Estratégia Concursos

Aula 00

ITEP-RN (Assistente Técnico Forense - Analista de Sistemas) Arquitetura e Sistemas Operacionais

Autor:
Equipe Informática e TI, Evandro Dalla Vecchia Pereira

30 de Setembro de 2024

Índice

Administração de Serviços de Diretório (Active Directory)

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! Por isso vamos ver em separado o LDAP, para depois vermos a AD, a seguir.

LDAP (Lightweight Directory Access Protocol)

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.

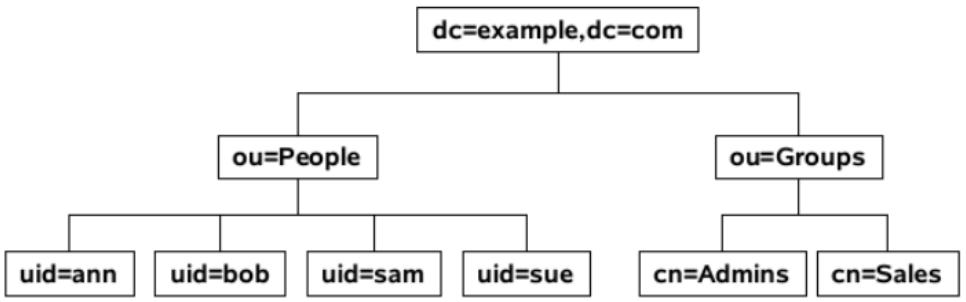
Um recurso é identificado pelo nome do servidor, separado do nome do recurso por uma contrabarra, como por exemplo:

\\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 em 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".

AD (Active Directory)

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).

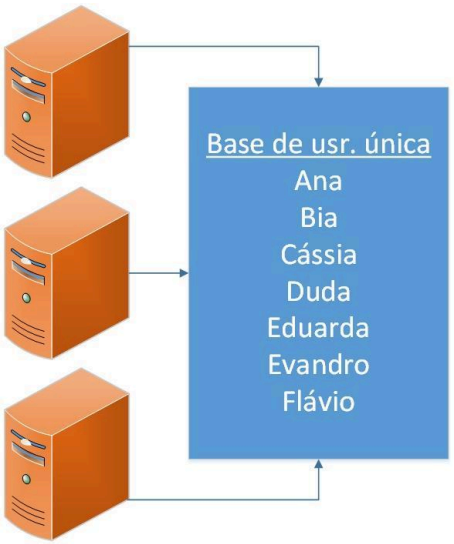
Imagine que uma empresa tenha três servidores (de arquivos, de e-mails e de um aplicativo empresarial - exemplo ao lado).

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).

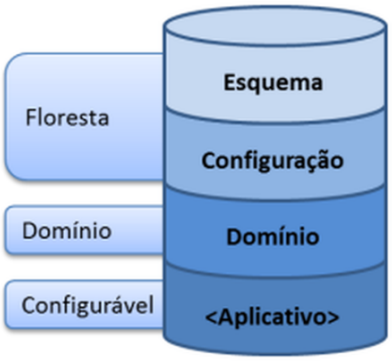
Para "transformar" um servidor membro em controlador de domínio (DC) e instalar o AD, existe o executável DCPROMO.EXE (versões mais antigas). No Windows Server 2012, o AD substitui tal ferramenta por um Gerenciador do Servidor e sistema de implantação baseado em Windows PowerShell.

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;

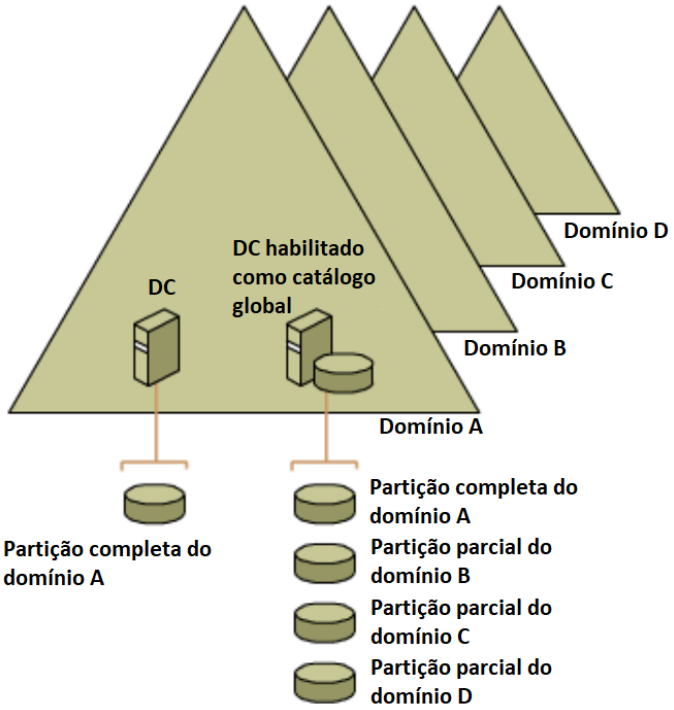
- Configuração: informações da configuração dos domínios, criando uma instância da estrutura lógica do AD;
- Domínio: contatos, usuários, grupos, computadores e OUs.



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□B□C, então A□C.

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

Administração de usuários, grupos, permissões e controles de acesso

Administrar o AD envolve gerenciar usuários, grupos, permissões e controles de acesso para garantir que os recursos de rede sejam utilizados de maneira segura e eficiente. Vamos ver cada um desses pontos a seguir.

Administração de Usuários

Para criar um usuário, pode-se abrir "Ferramentas Administrativas", ir até "Usuários e Computadores do Active Directory", navegar até a Unidade Organizacional (OU) onde se deseja criar o usuário. Depois é só criar o usuário (clicando com o botão direito na OU, selecionando "Novo", "Usuário", preenchendo as informações necessárias - nome, logon etc. - e definindo uma senha. Na sequência é só completar o assistente para criar o usuário.

Edição de Propriedades de um Usuário

Para abrir as propriedades do usuário é só clicar com o botão direito no usuário e selecionar "Propriedades". Na janela de propriedades é possível modificar diversos atributos, como informações de contato, membros de grupo, permissões etc.

Desativar ou Excluir um Usuário

Para desativar um usuário, é só clicar com o botão direito no usuário e selecionar "Desativar Conta". Para excluir um usuário, é só clicar com o botão direito no usuário e selecionar "Excluir".

Administração de Grupos

Para criar um novo grupo, é só ir em "Ferramentas Administrativas" e abrir "Usuários e Computadores do Active Directory", navegar até a OU onde se deseja criar o grupo, clicar com o botão direito na OU, selecionar "Novo", "Grupo", preencher as informações necessárias, como nome do grupo e tipo (grupo de segurança ou distribuição). Depois é só completar o assistente para criar o grupo.

Para adicionar usuários a um grupo, deve-se abrir as propriedades do grupo, clicar com o botão direito no grupo e selecionar "Propriedades"ir até a aba "Membros" e clicar em "Adicionar", procurar e selecionar os usuários que deseja adicionar ao grupo.

Administração de Permissões e Controles de Acesso

Para atribuir permissões a grupos ou usuários, deve-se abrir as propriedades do recurso (navegar até o recurso - pasta, arquivo etc. - no Explorador de Arquivos), clicar com o botão direito no recurso e selecionar "Propriedades". Para configurar as permissões deve-se ir para a aba

"Segurança" e clicar em "Editar", adicionar o grupo ou usuário ao qual deseja atribuir permissões e definir as permissões apropriadas (leitura, escrita, modificação etc.).

Group Policy Objects (GPO)

GPO é um conjunto de regras e configurações que são aplicadas a objetos em um domínio do AD. Essas regras podem afetar computadores, usuários ou ambos, e cobrem uma variedade de configurações, como segurança, rede, software, ambiente de trabalho etc.

Existem três tipos principais de GPOs:

- GPOs Locais: Aplicadas apenas a um computador localmente;
- GPOs de Domínio: Aplicadas a grupos de computadores e usuários dentro de um domínio AD;
- GPOs de Site: Aplicadas a todos os objetos dentro de um determinado site no AD.

Um GPO é composto por duas partes principais:

- Configurações de Computador: Afetam as configurações de hardware e software no nível do sistema, independentemente do usuário que está logado. Como exemplos, temos: políticas de senha, atualizações automáticas etc.;

- Configurações de Usuário: Afetam a experiência do usuário, como por exemplo a aparência da área de trabalho, permissões de software etc.

A aplicação de políticas GPO segue uma hierarquia conhecida como LSDOU:

- Local: GPOs aplicadas localmente em uma máquina;
- Site: GPOs configuradas para um site específico do AD;
- Domínio: GPOs aplicadas no nível do domínio AD;
- OU (Unidade Organizacional): GPOs aplicadas a uma OU específica, afetando todos os objetos contidos nela.

Mas, para que servem de fato as GPOs? Vamos ver dois exemplos:

- Gerenciamento de atualizações automáticas: Um administrador pode criar uma política que força todos os computadores do domínio a instalarem atualizações automáticas em um horário específico;

- Redirecionamento de pastas: GPOs podem ser utilizadas para redirecionar pastas como "Documentos" para um servidor centralizado. Desta forma, os dados são armazenados de forma segura.

Duas ferramentas para gerenciamento de GPOs são:

- Group Policy Management Console (GPMC): A interface gráfica usada para criar, editar, e gerenciar GPOs;

- Gpupdate /force: É um comando para forçar a aplicação imediata de GPOs em um computador.

Para abrir o Editor de Gerenciamento de Políticas de Grupo, deve-se ir até "Ferramentas Administrativas" e abrir "Gerenciamento de Política de Grupo". Para criar ou editar uma GPO,

deve-se navegar até a OU onde se deseja aplicar a política, clicar com o botão direito e selecionar "Criar um GPO neste domínio e vincular aqui", dar um nome à GPO e clicar em OK.

Para as configurações da GPO, deve-se clicar com o botão direito na GPO criada e selecionar "Editar". No Editor de Política de Grupo, deve-se realizar as configurações desejadas para "Configuração do Computador" ou "Configuração do Usuário".

1. (CEBRASPE/FUB/2018) 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: Correta

2. (FCC/TRT14/2016) 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: Letra E

QUESTÕES COMENTADAS - ADMINISTRAÇÃO DE SERVIÇOS DE DIRETÓRIO - MULTIBANCAS

1. (FCC/TRT14 - 2011) 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. Portanto, a alternativa B está correta e é o gabarito da questão.

Gabarito: Letra B

2. (IADES/EBSERH - 2013) 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). Portanto, a alternativa D está correta e é o gabarito da questão.

Gabarito: Letra D

3. (FCC/TRT15 - 2013) 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. Portanto, a alternativa A está correta e é o gabarito da questão.

Gabarito: Letra A

4. (IADES/TRE-PA - 2014) 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. Portanto, a alternativa C está correta e é o gabarito da questão.

Gabarito: Letra C

5. (IADES/TRE-PA - 2014) 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. Portanto, a alternativa C está correta e é o gabarito da questão.

Gabarito: Letra C

6. (FCC/SABESP - 2014) 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).

Portanto, a alternativa B está correta e é o gabarito da questão.

Gabarito: Letra B

7. (FCC/TRT14 - 2016) 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! Portanto, a alternativa E está correta e é o gabarito da questão.

Gabarito: Letra E

8. (FCC/DPE-AM - 2018) 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). Portanto, a alternativa E está correta e é o gabarito da questão.

Gabarito: Letra E

9. (CESPE/ABIN - 2018) 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). Portanto, a questão está errada.

Gabarito: Errada

10.(CONSULPLAN/COFEN - 2011) 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). Portanto, a alternativa C está correta e é o gabarito da questão.

Gabarito: Letra C

11.(UNIRIO/UNIRIO - 2014) 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. Portanto, a alternativa B está correta e é o gabarito da questão.

Gabarito: Letra B

12. (CESPE/MEC - 2015) 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.

Portanto, a questão está correta.

Gabarito: Correta

13. (Makiyama/Prefeitura de Salgueiro-PE - 2016) 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! Portanto, a alternativa C está correta e é o gabarito da questão.

Gabarito: Letra C

14. (FIOCRUZ/FIOCRUZ - 2016) 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 controler). Portanto, a alternativa B está correta e é o gabarito da questão.

Gabarito: Letra B

15. (FCC/TRF5 - 2017) 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 commited 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 2° 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.

Portanto, a alternativa B está correta e é o gabarito da questão.

Gabarito: Letra B

16. (IADES/Fundação Hemocentro de Brasília-DF - 2017) 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. Portanto, a alternativa A está correta e é o gabarito da questão.

Gabarito: Letra A

17. (COMPERVE/UFRN - 2018) 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. Portanto, a alternativa A está correta e é o gabarito da questão.

Gabarito: Letra A

18. (UFLA/UFLA - 2018) 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. Portanto, a alternativa C está correta e é o gabarito da questão.

Gabarito: Letra C

19. (FAURGS/TJ-RS - 2018) 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).

Portanto, a alternativa A está correta e é o gabarito da questão.

Gabarito: Letra A

20. (Quadrix/CRM-PR - 2018) 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 controler). Portanto, a questão está errada.

Gabarito: Errada

21. (FGV/AL-RO - 2018) 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.

Portanto, a alternativa A está correta e é o gabarito da questão.

Gabarito: Letra A

22. (CESPE/FUB - 2018) 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. Portanto, a questão está correta.

Gabarito: Correta

LISTA DE QUESTÕES - ADMINISTRAÇÃO DE SERVIÇOS DE DIRETÓRIO - MULTIBANCAS

1. (FCC/TRT14 - 2011) 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.

2. (IADES/EBSERH - 2013) 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.

3. (FCC/TRT15 - 2013) 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.

4. (IADES/TRE-PA - 2014) 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.

5. (IADES/TRE-PA - 2014) 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.

6. (FCC/SABESP - 2014) 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

7. (FCC/TRT14 - 2016) 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.

8. (FCC/DPE-AM - 2018) 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.

9. (CESPE/ABIN - 2018) 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.

10. (CONSULPLAN/COFEN - 2011) 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.

11. (UNIRIO/UNIRIO - 2014) 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.

12. (CESPE/MEC - 2015) Um formato conhecido como um Active Directory com menos recursos é o AD LDS ou Active Directory Lightweight Directory Services.

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

14. (FIOCRUZ/FIOCRUZ - 2016) 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

15. (FCC/TRF5 - 2017) 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 commited 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 2° 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.

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

17. (COMPERVE/UFRN - 2018) 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).

18. (UFLA/UFLA - 2018) 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.

19. (FAURGS/TJ-RS - 2018) 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.

20. (Quadrix/CRM-PR - 2018) O serviço de diretórios AD (Active Directory) foi criado com a finalidade de armazenar diversas senhas de um usuário para diferentes sistemas.

21. (FGV/AL-RO - 2018) 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.

22. (CESPE/FUB - 2018) 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.

GABARITO

GABARITO

1- B
2- D
3- A
4- C
5- C
6- B
7- E
8- E
9- Errada
10- C
11- B
12- Correta
13- C
14- B
15- B
16- A
17- A
18- C
19- A
20- Errada
21- A
22- Correta

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.