

Aula 00

*Arquitetura e Sistemas Operacionais p/
TCM-SP (Agente de Fiscalização -TI)
Com Videoaulas Pós-Edital*

Autor:

**Equipe Informática e TI, Evandro
Dalla Vecchia Pereira**

06 de Março de 2020

NTFS (New Technology File System)	2
<i>Questões Comentadas</i>	<i>6</i>
Protocolo LDAP	11
<i>Questões Comentadas</i>	<i>13</i>
Active Directory (AD)	18
<i>Questões Comentadas</i>	<i>22</i>
Administração de usuários, grupos, permissões, controles de acesso	29
<i>Questões Comentadas</i>	<i>34</i>
Noções de Remote Desktop e VDI	37
<i>Questões Comentadas</i>	<i>39</i>
Serviços de arquivo e de impressão em rede	42
<i>Questões Comentadas</i>	<i>45</i>
Lista de Questões	48
GABARITO	62



PROF. EVANDRO DALLA VECCHIA

Autor do livro "Perícia Digital - Da investigação à análise forense", Mestre em Ciência da Computação (UFRGS), Bacharel em Ciência da Computação (PUCRS), Técnico em Redes de Computadores (Ecom/UFRGS) e em Processamento de Dados (Urcamp). Perito Criminal na área de Perícia Digital desde 2004 no Instituto-Geral de Perícias/RS. Professor de pós-graduação em diversas instituições, nas áreas de Perícia Digital, Perícia Criminal e Auditoria de Sistemas. Lecionou na graduação de 2006 a 2017, nas instituições PUCRS, Unisinos, entre outras. Professor em cursos de formação e aperfeiçoamento de Peritos Criminais, Delegados, Inspetores, Escrivães e Policiais Militares.

Áreas de cursos ministrados pelo professor no Estratégia: Computação Forense, Arquitetura de Computadores e Sistemas Operacionais.

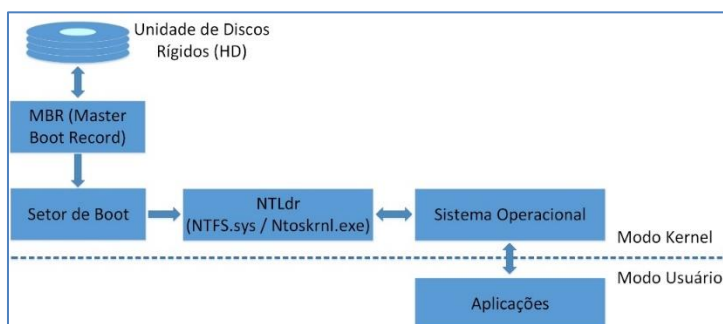
Entre em contato:   profevandrodallavecchia



NTFS (*NEW TECHNOLOGY FILE SYSTEM*)

O NTFS (*New Technology File System*) é o sistema de arquivos padrão para o Windows NT e seus derivados, não sendo suportado pelas versões anteriores (MS-DOS, Windows 95, 98 e Millennium). Foi criado para dar suporte a um sistema operacional **mais completo e confiável**, suprimindo as limitações e falta de recursos do sistema de arquivos FAT32.

A tabela de partições possui campos que descrevem a partição, sendo o campo “System ID” o responsável pela definição do sistema de arquivos (0x07 = NTFS). A arquitetura NTFS é a seguinte:



A descrição de tais componentes é mostrada abaixo:

Componente	Descrição
HD	Possui uma ou mais partições.
Setor de boot	Partição inicializável que armazena as informações sobre o volume e as estruturas do sistema de arquivos, além do código de boot que carrega o NTLdr.
MBR	Possui o código executável que o BIOS carrega na memória. O código procura na MBR a tabela de partições para verificar qual partição é a ativa (inicializável).
NTLdr.dll	Alterna para o modo protegido, inicia o sistema de arquivos e lê o conteúdo do arquivo Boot.ini. Essas informações determinam as opções iniciais e seleções de menu de inicialização.
NTFS.sys	Driver do sistema de arquivo NTFS.
Ntoskrnl.exe	Extraí informações sobre quais drivers de dispositivos devem ser carregados e em que ordem.



Modo Kernel	Modo de processamento que permite ao código ter acesso direto a todo o sistema de hardware e memória.
Modo usuário	Modo de processamento no qual os aplicativos são executados.

Em relação à estrutura física, os *clusters* em partições NTFS são numerados sequencialmente desde o início da partição (setor 0) até a área destinada aos dados. **Para todos os objetos armazenados é realizado um registro através da MFT (*Master File Table*)**, que possui uma estrutura similar a uma base de dados. Note que no sistema de arquivos FAT nós tínhamos uma tabela de mesmo nome (FAT).

Discos que utilizam MBR possibilitam o uso de partições básicas e dinâmicas. **Como o MBR possui uma limitação de partições com no máximo 2TB, deve-se utilizar volume dinâmico para criar um volume NTFS acima desse tamanho.** Volumes dinâmicos podem possuir até o tamanho máximo suportado pelo NTFS (256TB). **Quando utilizado um disco GPT (*GUID Partition Table*), o suporte a volumes maiores que 2TB também é garantido.**

A figura e a tabela a seguir mostram e descrevem a organização das estruturas utilizadas por uma partição NTFS.

Setor de Boot NTFS	Master File Table (MFT)	Dados do Sistema de Arquivos	Cópia da MFT
--------------------	-------------------------	------------------------------	--------------

Componente	Descrição
Setor de Boot NTFS	Possui informações sobre o leiaute do volume e as estruturas do sistema de arquivos, além do código de boot que carrega o sistema operacional.
<i>Master File Table</i> (MFT)	Possui as informações necessárias para acessar arquivos da partição NTFS, tais como os atributos de um arquivo.
Dados do Sistema de Arquivos	Armazena dados que não estão contidos na MFT.
Cópia da MFT	Possui cópia de registros essenciais para uma recuperação do sistema de arquivos caso haja um problema com a MFT original.



Quando um volume NTFS é formatado, o software utilizado para a formatação aloca os primeiros 16 setores para o setor de *boot* e o código *bootstrap*¹. A figura abaixo mostra o setor de boot de uma imagem de um pen drive com capacidade de 1GB.

00000000	EB 52 90 4E 54 46 53 20-20 00 20 00 02 08 00 00	eR-NIFS
00000010	00 00 00 00 00 00 F8 00 00-3F 00 FF 00 20 00 00 00	ø-?-ÿ
00000020	00 00 00 00 00 80 00 00 00-1C A4 1E 00 00 00 00 00	h.....
00000030	D6 46 01 00 00 00 00 00 00-02 00 00 00 00 00 00	ÖF.....
00000040	F6 00 00 00 01 00 00 00 00-6A F4 16 A8 18 17 A8 58	ö.....jô.....X
00000050	00 00 00 00 00 FA 33 C0 8E-0D BC 00 7C F6 68 C0 07	ûÄ Ð¾ ðhü.....
00000060	1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E	..hf È.....f>-N
00000070	54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 F6	TFSu-Ä»UÏ r-ü
00000080	55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC	U+u-Ä- u-éÿ.....
00000090	18 68 1A 00 B4 48 8A 16-0E 00 8B FA 16 1F CD 13	..h-..H.....ô-ï
000000a0	9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3	..Ä- X-rä;...uÜ
000000b0	0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8	..Ä.....Z3Ü+..+È
000000c0	66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8	fÿ.....Äÿ.....è
000000d0	4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D	K+ÈwÏ...ïf fÄu-
000000e0	66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16	f-ÜTCRaus-ü-r-ü
000000f0	68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66	h-»h- h-»FSFS
00000100	55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF	U-..h-..fa-..î-3Ä
00000110	0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E	..ò-üò*èþ.....f
00000120	06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00	..f-ï.....fh.....
00000130	00 66 50 06 53 68 01 00-68 10 0A B4 42 8A 16 0E	fP-Sh-..h-..B-..
00000140	00 16 1F 8B FA CD 13 66-59 5B 5A 66 59 66 59 1F	ôï-fÿ[Zfÿfÿ
00000150	0F 82 16 00 66 FF 06 11-00 03 16 0F 00 8E C2 FF	fÿ.....
00000160	0E 16 00 75 BC 07 1F 66-61 C3 A1 F6 01 E8 09 00	u-..faÄ;ö-è
00000170	A1 FA 01 E8 03 00 00 F4 EB-FD 8B F0 AC 3C 00 74 09	jü-è-öëÿ-ä<-t-..
00000180	B4 0E BB 07 00 CD 10 EB-F2 C3 0D 0A 45 72 72 6F	'»-..î-èöÄ- Error
00000190	20 64 65 20 64 69 73 63-6F 00 0D 0A 42 4F 4F 54	de disco-..BOOT
000001a0	4D 47 52 20 63 6F 6D 70-61 63 74 61 64 6F 00 0D	MGR compactado..
000001b0	0A 50 72 65 73 73 69 6F-6E 65 20 43 74 72 6C 2B	-Pressione Ctrl+
000001c0	41 6C 74 2B 44 65 6C 20-70 61 72 61 20 72 65 69	Alt+Del para rei
000001d0	6E 69 63 69 61 72 0D 0A-00 73 74 61 72 74 0D 0A	nciar-..start-..
000001e0	00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	
000001f0	00 00 00 00 00 00 8A 01-9A 01 AF 01 00 00 55 AA	

A tabela a seguir mostra os campos do setor de boot NTFS, suas devidas descrições e os valores do exemplo (pen drive de 1GB).

Posição (hexadecimal)	Nome do campo	Descrição	Valor do exemplo (pen drive)
0x0 a 0x2	Instrução Jump	Instrução JUMP de uma arquitetura x86.	0xEB5290
0x3 a 0xA	Identificador OEM	Identificador original do fabricante.	0x4E54465320202020 = "NTFS "
0xB a 0x23	BPB (BIOS Parameter Block)	Estrutura de dados que descreve o leiaute físico do volume.	Ver na figura...
0x24 a 0x53	BPB Estendido	Extensão do BPB.	Ver na figura...

¹ *Bootstrap*: programa que inicializa o S.O. durante o boot da máquina.

0x54 a 0x1FD	Código <i>Bootstrap</i>	Código responsável pela inicialização do sistema operacional.	Código binário, uma parte do texto é possível visualizar: "Erro de disco..."
0x1FE a 0x1FF	Marcador de fim do setor	Marca o fim do setor.	Assinatura "0xAA55" (<i>little endian</i>)

A **MFT** é uma base de dados relacional constituída de registros de arquivos nas linhas e de atributos de arquivos nas colunas. Possui pelo menos uma entrada para cada arquivo, incluindo a própria MFT. Nessa tabela são armazenadas as informações necessárias para acessar arquivos na partição.

Como a MFT armazena informações de si própria, os primeiros 16 registros são reservados para os arquivos de metadados, os quais são utilizados para descrever a MFT. Arquivos de metadados (nomes começados pelo símbolo de cifrão) são descritos abaixo:

Nome do arquivo	Registro MFT	Descrição
\$Mft	0	Possui um registro para cada arquivo/pasta no volume. Se a quantidade de informação de alocação for muito grande para um único registro, outros registros são alocados também.
\$MftMirr	1	Garante acesso à MFT caso haja falha em algum setor. É um espelhamento dos primeiros quatro registros da MFT.
\$LogFile	2	Informações utilizadas pelo NTFS para uma recuperação rápida. É utilizado para restaurar a consistência de metadados depois de uma falha do sistema. O tamanho do log depende do tamanho do volume, mas pode ser aumentado através do comando Chkdsk.
\$Volume	3	Informações sobre o volume, tais como o rótulo e a versão.
\$AttrDef	4	Lista de nomes de atributos, números e descrições.
.	5	Pasta raiz.
\$Bitmap	6	Representação do volume mostrando clusters alocados (bit 1) ou não alocados (bit 0).
\$Boot	7	Possui o BPB utilizado para montar o volume e código de bootstrap adicional utilizado, se o volume for inicializável.



\$BadClus	8	Possui os clusters defeituosos do volume.
\$Secure	9	Possui descritores únicos de segurança para todos os arquivos no volume.
\$Upcase	10	Converte caracteres minúsculos para compatibilidade com caracteres maiúsculos UNICODE.
\$Extend	11	Utilizado para extensões opcionais, tais como cotas, <i>reparse points</i> (conjunto de dados definidos para um usuário) e identificadores de objetos.
	12 a 15	Reservado para uso futuro.

As permissões NTFS são usadas quando queremos limitar de fato as permissões dos usuários a pastas e arquivos. **As permissões são cumulativas e a permissão negar tem prioridade sobre qualquer permissão.** Permissões para pastas possuem a mesma prioridade em relação a permissões para arquivos.

Outro quesito importante relacionado à segurança é a possibilidade de cifrar arquivos e pastas em nível de sistema de arquivo. Trata-se do **EFS (Encrypting File System)**, um componente do NTFS que habilita a criptografia transparente de arquivos utilizando algoritmos de criptografia padrão.

Um recurso de auto recuperação (*self-healing*) foi incorporado ao NTFS no Windows Vista e também no Windows Server 2008. Com tal recurso, torna-se desnecessária a utilização da ferramenta Chkdsk.exe para corrigir danos causados em volumes NTFS.

O conceito de AD (*Active Directory*) surgiu com o Windows 2000 Server (utilizando NTFS como sistema de arquivos). Objetos como usuários, grupos, membros dos grupos, senhas, contas de computadores, informações sobre o domínio, etc, ficam armazenados no banco de dados do AD.

O **LFS (Log File Service)** foi desenvolvido para prover registros (*logs*) e serviços de recuperação para o NTFS. O LFS consiste de uma série de rotinas em modo *kernel* (núcleo) utilizadas para acessar os arquivos de *log*, que são divididos em duas regiões: a área de reinicialização e a área de *log* “infinito”.

QUESTÕES COMENTADAS

1. (2009 – FCC – TRT - 3ª Região (MG) – Técnico Judiciário - Tecnologia da Informação)

No sistema de arquivos NTFS,

A) as permissões aplicadas nas pastas têm maior prioridade sobre as permissões aplicadas nos arquivos.



B) se um usuário possui permissão em um arquivo e esse mesmo usuário faz parte de um grupo que possui outra permissão, no mesmo arquivo, a permissão efetiva do usuário será aquela de menos privilégios.

C) se um usuário pertence a dois grupos que acessam a mesma pasta, e um dos grupos possui a permissão negar, independentemente da permissão que ele tiver no outro grupo, a permissão efetiva desse usuário na pasta será negar, pois negar tem prioridade sobre todas as outras permissões.

D) ao mover um arquivo ou pasta para outra partição, as permissões originais serão mantidas.

E) permissões explícitas não podem ser alteradas, a menos que o mecanismo de herança seja desativado.

Comentários:

As permissões NTFS são usadas quando queremos limitar de fato as permissões dos usuários a pastas e arquivos. As permissões são cumulativas e a permissão negar tem prioridade sobre qualquer permissão.

Gabarito: C

2. (2009 – UFSJ – UFSJ – Técnico de Tecnologia da Informação)

O Sistema de Arquivos determina a estrutura de armazenamento e manipulação de afirmar que dados em um HD (Hard Disk). Sobre os Sistemas de Arquivos, é INCORRETO

A) o NTFS é muito eficiente na área de tamanhos de cluster, permitindo formatar uma partição com o tamanho de cluster que se desejar.

B) nos sistemas de arquivos FAT16, FAT32 e NTFS, quanto maior for o tamanho do cluster, maior será o tamanho da partição.

C) o sistema operacional Linux pode ler informações gravadas no sistema de arquivo NTFS.

D) o NTFS é tecnicamente superior aos sistemas de arquivo FAT16 e FAT32. Porém, por permitir um melhor aproveitamento do HD com relação ao tamanho, apresenta menor segurança do que seus antecessores.

Comentários:

A primeira frase está estranha, mas o foco é a segunda. Vamos ver cada uma das alternativas: (A) quando você formata um volume NTFS, é possível escolher o tamanho de cluster dentre as opções mostradas; (B) alternativa complicada, pois o cluster pode ser maior mas a quantidade de clusters poderia ser menor, o que não tornaria o tamanho da partição maior! Essa afirmativa poderia ser INCORRETA, mas analisando as demais, a alternativa D parece uma melhor opção como a mais INCORRETA; (C) é possível montar sistemas de arquivos diversos no Linux, incluindo FAT32, NTFS, entre outros; (D) o ponto forte do NTFS é justamente a segurança, possibilitando o uso do EFS



(criptografia em nível de sistema de arquivo) e permissões de acesso, leitura e gravação de acordo com o usuário.

Gabarito: D

3. (2010 – FUNCAB – SEMARH-GO – Cientista da Computação)

Sobre o sistema de arquivo NTFS é correto afirmar que:

- A) é utilizado por algumas versões antigas do Windows e pelas primeiras versões do Linux, mas foi substituído por outros sistemas de arquivos mais modernos por possuir um limite de armazenamento de 2 GBytes.
- B) não permite o uso de arrays RAID, possui tolerância a falhas e permite acesso a dados de rede com segurança.
- C) possibilita ter um controle de acesso a arquivos com gerenciamento de usuários, incluindo suas permissões de acesso, leitura e escrita desses arquivos.
- D) é um sistema que contém acesso e indicações de onde estão as informações de cada arquivo através de um grupo de setores chamados de clusters (ou unidade de alocação).
- E) trabalha com alto grau de desfragmentação de disco e menor consistência de dados, com uma arquitetura de dados baseada em organização por setor que mantém os dados espalhados pelo disco.

Comentários:

O diferencial do NTFS é ter mecanismos que garantam maior confiabilidade e segurança, incluindo um controle de acesso a arquivos com gerenciamento de usuários (permissões de acesso).

Gabarito: C

4. (2015 – VUNESP – CRO-SP – Programador)

O recurso EFS do sistema de arquivos NTFS oferece ao sistema

- A) controle das alterações feitas no disco por meio de journaling.
- B) criptografia em nível de sistema de arquivos.
- C) indexação de arquivos para agilizar buscas.
- D) mecanismos para compressão dos arquivos em disco.
- E) permissões de controle de acesso ao sistema operacional.

Comentários:



Basta lembrar do significado da sigla EFS = Encryption File System, ou seja, criptografia em nível de sistema de arquivos.

Gabarito: B

5. (2016 – Makiyama – Prefeitura de Salgueiro - PE – Auxiliar de Enfermagem)

O Active Directory (AD) do Windows

- A) somente pode ser utilizado no sistema de arquivos FAT32.
- B) pode ser utilizado no sistema de arquivos FAT32 ou ExFAT.
- C) somente pode ser utilizado no sistema de arquivos NTFS.
- D) pode ser utilizado no sistema de arquivos FAT32 ou NTFS.

Comentários:

O conceito de AD (Active Directory) surgiu com o Windows 2000 Server (utilizando NTFS como sistema de arquivos).

Gabarito: C

6. (2016 – CESPE – Polícia Científica - PE – Perito Criminal - Ciência da Computação)

Acerca dos sistemas de arquivos para Windows, assinale a opção correta.

- A) No NTFS podem ser utilizadas permissões e criptografia para se restringir o acesso a determinados arquivos e a usuários autorizados.
- B) Os sistemas de arquivos FAT e FAT32 têm a capacidade de recuperar erros de disco automaticamente.
- C) Os sistemas de arquivos disponíveis para Windows são FAT, NTFS e EXT2.
- D) No NTFS, o acesso tanto de leitura quanto de gravação é mais rápido que no FAT32.
- E) Utilizando-se o FAT32, é possível criar uma partição em disco com suporte de até 4 GB.

Comentários:

(A) O NTFS surgiu para suprir a falta de mecanismos de segurança e confiabilidade no FAT32, como *journaling*, permissões de acesso, criptografia, entre outros; (B) Diferentemente do NTFS, o sistema de arquivos FAT não utiliza nenhum mecanismo de recuperação, como o *journaling*; (C) EXT2 é utilizado no Linux; (D) Por possuir *journaling*, o NTFS é mais lento, porém mais confiável; (E) Na verdade, esse é o tamanho máximo de um arquivo em FAT32, pois $2^{32} = 4.294.967.296$ bytes (4GB).

Gabarito: A



7. (2018 - FUNDATEC - AL-RS - Analista Legislativo - Analista de Tecnologia da Informação e Comunicação)

Existe um sistema de arquivos em que, para todo o objeto armazenado, é realizado um registro na Master File Table (MFT). Trata-se do:

- A) Ext2.
- B) Ext3.
- C) Ext4.
- D) FAT32.
- E) NTFS.

Comentários:

Em relação à estrutura física, os *clusters* em partições NTFS são numerados sequencialmente desde o início da partição (setor 0) até a área destinada aos dados. **Para todos os objetos armazenados é realizado um registro através da MFT (*Master File Table*)**, que possui uma estrutura similar a uma base de dados. Note que no sistema de arquivos FAT nós tínhamos uma tabela de mesmo nome (FAT).

Gabarito: E

8. (2019 - CS-UFG - IF Goiano - Técnico de Tecnologia da Informação)

Em geral, sistemas operacionais oferecem suporte a um ou mais sistemas de arquivos que controlam a forma como os dados são identificados, gravados e recuperados a partir dos meios de armazenamento. As últimas versões Windows têm adotado um sistema de arquivos primário que é denominado de

- A) NTFS
- B) EXT4
- C) ReiserFS
- D) ZFS

Comentários:

Desde o Windows NT o sistema de arquivos padrão para a instalação do sistema operacional é o NTFS. Antes disso era o FAT32.

Gabarito: A



PROTOCOLO LDAP

Antes de entendermos o que é e para que serve o *Active Directory* (AD), é importante entendermos o protocolo que fornece mecanismos de acesso aos objetos do AD. O **LDAP** (*Lightweight Directory Access Protocol*) já deixa claro até no nome que é esse protocolo!

Entidades internacionais (ITU, ISO, IETF, entre outras) trabalham na definição de padrões diversos, incluindo a padronização que dá suporte a serviços de diretórios. Um padrão de uso genérico é o **X.500** (da ISO) que possui uma grande abrangência, mas é muito complexo e não foi adotado em sua íntegra como um padrão de mercado. Um padrão mais “light” que de fato se tornou um padrão de mercado foi o LDAP.

O padrão LDAP define um sistema de nomeação hierárquico, no qual é possível referenciar qualquer objeto que esteja no AD. Um nome LDAP é composto pelo caminho completo do objeto (ex.: uma impressora, um computador etc.), partindo do domínio raiz até chegar ao objeto em si. Algumas abreviaturas (**atributos**) são utilizadas nessa nomenclatura hierárquica:

- cn: *common name* (nome da conta de um usuário, grupo etc.);
- sn: sobrenome (*surname*);
- ou: faz referência a uma unidade organizacional;
- dc: componente de domínio (normalmente o nome do domínio);
- o: nome da organização (geralmente o domínio raiz);
- c: *country* - país (normalmente não utilizado).

Vamos a um exemplo de um nome LDAP:

CN=evandrodv, OU=professores, DC=ti, DC=estrategiaconcursos.com.br → esse nome representa o usuário “evandrodv”, cuja conta está contida na unidade organizacional “professores”, no domínio “ti.estrategiaconcursos.com.br”. Obs.: os dois componentes de domínio foram concatenados.

Por padrão um servidor LDAP “**escuta**” na porta 389 (TCP) e as principais características do protocolo são:

- Baseado em padrão aberto: qualquer desenvolvedor pode acessar sua especificação e realizar a implementação;
- Possui APIs bem definidas: facilita a vida dos programadores;
- Maior velocidade de consulta que um BD relacional;
- Replicável e distribuível;
- Facilita a localização de informações e recursos: pesquisa feita nome.

Um recurso é identificado pelo nome do servidor, separado do nome do recurso por uma contrabarra, como por exemplo:

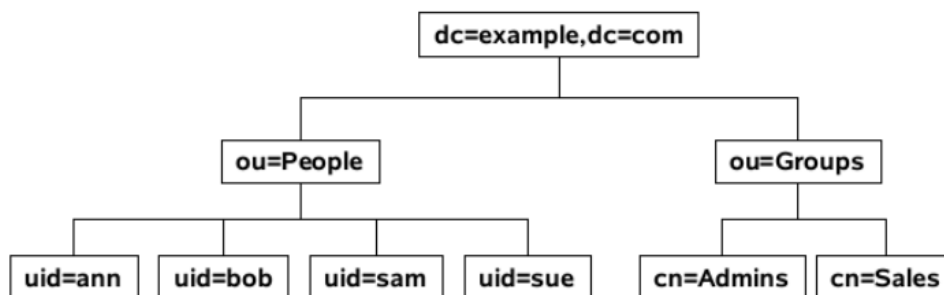
\\serv.estrategiaconcursos.com.br\curso01 → pasta compartilhada com o nome de compartilhamento “curso01” no servidor “serv” do domínio “estrategiaconcursos.com.br”. No lugar do nome DNS do servidor, poderia ser utilizado o endereço IP do servidor: \\192.168.1.5\curso01.



Algumas **operações (comandos)** que podem ser utilizados através do LDAP são:

- Bind: autentica e especifica a versão do protocolo LDAP;
- Search: procura/recupera entradas dos diretórios;
- Compare: compara uma entrada com determinado valor;
- Add: adiciona uma nova entrada;
- Delete: exclui uma entrada;
- Modify: modifica uma entrada;
- Modify DN: move ou renomeia uma entrada;
- Abandon: aborta uma requisição prévia;
- Unbind: fecha a conexão;
- Extended Operation: operação genérica para definir outras operações;
- StartTLS: protege a conexão com o TLS - implementada a partir da versão 3 do LDAP.

A representação dos dados é realizada através de uma estrutura hierárquica na forma de árvore (**Directory Information Tree - DIT**), a qual consiste em entradas de DNs (*Distinguished Names*). O LDAP utiliza a DIT como estrutura de dados fundamental:



Como podemos ver, a árvore de diretório possui uma forma hierárquica:

- Primeiro o diretório raiz;
- Após a rede corporativa, os departamentos e por fim os computadores dos usuários e os recursos de rede.

Alguns conceitos que também já foram cobrados em concursos são mostrados na sequência.

Schema: conjunto de objetos e atributos para o armazenamento. É modelado de acordo com o padrão X.500 da ISO.

Cada entrada (objeto) possui um identificador único (**dn - distinguished name**), o qual consiste de seu Relative Distinguished Name (RDN), construído de algum(ns) atributo(s) na entrada, seguido pelo DN da entrada pai.

Escalabilidade: é possível replicar servidores LDAP e incluir novos servidores à medida que aumenta a estrutura da organização. Ou seja, não é uma estrutura “engessada”.



QUESTÕES COMENTADAS

9. (2011 - FCC - 14ª Região)

Em relação ao LDAP, é INCORRETO afirmar:

- A) É derivado do sistema de diretórios X.500.
- B) É basicamente um sistema de diretórios que engloba o diretório em si e um protocolo denominado DAP.
- C) Normalmente um cliente conecta-se ao servidor LDAP, através da porta padrão 389 (TCP).
- D) A operação Compare tem como função testar se uma entrada tem determinado valor como atributo.
- E) Extended Operation é uma operação genérica para definir outras operações.

Comentários:

LDAP é o protocolo, não o diretório em si! O diretório é o *Active Directory*, se tivermos falando em Microsoft, por exemplo. Não chega a ser um problema se a banca colocar que o LDAP é um sistema de diretórios...mas o que mata a alternativa B é dizer que o protocolo é DAP, pois sabemos que é LDAP.

Gabarito: B

10.(2013 – IADES – EBSERH)

O LDAP (Lightweight Directory Access Protocol – Protocolo Leve de Acesso a Diretórios) é utilizado para acessar informações de diretórios, com base no X.500. Sobre o LDAP, julgue os itens a seguir.

- I - É um catálogo de informações que pode conter nomes, endereços, números de telefones, por exemplo.
- II - Permite localizar usuários e recursos em uma rede.
- III - O diretório é organizado hierarquicamente.
- IV - O LDAP é um sistema peer-to-peer.

A quantidade de itens certos é igual a

- A) 0.
- B) 1.
- C) 2.
- D) 3.
- E) 4.

Comentários:



(I) Através dos atributos (abreviaturas) é possível que o catálogo de informações contenha nome, sobrenome, telefone, entre outros. (II) É possível localizar usuários e recursos (impressoras, computadores etc.) através do comando *search*. (III) Existe um diretório raiz, após a rede corporativa, os departamentos e por fim os computadores dos usuários e os recursos de rede. (IV) É um sistema cliente/servidor! E a porta padrão no servidor é a 389 (TCP).

Gabarito: D



11.(2013 - FCC - TRT – 15ª Região)

Dentre as principais operações que podem ser efetuadas no protocolo LDAP, se encontram: Search: O servidor busca e devolve as entradas do diretório que obedecem ao critério da busca. Bind:

A) Essa operação serve para autenticar o cliente no servidor. Ela envia o DN (Distinguished Name), a senha do usuário e a versão do protocolo que está sendo usada.

B) Encerra uma sessão LDAP.

C) Adiciona uma nova entrada no diretório.

D) Renomeia uma entrada existente. O servidor recebe o DN (Distinguished Name) original da entrada, o novo RDN (Relative Distinguished Name), e se a entrada é movida para um local diferente na DIT (Directory Information Tree), o DN (Distinguished Name) do novo pai da entrada.

E) Apaga uma entrada existente. O servidor recebe o DN (Distinguished Name) da entrada a ser apagada do diretório.

Comentários:

Bind serve para autenticar! Unbind fecha (encerra) a conexão. Add adiciona uma nova entrada no diretório. Modify DN renomeia uma entrada existente. Delete serve para excluir uma entrada no diretório.

Gabarito: A

12.(2014 – IADES - TRE-PA)

O LDAP é um protocolo que funciona como serviço de diretório em redes TCP/IP. Sua porta padrão é a TCP/389 e a comunicação é feita a partir do cliente, que se liga ao servidor e envia requisições a este último. A respeito desse assunto, assinale a alternativa que apresenta a definição das operações básicas que um cliente pode solicitar a um servidor LDAP.

A) Search é usado para testar se uma entrada possui determinado valor.

B) Modify é a operação de adicionar uma entrada no servidor LDAP.

C) Unbind é a operação de fechamento da conexão entre cliente e servidor.

D) Start TLS é o comando para colocar no ar o servidor LDAP, no Linux.

E) Bind é um comando que busca ou recupera entradas no LDAP.

Comentários:

Compare é usado para testar se uma entrada possui determinado valor. Add é a operação de adicionar uma entrada no servidor LDAP. **Unbind serve para encerrar a conexão!** Start TLS protege a conexão com o TLS. Search é o comando que busca ou recupera entradas no LDAP.

Gabarito: C



13.(2014 - IADES - TRE-PA)

O LDAP é um serviço de diretório para redes padrão TCP/IP. Um uso comum desse serviço é a autenticação centralizada de usuários; nesse tipo de aplicação, o cliente inicia a comunicação, conectando-se ao servidor LDAP e enviando requisições, ao passo que o servidor responde com as informações contidas em sua base de dados. A respeito das operações que o cliente pode requisitar ao servidor LDAP, assinale a alternativa que corresponde a um pedido de conexão segura (criptografada), implementada a partir LDAPv3.

- A) Extend Operation.
- B) Init Security.
- C) StartTLS.
- D) Bind.
- E) Unbind.

Comentários:

StartTLS: protege a conexão com o TLS - implementada a partir da versão 3 do LDAP.

Gabarito: C

14.(2014 - FCC - SABESP)

Dentre os atributos comuns do protocolo LDAP está o atributo para armazenamento do sobrenome do usuário. A sigla utilizada para este atributo é

- A) co
- B) sn
- C) ln
- D) un
- E) ul

Comentários:

Alguns atributos:

- cn: *common name* (nome da conta de um usuário, grupo etc.);
- **sn: sobrenome (*surname*);**
- ou: faz referência a uma unidade organizacional;
- dc: componente de domínio (normalmente o nome do domínio);
- o: nome da organização (geralmente o domínio raiz);
- c: *country* - país (normalmente não utilizado).

Gabarito: B



15.(2016 - FCC - TRT-14ª Região)

Analista Judiciário - Tecnologia da Informação) – O LDAP define, dentre outras, a forma como um cliente de diretório pode acessar um servidor de diretório. O LDAP pode ser usado

- A) para enumerar objetos de diretório, mas não para localizá-los.
- B) para estabelecer uma conexão entre um cliente e um servidor LDAP, usando a porta padrão 485, via UDP.
- C) apenas em ambiente Windows, pois é um serviço de diretório proprietário.
- D) no Linux e configurado através do arquivo ldap-inf.xml, encontrado no diretório /etc.
- E) para consultar ou administrar o Active Directory.

Comentários:

(A) Pode localizar com a operação search. (B) A porta padrão é a 389 (TCP). (C) É um padrão aberto! Pode ser utilizado no Linux, Windows etc. (D) No Linux é configurado no arquivo ldap.conf no diretório /etc/openldap. (E) Pode ser utilizado no AD!

Gabarito: E

16.(2018 - FCC - DPE-AM)

Considere que o Técnico de Suporte deve criar uma nova entrada (conjunto de atributos) na estrutura de diretórios do servidor representada no formato LDIF do LDAP. O primeiro identificador da entrada deve ser

- A) cn.
- B) uid.
- C) sn.
- D) dc.
- E) dn.

Comentários:

Alguns atributos:

- cn: common name;
- sn: sobrenome (surname);
- dc: componente de domínio.

O primeiro identificador da entrada (“chave primária”) deve ser o dn (*distinguished name*).

Gabarito: E

17.(2018 - CESPE - ABIN)

Acerca de OAuth e LDAP (Lightweight Directory Access Protocol), julgue o item seguinte.



LDAP é um protocolo de diretórios que provê repositórios de informações de recursos de sistemas e serviços dentro de um ambiente centralizado e estritamente relacionado ao servidor. Por questão de limitação do padrão x.500, do qual foi originado, o LDAP não suporta funções de segurança e de acesso de cliente.

Comentários:

Vimos que tem, por exemplo, a operação StartTLS – a partir da versão 3 do LDAP, que protege a conexão com criptografia (através do protocolo TLS).

Gabarito: Errado

ACTIVE DIRECTORY (AD)

Antes de começar a falar sobre o *Active Directory* (AD) em si, é importante entendermos o que são os *workgroups* e o que são os diretórios (não são sinônimos de pastas).

Um *workgroup* (grupo de trabalho) é o cenário em que cada servidor é independente do outro, ou seja, não compartilham lista de usuários, grupos etc. É indicado para redes pequenas (até 10 usuários).

Imagine que uma empresa tenha três servidores (de arquivos, de e-mails e de um aplicativo empresarial - exemplo ao lado).

O usuário Ana pode acessar dois deles, podendo ter senhas diferentes para cada um, inclusive! Imagine a confusão que isso pode causar! Por isso *workgroup* é indicado para redes pequenas, senão seria um caos ter que cadastrar o mesmo usuário diversas vezes, um cadastro em cada servidor!



E o que é um **diretório**? É uma base de dados “única”. Os servidores possuem uma cópia da base (por isso coloquei única entre aspas), sendo que as alterações são replicadas entre os servidores. Isso permite redes de grandes proporções.

Para os mesmos usuários do exemplo anterior, podemos ver como ficaria com um diretório (ao lado). Veja que existe uma base única e todos os sete usuários estão nela.

Claro que visualmente temos essa impressão, mas na verdade os três servidores possuem cópias da mesma base e as atualizações são replicadas para que todos “enxerguem” os mesmos dados!



O diretório (*directory*) seria algo como um catálogo, mas geralmente se utiliza o termo “diretório” em português. Além dos usuários, são armazenados grupos, políticas de segurança, entre outros objetos.

Active Directory (AD): é o serviço de diretórios do Windows (a partir da versão 2000). Ele identifica todos os recursos disponíveis em uma rede, mantendo suas informações (contas de usuários, grupos, políticas de segurança etc.) em um banco de dados. Os recursos (impressoras, computadores etc.) ficam disponíveis para usuários e aplicações. Em relação ao sistema de arquivos, o AD deve ser utilizado com o NTFS.

Algumas funções do AD são:

- Replicações entre os controladores de domínio;
- Autenticação;
- Pesquisa de objetos na base de dados;
- Interface de programação para acesso aos objetos do diretório.

Domínio: agrupamento lógico de contas e recursos. Existem dois tipos de servidores:

- Controlador de Domínio (DC): realiza a autenticação de usuário (gera token), compartilham políticas de segurança. O token é utilizado para que o usuário não tenha que digitar a senha novamente;
- Servidor membro (*workgroup*): contas e grupos válidos somente no servidor (contas locais).

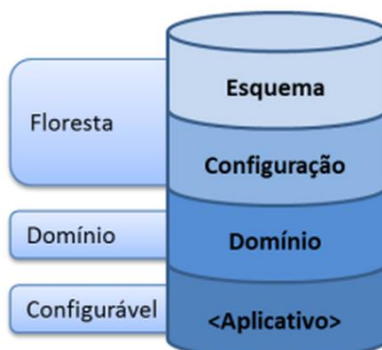
Para “transformar” um servidor membro em controlador de domínio (DC) e instalar o AD, existe o executável **DCPROMO.EXE** (**versões mais antigas**). No Windows Server 2012, o AD substitui tal ferramenta por um **Gerenciador do Servidor** e sistema de implantação baseado em Windows PowerShell.

Um domínio pode ser dividido em **OUs** (*Organizational Units* - Unidades Organizacionais). Isso possibilita a restrição de direitos administrativos em uma OU, independentemente dos demais objetos do domínio. Obs.: A utilização de OUs não é obrigatória!

As **partições** de um AD são:

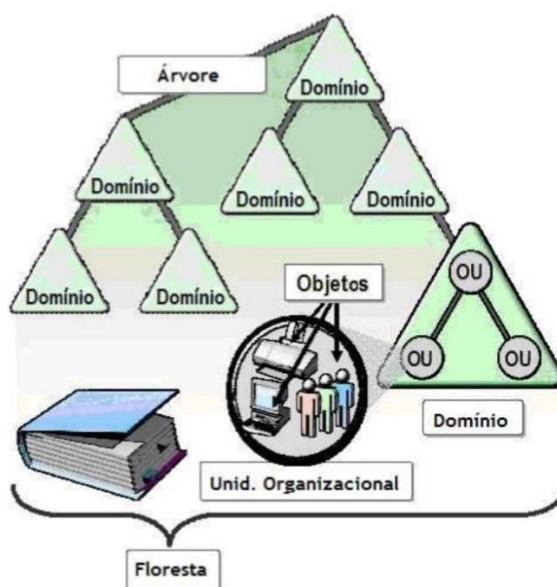


- Esquema: informações sobre classes e atributos de objetos;
- Configuração: informações da configuração dos domínios, criando uma instância da estrutura lógica do AD;
- Domínio: contatos, usuários, grupos, computadores e OUs.

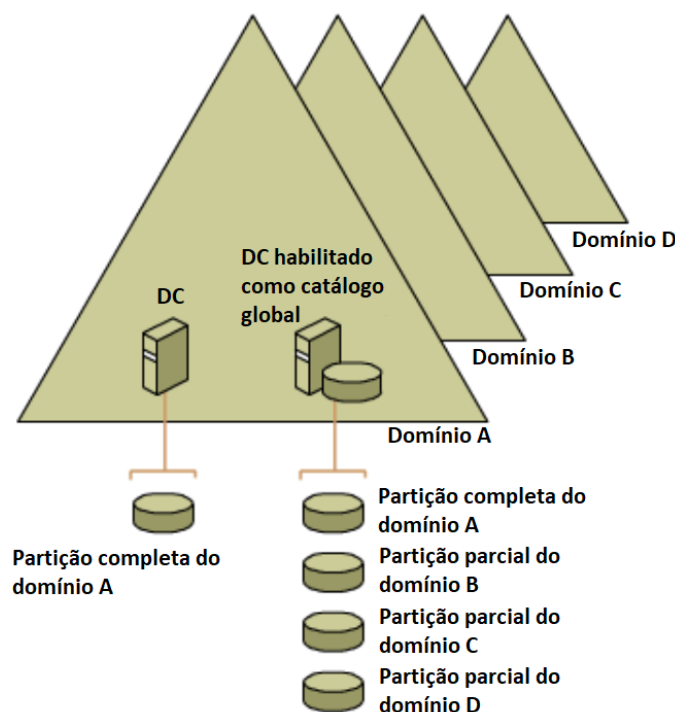


Árvores de Domínios: os recursos no AD são organizados de forma hierárquica, com o uso de domínios. Um usuário necessita estar cadastrado em apenas um domínio e pode receber permissões para acessar recursos em qualquer domínio. Para nomear os recursos o DNS (*Domain Name System*) é utilizado, sendo que ele deve estar instalado e bem configurado.

Floresta: é um conjunto de árvores. É comum em grupos de empresas, sendo que cada empresa do grupo mantém uma autonomia de identidade em relação às demais. A estrutura de uma floresta é utilizada para organizar as árvores com diferentes esquemas.



Catálogo Global: controlador de domínio (DC) que armazena uma cópia de todos os objetos do AD em uma floresta. Armazena uma cópia completa de todos os objetos no diretório para seu domínio e cópia parcial de todos os objetos para todos os outros domínios na floresta.



Quando há um único domínio é concedido acesso aos recursos para os usuários e grupos desse domínio. Quando há vários domínios ou florestas existem **relações de confiança**, o que permite que esses usuários e grupos tenham acesso a recursos em outros domínios ou florestas.

Existe a **transitividade** em uma relação de confiança. Por exemplo, se o domínio A confia no B e B confia no C, então A confia no C: $A \rightarrow B \rightarrow C$, então $A \rightarrow C$.

A relação de confiança **bidirecional** ocorre por padrão entre o domínio pai (A) e o filho (B), ou seja, $A \rightarrow B$ e $B \rightarrow A$. A relação de confiança **unidirecional** ocorre quando apenas A confia em B e B não confia em A: $A \rightarrow B$.

O **protocolo LDAP** (que já vimos em detalhes):

- É o padrão para o acesso e referência aos objetos do AD;
- Possibilita a criação de APIs (*Application Program Interfaces*), o que facilita a criação de aplicações integradas ao AD;
- Permite uma maior integração.

Alguns **serviços** do AD são:

- AD CS (*Certificate Services*): criação e gerenciamento de certificados de chaves públicas;
- AD DS (*Domain Services*): armazena informações sobre usuários, computadores, dispositivos etc.;
- AD FS (*Federation Services*): criação de identidade de acesso que opera através de múltiplas plataformas (Windows ou não);
- AD LDS (*Lightweight Directory Services*): provê praticamente a mesma funcionalidade do AD DS, mas não requer o desenvolvimento de domínios ou DCs (é mais “light”);
- AD RMS (*Rights Management Services*): serviços para habilitar a criação de soluções com proteção de informação.



Alguns **arquivos** do AD são:

- Ntds.dit: armazena no disco do servidor todos os dados (essa extensão DIT é de *Directory Information Tree*);
- Edb.chk: *checkpoint* utilizado para a recuperação (*recovery*) de um estado;
- Edb.log: arquivo de *log* de transações;
- Res1.log e Res2.log: arquivos de *log* reverso (usados quando não há espaço em disco);

Schema.ini: inicializa o Ntds.dit durante a promoção inicial do DC (servidor membro vira DC), depois de pronto não é mais utilizado.

QUESTÕES COMENTADAS

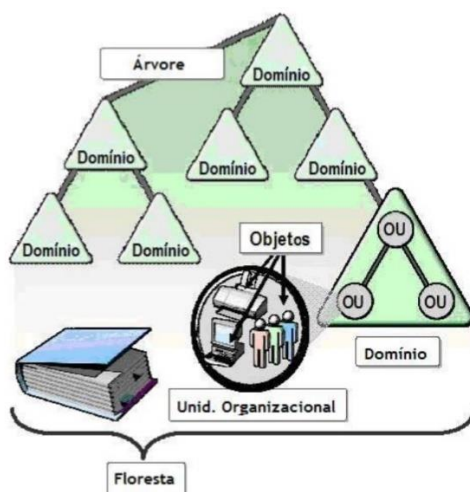
18.(2011 - CONSULPLAN – COFEN)

Qual dos componentes a seguir **NÃO** faz parte da estrutura lógica do Active Directory no Windows Server?

- A) Objects.
- B) Organizational Units.
- C) Domain Forests.
- D) Domains.
- E) Forests.

Comentários:

(A) Objetos são as contas de usuário, impressoras, computadores etc. (B) Unidades Organizacionais – OUs – são opcionais, ajudando a “organizar”). (C) **Florestas são de árvores e não de domínios!** (D) Domínios são agrupamentos lógicos de contas e recursos. (E) Florestas são conjuntos de árvores (o nome é intuitivo).



Gabarito: C



19.(2014 - UNIRIO - UNIRIO)

Active Directory está relacionado aos itens a seguir, EXCETO:

- A) Catálogo global.
- B) implementação de serviço de diretório no protocolo DHCP.
- C) Distribuição de Software Automática.
- D) Gerenciamento centralizado.
- E) Replicação automática.

Comentários:

O protocolo utilizado para o AD é o LDAP e não o DHCP! DHCP é aquele protocolo para distribuir endereços IP de forma dinâmica.

Gabarito: B

20.(2015 - CESPE - MEC)

Julgue o item que se segue, relativo a Active Directory, IIS e Terminal Service.

Um formato conhecido como um Active Directory com menos recursos é o AD LDS ou Active Directory Lightweight Directory Services.

Comentários:

Alguns serviços do AD são:

- AD CS (*Certificate Services*): criação e gerenciamento de certificados de chaves públicas;
- AD DS (*Domain Services*): armazena informações sobre usuários, computadores, dispositivos etc.;
- AD FS (*Federation Services*): criação de identidade de acesso que opera através de múltiplas plataformas (Windows ou não);
- **AD LDS (*Lightweight Directory Services*)**: provê praticamente a mesma funcionalidade do AD DS, mas não requer o desenvolvimento de domínios ou DCs (é mais “light”);
- AD RMS (*Rights Management Services*): serviços para habilitar a criação de soluções com proteção de informação.

Gabarito: Certo

21.(2016 - Makiyama - Prefeitura de Salgueiro/PE)

O Active Directory (AD) do Windows

- A) somente pode ser utilizado no sistema de arquivos FAT32.
- B) pode ser utilizado no sistema de arquivos FAT32 ou ExFAT.
- C) somente pode ser utilizado no sistema de arquivos NTFS.



D) pode ser utilizado no sistema de arquivos FAT32 ou NTFS.

Comentários:

Pense o seguinte: o AD surgiu no Windows 2000, quando já era utilizado o sistema de arquivos NTFS (a partir da versão XP). O NTFS possui atributos relacionados à segurança que o FAT não tem (proprietário do arquivo, por exemplo). Então, mesmo que você não se lembre da aula, pela lógica daria para acertar essa...TEM QUE UTILIZAR NTFS!

Gabarito: C

22.(2016 - FIOCRUZ - FIOCRUZ)

Em um servidor Windows 2008 utilizado apenas como servidor de arquivos será criado um ambiente com Active Directory Domain Services. Para iniciar o assistente de instalação do AD deve ser executado o comando:

- A) Promote.exe
- B) DCPromo.exe
- C) ADDS_Promo.exe
- D) DomainPromote.exe
- E) DCPromote.exe

Comentários:

Questão “decoreba”. Antes do Windows Server 2012 havia uma ferramenta que fazia a promoção de um servidor membro para DC (controlador de domínio). O nome do executável é DCPromo.exe (Promo de “promover” e DC de *domain controller*).

Gabarito: B

23.(2017 - UFMT - UFSBA - Analista de Tecnologia da Informação)

2017 - FCC - TRF-5ª Região

O Active Directory – AD

- A) tem um banco de dados denominado NTDS.dit e está localizado na pasta %SystemAD%\NTDS\ntds.dit em uma instalação default do AD. O diretório NTDS existirá em todos os servidores, independentemente de terem a função de Domain Controllers.
- B) ao ser instalado, cria 5 arquivos: 1) Ntds.dit, banco de dados do AD; 2) Edb.log, armazena todas as transações feitas no AD; 3) Edb.chk, controla transações no arquivo Edb.log já foram committed em Ntds.dit; 4) Res1.log, arquivo de reserva; 5) Res2.log, arquivo de reserva.
- C) pode ter um ou mais servidores com a função de Domain Controller – DC. Em um AD com três DCs, por exemplo, somente o DC-raiz é atualizado com todos os dados do AD. Esta operação recebe o nome de replicação do Active Directory.



D) pode ter Operational Units – OUs. As OUs podem ser classificadas de 3 formas diferentes: 1) Geográfica, as OUs representam Estados ou Cidades; 2) Setorial, as OUs representam setores ou unidades de negócio da estrutura da empresa; 3) Departamental, as OUs representam departamentos da empresa.

E) pode ter um ou dois domínios. O 2º domínio é denominado domínio-filho. O conjunto domínio-pai com seu domínio-filho é chamado de floresta, pois o domínio-filho pode ter vários ramos chamados de subdomínios.

Comentários:

Alguns arquivos do AD são:

- Ntds.dit: armazena no disco do servidor todos os dados (essa extensão DIT é de *Directory Information Tree*);
- Edb.chk: *checkpoint* utilizado para a recuperação (*recovery*) de um estado;
- Edb.log: arquivo de *log* de transações;
- Res1.log e Res2.log: arquivos de *log* reverso (usados quando não há espaço em disco);
- Schema.ini: inicializa o Ntds.dit durante a promoção inicial do DC (servidor membro vira DC), depois de pronto não é mais utilizado.

Gabarito: B

24.(2017 - IADES - Fundação Hemocentro de Brasília/DF)

O Active Directory (AD) é o

A) repositório de informações referentes a objetos da rede e também ao serviço que permite que essas informações sejam utilizadas.

B) mecanismo que permite aos usuários o acesso a recursos de outros domínios.

C) conjunto de arquivos que armazena informações de usuários, grupos e recursos.

D) mecanismo responsável pela cópia de todas as informações entre os controladores de domínio da floresta.

E) conjunto de uma ou mais árvores.

Comentários:

AD é o serviço de diretórios da Microsoft, onde são armazenados e gerenciados objetos (computadores, usuários, grupos etc.) e o LDAP é o protocolo utilizado para buscar e manipular tais informações.

Gabarito: A



25.(2018 - COMPERVE - UFRN)

O Active Directory (AD) é composto por diversos serviços, tais como, Active Directory Certificate Services (AD CS), Active Directory Domain Services (AD DS), Active Directory Federation Services (AD FS), Active Directory Lightweight Directory Services (AD LDS), e Active Directory Rights Management Services (AD RMS). O serviço que armazena os dados de diretório e gerencia a comunicação entre usuários e domínios, incluindo processos de logon de usuário, autenticação e pesquisas de diretório é o

- A) Active Directory Domain Services (AD DS).
- B) Active Directory Rights Management Services (AD RMS).
- C) Active Directory Certificate Services (AD CS).
- D) Active Directory Certificate Functions (AD CF).

Comentários:

O AD DS é o que na prática a maioria chama apenas de AD, ou seja, é o serviço que armazena os dados de diretório e gerencia a comunicação entre usuários e domínios, incluindo processos de logon de usuário, autenticação e pesquisas de diretório.

Gabarito: A

26.(2018 - UFLA - UFLA)

O Active Directory (AD) é um serviço de diretório nas redes Windows. Assinale a alternativa CORRETA:

- A) Quando um Administrador realiza alterações em um controlador de domínio (DC), é gerado um pacote chamado de Global Catalog (GC).
- B) A partição Schema contém informações sobre a estrutura do AD incluindo quais domínios, sites, controladores de domínio e cada serviço existente na floresta.
- C) Quando um Administrador realiza alterações em um controlador de domínio (DC), o servidor precisa atualizar a sua base do AD com os outros controladores de domínio da rede.
- D) A partição Configuração contém a definição dos objetos e atributos que são criados no diretório e as regras para criá-los e manipulá-los.

Comentários:

Quando um Administrador realiza alterações em um DC, o servidor precisa atualizar a sua base do AD com os outros DCs, o que é chamado de **replicação**. Assim há a impressão que há apenas uma base centralizada.

Gabarito: C



27.(2018 - FAURGS - TJ-RS)

No Active Directory (AD), o conjunto lógico composto por objetos ou recursos como computadores, usuários e grupos de objetos definidos administrativamente, e que compartilham a mesma base de dados, é denominado

- A) domínio.
- B) árvore.
- C) floresta.
- D) organizational units (OU).
- E) schema.

Comentários:

Domínio: agrupamento lógico de contas e recursos. Existem dois tipos de servidores:

- Controlador de Domínio (DC): realiza a autenticação de usuário (gera token), compartilham políticas de segurança. O token é utilizado para que o usuário não tenha que digitar a senha novamente;
- Servidor membro (*workgroup*): contas e grupos válidos somente no servidor (contas locais).

Gabarito: A

28.(2018 - Quadrix - CRM-PR)

Julgue o item a seguir, relativo a serviços de diretórios.

O serviço de diretórios AD (Active Directory) foi criado com a finalidade de armazenar diversas senhas de um usuário para diferentes sistemas.

Comentários:

Diversas senhas podem ser usadas em um *workgroup*, ex.: usuário “Maria” com senha “123456” no servidor 1 e outro cadastro de “Maria” com senha “654321” no servidor 2! O AD surgiu justamente para facilitar a vida dos administradores, com uma base única para todos os servidores que pertencem ao domínio como DC (*domain controller*).

Gabarito: Errado

29.(2018 - FGV - AL-RO)

O principal arquivo do Microsoft Active Directory que tem por função servir como base de dados para armazenar as informações sobre objetos de usuários, grupos e associação de grupos, é denominado

- A) Ntds.dit
- B) Edb.chk



- C) Edb.log.
- D) Res1.log.
- E) Schema.db.

Comentários:

Schema.ini existe! Schema.db não! Alguns arquivos do AD são:

- Ntds.dit: armazena no disco do servidor todos os dados (essa extensão DIT é de *Directory Information Tree*);
- Edb.chk: *checkpoint* utilizado para a recuperação (*recovery*) de um estado;
- Edb.log: arquivo de *log* de transações;
- Res1.log e Res2.log: arquivos de *log* reverso (usados quando não há espaço em disco);
- Schema.ini: inicializa o Ntds.dit durante a promoção inicial do DC (servidor membro vira DC), depois de pronto não é mais utilizado.

Gabarito: A

30.(2018 - CESPE - FUB)

Julgue o item seguinte, a respeito dos sistemas operacionais Windows e Linux.

No que se refere ao ambiente Windows, desde o Windows 2000, os nomes de domínio do Active Directory são, geralmente, os nomes DNS (domain name service) completos dos domínios.

Comentários:

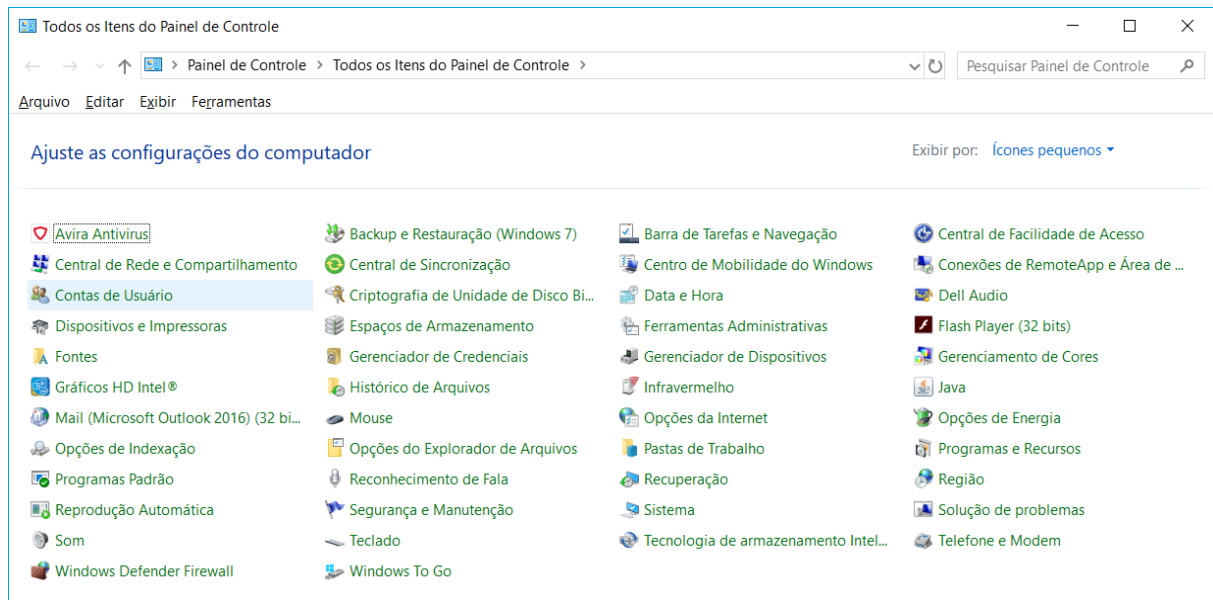
O DNS geralmente é utilizado para nomear e resolver os nomes dos domínios. Por isso o DNS deve estar instalado e bem configurado.

Gabarito: Certo

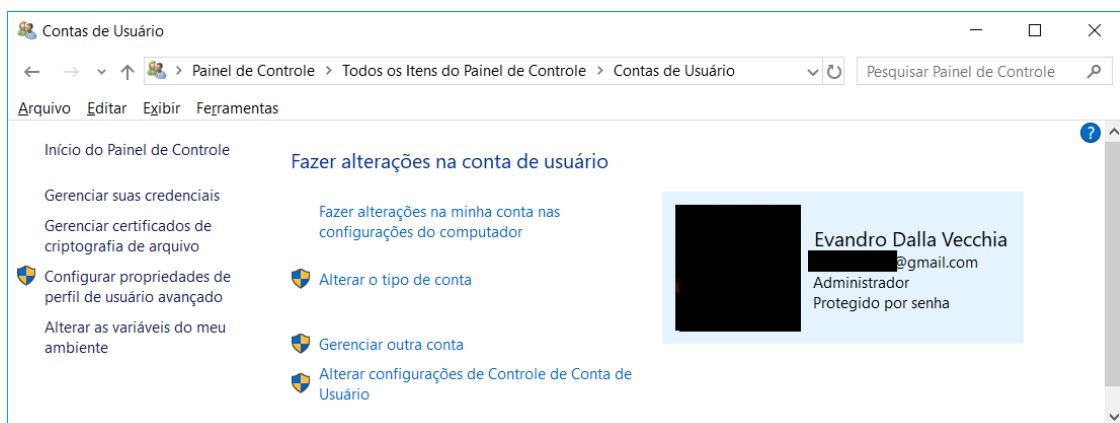


ADMINISTRAÇÃO DE USUÁRIOS, GRUPOS, PERMISSÕES, CONTROLES DE ACESSO

Muitas tarefas de administração se encontram no Painel de Controle, como é o caso das contas de usuário:



Ao clicar em Contas do Usuário, podemos ver algumas opções:

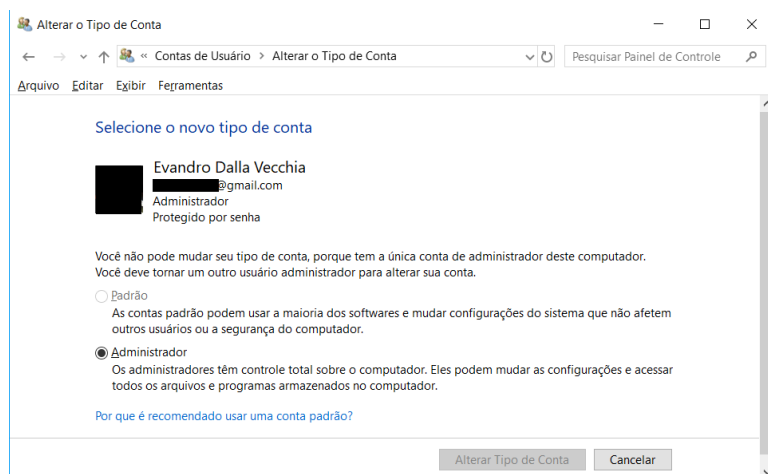


Na figura verificamos que só há um usuário com nome “Evandro Dalla Vecchia”, há um e-mail associado a ele, mostra que é uma conta do tipo Administrador e que é protegida por senha.

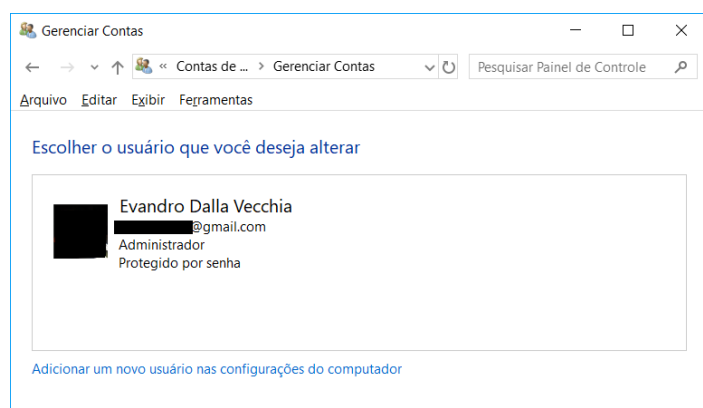


Ao clicar em “Alterar o tipo da conta” é possível escolher entre uma conta padrão ou Administrador.

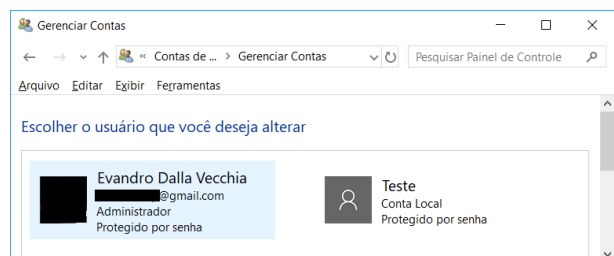
Note que no caso apresentado só há uma conta, então o sistema não permite que ela seja trocada para o tipo padrão, afinal o computador deve ter pelo menos uma conta de Administrador!



Ao clicar em “Gerenciar outra conta” é mostrada uma nova tela (mostrada ao lado). Há a opção “Adicionar um novo usuário nas configurações do computador”, a qual dá a opção de criar um novo usuário “membro da família” (cadastro na nuvem Microsoft) ou “adicionar outra pessoa a este PC”. O usuário a ser criado pode ser com ou sem conta Microsoft.



Para demonstrar, criei um usuário padrão “Teste” em uma conta local (sem conta Microsoft – note que não há e-mail associado) e digitei uma senha (tela ao lado).



Podemos verificar, então, alguns tipos de conta no Windows:

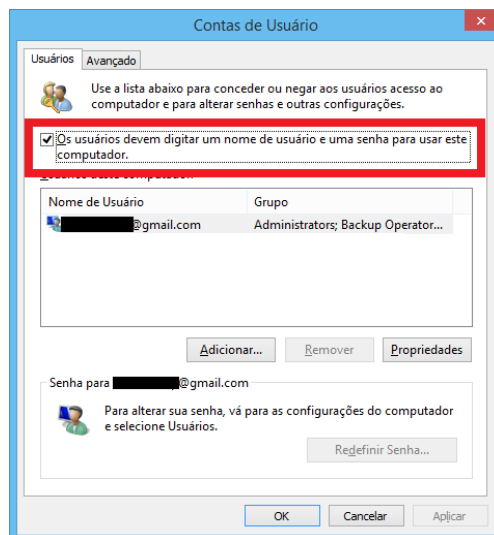
- Padrão: são aquelas utilizadas no dia a dia, não possuindo privilégios avançados (o que evita a instalação de um software malicioso por algum usuário com menos conhecimento, por exemplo);
- Administrador: contas que oferecem mais controle sobre um computador e só devem ser utilizadas quando necessário, como por exemplo alguns tipos de configuração avançada;
- Convidado: como o próprio nome sugere, são contas destinadas principalmente às pessoas que precisam usar temporariamente um computador.

E se segurança não for um aspecto importante e o usuário deseje entrar no sistema operacional sem digitar qualquer usuário e senha? O Windows permite isso, da seguinte forma:

- Na barra de pesquisa (ao lado do botão de Iniciar), digitar “netplwiz” e pressionar ENTER;
- Deve haver autorização com a senha de administrador;

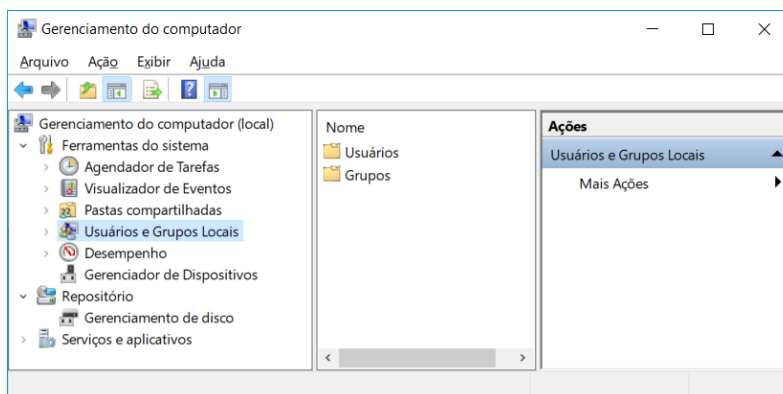


- Desmarcar a opção “Os usuários deve digitar um nome de usuário e uma senha para usar este computador” e autorizar a operação com a senha da conta Microsoft:



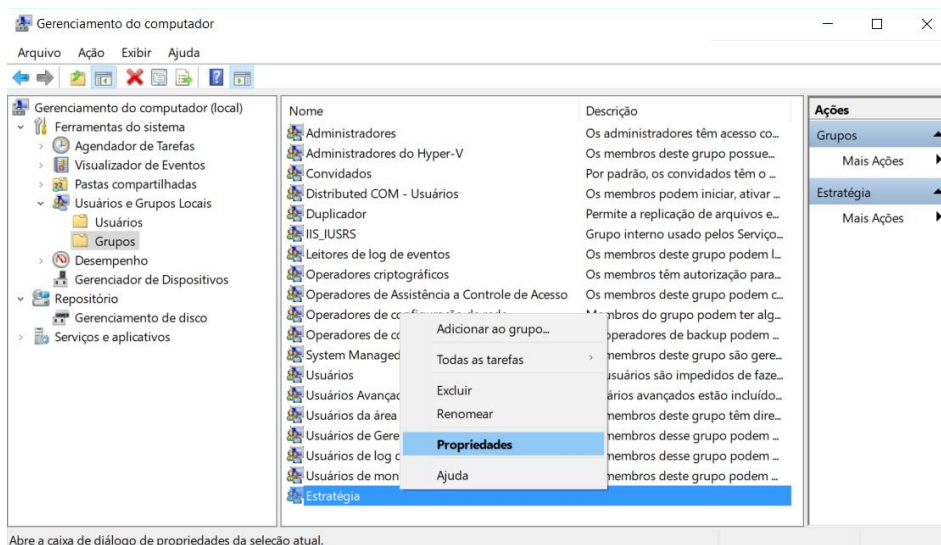
Importante: se for utilizado um certificado digital em uma credencial de usuário, deve haver o salvamento desse certificado no repositório pessoal do usuário.

Agora imagine que você tenha que adicionar 10 usuários, sendo que 5 deles devem possuir as mesmas permissões e os outros 5 devem possuir outras permissões. Nesse caso, o ideal é **criar grupos e definir as permissões por grupo**. Em “Gerenciamento do Computador” (pode buscar pelo menu Iniciar mesmo) é possível criar grupos, associar os usuários que devem pertencer a esse grupo e definir as permissões:



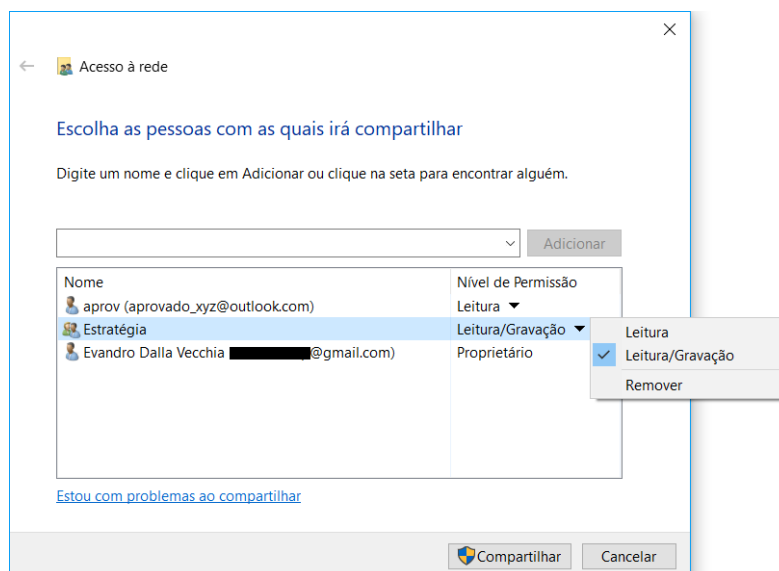
Continuando com o exemplo, criei um grupo “Estratégia”, sem adicionar ninguém e sem realizar qualquer tipo de configuração (tela abaixo). Depois é só clicar com o botão direito do mouse e clicar em propriedades, depois você pode adicionar os membros (usuários) que quiser. Eu adicionei o Evandro e o Teste.





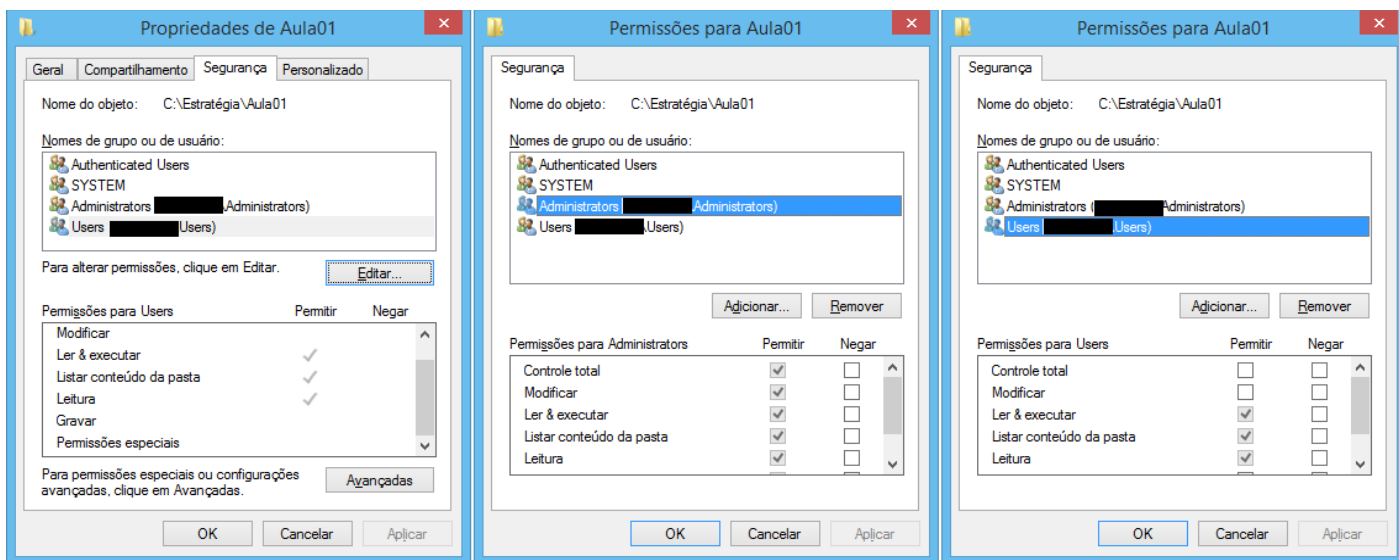
Ok, e como podemos definir quem pode ler, gravar, executar em um arquivo ou em uma pasta? Temos que definir as **permissões de acesso para um usuário ou um grupo**. Para isso, criei um novo usuário, desta vez vinculado a uma conta Microsoft aprovado_xyz@outlook.com (esse usuário não pertence ao grupo Estratégia).

Em um arquivo ou pasta basta clicar o botão direito do mouse, clicar em “Propriedades”, “Compartilhamento”, “Compartilhar...”. Agora é só digitar os usuários ou grupos e para cada um definir se pode ler, ler/escrever, ou remover o usuário ou grupo da lista. A tela abaixo mostra o compartilhamento de uma pasta. Ao grupo Estratégia foi dada permissão para ler e escrever. Para o usuário “aprov” foi dada permissão apenas para ler, e o usuário Evandro é o proprietário. Note que o ícone do Estratégia é diferente, pois é um grupo.



Além disso, é possível escolher um arquivo ou pasta específica e definir as permissões. Para isso é só clicar com o botão direito do mouse, “Propriedades”, “Segurança”, “Editar”:





Na sequência mostrada acima podemos ver que o padrão para os administradores é “Controle total”, enquanto para os usuários padrão a modificação não está habilitada. Claro que, sendo o dono do arquivo/pasta ou sendo um administrador, você pode alterar do jeito que quiser! Uma tabela completa do que pode ou ser feito de acordo com as permissões é mostrada abaixo.

Permissão para	Controle total	Modificar	Ler & executar	Listar conteúdo da pasta	Leitura	Gravar
Abrir pasta/ executar arquivo	x	x	x	x		
Listar pasta/ ler dados	x	x	x	x	x	
Ler atributos	x	x	x	x	x	
Ler atributos estendidos	x	x	x	x	x	
Criar arquivos/ escrever dados	x	x				x
Criar pastas/ anexar dados	x	x				x
Escrever atributos	x	x				x
Escrever atrib. estendidos	x	x				x
Excluir subpastas e arq.	x					
Excluir	x	x				



Ler permissões	x	x	x	x	x	x
Alterar permissões	x					
Tomar a propriedade	x					
Sincronizar	x	x	x	x	x	x

Sei que seria um desperdício de tempo decorar essa tabela, mas vale a pena dar uma olhada e tentar ver a lógica envolvida, para garantir a segurança de acesso/manipulação de arquivos e pastas pelos usuários do sistema.

QUESTÕES COMENTADAS

31.(2014 - IADES - CONAB)

No gerenciamento de contas de usuários do sistema operacional Windows 7, cada conta de usuário é representada por quatro elementos: um ícone, o nome da conta, o perfil do usuário e se ela é protegida por senha. Acerca das contas de usuário do Windows, assinale a alternativa correta.

- A) O ícone é uma figura-padrão e não pode ser alterado.
- B) O nome da conta, ao ser alterado, pode apresentar nomes iguais, desde que tenham perfis diferentes.
- C) O tipo de conta administrador dá poderes para o usuário criar nova conta, inclusive com perfil administrador.
- D) Recomenda-se que a senha seja igual ao nome da conta, na sua criação, para facilitar a memorização e forçar a substituição.
- E) Todo computador deve ter pelo menos um perfil visitante.

Comentários:

Sugiro que você faça os testes em seu computador...

(A) Claro que pode alterar, pode colocar qualquer figura! (B) Cada usuário cadastrado recebe um perfil, com um identificador único. Então pode haver dois usuários com o mesmo nome, sem problemas. (C) Uma conta com perfil de administrador pode tudo, inclusive criar outra conta com perfil de administrador! (D) Pelo contrário! Isso facilita que pessoas mal-intencionadas acesse sua conta! (E) Não há essa obrigação! Não precisa ter o perfil de visitante.

Gabarito: C



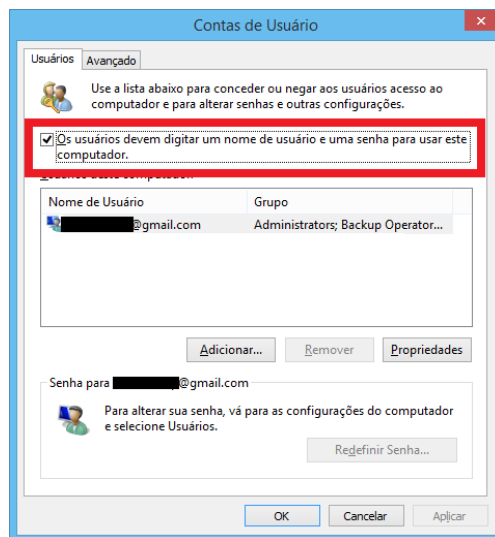
32.(2016 - CESPE - Polícia Científica-PE)

O gerenciamento de usuários no Windows

- A) impossibilita a criação de um grupo de usuários.
- B) permite alterar o nome da conta, alterar a imagem e configurar o controle dos pais, entre outras opções de modificação em uma conta de usuário.
- C) dispensa, no uso de um certificado digital em uma credencial de usuário, o salvamento desse certificado no repositório pessoal do usuário.
- D) impede o usuário de efetuar login sem uma conta de usuário
- E) exige a reinstalação do sistema operacional caso algum usuário do computador esqueça sua senha.

Comentários:

(A) Vimos que é possível criar um grupo (no exemplo usamos o nome Estratégia). **(B) Perfeito! Não comentamos na aula, mas é possível ter um controle dos pais sobre seus filhos.** (C) Não dispensa, não! Se o usuário tiver um certificado digital associado, esse certificado deve estar salvo no repositório de certificados do usuário. (D) É possível desabilitar o uso de senha para fazer o *login* (tela abaixo). (E) O administrador pode trocar a senha do usuário esquecido, portanto não é necessário reinstalar o Windows.



Gabarito: B

33.(2017 - FCC - TRF-5ª Região)

Um Técnico em Informática estava usando um computador com o sistema operacional Windows 7 em português e, através de um caminho via Painel de Controle, clicou em “O que é uma conta de usuário?”. O sistema exibiu uma janela com a seguinte informação:

Uma conta de usuário é uma coleção de dados que informa ao Windows quais arquivos e pastas você pode acessar, quais alterações pode fazer no computador e quais são suas preferências



pessoais, como plano de fundo da área de trabalho ou proteção de tela. As contas de usuário permitem que você compartilhe um computador com várias pessoas, enquanto mantém seus próprios arquivos e configurações. Cada pessoa acessa a sua conta com um nome de usuário e uma senha. Há três tipos de contas, cada tipo oferece ao usuário um nível diferente de controle do computador:

A) As contas Padrão são para o dia-a-dia; as contas Administrador oferecem mais controle sobre um computador e só devem ser usadas quando necessário; as contas Convidado destinam-se principalmente às pessoas que precisam usar temporariamente um computador.

B) As contas de Usuário são as que não necessitam de senha; as contas de Administrador exigem senha e são usadas para o controle do computador; as contas de Pais são usadas para ajudar a gerenciar o modo como as crianças usam o computador.

C) As contas Credenciais Genéricas são para usuários comuns; as contas Credenciais Administrador oferecem controle sobre o computador; as contas Credenciais do Windows com Certificado destinam-se a usuários que possuam um certificado digital.

D) As contas de Grupo Local são para usuários padrão; as contas de Grupo Administrativo oferecem controle sobre o computador, exigindo uma senha de administrador; as contas de Grupo Doméstico aceitam usuários padrão e administradores e permitem a criação de contas de usuários convidados.

E) As contas Usuário são as de usuários padrão e não necessitam de senha; as contas Administrador exigem senha e são usadas para o controle do computador; as contas Segurança Familiar são usadas para ajudar a gerenciar o modo como as crianças usam o computador.

Comentários:

As contas Padrão são para o dia-a-dia, pois não possuem privilégios avançados; as contas Administrador oferecem mais controle sobre um computador e só devem ser usadas quando necessário, evitando que pessoas com pouco conhecimento executem algum tipo de malware, por exemplo; as contas Convidado destinam-se principalmente às pessoas que precisam usar temporariamente um computador (o nome é bem sugestivo).

Gabarito: A

34.(2017 - CESPE - TRE-BA)

No Windows 7, o usuário estará apto a excluir subpastas e arquivos caso tenha a permissão de acesso especial de NTFS

I Modificar.

II Leitura.

III Ler & Executar.

IV Gravação.

V Controle Total.

Assinale a opção correta.



- A) Apenas os itens I, III e V estão certos.
- B) Apenas os itens II, III e IV estão certos.
- C) Apenas os itens I e IV estão certos.
- D) Apenas o item III está certo.
- E) Apenas o item V está certo.

Comentários:

Lembra daquela tabela?

Permissão para	Controle total	Modificar	Ler & executar	Listar conteúdo da pasta	Leitura	Gravar
Excluir subpastas e arq.	x					

Gabarito: E

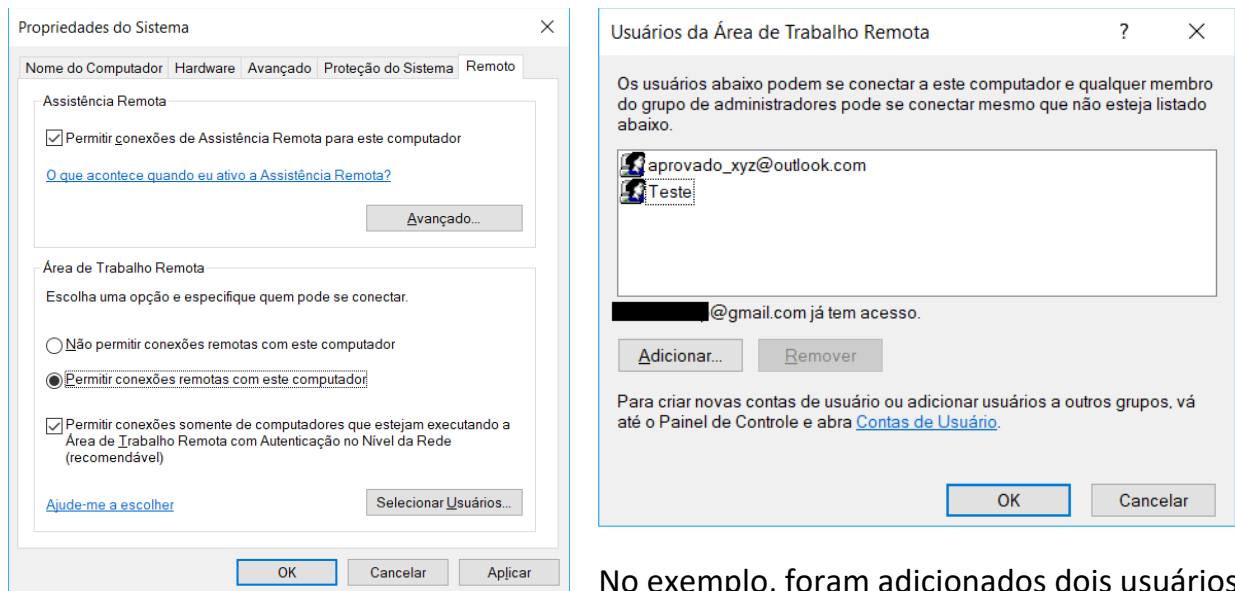
NOÇÕES DE REMOTE DESKTOP E VDI

Um recurso fundamental para os administradores de rede é o **Remote Desktop**, principalmente em redes grandes nas quais fica complicado se deslocar a cada computador para resolver algum problema. Com esse recurso é possível acessar remotamente as estações de trabalho e servidores e realizar as atividades necessárias.

É altamente recomendável que o Remote Desktop seja habilitado em todos os servidores, principalmente nos casos em que os servidores se encontram em salas separadas ou em outras localidades da empresa. Para ativar o Remote Desktop basta seguir esse caminho:

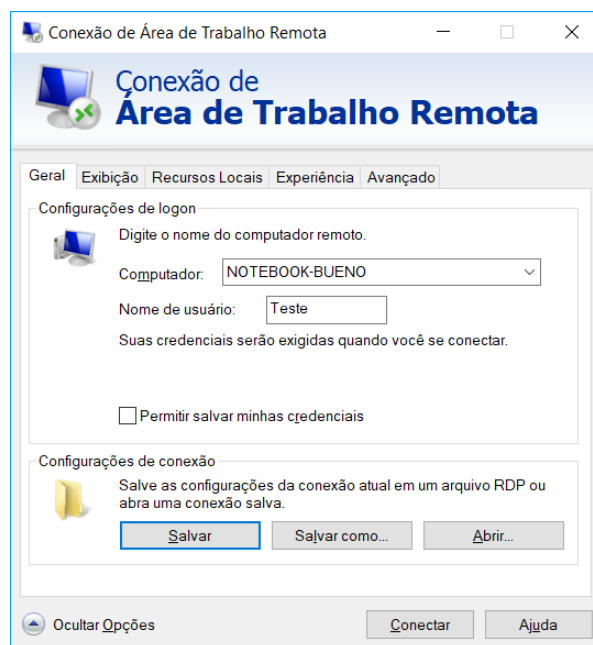
Painel de Controle → Sistema → Configurações Remotas → Permitir conexões remotas com este computador → Selecionar usuários:





No exemplo, foram adicionados dois usuários.

Bom, a parte do servidor está ok, mas e a parte do cliente? Aí entra o **RDC (Remote Desktop Connection)**, que pode ser chamado com o comando **mstsc** (comando com nome complicado, mas é a abreviatura de MS Terminal Services) ou através de navegação no menu Iniciar → Todos os Programas → Acessórios → Conexão de Área de Trabalho Remota:

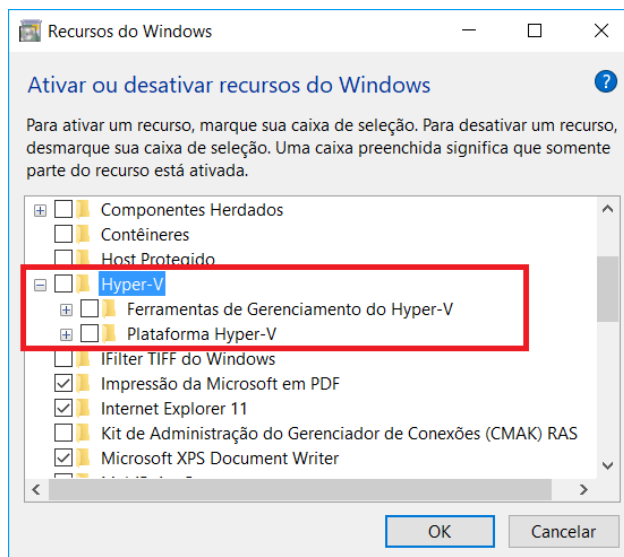


Agora vamos falar um pouco de **virtualização**. Uma sigla comumente utilizada é a **VDI (Virtual Desktop Infrastructure)**, que é uma tecnologia para prover e gerenciar *desktops* virtuais. Os *desktops* virtualizados são criados por uma máquina virtual (VM) controlada por um *hypervisor*.

Hypervisor é uma camada de software entre o hardware e o sistema operacional, sendo responsável por fornecer ao sistema operacional visitante a abstração da máquina virtual. É quem controla o acesso dos sistemas operacionais visitantes aos dispositivos de hardware.



O recurso padrão de *hypervisor* no Windows é o **Hyper-V**, que pode ser ativado através do caminho Painel de Controle → Programas e Recursos → Ativar ou desativar recursos do Windows:



QUESTÕES COMENTADAS

35.(2010 - CESPE - SERPRO)

Uma das formas de se obter acesso remoto ao Windows Server 2003, a partir de outra máquina com o Internet Explorer, é por meio da instalação do pacote Remote Desktop Web Connection ActiveX para hospedagem de terminal services, cuja limitação principal é não funcionar no IIS.

Comentários:

Na verdade, basta habilitar o Remote Desktop ou o Terminal Services. Ambos são modos de acesso remoto (vimos o Remote Desktop, que é mais simples) e necessitam que o serviço Terminal Services esteja instalado.

Gabarito: Errado

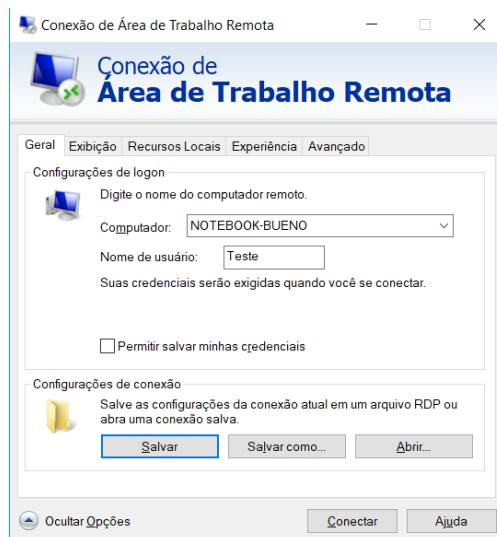
36.(2011 - CESPE - MEC)

O Remote Desktop Connection é o servidor padrão para o terminal services no Windows 2003.

Comentários:

O **RDC (Remote Desktop Connection)** é o **cliente**! Pode ser chamado com o comando **mstsc** (comando com nome complicado, mas é a abreviatura de MS Terminal Services) ou através de navegação no menu Iniciar → Todos os Programas → Acessórios → Conexão de Área de Trabalho Remota:





Gabarito: Errado

37.(2013 - FCC - MPE-SE)

No Windows Server 2008, a Memória Dinâmica permite o uso mais eficiente de memória enquanto mantém a consistência de desempenho e escalabilidade das cargas de trabalho. Implementar a Memória Dinâmica significa que níveis mais altos de consolidação de servidores podem ser obtidos com mínimo impacto sobre o desempenho. A Memória Dinâmica também significa que pode haver um número maior de desktops virtuais por host Hyper-V em cenários de

- A) múltiplos acessos simultâneos (Windows DataShare).
- B) servidores remotos RemoteFX.
- C) servidores cluster (ClusterMode).
- D) recuperação de erros (ServerRecover).
- E) VDI - Virtual Desktop Infrastructure.

Comentários:

O foco da questão é saber a que o Hyper-V está associado. Sabemos que se trata de um *hypervisor* do Windows, ou seja, uma camada de software entre o hardware e o sistema operacional, responsável por fornecer ao sistema operacional visitante a abstração da máquina virtual. Mesmo quem não conhecesse a sigla VDI, ao ler as alternativas poderia ver que apenas a alternativa E possui “virtualização” no nome. Resumindo: o *hypervisor* Hyper-V provê a estrutura necessária para fornecer uma infraestrutura de máquinas virtuais (ou *desktops* virtuais) - VDI.

Gabarito: E

38.(2014 - FCC - AL-PE)

O Windows Server 2008 R2 oferece os tipos I e II de virtualização.



- A) I -DirectAccess. II -De computadores clientes quando usado em conjunto com a VDI (Virtual Desktop Infrastructure))
- B) I - Power Shell 2.0. II- DirectAccess
- C) I - De servidores através do Hyper-V. II - De computadores clientes quando usado em conjunto com a VDI (Virtual Desktop Infrastructure)
- D) I - De servidores quando usado em conjunto com a VDI (Virtual Desktop Infrastructure) II - De computadores clientes através do Hyper-V
- E) I - De servidores através do Hyper-V. II - BranchCache

Comentários:

Dependendo a banca, pode ser dito que o Hyper-V fornece uma infraestrutura para máquinas virtuais (de uma forma geral), ou pode definir que o Hyper-V fornece tal infraestrutura para os servidores virtuais, enquanto *desktops* virtuais seriam utilizados com a VDI. No caso da FCC, fica clara essa divisão entre servidores virtuais e *desktops* virtuais.

Gabarito: C

39.(2014 - FGV - PROCEMPA)

Relacione alguns dos recursos que podem ser utilizados no Windows Server 2012 com suas respectivas funções.

1. AppLocker
 2. Windows PowerShell
 3. Hyper-V
 4. Remote Desktop Services
- () Sistema de virtualização para arquiteturas x86/x86_64.
- () Acesso a sessões em computadores físicos ou virtuais a partir de estações de trabalho, via rede corporativa ou Internet.
- () Implementador de políticas de controle de execução de programas.
- () Ambiente para administração do sistema por linha de comando.
- A) 3 – 4 – 1 – 2
- B) 2 – 3 – 1 – 4
- C) 4 – 3 – 1 – 2
- D) 3 – 4 – 2 – 1
- E) 4 – 3 – 2 – 1

Comentários:



Como nesta aula só vimos o Remote Desktop, vamos começar por ele e mesmo quem não saiba o restante vamos ver como daria para resolver:

Remote Desktop: O próprio nome já sugere qual a sua funcionalidade: o acesso a sessões em computadores, que podem ser físicos ou virtuais, a partir de estações de trabalho, via rede.

O PowerShell podemos simplificar como uma linha de comando mais poderosa.

O Hyper-V é o *hypervisor* padrão no Windows, utilizado para virtualização.

Talvez o menos conhecido seja o AppLocker, mas pelo nome “App” (aplicativo) e “Locker” (algo como trava ou coisa parecida) dá para deduzir que o que “sobrou” está correto: Implementador de políticas de controle de execução de programas.

Gabarito: A

40.(2016 - FCC - TRF-3ª Região)

Ao estudar a preparação da infraestrutura de virtualização a ser utilizada no ambiente Windows Server 2008 R2, um Técnico Judiciário de TI do Tribunal observou que o Hyper-V é usado para a virtualização do computador cliente quando usado em conjunto com a tecnologia

A) Virtual DNS Infrastructure - DNSSEC.

B) Basic Desktop Node - BDN.

C) Client Desktop Infrastructure - CDI.

D) Virtual Basic Client System - VBCS.

E) Virtual Desktop Infrastructure - VDI.

Comentários:

Novamente a FCC deixando claro que o Hyper-V virtualiza servidores, e em conjunto com a VDI virtualiza clientes (*desktops*).

Gabarito: E

SERVIÇOS DE ARQUIVO E DE IMPRESSÃO EM REDE

Quando falamos em serviços de arquivo e de impressão em rede, geralmente encontramos questões relacionadas ao Windows Server, embora seja possível aplicar os mesmos tipos de serviços em versões desktop (Windows XP, 7, 8, 10 etc).

Vamos começar pelo componente **FSRM (File Server Resource Manager - Gerenciador de Recursos de Servidor de Arquivos)**. Trata-se de um serviço no Windows Server que permite o **gerenciamento e classificação** dos dados armazenados nos servidores de arquivo. O FSRM possui os seguintes recursos:



- Gerenciamento de cotas: limita o espaço permitido para um volume ou uma pasta. Podem ser aplicados automaticamente a novas pastas criadas em um volume;
- Classificação de arquivos: fornece informações sobre os dados, automatizando os processos de classificação para gerenciar os dados com mais eficiência. Os arquivos podem ser classificados automaticamente por meio de regras de classificação de arquivo ou manualmente;
- Gerenciamento de triagens: controla os tipos de arquivos que o usuário pode armazenar em um servidor de arquivos. Ex.: proibir o armazenamento de arquivos com extensão EXE em armazenados em pastas pessoais compartilhadas em um servidor de arquivos.
- Relatórios de armazenamento: auxiliam na identificação de tendências no uso do disco e como seus dados são classificados.

Os recursos incluídos no FSRM podem ser configurados e gerenciados usando o aplicativo próprio ou através da utilização do Windows PowerShell.

Importante: O FSRM suporta somente volumes formatados com o sistema de arquivos NTFS.

Alguns exemplos de aplicações práticas com o uso do FSRM são:

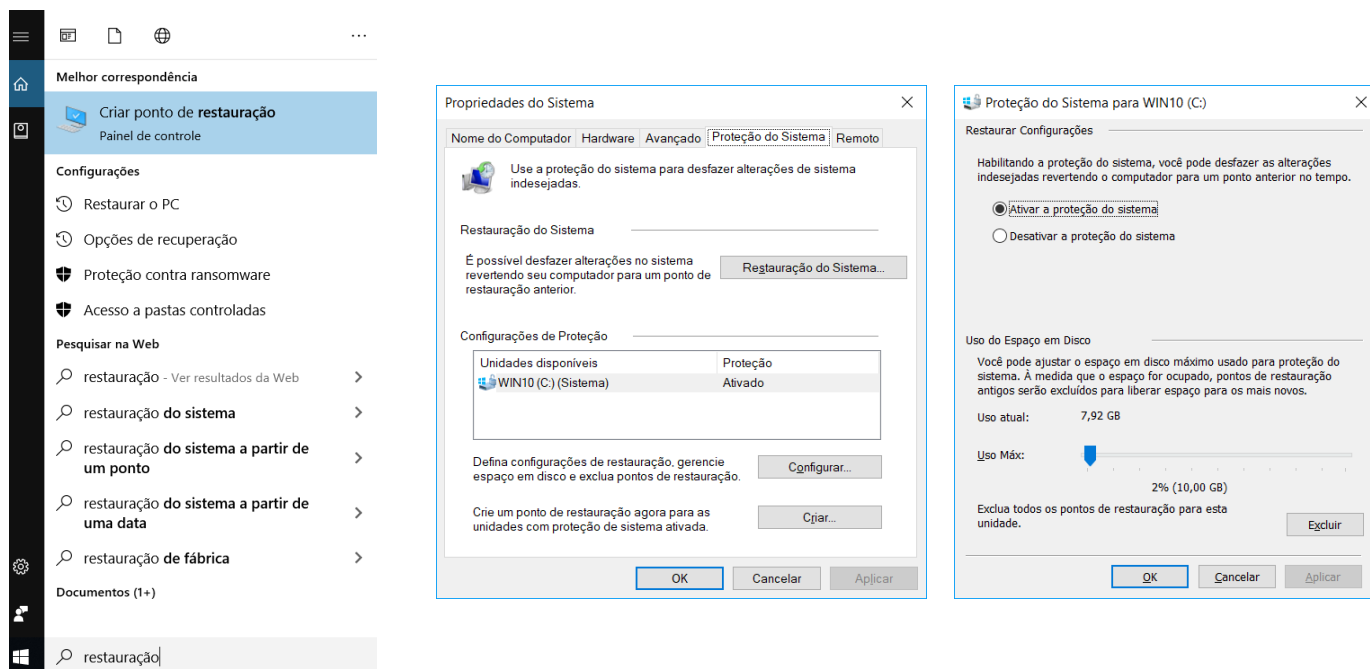
- Criar uma regra de classificação de arquivos que marque os arquivos que possuam pelo menos 5 números de CPF;
- Expirar os arquivos sem modificação nos últimos 5 anos;
- Criar uma cota de 500 MB para a pasta base de cada usuário e notifica-los quando estiverem usando 450 MB;
- Não permitir que arquivos de vídeo sejam armazenados em pastas pessoais compartilhadas;
- Agendar um relatório que será executado todo sábado às 23h, gerando uma lista que inclui os arquivos acessados mais recentemente dos cinco dias anteriores.

Um recurso interessante quando o assunto é serviço de arquivo é a *shadow copy (cópia sombra)*, que cria um espelho dos arquivos e os guarda em um HD externo ou uma outra partição do próprio computador. Se der algum problema (software malicioso, exclusão de arquivos acidentais etc.), é possível voltar ao ponto anterior ou fazer uma restauração do sistema.

Quando ativada a cópia sombra, há uma duplicação de documentos, fotografias e outros itens continuamente, além de manter um histórico que pode ser restaurado em caso de problemas. Imagine uma situação em que um *ransomware* criptografe seus arquivos e algum criminoso solicite um resgate para fornecer a senha. Se houver a *shadow copy* ativa, é só clicar sobre um item comprometido e revertê-lo para uma cópia antiga (que não estava criptografada).

Uma maneira de ativar a cópia sombra é através da pesquisa pela palavra “restauração”, clicar em “Criar ponto de restauração” → “Proteção do Sistema” → “Configurar...”:





Agora vamos falar um pouco da **impressão em rede** no Windows, começando por um passo a passo simplificado:

1. Usuário “envia” arquivo para impressão;
2. O Windows detecta o *driver* associado com a impressora de destino;
3. O serviço de *spooler* (fila de impressão) do cliente faz uma conexão RPC (*Remote Procedure Call*) com o spoolsv.exe;
4. O trabalho é colocado na fila (em *spool*) – arquivo .SHD (padrão: \System32\Spool\Printers);
5. A impressora recebe os comandos de impressão e gera uma imagem *bitmap*.

Detalhe: A impressora pode estar no AD (*Active Directory*) ou no Workgroup (redes pequenas).

Ao instalar uma impressora no Windows Server (*logical driver*), o administrador pode instalar *drivers* para outras versões de Windows: XP, Vista 7, 10 etc.

Existe um protocolo para impressão baseado no IP. É o **IPP** (*Internet Printing Protocol*). Caso a não suporte o IPP, deve-se instalar o IPP no Windows Server e instalar o IIS (*Internet Information Services*). Normalmente há interface via navegador (*browser*), ex.: <http://exemplo.com.br/printers> (lista das impressoras do domínio) ou <http://exemplo.com.br/nomeDaImpressora> (uma impressora específica).

Em relação às permissões para a impressão, existem três níveis:

- Imprimir: conectar à impressora, imprimir, pausar, reiniciar e continuar a impressão;
- Gerenciar documentos: “Imprimir” + controlar e gerenciar os documentos de qualquer usuário;
- Gerenciar impressoras: Anteriores + cancelar impressões pendentes, compartilhar a impressora, alterar as propriedades, eliminar a impressora e alterar as permissões de impressão.



O nível “Imprimir” é atribuído ao grupo “Todos” na instalação de uma impressora nova.

QUESTÕES COMENTADAS

41.(2010 - CESGRANRIO - ELETROBRAS)

Qual recurso nativo do Windows Server 2008 permite ao administrador implementar controle de cotas para pastas e volumes além de controlar e gerenciar o tipo de dados armazenados em seus servidores?

- a) NFS (Network File System).
- b) DFS (Distributed File System).
- c) DFSR (Distributed File System Replication).
- d) Disk Queue Length.
- e) FSRM (File Server Resource Manager).

Comentários:

O **FSRM (File Server Resource Manager - Gerenciador de Recursos de Servidor de Arquivos)** é um serviço no Windows Server que permite o **gerenciamento e classificação** dos dados armazenados nos servidores de arquivo. O FSRM possui os seguintes recursos:

- Gerenciamento de **cotas**: limita o espaço permitido para um volume ou uma pasta. Podem ser aplicados automaticamente a novas pastas criadas em um volume;
- **Classificação** de arquivos: fornece informações sobre os dados, automatizando os processos de classificação para **gerenciar os dados** com mais eficiência. Os arquivos podem ser classificados automaticamente por meio de regras de classificação de arquivo ou manualmente;
- Gerenciamento de **triagens: controla os tipos** de arquivos que o usuário pode armazenar em um servidor de arquivos. Ex.: proibir o armazenamento de arquivos com extensão EXE em armazenados em pastas pessoais compartilhadas em um servidor de arquivos.
- Relatórios de armazenamento: auxiliam na identificação de tendências no uso do disco e como seus dados são classificados.

Gabarito: E

42.(2011 - FCC - TRE-PE)

Sobre o sistema de impressão no Windows Server é correto afirmar:

- A) Todos os documentos são impressos diretamente na impressora sem passar pelo spooler do servidor.
- B) As impressoras podem ser publicadas no Active Directory, o que permite que usuários pesquisem por impressoras e localizem-nas mais facilmente.



- C) Um relatório (log) de impressão é gerado no cliente, com informações sobre o usuário que enviou o trabalho de impressão e a data/hora da impressão.
- D) O driver da impressora fica armazenado no cliente de impressão e deve ser instalado manualmente.
- E) Não há suporte ao acesso às impressoras via HTTP.

Comentários:

(A) Os documentos passam pelo *spooler* do servidor antes de serem impressos. (B) As impressoras podem ser publicadas no AD, assim como os computadores e outros recursos. Isso permite que usuários pesquisem por impressoras e as localizem mais facilmente. (C) Logs de impressão são gerados onde se encontra a impressora. Se ela está no servidor, é nele que o log deve ser gerado. (D) O driver “mostra” como os comandos devem ser enviados à impressora, portanto deve estar instalado no computador onde a impressora está conectada. Pode ser instalado manualmente (CD, por exemplo) ou automaticamente (Internet, por exemplo). (E) Existe suporte ao acesso às impressoras via HTTP. Exemplos:

- <http://exemplo.com.br/printers>
- <http://exemplo.com.br/nomeDaImpressora>

Gabarito: B

43.(2011 - CESPE - MEC)

No caso do serviço de impressão com Windows Server 2003, as portas 139 e 445 com protocolo TCP e as portas 137 e 138 com UDP têm de estar fechadas.

Comentários:

Questão sem pé nem cabeça! As portas mencionadas são utilizadas pelos serviços:

- 139 – NetBIOS;
- 445 – AD;
- 137, 138 – NetBIOS (também).

NetBios = *Network Basic Input/Output System*: API que permite que os aplicativos em computadores separados se comuniquem em uma rede local. S.O. mais antigos executavam o NetBIOS sobre o IEEE 802.2 e o IPX/SPX.

Gabarito: Errado

44.(2011 - CESPE - MEC)

A respeito do Windows Server 2012, julgue os itens a seguir.

No file server, é possível habilitar cópias de sombra de pastas compartilhadas, o que permite realizar a compressão de pastas e arquivos e mantê-los acessíveis ao usuário final.



Comentários:

As cópias de sombra são cópias realizadas periodicamente, de acordo com a configuração pré-estabelecida. Se acontecer algum problema, é possível restaurar essa cópia. Não se trata de compressão de pastas e arquivos acessíveis ao usuário final!

Gabarito: Errado

45.(2014 – CESPE - ANATEL)

O print server é capaz de gerenciar as filas de impressão e determinar permissões de segurança, além de impedir ou liberar o acesso de usuários às impressoras.

Comentários:

Além de gerenciar as filas de impressão, impedir/liberar o acesso de usuários, possui 3 níveis de permissão:

- Imprimir: conectar à impressora, imprimir, pausar, reiniciar e continuar a impressão;
- Gerenciar documentos: “Imprimir” + controlar e gerenciar os documentos de qualquer usuário;
- Gerenciar impressoras: Anteriores + cancelar impressões pendentes, compartilhar a impressora, alterar as propriedades, eliminar a impressora e alterar as permissões de impressão.

O nível “Imprimir” é atribuído ao grupo “Todos” na instalação de uma impressora nova.

Gabarito: Certo



LISTA DE QUESTÕES

1. (2009 – FCC – TRT - 3ª Região (MG) – Técnico Judiciário - Tecnologia da Informação)

No sistema de arquivos NTFS,

- A) as permissões aplicadas nas pastas têm maior prioridade sobre as permissões aplicadas nos arquivos.
- B) se um usuário possui permissão em um arquivo e esse mesmo usuário faz parte de um grupo que possui outra permissão, no mesmo arquivo, a permissão efetiva do usuário será aquela de menos privilégios.
- C) se um usuário pertence a dois grupos que acessam a mesma pasta, e um dos grupos possui a permissão negar, independentemente da permissão que ele tiver no outro grupo, a permissão efetiva desse usuário na pasta será negar, pois negar tem prioridade sobre todas as outras permissões.
- D) ao mover um arquivo ou pasta para outra partição, as permissões originais serão mantidas.
- E) permissões explícitas não podem ser alteradas, a menos que o mecanismo de herança seja desativado.

2. (2009 – UFSJ – UFSJ – Técnico de Tecnologia da Informação)

O Sistema de Arquivos determina a estrutura de armazenamento e manipulação de afirmar que dados em um HD (Hard Disk). Sobre os Sistemas de Arquivos, é INCORRETO

- A) o NTFS é muito eficiente na área de tamanhos de cluster, permitindo formatar uma partição com o tamanho de cluster que se desejar.
- B) nos sistemas de arquivos FAT16, FAT32 e NTFS, quanto maior for o tamanho do cluster, maior será o tamanho da partição.
- C) o sistema operacional Linux pode ler informações gravadas no sistema de arquivo NTFS.
- D) o NTFS é tecnicamente superior aos sistemas de arquivo FAT16 e FAT32. Porém, por permitir um melhor aproveitamento do HD com relação ao tamanho, apresenta menor segurança do que seus antecessores.

3. (2010 – FUNCAB – SEMARH-GO – Cientista da Computação)

Sobre o sistema de arquivo NTFS é correto afirmar que:



- A) é utilizado por algumas versões antigas do Windows e pelas primeiras versões do Linux, mas foi substituído por outros sistemas de arquivos mais modernos por possuir um limite de armazenamento de 2 GBytes.
- B) não permite o uso de arrays RAID, possui tolerância e falhas e permite acesso a dados de rede com segurança.
- C) possibilita ter um controle de acesso a arquivos com gerenciamento de usuários, incluindo suas permissões de acesso, leitura e escrita desses arquivos.
- D) é um sistema que contém acesso e indicações de onde estão as informações de cada arquivo através de um grupo de setores chamados de clusters (ou unidade de alocação).
- E) trabalha com alto grau de desfragmentação de disco e menor consistência de dados, com uma arquitetura de dados baseada em organização por setor que mantém os dados espalhados pelo disco.

4. (2015 – VUNESP – CRO-SP – Programador)

O recurso EFS do sistema de arquivos NTFS oferece ao sistema

- A) controle das alterações feitas no disco por meio de journaling.
- B) criptografia em nível de sistema de arquivos.
- C) indexação de arquivos para agilizar buscas.
- D) mecanismos para compressão dos arquivos em disco.
- E) permissões de controle de acesso ao sistema operacional.

5. (2016 – Makiyama – Prefeitura de Salgueiro - PE – Auxiliar de Enfermagem)

O Active Directory (AD) do Windows

- A) somente pode ser utilizado no sistema de arquivos FAT32.
- B) pode ser utilizado no sistema de arquivos FAT32 ou ExFAT.
- C) somente pode ser utilizado no sistema de arquivos NTFS.
- D) pode ser utilizado no sistema de arquivos FAT32 ou NTFS.

6. (2016 – CESPE – Polícia Científica - PE – Perito Criminal - Ciência da Computação)

Acerca dos sistemas de arquivos para Windows, assinale a opção correta.



- A) No NTFS podem ser utilizadas permissões e criptografia para se restringir o acesso a determinados arquivos e a usuários autorizados.
- B) Os sistemas de arquivos FAT e FAT32 têm a capacidade de recuperar erros de disco automaticamente.
- C) Os sistemas de arquivos disponíveis para Windows são FAT, NTFS e EXT2.
- D) No NTFS, o acesso tanto de leitura quanto de gravação é mais rápido que no FAT32.
- E) Utilizando-se o FAT32, é possível criar uma partição em disco com suporte de até 4 GB.

7. (2018 - FUNDATEC - AL-RS - Analista Legislativo - Analista de Tecnologia da Informação e Comunicação)

Existe um sistema de arquivos em que, para todo o objeto armazenado, é realizado um registro na Master File Table (MFT). Trata-se do:

- A) Ext2.
- B) Ext3.
- C) Ext4.
- D) FAT32.
- E) NTFS.

8. (2019 - CS-UFG - IF Goiano - Técnico de Tecnologia da Informação)

Em geral, sistemas operacionais oferecem suporte a um ou mais sistemas de arquivos que controlam a forma como os dados são identificados, gravados e recuperados a partir dos meios de armazenamento. As últimas versões Windows têm adotado um sistema de arquivos primário que é denominado de

- A) NTFS
- B) EXT4
- C) ReiserFS
- D) ZFS

9. (2011 - FCC - 14ª Região)

Em relação ao LDAP, é INCORRETO afirmar:

- A) É derivado do sistema de diretórios X.500.



- B) É basicamente um sistema de diretórios que engloba o diretório em si e um protocolo denominado DAP.
- C) Normalmente um cliente conecta-se ao servidor LDAP, através da porta padrão 389 (TCP).
- D) A operação Compare tem como função testar se uma entrada tem determinado valor como atributo.
- E) Extended Operation é uma operação genérica para definir outras operações.

10.(2013 – IADES – EBSERH)

O LDAP (Lightweight Directory Access Protocol – Protocolo Leve de Acesso a Diretórios) é utilizado para acessar informações de diretórios, com base no X.500. Sobre o LDAP, julgue os itens a seguir.

- I - É um catálogo de informações que pode conter nomes, endereços, números de telefones, por exemplo.
- II - Permite localizar usuários e recursos em uma rede.
- III - O diretório é organizado hierarquicamente.
- IV - O LDAP é um sistema peer-to-peer.

A quantidade de itens certos é igual a

- A) 0.
- B) 1.
- C) 2.
- D) 3.
- E) 4.

11.(2013 - FCC - TRT – 15ª Região)

Dentre as principais operações que podem ser efetuadas no protocolo LDAP, se encontram: Search: O servidor busca e devolve as entradas do diretório que obedecem ao critério da busca. Bind:

- A) Essa operação serve para autenticar o cliente no servidor. Ela envia o DN (Distinguished Name), a senha do usuário e a versão do protocolo que está sendo usada.
- B) Encerra uma sessão LDAP.
- C) Adiciona uma nova entrada no diretório.
- D) Renomeia uma entrada existente. O servidor recebe o DN (Distinguished Name) original da entrada, o novo RDN (Relative Distinguished Name), e se a entrada é movida para um local diferente na DIT (Directory Information Tree), o DN (Distinguished Name) do novo pai da entrada.
- E) Apaga uma entrada existente. O servidor recebe o DN (Distinguished Name) da entrada a ser apagada do diretório.



12.(2014 – IADES - TRE-PA)

O LDAP é um protocolo que funciona como serviço de diretório em redes TCP/IP. Sua porta padrão é a TCP/389 e a comunicação é feita a partir do cliente, que se liga ao servidor e envia requisições a este último. A respeito desse assunto, assinale a alternativa que apresenta a definição das operações básicas que um cliente pode solicitar a um servidor LDAP.

- A) Search é usado para testar se uma entrada possui determinado valor.
- B) Modify é a operação de adicionar uma entrada no servidor LDAP.
- C) Unbind é a operação de fechamento da conexão entre cliente e servidor.
- D) Start TLS é o comando para colocar no ar o servidor LDAP, no Linux.
- E) Bind é um comando que busca ou recupera entradas no LDAP.

13.(2014 - IADES - TRE-PA)

O LDAP é um serviço de diretório para redes padrão TCP/IP. Um uso comum desse serviço é a autenticação centralizada de usuários; nesse tipo de aplicação, o cliente inicia a comunicação, conectando-se ao servidor LDAP e enviando requisições, ao passo que o servidor responde com as informações contidas em sua base de dados. A respeito das operações que o cliente pode requisitar ao servidor LDAP, assinale a alternativa que corresponde a um pedido de conexão segura (criptografada), implementada a partir LDAPv3.

- A) Extend Operation.
- B) Init Security.
- C) StartTLS.
- D) Bind.
- E) Unbind.

14.(2014 - FCC - SABESP)

Dentre os atributos comuns do protocolo LDAP está o atributo para armazenamento do sobrenome do usuário. A sigla utilizada para este atributo é

- A) co
- B) sn
- C) ln
- D) un
- E) ul



15.(2016 - FCC - TRT-14ª Região)

Analista Judiciário - Tecnologia da Informação) – O LDAP define, dentre outras, a forma como um cliente de diretório pode acessar um servidor de diretório. O LDAP pode ser usado

- A) para enumerar objetos de diretório, mas não para localizá-los.
- B) para estabelecer uma conexão entre um cliente e um servidor LDAP, usando a porta padrão 485, via UDP.
- C) apenas em ambiente Windows, pois é um serviço de diretório proprietário.
- D) no Linux e configurado através do arquivo ldap-inf.xml, encontrado no diretório /etc.
- E) para consultar ou administrar o Active Directory.

16.(2018 - FCC - DPE-AM)

Considere que o Técnico de Suporte deve criar uma nova entrada (conjunto de atributos) na estrutura de diretórios do servidor representada no formato LDIF do LDAP. O primeiro identificador da entrada deve ser

- A) cn.
- B) uid.
- C) sn.
- D) dc.
- E) dn.

17.(2018 - CESPE - ABIN)

Acerca de OAuth e LDAP (Lightweight Directory Access Protocol), julgue o item seguinte.

LDAP é um protocolo de diretórios que provê repositórios de informações de recursos de sistemas e serviços dentro de um ambiente centralizado e estritamente relacionado ao servidor. Por questão de limitação do padrão x.500, do qual foi originado, o LDAP não suporta funções de segurança e de acesso de cliente.

18.(2011 - CONSULPLAN – COFEN)

Qual dos componentes a seguir NÃO faz parte da estrutura lógica do Active Directory no Windows Server?

- A) Objects.
- B) Organizational Units.
- C) Domain Forests.



- D) Domains.
- E) Forests.

19.(2014 - UNIRIO - UNIRIO)

Active Directory está relacionado aos itens a seguir, EXCETO:

- A) Catálogo global.
- B) implementação de serviço de diretório no protocolo DHCP.
- C) Distribuição de Software Automática.
- D) Gerenciamento centralizado.
- E) Replicação automática.

20.(2015 - CESPE - MEC)

Julgue o item que se segue, relativo a Active Directory, IIS e Terminal Service.

Um formato conhecido como um Active Directory com menos recursos é o AD LDS ou Active Directory Lightweight Directory Services.

21.(2016 - Makiyama - Prefeitura de Salgueiro/PE)

O Active Directory (AD) do Windows

- A) somente pode ser utilizado no sistema de arquivos FAT32.
- B) pode ser utilizado no sistema de arquivos FAT32 ou ExFAT.
- C) somente pode ser utilizado no sistema de arquivos NTFS.
- D) pode ser utilizado no sistema de arquivos FAT32 ou NTFS.

22.(2016 - FIOCRUZ - FIOCRUZ)

Em um servidor Windows 2008 utilizado apenas como servidor de arquivos será criado um ambiente com Active Directory Domain Services. Para iniciar o assistente de instalação do AD deve ser executado o comando:

- A) Promote.exe
- B) DCPromo.exe
- C) ADDS_Promo.exe
- D) DomainPromote.exe
- E) DCPromote.exe



23.(2017 - UFMT - UFSBA - Analista de Tecnologia da Informação)

2017 - FCC - TRF-5ª Região

O Active Directory – AD

A) tem um banco de dados denominado NTDS.dit e está localizado na pasta %SystemAD%\NTDS\ntds.dit em uma instalação default do AD. O diretório NTDS existirá em todos os servidores, independentemente de terem a função de Domain Controllers.

B) ao ser instalado, cria 5 arquivos: 1) Ntds.dit, banco de dados do AD; 2) Edb.log, armazena todas as transações feitas no AD; 3) Edb.chk, controla transações no arquivo Edb.log já foram committed em Ntds.dit; 4) Res1.log, arquivo de reserva; 5) Res2.log, arquivo de reserva.

C) pode ter um ou mais servidores com a função de Domain Controller – DC. Em um AD com três DCs, por exemplo, somente o DC-raiz é atualizado com todos os dados do AD. Esta operação recebe o nome de replicação do Active Directory.

D) pode ter Operational Units – OUs. As OUs podem ser classificadas de 3 formas diferentes: 1) Geográfica, as OUs representam Estados ou Cidades; 2) Setorial, as OUs representam setores ou unidades de negócio da estrutura da empresa; 3) Departamental, as OUs representam departamentos da empresa.

E) pode ter um ou dois domínios. O 2º domínio é denominado domínio-filho. O conjunto domínio-pai com seu domínio-filho é chamado de floresta, pois o domínio-filho pode ter vários ramos chamados de subdomínios.

24.(2017 - IADES - Fundação Hemocentro de Brasília/DF)

O Active Directory (AD) é o

A) repositório de informações referentes a objetos da rede e também ao serviço que permite que essas informações sejam utilizadas.

B) mecanismo que permite aos usuários o acesso a recursos de outros domínios.

C) conjunto de arquivos que armazena informações de usuários, grupos e recursos.

D) mecanismo responsável pela cópia de todas as informações entre os controladores de domínio da floresta.

E) conjunto de uma ou mais árvores.



25.(2018 - COMPERVE - UFRN)

O Active Directory (AD) é composto por diversos serviços, tais como, Active Directory Certificate Services (AD CS), Active Directory Domain Services (AD DS), Active Directory Federation Services (AD FS), Active Directory Lightweight Directory Services (AD LDS), e Active Directory Rights Management Services (AD RMS). O serviço que armazena os dados de diretório e gerencia a comunicação entre usuários e domínios, incluindo processos de logon de usuário, autenticação e pesquisas de diretório é o

- A) Active Directory Domain Services (AD DS).
- B) Active Directory Rights Management Services (AD RMS).
- C) Active Directory Certificate Services (AD CS).
- D) Active Directory Certificate Functions (AD CF).

26.(2018 - UFLA - UFLA)

O Active Directory (AD) é um serviço de diretório nas redes Windows. Assinale a alternativa CORRETA:

- A) Quando um Administrador realiza alterações em um controlador de domínio (DC), é gerado um pacote chamado de Global Catalog (GC).
- B) A partição Schema contém informações sobre a estrutura do AD incluindo quais domínios, sites, controladores de domínio e cada serviço existente na floresta.
- C) Quando um Administrador realiza alterações em um controlador de domínio (DC), o servidor precisa atualizar a sua base do AD com os outros controladores de domínio da rede.
- D) A partição Configuração contém a definição dos objetos e atributos que são criados no diretório e as regras para criá-los e manipulá-los.

27.(2018 - FAURGS - TJ-RS)

No Active Directory (AD), o conjunto lógico composto por objetos ou recursos como computadores, usuários e grupos de objetos definidos administrativamente, e que compartilham a mesma base de dados, é denominado

- A) domínio.
- B) árvore.
- C) floresta.
- D) organizational units (OU).
- E) schema.

28.(2018 - Quadrix - CRM-PR)



Julgue o item a seguir, relativo a serviços de diretórios.

O serviço de diretórios AD (Active Directory) foi criado com a finalidade de armazenar diversas senhas de um usuário para diferentes sistemas.

29.(2018 - FGV - AL-RO)

O principal arquivo do Microsoft Active Directory que tem por função servir como base de dados para armazenar as informações sobre objetos de usuários, grupos e associação de grupos, é denominado

- A) Ntds.dit
- B) Edb.chk
- C) Edb.log.
- D) Res1.log.
- E) Schema.db.

30.(2018 - CESPE - FUB)

Julgue o item seguinte, a respeito dos sistemas operacionais Windows e Linux.

No que se refere ao ambiente Windows, desde o Windows 2000, os nomes de domínio do Active Directory são, geralmente, os nomes DNS (domain name service) completos dos domínios.

31.(2014 - IADES - CONAB)

No gerenciamento de contas de usuários do sistema operacional Windows 7, cada conta de usuário é representada por quatro elementos: um ícone, o nome da conta, o perfil do usuário e se ela é protegida por senha. Acerca das contas de usuário do Windows, assinale a alternativa correta.

- A) O ícone é uma figura-padrão e não pode ser alterado.
- B) O nome da conta, ao ser alterado, pode apresentar nomes iguais, desde que tenham perfis diferentes.
- C) O tipo de conta administrador dá poderes para o usuário criar nova conta, inclusive com perfil administrador.
- D) Recomenda-se que a senha seja igual ao nome da conta, na sua criação, para facilitar a memorização e forçar a substituição.
- E) Todo computador deve ter pelo menos um perfil visitante.



32.(2016 - CESPE - Polícia Científica-PE)

O gerenciamento de usuários no Windows

- A) impossibilita a criação de um grupo de usuários.
- B) permite alterar o nome da conta, alterar a imagem e configurar o controle dos pais, entre outras opções de modificação em uma conta de usuário.
- C) dispensa, no uso de um certificado digital em uma credencial de usuário, o salvamento desse certificado no repositório pessoal do usuário.
- D) impede o usuário de efetuar login sem uma conta de usuário
- E) exige a reinstalação do sistema operacional caso algum usuário do computador esqueça sua senha.

33.(2017 - FCC - TRF-5ª Região)

Um Técnico em Informática estava usando um computador com o sistema operacional Windows 7 em português e, através de um caminho via Painel de Controle, clicou em “O que é uma conta de usuário?”. O sistema exibiu uma janela com a seguinte informação:

Uma conta de usuário é uma coleção de dados que informa ao Windows quais arquivos e pastas você pode acessar, quais alterações pode fazer no computador e quais são suas preferências pessoais, como plano de fundo da área de trabalho ou proteção de tela. As contas de usuário permitem que você compartilhe um computador com várias pessoas, enquanto mantém seus próprios arquivos e configurações. Cada pessoa acessa a sua conta com um nome de usuário e uma senha. Há três tipos de contas, cada tipo oferece ao usuário um nível diferente de controle do computador:

- A) As contas Padrão são para o dia-a-dia; as contas Administrador oferecem mais controle sobre um computador e só devem ser usadas quando necessário; as contas Convidado destinam-se principalmente às pessoas que precisam usar temporariamente um computador.
- B) As contas de Usuário são as que não necessitam de senha; as contas de Administrador exigem senha e são usadas para o controle do computador; as contas de Pais são usadas para ajudar a gerenciar o modo como as crianças usam o computador.
- C) As contas Credenciais Genéricas são para usuários comuns; as contas Credenciais Administrador oferecem controle sobre o computador; as contas Credenciais do Windows com Certificado destinam-se a usuários que possuam um certificado digital.
- D) As contas de Grupo Local são para usuários padrão; as contas de Grupo Administrativo oferecem controle sobre o computador, exigindo uma senha de administrador; as contas de Grupo Doméstico aceitam usuários padrão e administradores e permitem a criação de contas de usuários convidados.
- E) As contas Usuário são as de usuários padrão e não necessitam de senha; as contas Administrador exigem senha e são usadas para o controle do computador; as contas Segurança Familiar são usadas para ajudar a gerenciar o modo como as crianças usam o computador.



34.(2017 - CESPE - TRE-BA)

No Windows 7, o usuário estará apto a excluir subpastas e arquivos caso tenha a permissão de acesso especial de NTFS

I Modificar.

II Leitura.

III Ler & Executar.

IV Gravação.

V Controle Total.

Assinale a opção correta.

A) Apenas os itens I, III e V estão certos.

B) Apenas os itens II, III e IV estão certos.

C) Apenas os itens I e IV estão certos.

D) Apenas o item III está certo.

E) Apenas o item V está certo.

35.(2010 - CESPE - SERPRO)

Uma das formas de se obter acesso remoto ao Windows Server 2003, a partir de outra máquina com o Internet Explorer, é por meio da instalação do pacote Remote Desktop Web Connection ActiveX para hospedagem de terminal services, cuja limitação principal é não funcionar no IIS.

36.(2011 - CESPE - MEC)

O Remote Desktop Connection é o servidor padrão para o terminal services no Windows 2003.

37.(2013 - FCC - MPE-SE)

No Windows Server 2008, a Memória Dinâmica permite o uso mais eficiente de memória enquanto mantém a consistência de desempenho e escalabilidade das cargas de trabalho. Implementar a Memória Dinâmica significa que níveis mais altos de consolidação de servidores podem ser obtidos com mínimo impacto sobre o desempenho. A Memória Dinâmica também significa que pode haver um número maior de desktops virtuais por host Hyper-V em cenários de

A) múltiplos acessos simultâneos (Windows DataShare).

B) servidores remotos RemoteFX.

C) servidores cluster (ClusterMode).



D) recuperação de erros (ServerRecover).

E) VDI - Virtual Desktop Infrastructure.

38.(2014 - FCC - AL-PE)

O Windows Server 2008 R2 oferece os tipos I e II de virtualização.

A) I -DirectAccess. II -De computadores clientes quando usado em conjunto com a VDI (Virtual Desktop Infrastructure))

B) I - Power Shell 2.0. II- DirectAccess

C) I - De servidores através do Hyper-V. II - De computadores clientes quando usado em conjunto com a VDI (Virtual Desktop Infrastructure)

D) I - De servidores quando usado em conjunto com a VDI (Virtual Desktop Infrastructure) II - De computadores clientes através do Hyper-V

E) I - De servidores através do Hyper-V. II - BranchCache

39.(2014 - FGV - PROCEMPA)

Relacione alguns dos recursos que podem ser utilizados no Windows Server 2012 com suas respectivas funções.

1. AppLocker

2. Windows PowerShell

3. Hyper-V

4. Remote Desktop Services

() Sistema de virtualização para arquiteturas x86/x86_64.

() Acesso a sessões em computadores físicos ou virtuais a partir de estações de trabalho, via rede corporativa ou Internet.

() Implementador de políticas de controle de execução de programas.

() Ambiente para administração do sistema por linha de comando.

A) 3 – 4 – 1 – 2

B) 2 – 3 – 1 – 4

C) 4 – 3 – 1 – 2

D) 3 – 4 – 2 – 1

E) 4 – 3 – 2 – 1

40.(2016 - FCC - TRF-3ª Região)



Ao estudar a preparação da infraestrutura de virtualização a ser utilizada no ambiente Windows Server 2008 R2, um Técnico Judiciário de TI do Tribunal observou que o Hyper-V é usado para a virtualização do computador cliente quando usado em conjunto com a tecnologia

- A) Virtual DNS Infrastructure - DNSSEC.
- B) Basic Desktop Node - BDN.
- C) Client Desktop Infrastructure - CDI.
- D) Virtual Basic Client System - VBCS.
- E) Virtual Desktop Infrastructure - VDI.

41.(2010 - CESGRANRIO - ELETROBRAS)

Qual recurso nativo do Windows Server 2008 permite ao administrador implementar controle de cotas para pastas e volumes além de controlar e gerenciar o tipo de dados armazenados em seus servidores?

- a) NFS (Network File System).
- b) DFS (Distributed File System).
- c) DFSR (Distributed File System Replication).
- d) Disk Queue Length.
- e) FSRM (File Server Resource Manager).

42.(2011 - FCC - TRE-PE)

Sobre o sistema de impressão no Windows Server é correto afirmar:

- A) Todos os documentos são impressos diretamente na impressora sem passar pelo spooler do servidor.
- B) As impressoras podem ser publicadas no Active Directory, o que permite que usuários pesquisem por impressoras e localizem-nas mais facilmente.
- C) Um relatório (log) de impressão é gerado no cliente, com informações sobre o usuário que enviou o trabalho de impressão e a data/hora da impressão.
- D) O driver da impressora fica armazenado no cliente de impressão e deve ser instalado manualmente.
- E) Não há suporte ao acesso às impressoras via HTTP.

43.(2011 - CESPE - MEC)

No caso do serviço de impressão com Windows Server 2003, as portas 139 e 445 com protocolo TCP e as portas 137 e 138 com UDP têm de estar fechadas.



44.(2011 - CESPE - MEC)

A respeito do Windows Server 2012, julgue os itens a seguir.

No file server, é possível habilitar cópias de sombra de pastas compartilhadas, o que permite realizar a compressão de pastas e arquivos e mantê-los acessíveis ao usuário final.

45.(2014 – CESPE - ANATEL)

O print server é capaz de gerenciar as filas de impressão e determinar permissões de segurança, além de impedir ou liberar o acesso de usuários às impressoras.

GABARITO

1. C
2. D
3. C
4. B
5. C
6. A
7. E
8. A
9. B
10. D
11. A
12. C
13. C
14. B
15. E
16. E
17. Errado
18. C
19. B
20. Certo
21. C
22. B
23. B
24. A
25. A

26. C
27. A
28. Errado
29. A
30. Certo
31. C
32. B
33. A
34. E
35. Errado
36. Errado
37. E
38. C
39. A
40. E
41. E
42. B
43. Errado
44. Errado
45. Certo



ESSA LEI TODO MUNDO CONHECE: PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.



1 Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.



2 Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).



3 Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).



4 Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).



5 Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).



6 Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).



7 Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.



8 O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.