem ser consideradas como implementações de infraestrutura disponíveis pelo Windows Server 2012 R2? Marque todas as que se aplicam.

- a) DNS
- b) IIS
- c) DHCP
- d) Remote Desktop Services
- e) Apache
- f) Microsoft Dynamics

1.22) Você está atuando como um consultor Microsoft em diversos clientes de sua cidade. Sua principal atividade é orientar as empresas com soluções mais adequadas para cada ambiente de máquinas em atividade. Em um de seus clientes é identificado a necessidade de mudança do Windows Server em sua versão mais antiga para a mais atual. Pensando neste cenário de trabalho, diga qual das instalações a seguir permite o Upgrade para a versão 2012 R2 do Windows Server.

- a) Windows Server 2003 Standard to Windows Server 2012 Standard
- b) Windows Server 2008 Standard to Windows Server 2012 Standard
- c) Windows Server 2008 R2 32-bit to Windows Server 2012 64-bit
- d) Windows 7 Ultimate to Windows Server 2012 Essentials

1.23) Que recurso deve ser utilizado para converter o Windows Server 2012 de área gráfica para sua versão Server Core?

- a) Graphical Management Tools and Infrastructure
- b) Server Graphical Shell
- c) Windows PowerShell
- d) Microsoft Management Console

1.24) Qual é o nome do diretório onde o Windows armazena todos os módulos do sistema operacional que pode precisar instalar em um momento posterior?

- a) Windows
- b) WinSxS
- c) Bin
- d) System32

1.25) Imagine que você é o administrador de redes da empresa Sbrubles LTDA. Esta empresa possui uma Matriz em São Paulo, e diversas filiais e sucursais pelo Brasil. A rede da empresa contém um domínio do Active Directory chamado `htbraz.com` com o nível funcional da floresta como Windows Server 2008 R2. Todos os servidores da empresa possuem o Windows Server 2012 R2 atualizados.

Dentro da estrutura, você identifica que todas as contas de computadores direcionadas ao departamento de marketing estão em uma unidade organizacional (OU), nomeada como `Departamentos de Marketing\Computadores`.

Você também identifica que todas as contas de usuário para o departamento de marketing estão em uma OU chamada `Departamentos de Marketing\Users`. Todas as contas de usuário do departamento de marketing são membros de um grupo de segurança global chamado `MarketingUsers`. Todas as contas de computador da equipe de marketing são membros de um grupo de segurança global chamada `MarketingComputers`.

Neste domínio, você identifica que existem objetos de Diretiva de Grupo (GPOs), sendo aplicados por diversas Unidades Organizacionais.

Observando a configuração ativa, é possível notar a existência de dois objetos de Configuração de Senha, nomeados como `SENHA_01` e `SENHA_02`.

- `SENHA_01` está sendo aplicada para `MarketingUsers`.
- `SENHA_02` está sendo aplicada para `MarketingComputers`.

Localização	Mínimo de caracteres de senha
GPO1	5

Localização	Mínimo de caracteres de senha
GPO2	6
SENHA_01	10
SENHA_02	12
Default Domain Policy	7

Sabendo de cada detalhe da questão citada, responda: qual é o mínimo de caracteres utilizados para a senha dos usuários de Marketing?

- a) 7
- b) 5
- c) 6
- d) 10
- e) 12
- f) Nenhuma das alternativas

1.26) Você se tornou um administrador de redes, trabalhando para a empresa Sbrubles LTDA, prestando serviços para a HTBRAZ LTDA. A rede que você administra contém um domínio do Active Directory chamado sbrubles.local. O domínio contém um servidor chamado SUPERSERVER01, que executa o Windows Server 2012 Standard R2. O servidor SUPERSERVER01 possui instalado a função File Server Resource Manager (Servidor de arquivos). Você recebe a tarefa para configurar o servidor de arquivos, para que cada usuário receba um e-mail informando que sua cota está excedida. Que configuração precisa ser feita para resolver esta atividade?

- a) Modificar os membros do grupo Usuários de log de desempenho
- b) Configurar o servidor em Opções do Gerenciador de Triagem de arquivos
- c) Criar uma regra de classificação
- d) Não é possível efetuar essa configuração

1.27) Sua rede contém cerca de quatro controladores de domínio com um único domínio, chamado htbraz.local. Essa rede possui cerca de 500 estações clientes com desktops, notebook e

tablets que executam o Windows 8, Windows 8.1 e Windows 10. Sua rede possui cerca de 30 servidores legado, todos com o Windows Server 2012 R2.

Os computadores cliente de sua estrutura de redes se conectam à internet através de um proxy web de plataforma Open. Um de seus colegas de trabalho implanta um servidor chamado SERVER1, que possui funções de servidor DNS Instalada. Você então configura todos os computadores clientes para utilizar o servidor SERVER1 como seu servidor DNS primário. É necessário agora impedir o servidor SERVER1 tente resolver nomes de hosts de internet para os computadores cliente de sua rede. Que configurações você deve fazer para atender essa respectiva demanda? Escolha duas alternativas.

- a) Criar uma zona primária com o nome "root"
- b) Definir as configurações de segurança da zona htbraz.com
- c) Criar um apontamento para 192.166.0.1
- d) Criar uma zona primária com o nome "."
- e) Criar uma zona Stub chamada de "root"
- f) Remover todos os hoot hints
- g) Criar um Zonte primária chamada "GlobalNames"

1.28) Que comando a seguir permite o ingresso em um domínio de modo Offline?

- a) `djoin.exe /provision /domain htbraz.local /machine edupopov /savefile c:\edupopov-join.txt`
- b) `Netdom join %computername% /domain:htbraz.local /UserD:Administrator /PasswordD:*`
- c) Não é possível ingressar em um domínio de modo Offline
- d) `Netdom renamecomputer %computername% /newname:SaoPaulo`

1.29) Quais são os requisitos para que seja possível a adição um computador ao domínio em modo Off-line? Marque todos os pré-requisitos possíveis que sejam pertinentes.

- a) Um usuário com permissão para inclusão de computadores no domínio
- b) Acesso ao prompt de comando com privilégios elevados para usar o `djoin.exe` com a opção `/provision`

- c) Não é possível efetuar esse processo offline se a pessoa não estiver conectada a um link de pelo menos 512K
- d) Arquivo sbrubles-join.txt com as informações contendo os dados do domínio
- e) É necessário que seja desativado o firewall de todas as estações de trabalho
- f) No computador que será adicionado ao domínio, você deve possuir acesso ao prompt de comando com privilégios elevados para usar o djoin.exe com a opção /requestODJ
- g) É preciso que todas as máquinas sejam virtualizadas

1.30) A empresa em que você atua disponibilizou diversos servidores com o Windows Server 2012 R2 em modo de instalação Server Core. As licenças destes servidores seguem com a chave em formato MAK, ou seja, será necessária a ativação através de uma linha telefônica ou até mesmo da internet. Qual das opções a seguir permite a ativação do Windows Server 2012 R2 em sua instalação em modo Server Core?

- a) sconfig.cmd
- b) slmgr.vbs
- c) netsh
- d) netdom

1.31) Você agora atua como analista de infraestrutura em uma empresa chamada Sbrubles AS. Esta empresa possui três filiais já em funcionamento e pretende abrir uma sucursal em outro estado. Nesta sucursal, serão mantidos apenas servidores em modo Server Core. Qual dos comandos a seguir permite que um servidor com o Windows Server 2012 R2 em modo de instalação Server Core ingresse ao domínio?

- a) Netdom renamecomputer %computername% /newname:Melbourne
- b) Get-WindowsFeature | Where-Object {\$_.InstallState -eq "Installed"}
- c) Install-WindowsFeature NLB
- d) Netdom join %computername% /domain:adatum.com /UserD:Administrator /PasswordD:*

1.32) Você está atuando como administrador de redes pela empresa HTBRAZ em um provedor de internet chamado Sbrubles.

A empresa efetuou a compra e instalação de diversos servidores com o Windows Server 2012 R2 Datacenter em modo Server Core. Toda a administração destes servidores será feita através de linha de comando.

Qual das ferramentais de linha de comandos a seguir permite adicionar e remover funções e recursos em um computador que esteja executando a opção de instalação Server Core, usando os cmdlets do Windows PowerShell? Marque duas opções.

- a) `Netdom renamecomputer %computername% /newname:Melbourne`
- b) `Get-WindowsFeature | Where-Object {$_.InstallState -eq "Installed"}`
- c) `Install-WindowsFeature NLB`
- d) `Netdom join %computername% /domain:adatum.com /UserD:Administrator /PasswordD:*`

1.33) Baseando nosso conhecimento nas melhores práticas da implementação de controladores de domínio, é recomendado que o Domain Controller também tenha a função de DNS. Esta afirmação é:

- a) Verdadeira
- b) Falsa

1.34) Podemos definir que o ambiente gráfico do Windows Server 2012 é:

- a) Uma role
- b) Uma feature
- c) Um serviço
- d) Um app

1.35) Em um de seus clientes será necessário efetuar o levantamento relacionado ao parque de máquinas disponíveis dentro da empresa. Tal levantamento se deve ao fato de a diretoria de TI solicitar a implantação do ReFS em suas estações de trabalho. Seguindo a documentação oficial, quais sistemas operacionais listados a seguir suportam nativamente o ReFS? Marque todos os que se aplicam.

- a) Windows 8
- b) Windows 8.1
- c) Windows 7 Ultimate
- d) Windows Server 2012 R2
- e) Windows Server 2003 R2
- f) Windows Server 2008
- g) Windows Server 2008 R2
- h) Windows Server 2012

1.36) Você é o administrador de redes da Sbrubles S/A e possui um servidor chamado SRV1, com o Windows Server 2012 R2 instalado e atualizado, porém sem nenhuma função instalada atualmente. Um de seus colegas, que atua como analistas de infraestrutura, monta uma imagem de extensão ISO do Windows Server 2012 R2 na pasta c:\Mount, e precisa instalar a função de DHCP neste SRV1 utilizando o Server Manager. Que pasta você poderia especificar como caminho alternativo para os arquivos de origem do sistema operacional?

- a) WinSxS
- b) Setup
- c) Resources
- d) Tracing
- e) System32

15.2 ACESSO A DADOS

2.1) Imagine que você administra uma floresta com apenas um domínio chamado htbraz.local. Este domínio possui cerca de três controladores de domínio e dois servidores DNS. Estes controladores de domínio estão em um único site localizado fisicamente em um único prédio. Qual dos itens relacionados a seguir permite o gerenciamento de uma coleção de domínios que compartilham um domínio raiz comum e um namespace DNS?

- a) Esquema
- b) Site
- c) Árvore de domínios
- d) Floresta

2.2) Embora o banco de dados do ADDS seja um único arquivo denominado NTDS.DIT, é exibido, gerenciado e replicado como se consistisse de seções ou instâncias distintas dentro dos controladores de domínio. Pensando nesta explicação, identifique qual dos itens a seguir é uma seção do banco de dados do AD DS?

- a) Esquema
- b) Partição
- c) Política de Grupo (GPO)
- d) Unidade Organizacional

2.3) Se entendermos que os componentes lógicos do AD DS são estruturas que você usa para implementar um design lógico do Active Directory apropriado para uma determinada organização, então podemos dizer que é possível controlar qualquer objeto ou rotina organizacional que seja criada em nossa estrutura. Baseado no conhecimento de tal controle, diga qual dos itens a seguir é uma coleção de domínios que compartilham um AD DS comum?

- a) Esquema
- b) Site
- c) Árvore de domínios
- d) Floresta

2.4) Quando nos baseamos pelo conceito de que os componentes lógicos do AD DS são estruturas que você pode utilizar para implementar um design do Active Directory que seja apropriado para uma organização, qual dos itens a seguir é uma lista de tipos e atributos que todos os objetos do AD DS utilizam?

- a) Partição
- b) Esquema
- c) Domínio
- d) Árvore de domínio
- e) Floresta
- f) Site
- g) UO
- h) GPO

2.5) Relembrando o conceito de que os componentes lógicos do

AD DS são estruturas que você usa para implementar um design do Active Directory, qual dos itens a seguir é uma coleção de domínios que compartilham um AD DS comum?

- a) Partição
- b) Esquema
- c) Domínio
- d) Árvore de domínio
- e) Floresta
- f) Site
- g) UO
- h) GPO

2.6) Relembrando o conceito de que os componentes lógicos do AD DS são estruturas que você usa para implementar um design do Active Directory, qual dos itens a seguir é uma coleção de usuários, grupos e computadores conforme definidos por suas localizações físicas?

- a) Partição
- b) Esquema
- c) Domínio
- d) Árvore de domínio
- e) Floresta
- f) Site
- g) UO
- h) GPO

2.7) Qual dos itens a seguir é uma seção do banco de dados do AD DS?

- a) Partição
- b) Esquema
- c) Domínio
- d) Árvore de domínio
- e) Floresta
- f) Site
- g) UO
- h) GPO

2.8) Já sabemos que é possível usar Unidades Organizacionais para representar estruturas hierárquicas lógicas dentro de qualquer organização. Sendo assim, cada domínio do AD DS contém um

conjunto padrão de contêineres e Unidades Organizacionais que são criados quando você instala o AD DS. Qual dos itens a seguir pertence ao conjunto padrão de contêineres e UOs que são criados quando você instala o AD DS?

- a) Contêiner de domínio. Serve como o contêiner raiz da hierarquia.
- b) Contêiner interno. Armazena uma série de grupos padrão.
- c) Contêiner de usuários. O local padrão para as novas contas de usuário e os grupos que você cria no domínio. O contêiner de usuários também contém as contas de administrador e convidado para o domínio, além de alguns grupos padrão.
- d) Contêiner de computadores. O local padrão para as novas contas de computador que você cria no domínio.
- e) UO de controladores de domínio. O local padrão para as contas de computador de controladores de domínio. Essa é a única UO que está presente em uma nova instalação do AD DS.
- f) Todas as anteriores estão corretas.

2.9) Você é o administrador de redes pleno de uma consultoria chamada Sbrubles AS. A rede pela qual você oferece suporte contém um domínio do Active Directory, chamado sbrubles.local. Nesta rede, todos os servidores rodam o Windows Server 2008 R2 ou Windows Server 2012 R2. Todos os controladores de domínios estão com o Windows Server 2012 R2 Standard instalados e atualizados. Todas as estações clientes executam ou Windows 7 Pro ou Windows 8.1 Pro.

O domínio contém um servidor membro nomeado Server1, que executa o Windows Server 2012 que possui a função de servidor de arquivos e serviços de armazenamento instalado. Neste server1, você criar um compartilhamento chamado TI_Share1. Sua equipe precisa se certificar de que todos os usuários da rede possam usar versões anteriores de seus arquivos pessoais a qualquer momento dentro desse compartilhamento TI_Share1. O que pode ser configurado em Server1 para atender esta demanda?

- a) Windows Server Backup schedule
- b) Data Recovery agent
- c) Configurações de Shadow Copies

d) Propriedades da lixeira

2.10) Você possui um servidor chamado Server1 executando o Windows Server 2012 R2 Standard Edition. A equipe de suporte precisa desabilitar o acesso ao Windows Explorer, Internet Explorer e todos os componentes e arquivos relacionados do Server1 de forma simples e prática. O que você deve executar em Server1 para realizar essa tarefa?

- a) Uninstall-WindowsFeatures Server-Gui-Shell Remove
- b) msixec.exe /uninstall iexplorer.exe /x
- c) Uninstall-WindowsFeatures Server-Gui-Mgmt-Infra | Server-Gui-Shell Remove
- d) Uninstall-WindowsFeatures Server-Gui-Mgmt-Infra Remove

2.11) Qual dessas versões de Windows Server podem ser gerenciadas remotamente pelo Server Manager do Windows Server 2012 R2, após a aplicação do winrm quickconfig? Marque todas as opções corretas.

- a) Windows Server 2000
- b) Windows Server 2008
- c) Windows Server 2008 R2
- d) Windows Server 2003 R2
- e) Windows NT

2.12) Qual das opções a seguir pode ser considerada um benefício sobre a utilização dos grupos de servidores pelo Server Manager?

- a) Você pode utilizar server groups para designar privilégios para servidores adicionando eles em um server group.
- b) Você pode utilizar server groups para facilitar o gerenciamento de servidores de diferentes localidades geográficas.
- c) Você pode utilizar server groups para facilitar a delegação de permissões para servidores utilizados por diferentes departamentos na sua empresa.
- d) Você pode utilizar o server groups para criar uma coleção de hierarquias entre os grupos de servidores que ajudam na administração de sua equipe de TI

2.13) Qual das seguintes tarefas de gerenciamento de serviço

podem ser realizadas utilizando um “Services tile” em uma das páginas do Server Manager? Marque todas as que se aplicam.

- a) Parar um serviço
- b) Pausar um serviço
- c) Iniciar um serviço
- d) Alterar a opção de Start Type de um serviço

2.14) Qual dos processos a seguir permite configurar um servidor com Windows Server 2012 para receber configurações remotas pelo Server Manager?

- a) Va até o firewall, abra a porta 3389 e libere o acesso para o usuário
- b) Va até a guia remoto na tela de sistema e acione a assistência remota
- c) Use o Set-ExecutionPolicy -ExecutionPolicy RemoteSigned, e depois o Configure-SMRemoting.exe -force -enable
- d) Não é possível efetuar

2.15) O Dotnet Framework 3.5 não pode ser baixado da internet, pois agora ele é uma Feature (Recurso) do próprio Windows Server 2012. Esta afirmação é:

- a) Verdadeira
- b) Falsa

2.16) Os analistas Rogerio e Eduardo possuem notebooks com o Windows 8.1 Pro instalado, e administram uma rede com servidores Windows Server 2012 R2 e Windows Server 2008 R2. Todos os pacotes de atualização e updates de segurança estão atualizados. Qual das ferramentas a seguir pode ser usada para administração remota destes servidores?

- a) Admin Pack
- b) RSAT
- c) Server Manager Admin Pack
- d) Delpref

2.17) Qual dos itens a seguir não é suportado pela ReFS?

- a) Quotas de disco
- b) Booting

- c) Encriptação EFS
- d) Compactação
- e) Todas as alternativas

2.18) Você administra uma rede com cerca de duzentas estações de trabalho. Nesta rede, existem diversos servidores legado com três servidores dedicados ao controle do domínio. Um técnico de uma sucursal entra em contato informando que um dos servidores membros não permite a configuração de cotas de discos e compactação de arquivos. O técnico da sucursal efetuou diversos testes na mesma unidade de disco do servidor. Que ação deve ser efetuada para identificação do problema?

- a) Verificação do funcionamento das políticas de grupo
- b) Validação do sistema de arquivos
- c) Converta o disco para disco dinâmico
- d) Reinstale o sistema operacional através de uma mídia externa

15.3 CONFIGURAÇÃO DO HYPER-V

3.1) Qual é o requisito básico para que um disco externo seja adicionado como disco em uma máquina virtual?

- a) O disco deve estar off-line
- b) O disco não pode estar off-line
- c) O disco deve possuir o formato GPT
- d) Somente é possível adicionar discos externos na versão 2012 R2

3.2) Você é o administrador de redes da empresa Sbrubles S/A. Seu parque de servidores contempla diversos equipamentos com sistemas variados com Windows Server 2012 R2, Windows Server 2008 R2 e servidores Linux. Você então dedica alguns servidores com o Hyper-V Server 2012 R2. Você precisa subir diversos servidores virtuais, e precisa maximizar a performance de seu ambiente. Que ação seria recomendada para o ambiente?

- a) Desative a memória dinâmica das máquinas virtuais
- b) Utilize discos dinâmicos
- c) Utilize discos diferenciais
- d) Utilize um Failover Cluster

3.3) A rede que você administra possui diversos servidores e um único domínio do Active Directory, chamado `htbraz.local`. Esse domínio possui um servidor chamado `Server1`, que executa o Windows Server 2012 R2 atualizado. O servidor `Server1` tem a função de servidor Hyper-V 3.0 instalado. O domínio `htbraz.local` contém diversas máquinas virtuais e, entre elas, uma chamada `VM1`.

Um prestador de serviço que atua como desenvolvedor deseja anexar um programador depurador à `VM1`. Você, como especialista, precisa se certificar de que o desenvolvedor pode se conectar a `VM1` e utilizar a VM Pipe. Que configuração de máquina virtual você deve fazer para que isso ocorra?

- a) Network Adapter
- b) BIOS
- c) Processador
- d) COM 1
- e) Nenhuma das alternativas

3.4) Você faz parte de uma equipe de administradores de redes que atua para a empresa HTBRAZ. A HTBRAZ possui um domínio chamado `htbraz.local`, onde todos os servidores na rede estão com o Windows Server 2012 R2 instalado. Em uma conversa com outros especialistas, vocês entram em um debate sobre os formatos VHD e VHDX. Qual das seguintes afirmações é verdadeira com relação aos arquivos VHDX? Escolha todas as que se aplicarem.

- a) Ele suporta capacidade de armazenamento de disco rígido virtual de até 64 GB
- b) Ele suporta capacidade de armazenamento de disco rígido virtual de até 64 TB
- c) Ele não fornece proteção contra corrupção de dados durante falhas de energia
- d) Ele tem a capacidade de armazenar metadados personalizados sobre o arquivo que o usuário pode querer gravar

RESPOSTAS DO SIMULADO

16.1 INSTALAÇÃO E CONFIGURAÇÃO

Exercício 1.1

Resposta: C

Explicação: É interessante lembrar-se de que o tamanho da partição pode variar pela quantidade de memória RAM instalada. O arquivo de paginação pode aumentar brutalmente de tamanho, dependendo da quantidade de RAM física instalada. O arquivo de paginação fica na unidade `C:\`, e é chamado de `pagefile.sys`.

Exercício 1.2

Resposta: B, C, E e H

Explicação: A instalação em modo Server Core permite um aumento interessante da segurança, porém devido a remoção da interface gráfica, algumas funções e alguns recursos ficam inviáveis de execução. Será necessário conhecer quais funções e recursos estão ou não disponíveis pelo modo de instalação Server Core para alcançar uma boa pontuação nesta primeira prova relacionada ao MCSA. Para auxiliar você a fixar o conhecimento, segue uma tabela descritiva.

Recursos disponíveis / Server Core	Recursos indisponíveis / Server Core

Active Directory Certificate Services	Active Directory Federation Services
Active Directory Domain Services	Application Server
Active Directory Lightweight Directory Services	Fax Server
Active Directory Rights Management Services	Network Policy and Access Services
DHCP Server	Remote Desktop Services; Remote Desktop Gateway; Remote Desktop Session Host; Remote Desktop Web Access
DNS Server	Volume Activation Services
File and Storage Services	Windows Deployment Services
Hyper-V	-
Print an Document Services	-
Remote Access	-
Web Server (IIS)	-
Windows Server Update Services	-

Exercício 1.3

Resposta: C

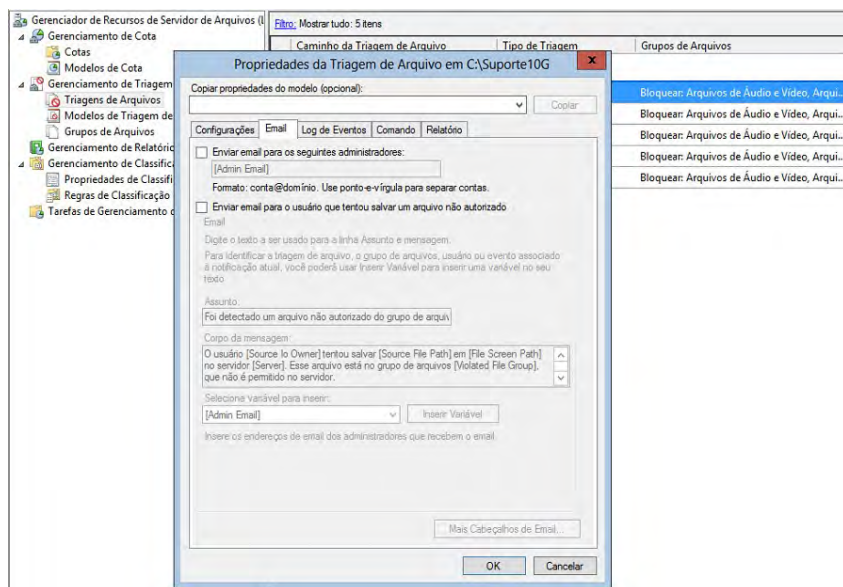
Explicação: A ferramenta `dism.exe` é uma velha conhecida dos administradores de redes e por quem prestou a prova 70-680. Esta ferramenta possui uma série de funcionalidades direcionadas ao tratamento de imagens do Windows. Note que a questão orienta você a executar o comando de menor esforço administrativo com a sintaxe correta. O arquivo `ServerHTB.win` representa a imagem de extensão `.win`, localizada em `C:\`. O comando segue uma estrutura lógica, portanto primeiro identifique a imagem, depois efetue liberação da função, para só então efetuar a montagem através de um diretório qualquer. Aqui nosso diretório foi o `mount`

em C:\ .

Exercício 1.4

Resposta: A

Explicação: Neste ponto, os detalhes fazem a diferença. Veja que os volumes que trabalham com MBS possuem tamanhos específicos de 2TB. Isso significa que a necessidade deste cliente só pode ser contemplada com a conversão do disco para o formato GPT, que suporta tamanhos superiores a 2TB. Para executar a conversão de um disco para o formato GPT, recomendo a utilização do comando `diskpart` . Lembre-se de que é possível a conversão dos discos para básico, dinâmico, GPT e MBR, respeitando sempre a limitação de armazenamento. A figura XPTO 01 demonstra bem essa informação



Exercício 1.5

Resposta: D

Explicação: Cada versão do sistema operacional possui limitações, logo, conheça os detalhes de cada uma para não cometer deslizes durante a interpretação dos enunciados das questões durante a prova. Este servidor é direcionado ao público Small Business (pequenos) e seus serviços de impressão e aplicações, não exigindo grande complexidade.

Exercício 1.6

Resposta: C

Explicação: Neste caso, o servidor com a licença para o Windows Server 2012 R2 Essentials possui todas as características das versões anteriores, menos a disposição para virtualização e para o Active Directory. Cada versão possui ferramentas específicas e um valor agregado, ou seja, você paga mais pelas melhores ferramentas.

Exercício 1.7

Resposta: A e B

Explicação: O modo de instalação Server Core está disponível apenas nas edições Datacenter e Standard do Windows Server 2012 R2.

Exercício 1.8

Resposta: A

Explicação: A ferramenta `sconfig.cmd` está disponível também em versões anteriores, como o Windows Server 2008 e Windows Server 2008 R2. Esta ferramenta é utilizada no Windows Server 2012 e Windows Server 2012 R2 para sua rápida configuração, extremamente útil em instalações do tipo Server Core.

Exercício 1.9

Resposta: F

Exercício 1.10

Respostas: B, C, F e H

Explicação: É importante lembrar de que nem todas as ferramentas convencionais do Windows possuem funcionalidade ativa em instalações Server Core. Aqui destacamos algumas das mais importantes, e que podem ser usadas para direcionamento de estudo e também no dia a dia.

Exercício 1.11

Resposta: A

Explicação: Será necessário trabalhar em modo de instalação Server Core quando houver necessidades relacionadas ao aumento de performance e segurança do servidor. Portanto, tais movimentações comuns através de linha de comando deverão ser aplicadas constantemente. O comando `netdom` fica disponível com a instalação do Active Directory, e permite ao administrador de redes validar e alterar algumas atividades do controlador de domínio, como a mudança de nome de uma estação de trabalho ou servidor.

Exercício 1.12

Resposta: C

Explicação: A ferramenta de ativação do Windows Server é chamada de `slmgr.vbs`, porém lembre-se de que este comando está descrito aqui em seu caminho completo. Logo, a resposta exige que você saiba não só a existência da ferramenta de linha de comando, mas sua forma de funcionamento em conjunto com o `cscript`.

Exercício 1.13

Resposta: B, C

Explicação: É possível liberar o acesso remoto em um servidor com instalação Server Core através de linha de comando e pelo painel de configurações rápidas chamado de `sconfig.cmd`. É muito interessante conhecer todas as alternativas possíveis para facilitar tanto seu suporte em ambientes sem a instalação da área gráfica quanto para momentos de avaliação em empresas e corporações.

Exercício 1.14

Resposta: B

Explicação: Uma das características mais comuns da administração de redes com o Windows Server 2012 R2 é a mudança de modo de instalação Server Core, para o modo de instalação gráfica. É importante lembrar de que essa característica de mudança de ambiente não está disponível para o Windows Server 2008 R2. Caso você precise converter um com Windows Server 2008 R2 em modo Server Core para uma instalação completa, será primeiro necessário atualizar este servidor para Windows Server 2012 e, somente então, efetuar a mudança.

Exercício 1.15

Resposta: D

Explicação: O processo contrário também é parte do dia a dia dos administradores de redes. Portanto, conhecer os `cmdlets` de instalação e remoção de funções e recursos é extremamente importante. O parâmetro `Server-Gui-Shell -remove` elimina o ambiente gráfico e, após o boot do servidor, somente o modo de instalação `Server Core` é carregado. Diversos administradores de redes fazem todas as configurações possíveis compatíveis com o ambiente `Server Core`, e depois removem a interface gráfica para aumentar a segurança.

Exercício 1.16

Resposta: C

Explicação: Discos em formato `GPT` suportam partições superiores a 2 TB. Não se esqueça desse detalhe quando dimensionar unidades lógicas em discos com tamanho superior a 2 TB.

Exercício 1.17

Resposta: A

Explicação: A `ReFS` é chamada de Sistema de Arquivos Resiliente. Isso significa que esse tipo de sistema de arquivos oferece mais segurança para os dados alocados em um disco de armazenamento.

Veja mais em: <https://technet.microsoft.com/pt-br/library/hh831724.aspx>

Exercício 1.18

Resposta: D

Exercício 1.19

Resposta: F

Exercício 1.20

Resposta: B

Exercício 1.21

Respostas: A, C

Exercício 1.22

Resposta: B

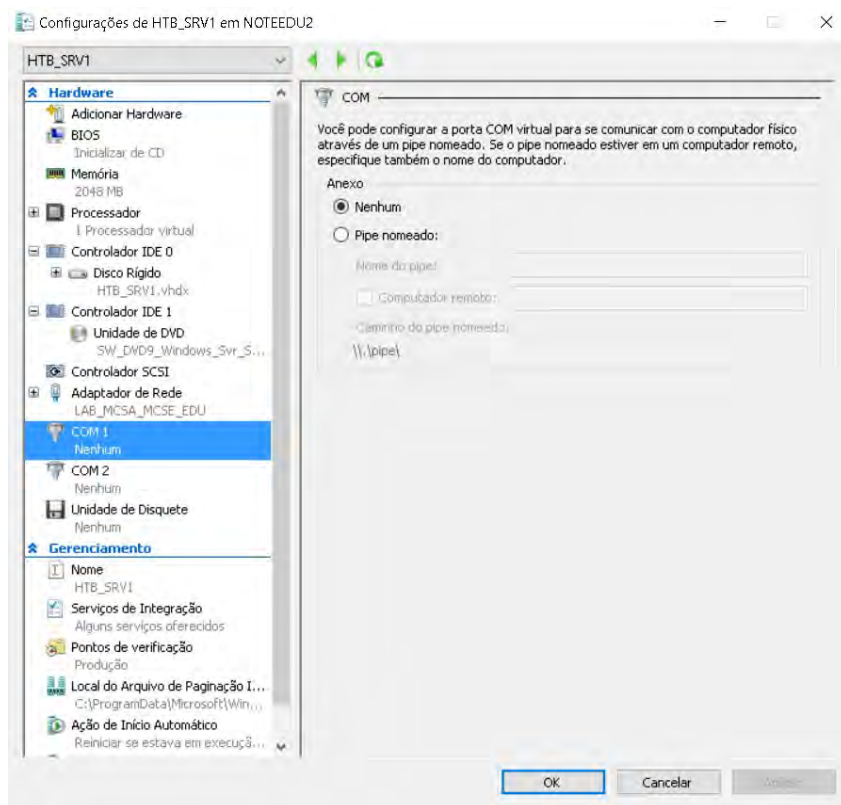
Explicação: Não é de hoje que as versões e edições do Windows recebem restrições quanto a upgrade e migrações. Conheça bem as características de upgrade entre versões e edições para evitar problemas.

Exercício 1.23

Resposta: A

Explicação: Veja bem, a conversão da área gráfica para o modo de instalação Server Core pode ser feito pela própria área gráfica,

quando o inverso não é possível, conforme demonstra a próxima figura. Lembre-se de que este item é um recurso que pode ser desinstalado através do Server Manager.



Exercício 1.24

Resposta: B

Explicação: A pasta `winSxS` armazena todos os arquivos principais do sistema operacional e possui um tamanho considerável em relação às demais pastas. Esta pasta está presente no Windows Server 2012 R2 e também no Windows 8.1, valendo um olhar crítico para conhecimento aprimorado do Windows

Server 2012 R2.

Exercício 1.25

Resposta: D

Explicação: Esta pergunta pode parecer bem confusa, mas isole de forma lógica os parâmetros da resposta. A GPO `SENHA_01` está sendo aplicada em `MarketingUsers`, onde estão efetivamente os usuários, ou seja, pela tabela apresentada é possível identificar que a resposta oferece 10 caracteres para a senha.

Exercício 1.26

Resposta: B

Explicação: É possível configurar o disparo de e-mails aos usuários pelo servidor de arquivos. Use o Gerenciador de Recursos do Servidor de Arquivos. A próxima figura demonstra bem a tela de configuração.



Exercício 1.27

Respostas: D, F

Explicação: Para atender as solicitações diárias relacionadas a resolução de nomes, é necessário entender a estrutura de funcionamento de determinadas configurações. Veja bem, a solicitação pede que seja suspenso qualquer resolução de nomes de hosts de internet direcionados para SERVER1 . Essa atividade só é possível criando uma entrada com um . (ponto) e pela remoção dos host hints .

Exercício 1.28

Resposta: A

Explicação: A adição de estações de trabalho de modo off-line é algo relativamente novo, que pode ajudar muito quando estamos com o link fora de operação em filiais e sucursais muito distantes. Esta técnica é usada quando a rede não possui nenhum contato com o controlador de domínio. A ferramenta de linha de comando `djoin` é o segredo para responder esta questão, e deve ser conhecido por todos os administradores de redes que se proponham a prestar suporte em ambientes com o Windows Server 2012 R2.

Exercício 1.29

Respostas: A,B,D,F

Explicação: O ingresso em domínio em modo off-line é um recurso que pode ser utilizado para ingressar um computador em um domínio quando este não tem uma conexão de rede ativa. Esse recurso pode ser útil em situações nas quais a conectividade é intermitente, como quando você está implantando um servidor em um site remoto que está conectado via uplink de satélite. Este recurso também é usado em situações nas quais nasce uma nova filial da empresa antes da ativação do link de dados com a matriz. Pode-se adiantar etapas no processo de preparação do ambiente através desta técnica.

1. Faça login no controlador de domínio com uma conta de usuário que possua os direitos apropriados para ingressar outros computadores no domínio.
2. Abra um prompt de comando com privilégios elevados e use o comando `djoin.exe` com a opção `/provision` . Você também precisa especificar o domínio no qual deseja ingressar o computador, o nome do computador que será ingressado no domínio e o nome do arquivo de salvamento que será transferido para o destino do ingresso em domínio offline.

Por exemplo, para ingressar o computador `Sbrubles` ao domínio `htbraz.com` usando o arquivo de salvamento `sbrubles-join.txt` , digite o seguinte comando:

```
djoin.exe /provision /domain htbraz.com /machine  
sbrubles /savefile c:\sbrubles-join.txt .
```

3. Transfira o arquivo de salvamento gerado para o novo computador e, em seguida, execute o comando `djoin.exe` com a opção `/requestODJ` . Por exemplo, para realizar o ingresso em domínio offline, após a transferência do arquivo de salvamento `sbrubles-join.txt` ao computador `sbrubles` , você deve executar o seguinte comando a partir de um prompt de comando com privilégios elevados em Canberra: `djoin.exe /requestODJ /loadfile sbrubles-join.txt /windowspath %systemroot% /localos` .
4. Reinicie o computador para concluir a operação de ingresso em domínio.

Exercício 1.30

Resposta: B

Exercício 1.31

Resposta: D

Exercício 1.32

Resposta: B, D

Exercício 1.33

Resposta: A

Explicação: Em um ambiente real de produção, quando utilizamos o AD DS (Serviços de Domínio Active Directory) juntamente ao armazenamento integrado ao diretório das zonas de DNS, é possível alcançar níveis elevados de segurança, tolerância a falhas, além de implantação e gerenciamento simplificados.

Veja mais em: <http://htbraz.blogspot.com.br/2013/02/boas-praticas-com-o-dns.html>

Exercício 1.34

Resposta: B

Explicação: Palavras-chaves são importantes, não se esqueça. A interface gráfica do Windows Server 2012 é uma Feature que pode ser instalada e desinstalada livremente. Em seu antecessor, Windows Server 2008, era possível apenas remover a interface gráfica (GUI).

Exercício 1.35

Resposta: A, B, D, H

Explicação: A ReFS, também conhecida como Resilient File

System , é um sistema de arquivos local que maximiza a disponibilidade de dados gravados em disco. Este sistema de arquivos possui arquitetura diferenciada e não é suportado por todos os sistemas operacionais de mercado.

Exercício 1.36

Resposta: C

Explicação: Lembre-se de que a pasta padrão para se manter os arquivos do Windows Server 2012 R2 é a `winSxS` . Portanto, a montagem deve ser executada ali, principalmente quando existe a exigência de um maior permissionamento de acesso aos dados de instalação. A pasta `winSxS` pode alcançar um tamanho considerável em alguns servidores e existem diversos posts pela internet ensinando como efetuar a limpeza de seu conteúdo. Eu, como especialista, não recomendo sua limpeza, mas isso depende muito de situação para situação. A prova não cobrará de você detalhes dessa pasta, mas apenas seu conhecimento prévio.

16.2 ACESSO A DADOS

Exercício 2.1

Resposta: C

Exercício 2.2

Resposta: B

Explicação: O `NTDS.DIT` é a base de dados do Active Directory, que nada mais é do que um banco de dados que armazena os objetos disponíveis em uma organização. Todo banco de dados possui uma estrutura funcional, sessões e uma lógica de

operações. Conhecer essa estrutura pode ajudar a corrigir problemas de replicação, corrompimento de dados e até paradas de funcionamento.

Exercício 2.3

Resposta: D

Exercício 2.4

Resposta: B

Explicação: Este enunciado foi elaborado para confundir quem lê, sem o conhecimento correto da estrutura de funcionamento de um controlador de domínio. Basicamente, quando simplificada, a pergunta questiona sobre qual das FSMO possui a gestão dos objetos do AD DS. Neste caso, convém lembrar de que existem cinco FSMOs, em que duas estão relacionadas à floresta e três estão relacionadas ao domínio.

Exercício 2.5

Resposta: E

Exercício 2.6

Resposta: F

Exercício 2.7

Resposta: A

Explicação: Embora o banco de dados seja um arquivo denominado NTDS.DIT, ele é exibido, gerenciado e replicado como se consistisse de seções ou instâncias distintas. Essas são chamadas de partições, que também são conhecidas como contextos de

nomenclatura.

Exercício 2.8

Resposta: F

Explicação: Nenhum dos contêineres padrão em domínios do AD DS podem conter GPOs vinculados a eles, exceto a UO de controladores de domínio e o próprio domínio. Todos os outros contêineres são apenas pastas. Para vincular uma ou mais GPOs a fim de aplicar configurações e restrições, crie uma hierarquia de UOs e, em seguida, vincule GPOs a elas.

Exercício 2.9

Resposta: C

Explicação: As cópias de sombra, ou Shadow Copies, não são exatamente uma novidade. Sua implementação está disponível em versões mais antigas, como o Windows Server 2003, até os mais atuais, como o Windows Server 2012 R2. Este recurso é extremamente valioso para as equipes de suporte, visto que o próprio usuário pode restaurar versões antigas de seus arquivos sem a necessidade da intervenção de equipes técnicas.

Exercício 2.10

Resposta: A

Explicação: Veja bem, todas as aplicações que o enunciado solicita remoção estão ligados diretamente ao ambiente gráfico. Quando utilizamos o comando `Uninstall-WindowsFeatures Server-Gui-Shell Remove`, o ambiente gráfico e o acesso às ferramentas relacionadas serão removidos.

Exercício 2.11

Respostas: B,C

Explicação: É importante lembrar de que podemos gerenciar outros servidores pelo Server Manager do Windows Server 2012 R2. Contudo, devemos nos atentar ao fato de que apenas servidores a partir do Windows Server 2008 podem ser gerenciados remotamente após a aplicação do comando `winrm quickconfig`.

Exercício 2.12

Resposta: B

Exercício 2.13

Resposta: A, B, C

Exercício 2.14

Resposta: C

Exercício 2.15

Resposta: A

Exercício 2.16

Resposta: B

Explicação: O RSAT é um pacote de ferramentas que permite a administração remota de servidores através de estações de trabalho que possuam o sistema operacional Windows 8, Windows 8.1 ou Windows 10. É uma versão melhorada do antigo Admin Pack, usado pelos administradores de redes com estações Windows XP Professional. É importante citar aqui que o RSAT possui uma versão

compatível com o Windows 7, porém sem integrar todas as funcionalidades do atual Server Manager do Windows Server 2012 R2.

Exercício 2.17

Resposta: E

Exercício 2.18

Resposta: B

Explicação: A primeira ação a ser efetuada é a verificação do sistema de arquivos presente nesta unidade. É muito possível que o sistema de arquivos esteja como ReFS . Apesar de mais resilientes, o ReFS elimina qualquer possibilidade do uso de cotas de disco e compactação.

16.3 CONFIGURAÇÃO DO HYPER-V

Exercício 3.1

Resposta: A

Explicação: É importante se lembrar de que as máquinas virtuais somente conseguem acessar discos externos USB, Sata e SAS se estiverem em modo off-line nos servidores Host. É importante ressaltar ainda que pen-drives e dispositivos como cartões SD não são reconhecidos para essa atividade.

Exercício 3.2

Resposta: A

Explicação: A memória dinâmica é um recurso poderoso

quando não temos hardware suficiente para subir todos os servidores necessários. Porém, quando precisamos de performance elevada, é altamente recomendável desativar a memória dinâmica.

Exercício 3.3

Resposta: D

Explicação: Esta opção conecta à porta serial virtual a um “tubo” (pipe) do Windows, chamado de `operatingsystem host` ou um computador na rede. Um named pipe, ou “tubo”, é uma porção da memória que pode ser usada por um processo para passar a informação para um outro processo, de modo que a saída de um é a entrada do outro.

Os pipes nomeados podem ser usados para criar um cabo de modem nulo virtual entre duas máquinas virtuais, ou entre a máquina virtual e um programa de depuração no sistema operacional hospedeiro que suporta o uso de pipes. Ao ligar duas portas seriais virtuais para o mesmo pipe nomeado, você pode criar um *virtual cable connection*. Os pipes nomeados são úteis para depuração ou para qualquer programa que requer uma conexão de modem.

Para ver os pipes nomeados de uma máquina virtual, clique com o botão direito em cima da VM, então clique em configurações. Clique agora em *COM1*, conforme demonstrado pela figura a seguir. Este recurso também é muito útil quando pretendemos interconectar impressoras paralelas ou seriais para uso nas máquinas virtuais.

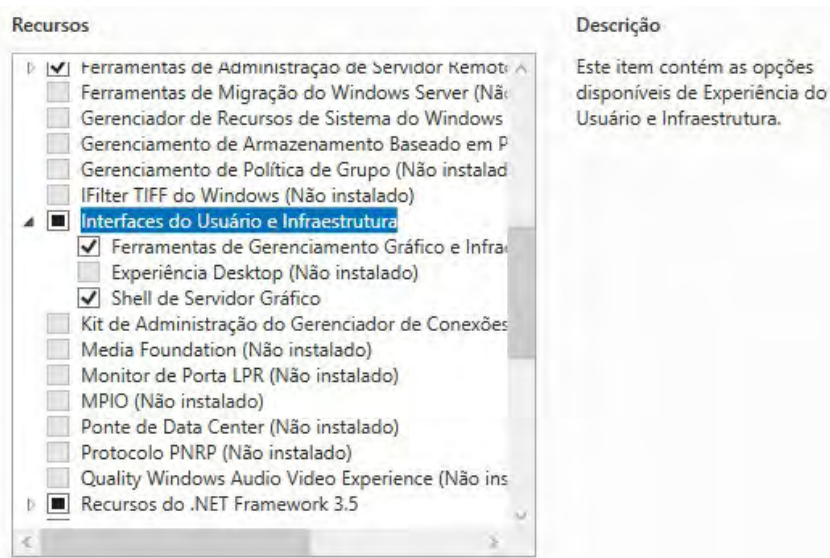


Figura 16.4: [http://technet.microsoft.com/en-us/library/ee449417\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee449417(v=ws.10).aspx)

Exercício 3.4

Respostas: B, D

Explicação: Os arquivos VHDX são aprimorados em relação aos arquivos VHD, incluindo espaço e resiliência. Será necessário conhecer bem o formato dos arquivos VHDX e VHD para não cair em pegadinhas da prova. Diversos cenários serão aplicados a estes fatores.