č.o	otázka	
1	ad	Active Directory je implementace adresářových služeb LDAP firmou Microsoft pro použití v prostředí systému Microsoft Windows. Active Directory umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Active Directory ukládá své informace a nastavení v centrální organizované databázi.Služba Active Directory obsahuje logické i fyzické struktury součástí sítě. a) Logické 1.Organizační jednotky 2.Domény 3.Stromy domén 4.Lesy domén b) Fyzické 1.Podsítě 2.Sítě
2	agpm	Microsoft® Advanced Group Policy Management pomáhá zajišťovat trvalou konfiguraci požadovaných nastavení zabezpečení v počítačích prostřednictvím vyšší kontroly a správy objektů zásad skupiny (GPO). Díky přidané správě změn objektů zásad skupiny a jejich offline úpravám je kontrola počítačů snazší. Výsledkem jsou nižší rizika a omezení výpadků koncových uživatelů způsobených konfliktními či nesprávně nakonfigurovanými objekty zásad skupiny.
3	application pool	Díky app pool běží aplikace samostatně, jedna nesestřelí ostatní procesy. Navíc běží odděleně od inetinfo. Recycling-automatický restart (-po čase,-po určitém počtu požadavků, -v určitou dobu, -podle paměti) rozděluje aplikace tak, aby nemohly ovlivňovat další aplikace na serveru. Toho dosahují pomocí tzv. worker process isolation módu. Od IIS 7 se navíc rozlišuje, jak zpracovat požadavek, který zahrnuje spravované prostředky – buď pomocí Integrated módu nebo Classic módu.
4	HPC architecture	Prvních 10 nejvýkonnějších superpočítačů v žebříčku TOP500 má stejnou základní architekturu. Každý z nich je clusterem MIMD (Multiple Instruction stream, Multiple Data stream) multiprocesorových sestav, přičemž každý z procesorů je architektury SIMD (Single Instruction/Multiple Data. Superpočítače se radikálně liší počtem multiprocesorových jednotek na cluster, počtem procesorů na jednu jednotku a počtem současně vykonavatelných instrukcí na jeden SIMD procesor.

5	archiving and backup	Zálohování tvoří „pojistku“ před havárií, zálohujeme proto, abychom byli schopni rychle obnovit plně funkční stav systému. Zálohy by měly být co nejnovější abychom v případě že musíme obnovovat přišli o co nejméně dat Typy záloh: -Normal(full) - zálohují se všechny vybrané soubory bez ohledu na to, zdali se od poslední zálohy změnily -Copy - jako běžné kopírování -Incremental - Zálohuje se pouze to, co se změnilo od poslední zálohy. Mění se atribut archive - Differential - Zálohuje se pouze to, co se změnilo od poslední zálohy. Nemění se atribut archive - Daily copy - zálohuje se vše, co se během dne změnilo. Archivace slouží k ukládání dat na bezpečném místě, jsou určena k pozdějšímu využití. Nedělá se tak často, jako zálohy. Většinou na externím mediu, např. optické medium
6	What is Auditing? Where can we find information about audits and what is all we need to do to ensure that audits are conducted?	Automatické sledování událostí, informace o auditech jsou v Event vieweru v Security. Nastavují se přes místní zásady zabezpečení nebo potom v Group Policy Audit je činnosti sítě je z pohledu zabezpečení velmi důležitým procesem. Jinak je totiž téměř nemožné zjistit, že se například již podvacáté za poslední dvě minuty nezdařilo přihlášení uživatele, že došlo k uzamčení uživatelského účtu nebo například že se neoprávněný uživatel snažil přistoupit k souborům ve sdílené složce, ke kterým nemá uděleno potřebné oprávnění. Vždy je možné auditovat úspěšné pokusy a neúspěšné pokusy. Zatímco u sledování pří-stupu k objektům nemusí být úspěšné pokusy pro správce zajímavé (nepřinášejí žádnou Informaci, neboť došlo k události, která se očekávala), mohou být užitečné u auditu přihlášení. Při konfiguraci auditu je tak třeba zvážit, co auditovat.
7	What is DHCP?	DHCP (Dynamic Host Configuration Protocol) je v informatice název protokolu z rodiny TCP/IP nebo označení odpovídajícího DHCP serveru či klienta. Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu a adresu DNS serveru. Platnost přidělených údajů je omezená, proto je na počítači spuštěn DHCP klient, který jejich platnost prodlužuje.
8	what DNS is and how the name translates	DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes de facto jako distribuovaná databáze síťových informací.Systém DNS je celosvětově distribuovanou databází uchovávající záznamy o tom, která IP adresa patří ke kterému doménovému jménu, přitom IP adresa může mít doménových jmen i více. O databázi se starají programy zvané jmenné servery, které data z datábaze poskytují klientům, tzv. resolverům.

9	What is a domain, a domain tree, a forest, a connection option (instead of a "connection" was probably another word)	Doména je logická skupina počítačů sdílející společnou centrální adresářovou databázi (AD). Doménový strom je hierarchické spojení domén vytvořené vztahem rodič-potomek, všechny domény v rámci stromu sdílejí stejný jmenný prostor, schéma je stejné v rámci doménového stromu. Doménová struktura je bezpečnostní a administrativní hranice všech objektů, které se v ní nacházejí. Typ vztahu důvěryhodnosti, parent-child
10	What is virtualization?	Virtualizace umožňuje, aby na jednom fyzickém serveru (na jednom hardware) běželo více oddělených serverů s vlastním operačním systémem. Fyzický server každému takovému virtuálnímu serveru emuluje virtuální hardware (procesor, paměť, disk, síťová karta, mechaniky, periferní zařízení a další). To, že je server virtualizovaný, však zákazník na první pohled nepozná. Má svůj server s procesory, pamětí a dalšími komponentami, na tom mu běží nějaký operační systém dle jeho volby, má k němu plný přístup a pracuje s ním jako kdyby tento jeho operační systém běžel na vlastním hardware
11	What is virtualizationWhat is the understanding of a system's state of backup?	Aktuální konfigurace počítače, patří sem zejména: Registry Registrační databáze tříd modelu COM+ Spouštěcí soubory včetně systémových souborů Databáze Certifikační služby Adresářová služba Active Directory Adresář SYSVOL Informace o Clusterové službě Adresář s metadaty služby IIS Systémové soubory, které jsou chráněny systémem Windows V programu Backup jsou tyto systémové součásti označeny jako data Stav systému. Přesné systémové součásti, ze kterých se skládají data Stav systému, závisejí na operačním systému počítače a na konfiguraci.
12	DFS	Systém DFS je prakticky rozcestníkem, který zjednodušuje orientaci a přístup uživatelů k různým sdíleným složkám, které mohou být „rozházené" po různých serverech v síti. Distribuovaný systém souborů DFS (Distributed File System) umožňuje správci seskupovat sdílené složky rozmístěné po síti do jedné DFS má vždy takzvaný kořen - tím je sdílená složka, ve které jsou odkazy (něco jako zástupci) na místní i vzdálené sdílené složky. Uživatelům tak při plném využiti systému DFS nyní stačí pamatovat si pouze jedinou cestu ke sdílené složce, neboť poté se dostanou ke všem složkám, ke kterým potřebují.

13	Disk array (RAID x etc)	(přednáška č.4 - bezpečnost dat; slide 3 - 6) RAID (Redundant Array of Independent Disks) RAID 0 (stripping) -není redundantní, př, Disk1(A1,A3,A5,A7), Disk2(A2,A4, A6, A8). Při havárii jednoho z disků ztratíme všechny data. JInak výhodou je zrychlení zápisu RAID 1 (mirroring) - na discích se nacházejí stejná data (zrcadlí se), takže v případě havárie jednoho z disků nepřicházíme o data. Ale zase klade větší nároky na zdroje (potřebuje více místa) RAID 5 - stripping s distribuovanou paritou, vyžaduje min. 3 disky, lze použít i více (až 32). Není vhodná pro vysokou I/O zátěž. Při havárii nedochází ke ztrátě dat. RAID6 - princip shodný s RAID5, ale používá dvojtou paritu; vhodný pro velké pole disků
14	DNS cache	Téměř každý DNS server funguje zároveň jako DNS cache. Při opakovaných dotazech pak nedochází k rekurzivnímu prohledávání stromu, ale odpověď je získána lokálně. V DNS záznamech je totiž uložena i informace jak dlouho lze záznam používat (TTL) a lze také zjistit, zda byl záznam změněn. Po vypršení platnosti je záznam z DNS cache odstraněn.
15	domain, structure, tree, relationships between them	1. Doména je základním prvkem logické struktury AD. V doméně jsou přímo uloženy objekty (může se jednat o milióny), které do dané domény patří. 2. Doménová struktura je bezpečnostní a administrativní hranice všech objektů, které se v ní nacházejí. 3. Strom je seskupení nebo hierarchická organizace jedné nebo více domén. 4. Vztahy důvěryhodnosti představují ověřovací kanály, které zajišťují uživatelům v určité doméně přístup k prostředkům v jiné doméně.
16	dynamic DNS update	Dynamicky update umožňuje klientským počítačům DNS, registrovat a dynamicky aktualizovat záznamy o prostředcích na serveru DNS kdykoliv nastane změna. Toto snizuje potřeby pro manuální administraci zonovych záznamů, konkrétně pro ty klienty, kteří často mění misto a používají DHCP pro získání IP adresy.
17	event viewer	Konzola pro sledování veškerých událostí systému, každá událost má svůj Zdroj, ID, datum, čas, počítač, typ události (informace, varování, chyba, úspěch auditu, selhání auditu). Události se dělí na: 1. Základní systémové (apps, systém, security) 2. Aplikační (pro některé služby) (DNS, ad, DFS replication) 3. Ostatní logy (detailní logy jedn otlivých činností) Logy můžeme filtrovat. Logy se ukládají do souborů *.evtx
18	GP	nástroj pro hromadnou správu oprávnění a nastavení aplikovaných jak na celý počítač, tak na přihlášeného uživatele. Používá se pro: - aplikování firemních standardů (skrytí ovládacích panelů, síťové tiskárny, spuštění scriptů) - aplikování zabezpečení (změna oprávnění na určitých složkách, složitost hesla, skupiny s možností se lokálně přihlásit) - hromadná instalace aplikací (Office, Adobe Reader, atd.)

19	GPO management - principles	
20	FSMO role	-Hlavní server schémat (Schema Master): Jeden držitel role hlavního serveru v jedné doménové struktuře. Držitel role FSMO hlavního serveru schémat je řadič domény zodpovědný za aktualizace ve schématu adresářů. - Hlavní server názvů domén (Domain Naming Master): Jeden držitel role hlavního serveru v jedné doménové struktuře. Držitel role FSMO hlavního serveru názvů domén je řadič domény zodpovědný za provádění změn v oboru názvů adresáře založeném na doméně v celé doménové struktuře. - Hlavní server infrastruktury (Infrastructure Master): Jeden držitel role hlavního serveru v jedné doméně. Držitel role FSMO infrastruktury je řadič domény zodpovědný za aktualizaci identifikátoru SID a rozlišujícího názvu v odkazu na objekt mezi doménami. - Hlavní server relativních ID (RID Master): Jeden držitel role hlavního serveru v jedné doméně. Držitel role FSMO hlavního serveru relativních ID (RID) je jeden řadič domény zodpovědný za zpracování požadavků fondu RID ze všech řadičů domény v dané doméně. - Emulátor primárního řadiče domény (PDC Emulator): Jeden držitel role hlavního serveru v jedné doméně. Držitel role FSMO emulátoru primárního řadiče domény je řadič domény systému Windows, který se pracovním stanicím, členským serverům a řadičům domény, které používají starší verze systému Windows, inzeruje jako primární řadič domény. Jedná se také o hlavní prohledávač domény, který zároveň zpracovává neshody v heslech.
21	IIS	Internet Information Services (IIS) je aplikace webového serveru a nastavení modulů funkce, vytvořených společností Microsoft pro použití s Microsoft Windows. Jedná se o nejpoužívanější webový server po Apache HTTP Server. IIS 7.5 podporuje HTTP, HTTPS, FTP, FTPS, SMTP a NNTP. Je nedílnou součástí řady Windows Server výrobků, stejně jako některých edicích systému Windows XP, Windows Vista a Windows 7. IIS není ve výchozím nastavení zapnuta.

22	Installation S2008 + role	Role: Active Directory Domain Services (ADDS). Active Directory Federation Services (ADFS), Active Directory Lightweight Directory Services (ADLDS), Active Directory Certificate Services (ADCS), Active Directory Rights Management Services (ADRMS). Služby identit a certifikátů umožňují administrátorům spravovat uživatelské účty a digitální certifikáte jim umožňují přístup ke konkrétním službám a systémům. Federation management services zase otevírají cestu ke správě sdílených prostředků mezi ověřenými partnery a zákazníky s možností, aby např. konzultant IT mohl použít firemní přihlašovací údaje k připojení do sítě klienta. Active Directory Metadirectory Services. ROLE:Stand alone, Member server – Aplication server, Domain Controller. File server, Domain Controller, Print server, DHCP server, DNS server, Mail server, Database server, SMS server, IIS server (web) typy instalace: - core - nainstaluje se příkazák, vhodné pro servery - full - včetně gui

23	IIS write what services it provides	1. Common HTTP Features - základní webserver - Static Content, Default Document, Directory Browsing, HTTP Errors, HTTP Redirection 2. Application Development Features - .NET aplikační server - ASP.NET, .NET Extensibility, ASP, CGI, ISAPI Extensions, ISAPI Filters, Server-Side Includes 3. Health and Diagnostics Features -služby pro logování a diagnostiku serveru - HTTP Logging, Logging Tools, Request Monitor, Tracing, Custom Logging, ODBC Logging 4. Security Features -služby pro zabezpečení -Basic Authentication, Windows Authentication, Digest Authentication, Client Certificate Mapping Authentication, IIS Client Certificate Mapping Authentication, URL Authorization, Request Filtering, IP and Domain Restrictions 5. Performance Features -zlepšení výkonu serveru -Static Content Compression, Dynamic Content Compression 6. Management Tools -služby pro management serveru, scripty a console -IIS Management Console, IIS Management Scripts and Tools, Management Service, IIS 6.0 Management Compatibility, IIS Metabase Compatibility, IIS 6 WMI Compatibility, IIS 6 Scripting Tools. IIS 6 Management Console 7. Windows® Process Activation Service -Process Model, .NET Environment, Configuration APIs 8. File Transfer Protocol (FTP) Publishing Service Features -ftp server -FTP Server, FTP Management Console 9. Simultaneous Connection Limits -dle verze OS (WS2008 neomezené)
24	how to access the domain via the command line	Správa už.účtu, správa skupin – dsadd resetování hesla uživatele, povolení a zakázání už.účtu – dsmod nalezení skupiny – dsget hledání v rámci AD – dsquery

25	how to delete an object in AD and how to restore it?	- když je objekt smazán, není odstraněn z databáze, objekt je po smazání označen pro pozdější odstranění, tento příznak je replikován na ostatní řadiče, teprve později je proces garbage collection fyzicky odstraní z databáze, tyto objekty jsou nazývány tombstones, garbage collection také maže nepotřebné logy, následně proces spustí vlákno defragmentace Obnova: Kromě autoritativní obnovy ze zálohy existuje nástroj od Microsoft ADRESTORE. EXE. Je to řádková utilitka, která po instalaci umožňuje obnovit objekt pomocí adrestore -r

26	what groups are in the security dependency domain, describe the individual groups and how to set them up	Typy skupin : Security Distribution Local Rozsah skupin: Domain local group - are best used for granting access rights to resources such as file systems or printers that are located on any computer in the domain where common access permissions are required. The advantage of domain local groups used to protect resources is that members of the domain local groups can come from both inside the same domain and outside the domain. Typically, resource servers are in domains that have trust to one or more Master User Domains, or what are known as account domains (A domain local group can be used to grant access to resources on any computer only in native mode domains. In mixed mode, domain local groups must be on domain controllers only.) Global group - are used for combining users who share a common access profile based on job function or business role. Typically, organizations use global groups for all groups where membership is expected to change frequently. These groups can only have as members user accounts defined in the same domain as the global group. Global groups can be nested to allow for overlapping access needs or to scale for very large group structures. The most convenient way to grant access to global groups is by making the global group a member of a resource group that is granted access permissions to a set of related project resources. Universal group - are used in larger, multidomain organizations where there is a need to grant access to similar groups of accounts defined in multiple domains. It is better to use global groups as members of universal groups to reduce overall replication traffic from changes to universal group membership. Users can be added and removed from the corresponding global group within their account domains and a small number of global groups are the direct members of the universal group. Universal groups are easily granted access by making them a member of a domain local group used to grant access permissions to resources. Universal groups are used only in multiple domain trees or forests that have a global catalog. A Windows 2000 domain must be in native mode to use universal groups. A domain model that has only a single domain does not need or support universal groups. Computer local group - are security groups that are specific to a computer and are not recognized elsewhere in the domain. If a member server is a file server and hosts 100 gigabytes (GB) of data on multiple shares, you can use a local server group for administrative tasks performed directly on that computer or for defining local access permission groups.
27	how is the difference between the integrated zone	zóna integrovaná do Active Directory: jedná se o primární zónu, která nemá záznamy v textovém souboru, ale ukládá je přímo do databáze AD

	and the zone in the text file	

28	What is the difference between iterative translation and forwarding	Iterativní dotaz směřuje na server DNS, odpovědi mohou přijít z dalších serverů. Forwarding používá rekurzivní dotaz.
29	How can we protect users' mail from viruses, spam, and attacks?	Antispam, nastavení firewallu, vytvoření nového poštovního účtu, antivirový program, filtrování pošty
30	Configuration files IIC 7.x and dependency between them	Server-level configuration is stored in the following configuration files: Machine.config. This file is located in %windir%\Microsoft. NET\Framework\framework_version\CONFIG. Root Web.config for the .NET Framework. This file is located in %windir%\Microsoft. NET\Framework\framework_version\CONFIG. ApplicationHost.config. This file is located in %windir%\system32\inetsrv\config. Site, application, and virtual and physical directory configuration can be stored in one of the following locations: A server-level configuration file. When configuration for a site, application, directory, or URL is stored in a server-level configuration file, you must use a location tag to specify the site, application, directory, or URL to which the configuration applies. A parent-level Web.config file. When configuration for an application, directory, or URL is stored in a parent-level configuration file, you must use a location tag to specify the child at which the configuration applies. The Web.config file for the site, the application, or the directory. When you configure settings for an application, directory, or URL, the configuration is stored in the same directory as the site, application, or directory. You do not need to use location tags. --- Neco v cestine: IIS 7 má globální konfigurační soubor, který obsahuje výchozí nastavení webového serveru a v něm běžících aplikací. Každá aplikace má pak svůj vlastní konfigurační soubor, kterým v podstatě „přepisuje“ výchozí nastavení webového serveru IIS 7.
31	user credentials and how to set up UAC	http://optimalizovane-it.cz/windows-7/user-account-control-uac-ve-windows-7-technicky-popis.html

32	Jake has DHCP the most important utility	DHCP tools Tyto nástroje jsou spojeny s DHCP 1. DHCP snap-in The DHCP snap-in allows you to perform a variety of administrative tasks for your DHCP servers: Create and manage scopes, including superscopes and multicast scopes. Create and manage properties for scopes, such as options, reservations, and exclusion ranges. Review active leases for each scope. Category The DHCP snap-in Microsoft Management Console (MMC) appears as an administrative tool after you install DHCP by using Control Panel. The DHCP snap-in can also be added to Windows Server 2003 or Windows XP by installing the Windows Server 2003 Administrative Tools Pack. This allows remote administration of DHCP servers running Windows 2000 Server or Windows Server 2003 from a Windows XP-based workstation. 2. Netsh Netsh is a command-line scripting tool that allows you to display or modify the network configuration of a computer. Netsh also provides a scripting feature that allows you to run a group of commands in batch mode against a specified computer. Netsh can also save a configuration script in a text file for archival purposes or for reuse in configuring other servers. Commands in the netsh dhcp context provide a command-line method to help with the administration of DHCP servers. Netsh provides an equivalent alternative to console-based management. All commands in netshdhcp context can also be executed against a specified remote server. For more information, see Netsh Commands for Dynamic Host Configuration Protocol server 3. Network Monitor You can use the Network Monitor tool or a commercial packet analyzer (also known as a network sniffer) to capture and view packets such as DHCP messages. In Windows 2000 Server, Windows Server 2003, and Windows Server 2008, Network Monitor is installed as an optional management and monitoring component by using Control Panel. After it is installed, you can run Network Monitor from the Administrative Tools folder.
33	Design for local PC administration	AD Users and Computers – vytvoření doménových účtů, rozdělení do kategorií, přidělení práv, Group Policy Management – nastavení politik pro PC, skupiny PC Remote Desktops – vzdálené připojení na PC

34	describe Event log, local disk manager, messenger, and dns client	Event log - The event logs record events that happen on the computer. Examining the events in these logs can help you trace activity, respond to events, and keep your systems secure. Configuring these logs properly can help you manage the logs more efficiently and use the information they provide more effectively. Local disk manager - řekl bych že disk manager pro tvorbu partition, volumes atd (nevim jistě) Messenger - "net send", Using the Messenger Service in Windows gives you varying results that depend on the command options or interface you use to send messages. The method you use determines whether the message is a local Broadcast or a directed datagram, and to which NetBIOS name the message is to be sent. DNS client - The DNS Client service is the client component that resolves and caches Domain Name System (DNS) domain names. When the DNS Client service receives a request to resolve a DNS name that it does not contain in its cache, it queries an assigned DNS server for an IP address for the name. If the DNS Client service receives the requested address, it stores the name and address in its cache to resolve future requests without having to query the DNS server. All computers that use DNS to resolve domain names (including DNS servers and domain controllers) use the DNS Client service for this purpose.
35	The command we use to install the domain. What is needed for installation domains. Some important domains at the domain.	
36	Protocols for Windows security. Description of security DACL, ACE (setup and use)	Kerberos V 5 - Standard protokolu pro autentizaci uživatelů a systémů. Je primárním autentizačním mechanizmem pro Windows 2000 a vyšší NT LAN Manager (NTLM) - Primární autentizační protokol pro systémy Windows NT. Secure Socket Layer/Transport Layer Security (SSL/TLS) - Primární mechanizmus pro autentizaci pro přístupy k zabezpečeným webovým serverům. DACL - list 1 nebo více ACL nad objektem též: (DACL) An access control list that is controlled by the owner of an object and that specifies the access particular users or groups can have to the object. A podle všeho je to shluk ACEček ACE - Allow/Deny pro jednotlivé činnosti nad objektem pro uživatele, či skupinu AD
37	ITIL elements	vytvoření domény - dcpromo

38	Registry	teoreticky - hierarchická databáze obsahující nastavení pro Windows OS a aplikace, prakticky - místo, kde nalezneme nastavení systému a aplikací, která nejsou jinak dostupná, typy objektů: klíč (registry key)e kvivalent složky / adresáře, hodnota (registry value) obsahuje data (vlastní nastavení), HKEY_LOCAL_MACHINE (HKLM) , HKEY_USERS (HKU), HKEY_CURRENT_USER (HKCU), registry mají binární strukturu, každá hodnota má definován datový typ, nejčastěji používané - REG_SZ (řetězec UTF-16), REG_MULTI_SZ (pole řetězců UTF-16), REG_DWORD (číselná hodnota 32bit), REG_QWORD (číselná hodnota 64bit), REG_BINARY (libovolná data)

39	the distribution of groups according to scope and security, strategy of use and their description	podle rozhsahu: -domain local – oprávnění pro jednu doménu, členy uživ. A pc ze stené domény -global – oprávnění pro objekty v libovolné doméně v rámci forestu, členy pouze skupiny ze stejné domény -universal – oprávnění v různých doménách forestu Group strategies: A – Accounts, G – groups, U – universal groups, DL – domain local groups, P- permissions, L-local groups; Strategie : AGP, AG DL P, A G U DL P, A GG DL P, A GL P
40	splitting bills and shortly about them	Účty počítačů Proč mají počítače účty - Identifikují počítače v doméně -Umožňují ověřování a audit přístupů k síti a síťovým prostředkům -Umožňují nastavit práva pro počítače (např. při instalaci softwaru) Účty uživatelů
41	groups	Shlukují objekty stejného typu (např. uživatele), kterým poté můžeme nastavit různá přístupová práva a oprávnění. Př. skupina "knihovnice" bude mít jistě jinačí práva než skupina "administrátoři"

42	services (print spool, etc)	AD, DNS, IIS, DHCP, Windows Update, Motivy, Windows Defender, Systémový čas, každá serverová aplikace by měla být nainstalována jako služba, http://buchtic.bloguje.cz/251263-systemove-sluzby-windows.php
43	Sprava systemovych suborov	
44	System Event Notifier, Terminal Services, Windows Time, Workstation	Služba pro oznamování událostí systému Vzdálené síťové připojení a přístup k prostředkům PC Synchronizace času v doméně API redirector, který poskytuje počítači přístup k síti
45	WS 2008 license types and when to use	foundation - základ pro malé firmy standard - běžný standard enterprise - clustering, cena cca 65tis datacenter - cena cca 150k Web-server HPC - pro super servery Win.Small Bussiness server 2008 Standard/Premium typy instalace: - core - nainstaluje se příkazák, vhodné pro servery - full - včetně gui

46	DNS record types and description	Běžné typy záznamů: ◦ A – IPv4 host; AAAA – IPv6 host ◦ CNAME – alias ◦ MX – mail exchanger ◦ SRV – service locator ◦ PTR – pointer (reverzní překlad) ◦ SOA – start of authority; definuje některé parametry zóny ◦ NS – name server
47	Levels of MS 2008 server installation, dependency on compatibility with other OSs, description of levels (Forest and Domain level)	foundation - základ pro malé firmy standard - běžný standard enterprise - clustering, cena cca 65tis datacenter - cena cca 150k Web-server HPC - pro super servery Win.Small Bussiness server 2008 Standard/Premium typy instalace: - core - nainstaluje se příkazák, vhodné pro servery - full - včetně gui
48	UAC levels	Ve Windows 7 a 2008 R2 jsou 4 úrovně: ◦ „Always notify“ (také ve Vista a 2008 R1) Vyžaduje potvrzení pro všechny použití Administrátorských práv ◦ „Default“ – Vyžádání oprávnění pro programy Nevyžaduje notifikaci pro konfiguraci systému ◦ „Default without secure desktop“ - Vyžádání oprávnění pro programy bez zabezpečené plochy (secure desktop) ◦ „Never notify“ (také ve Vista a 2008 R1) Vypnutí funkce UAC
49	Network attacks, protection	backdoor, scanování portů, sociální metody, odposlech ethernetu, přetečení zásobníku, útoky proti www, IP spoofing Zábrany: autentizace uživatelů sítě, zabezpečení stanic, zabezpečení provozu, zabezpečení LAN
50	Advantages and disadvantages of CMD	- oproti Linuxové consoli nepřehledné a slabý systém doplňování příkazů a adres tabulátorem - větší nároky na programátora - rychlost práce závisí na zkušenosti a znalosti příkazů + nehrozí překlik + rychlost práce + odpadá hledání něčeho v hlubokých nabídkách, či nepřehledných GUI + admin není omezován GUI + možnost vzdálené správy přes telnet

51	Name and describe some of the ITIL components and draw an ITIL work pattern.	Service Desk, Configuration Management, Incident Management, Problem Management, Change Management, Release Management Incident Management – proces zajišťující co nejrychlejší obnovení dodávky služby a minimalizaci důsledků výpadků služeb na obchodní činnost Release Management – proces zajišťující úspěšnou distribuci a nasazení změny do ICT infrastruktury Problem Management – proces zjišťování původních příčin incidentů
52	name the DNS zones	Zóny dělíme na: ◦ Obyčejné (data v textovém souboru) ◦ AD Integrované (data v databázi AD) -Dostupné jen na doménových řadičích AD ◦ Primární -Zapisovatelná kopie DNS zóny, kadá zóna má právě jednu primární kopii ◦ Sekundární -Existuje pouze pro čtení, aktualizuje se tzv. „zone transfery“ z primární zóny -Slouží pro redundanci a rozložení zátěže -V případě lze povýšit na primární ◦ Stub
53	Explain what these services are: Alterer (? Not sure), Automatic Update, DHCP Client, Computer Browser	Alerter service: sluzba microsoftu, pouziva se pro posilani administrativnich upozorneni, upozornuje uzivatele na bezpecnost, pristup a relacni problemy Automatic Update: umoznuje stahovat a instalovat Windows Update. Pokud je tato sluzba vypnuta, pozitac neni schopen automatickych updatu nebo Windows Update Web site. DHCP Client: Spravuje sitovou konfiguraci pomoci registrace a updatu IP adres a DNS jmen Computer Browser: udrzuje aktualizovany seznam pocitacu v siti a dodava tento seznam pocitacum urcenym jako prohlizece
54	certificate life cycle, and its attributes	Začíná vytvořením žádosti. Poté dojde k vydání certifikátu a ten je zkontrolován a můžeme jej použít. Poté následuje buď expirace certifikátu, nebo během té doby můžeme tento certifikát odvolat (například někdo zaútočí na náš server apod.). Už před expirací může dojít k obnovení certifikátu a opět zde platí, že je můžeme pak odvolat nebo expirovat. A tak dokola stále.

55	methods of authentication in IIS	1. Anonmní(defaultní) - veřejný přístup pro kohokoli bez ověření 2. Basic - používá windows účty, součást HTML 1.0, umožňuje i ověření skrze proxy, není bezpečné pokud nepoužijeme SSL/TLS, umožňuje integraci s protokolem Kerberos, vyžaduje vytvoření individuálních windows účtů 3. Digest - odstraňuje hlavní slabinu Basic tj posílání hesla jako prostý text, nevyžaduje SSL/TLS k ochraně hesla, pracuje i s proxy a firewallem, ale vyžaduje IE5+, nemůže delegovat oprávnění, vyžaduje uložený hesla v prostém textu kvůli reverzivního překladu, vyžaduje vytvoření účtů v AD, bez použití SSL/TLS bývá cíl replay útoků 4. Integrovaná Windows (defaultní) - známá též jako NTLM, používá NTLM nebo Kerberos, nejlepší volba pro intranet, nejde se přihlásit přes firewall, neumožňuje delegaci do ostatních serveru, je-li vybráno NTLM 5. Klientské certifikáty - velká bezpečnost, poskytuje obousměrnou autentizaci serveru a klienta, umožňuje přistupovat k síťovým zdrojům, nepracuje se všemi prohlížeči, vyžaduje SSL/TLS, nemůže delegovat oprávnění, složitější nastavování
55	methods of authentication in IIS	1. Anonmní(defaultní) - veřejný přístup pro kohokoli bez ověření 2. Basic - používá windows účty, součást HTML 1.0, umožňuje i ověření skrze proxy, není bezpečné pokud nepoužijeme SSL/TLS, umožňuje integraci s protokolem Kerberos, vyžaduje vytvoření individuálních windows účtů 3. Digest - odstraňuje hlavní slabinu Basic tj posílání hesla jako prostý text, nevyžaduje SSL/TLS k ochraně hesla, pracuje i s proxy a firewallem, ale vyžaduje IE5+, nemůže delegovat oprávnění, vyžaduje uložený hesla v prostém textu kvůli reverzivního překladu, vyžaduje vytvoření účtů v AD, bez použití SSL/TLS bývá cíl replay útoků 4. Integrovaná Windows (defaultní) - známá též jako NTLM, používá NTLM nebo Kerberos, nejlepší volba pro intranet, nejde se přihlásit přes firewall, neumožňuje delegaci do ostatních serveru, je-li vybráno NTLM 5. Klientské certifikáty - velká bezpečnost, poskytuje obousměrnou autentizaci serveru a klienta, umožňuje přistupovat k síťovým zdrojům, nepracuje se všemi prohlížeči, vyžaduje SSL/TLS, nemůže delegovat oprávnění, složitější nastavování
57	sharing	nastavujeme sdílené položce oprávnění skryté sdílení - poslední znak $, nemá vliv na oprávnění, položka se klientovi nezobrazí, používá se např ke sdílení skriptů

58	politics what it is and what it serves	Nastavují se v Group Policy Management Editor. Zde můžeme nastavit až 2000 různých nastavení počínaje délkou hesla až po ikonkou na ploše. Takto vytvořená a nastavená politika se poté "linkuje" v Group Policy Managementu (gpmc.msc) na různé doménové objekty, tj. skupiny či organizační jednotky. Polity, resp. GPO linky mají několik atributů. Enforced - politika má přednost před ostatními, "protlačí se". Pak Link enabled/ disabled; Deleted - link lze odstanit, ale GPO zůstane; a multiple links - případ kdy je více GPO nalinkováno na nějaký kontejner. Důležité je stanovení pořadí politik!
59	what is WINS and its use	WINS - je MS implementace NetBIOS Name Serveru (NBNS) proWindows, sloužící jako name server pro jména počítačů v síťovém prostředí NetBIOS.Poskytuje distribuovanou databázi, která mapuje názvy pro rozhraní NetBIOS na IP adresy. Tato služba byla vytvořena za účelem řešení problémů vyplývajících z překladu názvů pro rozhraní NetBIOS ve směrovaných prostředích.
60	Netbios	NetBIOS - je softwarový interface (API) pro přístup k síťové komunikaci na úrovni relační (session) vrstvy. Konkrétní transportní protokol, jakož i fyzické adresy stanic, jsou před programátorem skryty. NetBIOS je především soubor standardních funkcí, ty jsou nezávislé na nižších vrstvách (a tedy formátu paketů). Např. v sítích Microsoft, je pro transport využito protokolu NetBEUI (v rámcích LLC ?), případně TCP/IP a někdy též IPX/SPX.
61	Explain what are the user rights and permissions (Permissions) Provide examples of where they are used. And what are the differences between them?	Práva - Akce v systému (změna času, nastavení systému,...) Oprávnění - Operace s objekty (Read/Write/...)
